

PowerFlex 8/24/48 Port GbE PoE Managed Switch User's Guide

Updated October 30, 2013



PowerFlex 8/24/48 Port GbE PoE Managed Switch

User's Guide





© 2013 Allworx Corp, a Windstream Communications company. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise without the prior written permission of Allworx Corp. All brand and product names referenced in this guide are trademarks or registered trademarks of their respective companies.

Software in this product is © 2013 Allworx Corp, a Windstream Communications company, or its vendors. All rights are reserved. The software is protected by United States of America copyright laws and international treaty provisions applicable worldwide. [Allworx® Software Products End User License Agreement](#)

Purpose

This guide gives specific information on how to operate and use the management functions of the switch.

Audience

Intended use: For use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Warranty

Find a copy of the specific warranty terms applicable to this product at www.allworx.com.

Conventions

This guide uses the following conventions throughout this guide to show information:



Notification for installation, operation, maintenance, performance, or general tips that are important, but not hazardous to anything or anyone.



Description of a potentially hazardous situation, which if not avoided, could result in death or serious or moderate injury. It can also advise against unsafe practices.



Description of a potentially hazardous situation, which if not avoided, could result in minor or moderate injury. It can also advise against unsafe practices.

Compliances and Safety Statements

FCC – Class A

This equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user must correct the interference at their own expense.



CAUTION: changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate the equipment.

It is possible to use unshielded twisted-pair (UTP) for RJ-45 connections - Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, Category 5, 5e, or 6 for 1000 Mbps connections. For fiber optic connections, it is possible use a 50/125 or 62.5/125 micron multimode fiber or 9/125 micron single-mode fiber.

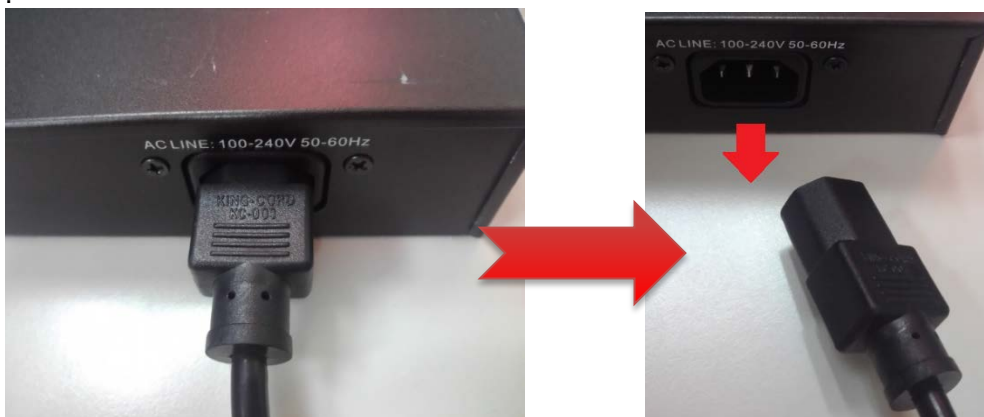
CE Mark Declaration of Conformance for EMI and Safety (EEC)

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN61000-3 and the Generic European Immunity Standard EN55024.

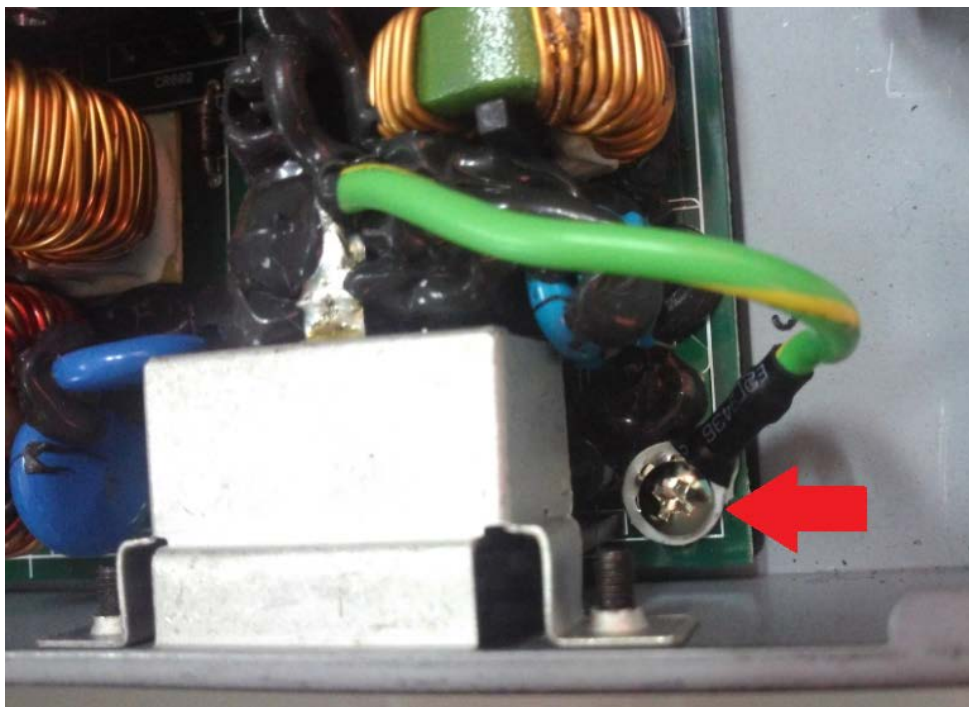


Caution: Maintenance Personnel:

To avoid electric shock, turn the power off and detach the input power cord prior to doing any equipment maintenance.



After completing the equipment maintenance, verify the ground connection and setup.



Revision History

This section summarizes the changes in each revision of this guide.

Release	Date	Revision
V2.29	09/09/2013	A3
V1.52	05/22/2013	A2
V1.07	10/17/2011	A1

Table of Contents

1	Introduction	1
1.1	Overview	1
1.2	Overview of this User's Guide	1
2	Operation of Web-Based Management	2
2.1	Initial Configuration.....	2
2.2	IP Configuration.....	2
3	System Configuration.....	4
3.1	System Information	4
3.2	Time	7
3.3	Account	10
3.4	IP	13
3.5	SYSLOG.....	16
3.6	SNMP	19
3.7	Groups.....	24
3.8	Views.....	25
3.9	Access.....	26
3.10	Trap.....	27
4	Configuration	29
4.1	Port.....	29
4.2	ACL	38
4.3	Aggregation	46
4.4	LACP	48
4.5	Spanning Tree.....	51
4.6	IGMP Snooping.....	62
4.7	MLD Snooping.....	70
4.8	MVR	77
4.9	LLDP	81
4.10	PoE	98
4.11	VLAN.....	107
4.12	Voice VLAN.....	119
4.13	GARP	123
4.14	GVRP	126
4.15	QoS	129
4.16	sFlow Agent.....	147
4.17	Loop Protection	149
4.18	Single IP	151
4.19	Easy Port.....	153
4.20	Mirroring	155
4.21	Trap Event Severity.....	157
4.22	SMTP Configuration	158
4.23	UPnP	159
5	Security.....	160

5.1	IP Source Guard.....	160
5.2	ARP Inspection.....	163
5.3	DHCP Snooping.....	166
5.4	DHCP Relay.....	168
5.5	NAS.....	171
5.6	AAA.....	183
5.7	Port Security.....	192
5.8	Access Management.....	198
5.9	SSH.....	200
5.10	HTTPS.....	201
5.11	Auth Method.....	202
6	Maintenance	203
6.1	Restart Device.....	203
6.2	Firmware	204
6.3	Save / Restore.....	206
6.4	Export / Import.....	208
6.5	Diagnostics.....	210
7	Glossary of Web-based Management	213

1 Introduction

1.1 Overview

This user's manual instructs how to install, configure and monitor the PowerFlex™ 8/24/48 port switch through the built-in web-based management.

The PowerFlex 8/24/48 series, the next generation L2+ managed switches, is a portfolio of affordable managed switches that provides a reliable business network infrastructure. These switches deliver intelligent features needed to improve the availability of critical business applications, protect sensitive information, and optimize network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry level networking including small business or enterprise applications and helps create a more efficient, better-connected workforce.

PowerFlex 8/24/48 L2+ Managed Switches provide 8, 24 or 48 100/1000 ports, depending on the model; the specifications are as follows:

- L2+ features provide better manageability, security, QoS, and performance.
- High port count design with all Gigabit Ethernet ports
- Support guest VLAN, voice VLAN, Port based, tag-based and Protocol based VLANs.
- Support 802.3az Energy Efficient Ethernet standard
- Support 802.3at High power PoE Plus standard
- Support IPv6/ IPv4 Dual stack
- Support sFlow
- Support Easy-Configuration-Port for easy implementation of IP Phones, IP Cameras or Wireless environment.

1.2 Overview of this User's Guide

- Chapter 2 "Operation of Web-based Management"
- Chapter 3 "Maintenance"

2 Operation of Web-Based Management

2.1 Initial Configuration

This chapter describes configuring and managing the PowerFlex series switches through the web user interface. With this facility, users can easily access and monitor the switch, including MIBs status, port activity, Spanning tree status, port aggregation status, and multicast traffic, VLAN, and priority status, and even illegal access record and so on.

The PowerFlex Series switches ship with a preconfigured firmware image. This eliminates the need to make changes to the switch in order for it to work with the Allworx servers and phones. The default configuration is detailed below. Following the instructions below makes the server, switch, and phones a plug-n-play network.

2.2 IP Configuration

The switch has DHCP enabled to obtain an address from the Allworx server. If for some reason DHCP fails, the switch falls back to the configured static IP.



NOTE: If DHCP has failed in a multiple PowerFlex switch configuration, it will be necessary to disconnect each switch from the others before attempting to log into the switches using the default IP.

IP Address	192.168.2.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254
Username	admin
Password	<blank>

Once the switch has obtained its IP address, users may determine its current address from the DHCP lease table of the network's DHCP server. In a default configuration, an Allworx server is the DHCP server. The IP information may be viewed by navigating to the **Servers>DHCP** page of the Allworx server. In the "Active Leases" section, match the hardware address in the table to the MAC address printed on the label of the PowerFlex switch. Access the switch via the web interface using the associated IP address. For instance, browse to <http://192.168.2.x> using a web browser. A pop-up screen prompts users to enter the username and password.

The default username is "**admin**" and password is **empty**.



NOTE: It is recommended for security purposes to change the username and password after initial login.

The PowerFlex Series supports a simple user management function enabling only one administrator to configure the system at any given time. If there are two or more users using administrator's identity, only the first user to login is able to configure the system. The other logged in users, even with

administrator's identity, can only monitor the system. Those who are not configured as administrators can only monitor the system. A maximum of only three users can log in to the switch at once.

Figure 1: Login Page



NOTE: To optimize the display effect, use Microsoft IE 6.0 or above, Netscape V7.1 or above or FireFox V1.00 or above and have the resolution set to 1024x768.

To configure a function or parameter, access the online Help in the web GUI.

3 System Configuration

This chapter describes all the basic configuration tasks which include the System Information and management of the Switch (e.g. Time, Account, IP, Syslog and SNMP.)

3.1 System Information

After log in, the switch displays the system information. This is the default page and displays the basic information of the system, including "Model Name", "System Description", "Contact", "Device Name", "System Up Time", "BIOS Version", "Firmware Version", etc.

3.1.1 Information

The switch system information is provided here.

To view the System Information from the web interface:

Navigate to **System > System Information > Information**.

Figure 2: System Information

System Information		Auto-refresh <input type="checkbox"/> Refresh
Model Name	PowerFlex P810	
System Description	8-Port 10/100/1000Base-T + 2 TP/(100/1G) SFP Combo PoE+ L2 Plus Managed Switch	
Location		
Contact		
Device Name	PowerFlex P810	
System Date	2011-01-01 00:03:27	
System Uptime	0d 00:03:27	
BIOS Version	v1.00	
Firmware Version	v2.29 2013-08-07	
Hardware-Mechanical Version	v1.01-v1.01	
Series Number	P0810000ADD0040014	
Host IP Address	192.168.2.200	
Subnet Mask	255.255.255.0	
Gateway IP Address	192.168.2.254	
Host MAC Address	00-0a-dd-04-00-14	
Console Baudrate	115200	
RAM Size	64MB	
Flash Size	16MB	
Bridge FDB Size	8192 MAC Addresses	
Transmit Queue	8 queues per port	
Maximum Frame Size	9600	

Parameter	Description
Model Name	The device model name.
System Description	A brief description of the switch.
Location	User-defined location of the switch.
Contact	User-defined contact person for switch administration. Configure this parameter through the device user interface or SNMP.
Device name	User-defined name for the switch.



System Date	Display the system time and date. Format: year, day of week, month, hours : minutes : seconds.
System up time	Time the system has been up since powering on or last reboot. Format: days, hours : minutes : seconds.
BIOS version	The switch BIOS version.
Firmware version	The switch firmware version.
Hardware-Mechanical version	The version of Hardware and Mechanical. The figure before the hyphen is the version of the electronic hardware; the one after the hyphen is the version of mechanical.
Series number	The serial number is assigned by the Manufacturer.
Host IP address, Subnet Mask and Gateway IP Address	The IP address, subnet mask and gateway IP address set on the switch.
Host MAC address	The Ethernet MAC address of the management agent in the switch.
RAM size	The size of the RAM switch in MB.
Flash size	Switch flash memory size in MB.
Bridge FDB size	Displays the bridge RDB size.
Transmit Queue	Displays the device's transmit hardware priority queue information.
Maximum Frame size	Display the device maximum frame size.

3.1.2 Configuration

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

To configure System Information in the web interface:

1. Navigate to **System > System Information > Configuration**.
2. Specify the System Contact, System Name and System Location information.
3. Click **Apply**.

Figure 3: System Configuration

System Information Configuration

System Contact	<input type="text"/>
System Name	PowerFlex P810
System Location	<input type="text"/>

Apply Reset

Parameter	Description
System Contact	The contact person for this managed switch, along with the contact information. The string length is 0 to 255, and the content is ASCII characters from 32 to 126.
System Name	An assigned name for this managed switch. 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 string length is 0 to 255.
System Location	The physical location of this switch (e.g., telephone closet, 3rd floor). The string length is 0 to 255, and the content is ASCII characters from 32 to 126.

3.2 Time

This page enables configuring the system time manually or automatically using NTP server(s).

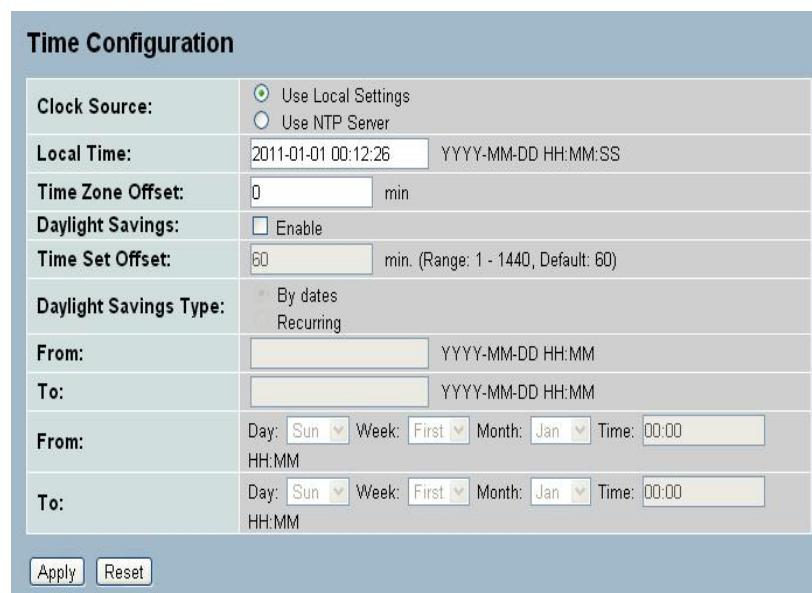
3.2.1 Manual

Manual setting is simple, just enter “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item.

To configure system time manually from the web interface:

1. Navigate to **System > Time > Manual**.
2. Specify the parameters in each field.
3. Click **Apply**.

Figure 4: Manual Time Configuration



Time Configuration

Clock Source: ☒ Use Local Settings ☐ Use NTP Server

Local Time: 2011-01-01 00:12:26 YYYY-MM-DD HH:MM:SS

Time Zone Offset: 0 min

Daylight Savings: ☐ Enable

Time Set Offset: 60 min. (Range: 1 - 1440, Default: 60)

Daylight Savings Type: ☒ By dates ☐ Recurring

From: YYYY-MM-DD HH:MM

To: YYYY-MM-DD HH:MM

From: Day: Sun Week: First Month: Jan Time: 00:00 HH:MM

To: Day: Sun Week: First Month: Jan Time: 00:00 HH:MM

Parameter	Description
Clock Source	Select “Use local Settings” or “Use NTP Server” for the clock source.
Local Time	Display the current time of the system.
Time Zone Offset	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Daylight Saving	<p>Daylight saving is adopted in some countries. If set, it adjusts the time lag or advance in unit of hours, according to the starting date and the ending date. For example, if setting the day light saving to be 1 hour, when the time passes over the starting time, the system time increases by one hour after one minute at the time since it passed over and when the time passes over the ending time, the system time decreases by one hour after one minute at the time since it passed over.</p> <p>The valid configurable day light saving time is -5 ~ +5 step one hour. A zero for this parameter indicates no adjustment to the current time, equivalent to in-act daylight saving. Users do not need to set the starting/ending date as well. If setting daylight saving to be non-zero, set the starting/ending date as well; otherwise, the daylight saving function is not active.</p>



Time Set Offset	Provide the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. Default is 60 mins.
Daylight Saving type	Select " By Dates" or "Recurring".
From	Configure Daylight saving start date and time. The format is "YYYY-MM-DD HH:MM".
To	Configure Daylight saving end date and time. The format is "YYYY-MM-DD HH:MM"

3.2.2 NTP

Use the Network Time Protocol to synchronize the network time based on Greenwich Mean Time (GMT). If using the NTP mode, users can manually set up to 5 NTP servers. The switch syncs the time in a short time after pressing the **Apply** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

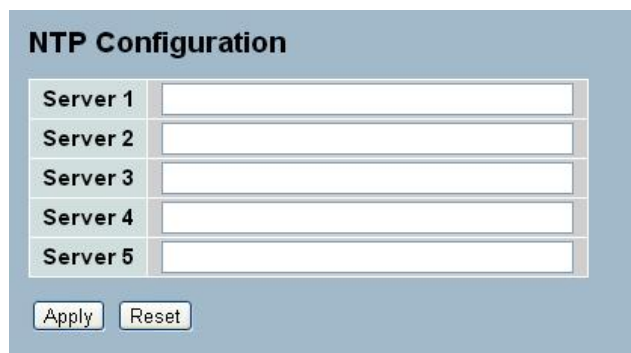
Time Zone is an offset time off GMT. Select the time zone first, and then do a time sync via NTP. The switch combines this time zone offset and updated NTP time to calculate the local time; otherwise, the time is incorrect. The switch supports configurable time zone from -12 to +13 step 1 hour.

Default Time zone: +8 Hrs.

To configure Time in the web interface:

1. Navigate to **System > Time > NTP**.
2. Specify the NTP server address (es).
3. Click **Apply**.

Figure 5: NTP Configuration



The screenshot shows a web interface for NTP configuration. It has a title 'NTP Configuration' at the top. Below the title are five input fields, each preceded by a label 'Server 1', 'Server 2', 'Server 3', 'Server 4', and 'Server 5' respectively. At the bottom of the form are two buttons: 'Apply' and 'Reset'.

Parameter	Description
Server 1 to 5	Provide the NTP IPv4 or 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 only appear once. It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34

3.3 Account

Only the administrator can create, modify, or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. It is necessary to confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. There can be only one administrator account, but there can be up to 4 guest accounts. No one can delete the administrator account.

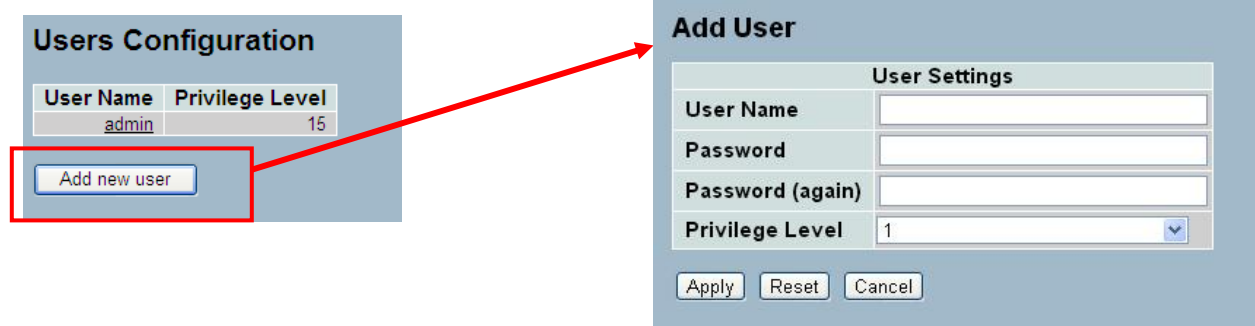
3.3.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.

To configure Account in the web interface:

1. Navigate to **System > Account > Users**.
2. Click **Add new user**.
3. Specify the User Name and password for the user along with the Privilege Level.
4. Click **Apply**.

Figure 6: User Account Configuration



Parameter	Description
User Name	The name identifying the user. This is also a link to Add/Edit User.
Password	The string length is 0 to 255, and the content is the ASCII characters from 32 to 126.
Password (again)	Retype the password typed in the Password field.
Privilege Level	The privilege level of the user. The range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. granted full control of the device. . User's privilege should be same or greater than the group privilege level to have access of that group. By default, most groups' privilege level 5 has the read-only access and privilege level 10 has the read-write access. System maintenance (software upload, factory defaults and etc.) requires user privilege level 15. In general, 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.

3.3.2 Privilege Level

This page provides an overview of the privilege levels. Each group can have the Privilege Levels set from 1 to 15.

To configure Privilege Level in the web interface:

1. Navigate to System > Account > Privilege Level.
2. Specify the Privilege parameter.
3. Click **Apply**.

Figure 7: Privilege Level Configuration

Privilege Level Configuration

Group Name	Privilege Levels
Account	10
Aggregation	10
Diagnostics	10
EEE	10
Easyport	10
GARP	10
GVRP	10
IP	10
IPMC Snooping	10
LACP	10
LLDP	10
LLDP MED	10
Loop Detection	10
MAC Table	10
MRP	10
MVR	10
MVRP	10
Maintenance	15
Mirroring	10
POE	10
Ports	10
Private VLANs	10
QoS	10
SFlow	10
SMTP	10
SNMP	10
Security	10
Spanning Tree	10
System	10
Trap Event	10
VCL	10
VLANs	10
Voice VLAN	10

Save
Reset

Parameter	Description
Group Name	<p>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 contain more than one. The following description defines these privilege level groups in detail:</p> <p>System: Contact, Name, Location, Timezone, Log.</p> <p>Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and 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 under 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 access to that group.</p>

3.4 IP

IP stands for Internet Protocol. It is a protocol used for communicating data across a (inter)network.

IP is a “best effort” system, which means that there is no assurance that a packet of information sent reaches the destination in the same condition. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) has an Internet Protocol address. This IP address identifies the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bit IP addresses enabling for over four billion unique addresses. The practice of webmasters taking addresses in large blocks (the bulk of which remain unused), drastically reduces this number. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit IP addresses. A three with thirty-nine zeroes after it can represent this number roughly. However, IPv4 is still the protocol of choice for most of the Internet.

3.4.1 IPV4

Obtain the IPv4 address for the switch via DHCP Server. To configure an address manually, change the switch default settings to values that are compatible with the network. It may be necessary to establish a default gateway between the switch and management stations that exist on another network segment.

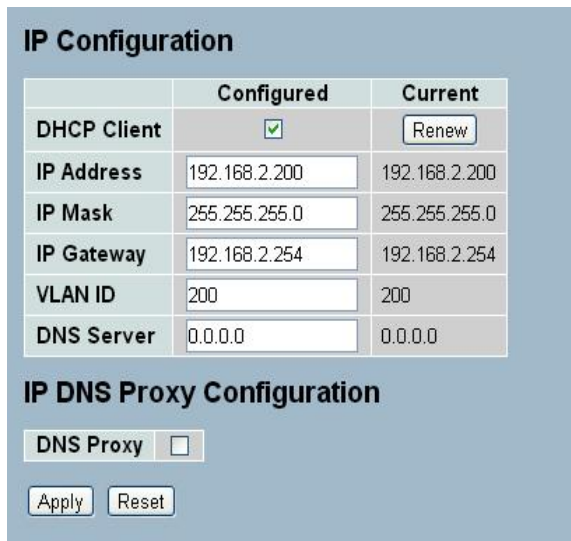
Use the Configured column to view or change the IP configuration.

Use the Current column to display the active IP configuration.

To configure an IP address in the web interface:

1. Navigate to **System > IPV4**.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click **Apply**.

Figure 8: IP Configuration



	Configured	Current
DHCP Client	<input checked="" type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	192.168.2.200	192.168.2.200
IP Mask	255.255.255.0	255.255.255.0
IP Gateway	192.168.2.254	192.168.2.254
VLAN ID	200	200
DNS Server	0.0.0.0	0.0.0.0

IP DNS Proxy Configuration

DNS Proxy ☐



Parameter	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Provide the IP address for the switch in the dotted decimal notation.
IP Mask	Provide the IP mask for the switch in the dotted decimal notation.
IP Gateway	Provide the IP address of the gateway in the dotted decimal notation.
VLAN ID	Provide the management VLAN ID. The range is 1 to 4095.
DNS Server	Provide the IP address of the DNS Server in the dotted decimal notation.
DNS Proxy	When DNS proxy is enabled, the switch will relay DNS requests to the current configured DNS server, and reply as a DNS resolver to the client device on the network.

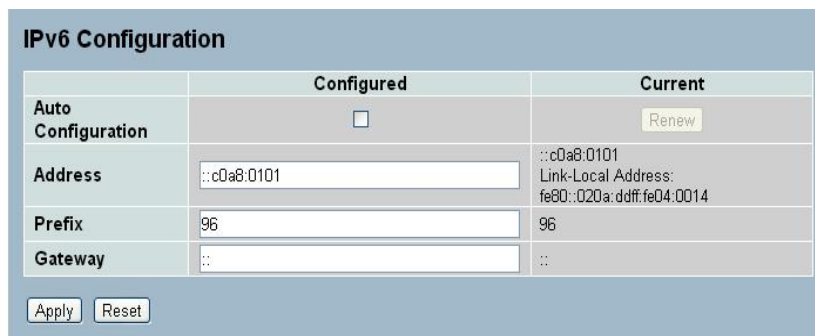
3.4.2 IPV6

This section describes how to configure the switch's managedIPv6 information. Use the Configured column to view or change the IPv6 configuration and the Current column displays the active IPv6 configuration

To configure Management IPv6 of the switch in the web interface:

1. Navigate to System > IPv6 Configuration.
2. Specify the IPv6 settings, and enable Auto Configuration service, if required.
3. Click **Apply**.

Figure 9: IPv6 Configuration



	Configured	Current
Auto Configuration	<input type="checkbox"/>	Renew
Address	<input type="text" value="::c0a8:0101"/>	::c0a8:0101 Link-Local Address: fe80::020a:ddff:fe04:0014
Prefix	<input type="text" value="96"/>	96
Gateway	<input type="text" value="::"/>	::

Apply Reset

Parameter	Description
Auto Configuration	Enable IPv6 auto-configuration by checking this box. If it fails and the configured IPv6 address is zero, the router may delay responding to a router solicitation for a few seconds. The total time needed to complete auto-configuration can be significantly longer.
Address	Provide the IPv6 address for the switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Prefix	Provide the IPv6 prefix for the switch. The range is 1 to 128.
Gateway	Provide the IPv6 gateway address for thie switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'

3.5 SYSLOG

The Syslog is a standard for logging programming messages. It enables separation of the software that generates messages from the system that stores the messages and the software that reports and analyzes the messages; used for informational, analysis and debugging messages; and supported by a wide variety of devices and receivers across multiple platforms.

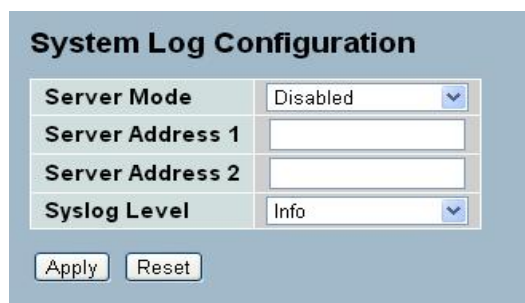
3.5.1 Configuration

This section describes how to configure the system log.

To configure Syslog configuration in the web interface:

1. Navigate to System > Syslog > Configuration.
2. Specify the syslog mode and IP Address of the Syslog server(s).
3. Specify the Syslog level.
4. Click **Apply**.

Figure 10: Syslog Configuration



System Log Configuration	
Server Mode	Disabled
Server Address 1	
Server Address 2	
Syslog Level	Info
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Parameter	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, syslog messages will be sent to the syslog server. The syslog protocol is based on UDP and received on UDP port 514. Syslog packets will be sent out even if the syslog server does not exist. Possible modes are: Enabled: Enable server mode operation. Disabled: Disable server mode operation.
Server Address 1	IPv4 address of syslog server. If the switch has DNS enabled, the host name can be entered.
Server Address 2	IPv4 address of alternate syslog server. If the switch has DNS enabled, the host name can be entered.
Syslog Level	Indicates what kind of messages will be sent to the syslog server. Possible levels are: Debug, Info, Notice, Warning, Error, Critical, Alert, Emergency.

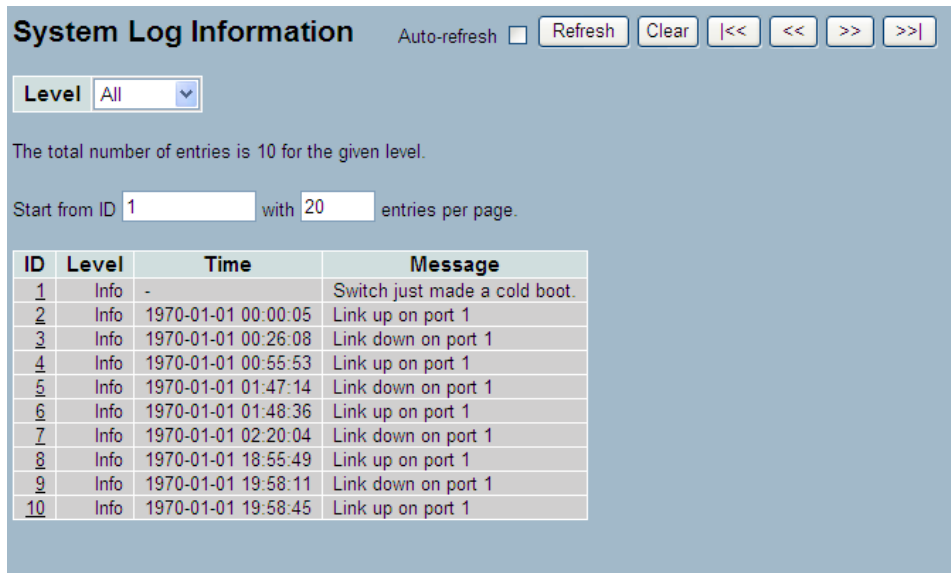
3.5.2 Log

This section displays the system log information of the switch.

To display the log configuration in the web interface:

Navigate to **System > Syslog > Log**.

Figure 11: Syslog Log Display



ID	Level	Time	Message
1	Info	-	Switch just made a cold boot.
2	Info	1970-01-01 00:00:05	Link up on port 1
3	Info	1970-01-01 00:26:08	Link down on port 1
4	Info	1970-01-01 00:55:53	Link up on port 1
5	Info	1970-01-01 01:47:14	Link down on port 1
6	Info	1970-01-01 01:48:36	Link up on port 1
7	Info	1970-01-01 02:20:04	Link down on port 1
8	Info	1970-01-01 18:55:49	Link up on port 1
9	Info	1970-01-01 19:58:11	Link down on port 1
10	Info	1970-01-01 19:58:45	Link up on port 1

Parameter	Description
Auto-refresh	Evokes automatic periodic refresh of the log messages.
Level	Level of the system log entry.
ID	ID (≥ 1) of the system log entry.
Time	The time of the system log entry based on the system time.
Message	Display a detailed log detail message.
Upper right icons (Refresh, clear, etc.)	Click to refresh or clear the system log and to go to next and previous page entries.

3.5.3 Detailed Log

This section provides a detailed message of each log entry.

To display the detailed log configuration in the web interface:

Navigate to System > Syslog > Detailed Log.

Figure 12: Detailed Syslog Information

Detailed System Log Information							
ID	1						
Message <table border="1"> <tr> <td>Level</td> <td>Info</td> </tr> <tr> <td>Time</td> <td>-</td> </tr> <tr> <td>Message</td> <td>Switch just made a cold boot.</td> </tr> </table>		Level	Info	Time	-	Message	Switch just made a cold boot.
Level	Info						
Time	-						
Message	Switch just made a cold boot.						

Parameter	Description
ID	ID (≥ 1) of the system log entry.
Message	Display a detailed log detail message.
Upper right icons (Refresh, clear, etc.)	Click to refresh or clear the system log and to go to next and previous page entries.

3.6 SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, if a correct installation of the Management Information Base (MIB) on the managed devices. Using an SNMP protocol to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the Management Information Base (MIB), described in the form of SMI syntax. The SNMP agent running on the switch responds to the request issued by the SNMP manager.

It is passive except when issuing trap information. The system has a switch to turn on or off the SNMP agent. Setting the field SNMP to "Enable" starts the SNMP agent. Access all supported MIB OIDs, including RMON MIB via SNMP manager. If the field SNMP is set to "Disable", the SNMP agent de-activates, and ignores the related Community Name, Trap Host IP Address, Trap and all MIB counters.

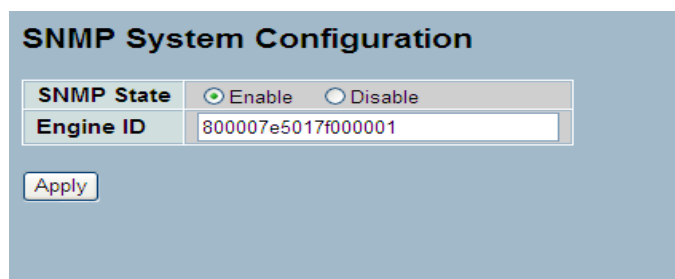
3.6.1 System

This section enables globally enabling or disabling SNMP on the switch.

To configure SNMP via the web interface:

1. Navigate to **System > SNMP > System**.
2. Select the Enable or Disable radio buttons to turn on or off the SNMP function.
3. Specify the Engine ID
4. Click **Apply**.

Figure 13: SNMP System Configuration



The screenshot shows the 'SNMP System Configuration' web page. It features two radio buttons for 'SNMP State': 'Enable' (selected) and 'Disable'. Below this is a text field for 'Engine ID' containing the value '800007e5017f000001'. An 'Apply' button is located at the bottom left of the configuration area.

Parameter	Description
SNMP State	Enable or Disable SNMP on the switch. Enable: Enable SNMP state operation. Disable: Disable SNMP state operation.
Engine ID	SNMPv3 engine ID. Syntax: 0-9,a-f,A-F, min 5 octet, max 32 octet, fifth octet cannot be 00.

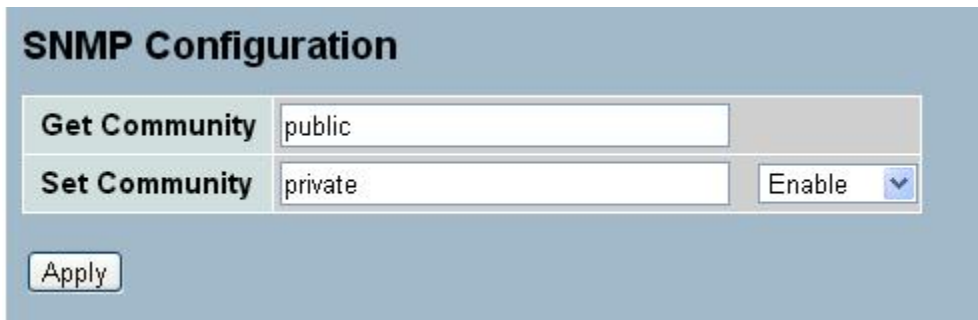
3.6.2 Configuration

The SNMP Get (Read) and Set (Write) community strings are set on this page. The default values are public and private. Enable is the Set community.

To configure the community strings via the web interface:

1. Navigate to **System > SNMP > Configuration**.
2. Specify the Get and Set community strings.
3. Click **Apply**.

Figure 14: SNMP Configuration



The screenshot shows the 'SNMP Configuration' web interface. It has a title bar 'SNMP Configuration'. Below it, there are two rows of input fields. The first row is 'Get Community' with a text box containing 'public'. The second row is 'Set Community' with a text box containing 'private' and a dropdown menu set to 'Enable'. At the bottom left, there is an 'Apply' button.

Parameter	Description
Get Community	The Get or read community string.
Set Community	<p>The Set or write community string. The set community can be enabled or disabled to allow or deny set operations.</p> <p>Indicates the community access string to permit access to SNMPv3 agent. The string length is 1 to 32, and the content is ASCII characters from 33 to 126. The community string will be treated as security name and map an SNMPv1 or SNMPv2c community string.</p>

3.6.3 Communities

Use the function to configure SNMPv3 communities. The Community and Username must be unique. The maximum Group Number is 4.

To configure **SNMP Communities** via the web interface:

1. Navigate to **System > SNMP > Communities**.
2. Click **Add new community**.
3. Specify the SNMP community parameters.
4. Click **Apply**.

Figure 15: SNMP Communities



Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next Apply.
Community	The community access string to permit access to SNMPv3 agent. The string length is 1 to 32, and the content is ASCII characters from 33 to 126. The community string will be treated as security name and map an SNMPv1 or SNMPv2c community string.
User Name	The User Name access string to permit access to SNMPv3 agent. The length is restricted to 1-32.
Source IP	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.

3.6.4 Users

Use the function to configure SNMPv3 users. Max Group Number: 10

To configure SNMP Users via the web interface:

1. Navigate to **System > SNMP > Users**.
2. Specify the security parameters.
3. Click **Apply**.

Figure 16: SNMP Users Configuration

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next Apply.
User Name	A string identifying the user name. The string length is 1 to 32, and the content is ASCII characters from 33 to 126.
Security Level	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <p>NoAuth, NoPriv: No authentication and no privacy.</p> <p>Auth, NoPriv: Authentication and no privacy.</p> <p>Auth, Priv: Authentication and privacy.</p> <p>The value of security level cannot be modified if entry already exists. So ensure that the value is set correctly during initial configuration.</p>
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>



Authentication Password	A string identifying the authentication password phrase. For MD5 authentication protocol, the string length is 8 to 32. For SHA authentication protocol, the string length is 8 to 40. The content is ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: No privacy protocol. DES: An optional flag to indicate that this user uses DES authentication protocol.
Privacy Password	A string identifying the privacy password phrase. The string length is 8 to 32, and the content is ASCII characters from 33 to 126.

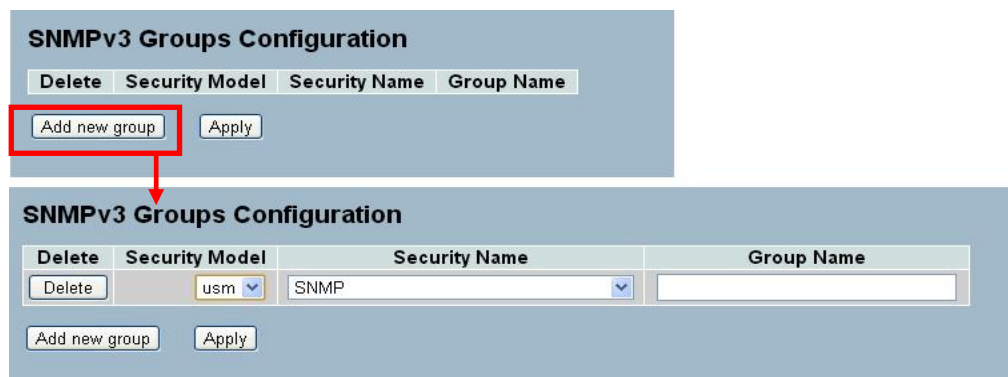
3.7 Groups

Use the function to configure SNMPv3 groups. Max Group Number: v1: 2, v2: 2, v3:10.

To configure SNMP Groups via the web interface:

1. Navigate to **System > SNMP > Groups**.
2. Specify the group security parameters.
3. Click **Apply**.

Figure 17: SNMP Groups Configuration



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

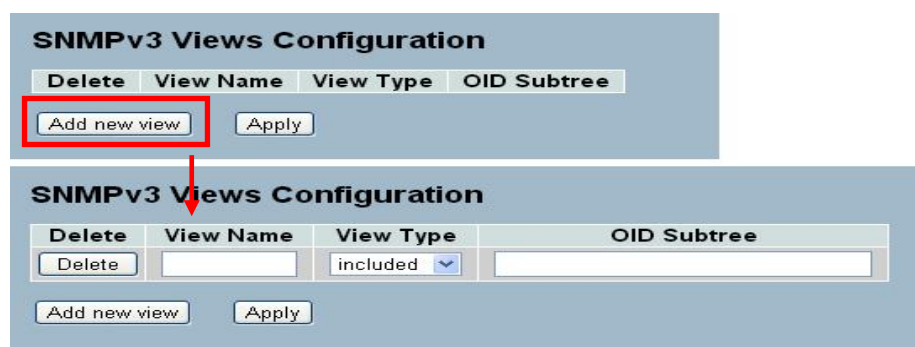
3.8 Views

Use the function to configure SNMPv3 view. Max Group Number: 28.

To configure SNMP Views Configuration via the web interface:

1. Navigate to **System > SNMP > Views**.
2. Click **Add new view** and specify the SNMP View parameters.
3. Click **Apply**.

Figure 18: SNMP Views Configuration



Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name. The string length is 1 to 32, and the 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 OID length is 1 to 128. The string content is digital number or asterisk(*).

3.9 Access

The function is used to configure SNMPv3 access. Max Group Number : 14

To configure the SNMP Access via the web interface:

1. Navigate to **System > SNMP > Access**.
2. Click **Add new access**, and specify the SNMP Access parameters.
3. Click **Apply**.

Figure 19: SNMP Accesses Configuration

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="button" value="Delete"/>	<input type="button" value="Add new access"/>				

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="button" value="Delete"/>	<input type="button" value="Add new access"/>	<input type="button" value="Apply"/>	<input type="button" value="Add new access"/>	<input type="button" value="Apply"/>	<input type="button" value="Apply"/>

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name. The string length is 1 to 32, and the 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 the current values Are requested. The string length is 1 to 32, and the content is ASCII characters from 33 to 126. Write View Name.
Write View name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The string length is 1 to 32, and the content is ASCII characters from 33 to 126.

3.10 Trap

The function is used to configure SNMP traps. Max Group Number : 6.

To configure SNMP Trap setting:

1. Navigate to **System > SNMP > Trap**.
2. Click on the trap number to modify.
3. Modify the parameters of the trap entry.
4. Click **Apply**. To revert to the original settings, click **Reset**.

Figure 20: SNMP Trap Host Configuration

Trap Hosts Configuration

Delete	No	Version	Server IP	UDP Port	Community/Security Name	Severity Level	Security Level	Authentication Protocol	Privacy Protocol
	1								
	2								
	3								
	4								
	5								
	6								

Apply

Trap Host Configuration

Trap Version	v2c
Server IP	0.0.0.0
UDP Port	162
Community/Security Name	
Severity Level	Info
Security Level	NoAuth, NoPriv
Authentication Protocol	MD5
Authentication Password	
Privacy Protocol	DES
Privacy Password	

Apply Reset

Parameter	Description
Delete	Check to delete the entry - deleted during the next save.
Trap Version	Select v2c or v3 trap.
Server IP	Server IP address to send the trap.



UDP Port	Port on which trap is sent to the server. Default: 162.
Community / Security Name	The length of "Community / Security Name" string is restricted to 1-32.
Security Level	Indicates what kind of message will be sent to the server. NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.
Authentication Protocol	Select MD5 or SHA for authentication.
Authentication Password	The length of 'MD5 Authentication Password' is restricted to 8 – 32. The length of 'SHA Authentication Password' is restricted to 8 – 40.
Privacy Protocol	The privacy protocol is set to DES encryption.
Privacy Password	The length of ' Privacy Password ' is restricted to 8 – 32.

4 Configuration

This chapter describes all the network configuration tasks which include the Ports, Layer 2 network protocols (e.g. VLANs, QoS, IGMP, ACLs, and PoE etc.) and other settings on the switch.

4.1 Port

This section enables configuring the port parameters such as speed/duplex settings or enabling and disabling a port.

4.1.1 Configuration

This section describes how to view the current port configuration and how to configure ports to non-default settings, including

- Linkup/Linkdown
- Speed (Current and configured)
- Flow Control (Current Rx, Current Tx and Configured)
- Maximum Frame Size
- Excessive Collision Mode
- Power Control

To configure port settings via the web interface:

1. Navigate to **Configuration > Port > Configuration**.
2. Specify the Speed Configured, Flow Control, Maximum Frame size, Excessive Collision mode, and Power Control.
3. Click **Apply**.

Figure 21: Port Configuration

The screenshot shows the 'Port Configuration' web interface. At the top right is a 'Refresh' button. Below the title is a table with columns: Port, Link, Current, Speed (Configured), Current Rx, Current Tx, Flow Control (Configured), Maximum Frame Size, Excessive Collision Mode, and Power Control. The table lists ports 1 through 10B. Port 1 is up (green dot) with speed 1Gfdx. Ports 2-10B are down (red dots) with speed Auto. All ports have a Maximum Frame Size of 9600, Excessive Collision Mode set to Discard, and Power Control set to Disabled. At the bottom are 'Apply' and 'Reset' buttons.

Port	Link	Current	Speed		Flow Control		Maximum Frame Size	Excessive Collision Mode	Power Control
			Current	Configured	Current Rx	Current Tx			
*			<>					<>	<>
1	● 1Gfdx		Auto		×	×	9600	Discard	Disabled
2	● Down		Auto		×	×	9600	Discard	Disabled
3	● Down		Auto		×	×	9600	Discard	Disabled
4	● Down		Auto		×	×	9600	Discard	Disabled
5	● Down		Auto		×	×	9600	Discard	Disabled
6	● Down		Auto		×	×	9600	Discard	Disabled
7	● Down		Auto		×	×	9600	Discard	Disabled
8	● Down		Auto		×	×	9600	Discard	Disabled
9A	● Down		Auto		×	×	9600	Discard	Disabled
10A	● Down		Auto		×	×	9600	Discard	Disabled
9B	● Down		Auto				9600		
10B	● Down		Auto				9600		

Apply Reset



Parameter	Description
Port	This is the port number.
Link	The current link state is displayed. Green indicates the link is up at 1 Gbps full-duplex, amber indicates the link is up at 100 Mbps full-duplex. Red indicates that the link is down.
Current Link Speed	Displays the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Auto: Automatically negotiates the highest speed that is compatible with the link partner. Disabled: Disables the switch port operation..
Flow Control	When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame Size	Enter the maximum frame size for the switch port, including FCS.
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart backoff algorithm after 16 collisions.
Power Control	The Usage column displays the current percentage of the power consumption per port. The Configured column enables changing the power savings mode parameters per port. Disabled: All power savings mechanisms disabled. ActiPHY: Link down power savings enabled. PerfectReach: Link up power savings enabled. Enabled: Both link up and link down power savings enabled

4.1.2 Port Description

The section describes how to configure the port's alias or any description for the port identity.

To configure port description via the web interface:

1. Navigate to **Configuration > Port > Port Description**.
2. Specify the port alias or description - an alphanumeric string.
3. Click **Apply**.

Figure 22: Port Description

Port	Description
1	To Allworx LAN
2	To Allworx WAN
3	
4	
5	
6	
7	
8	
9A	Uplink
10A	Uplink
9B	Uplink
10B	Uplink

Apply Reset

Parameter	Description
Port	This is the port number.
Description	Description of device ports CANNOT contain " # % & ' + \.

4.1.3 Traffic Overview

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

To display the port statistics overview in the web interface:

1. Navigate to **Configuration > Port > Traffic Overview**.
2. Check the “Auto-refresh” check box for periodic page refresh.
3. Click **Refresh** to update the port statistics or click **Clear** to clear all information on the ports.

Figure 23: Port Statistics Overview

Port Statistics Overview									
Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/>									
Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	7619	10650	1514026	3332717	0	0	0	0	29
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

Parameter	Description
Port	This is the port number.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.

4.1.4 Detailed Statistics

The section provides detailed traffic statistics for a specific switch port. Use the port select box to select a port.

To display the per port detailed statistics in the web interface:

1. Navigate to **Configuration > Port > Detailed Statistics**.
2. Scroll the Port Index to select the port to display the detailed statistics.
3. Check the “Auto-refresh” check box for periodic page refresh.
4. Click **Refresh** to refresh the port statistics or click **Clear** to clear all statistics on the ports.

Figure 24: Port Detail Statistics Overview

Detailed Port Statistics Port 1			
Port 1		Auto-refresh <input type="checkbox"/>	Refresh Clear
Receive Total		Transmit Total	
Rx Packets	7637	Tx Packets	10688
Rx Octets	1518566	Tx Octets	3337459
Rx Unicast	7183	Tx Unicast	4974
Rx Multicast	29	Tx Multicast	5714
Rx Broadcast	425	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	4761	Tx 64 Bytes	72
Rx 65-127 Bytes	200	Tx 65-127 Bytes	5380
Rx 128-255 Bytes	86	Tx 128-255 Bytes	2866
Rx 256-511 Bytes	2588	Tx 256-511 Bytes	97
Rx 512-1023 Bytes	2	Tx 512-1023 Bytes	2139
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	134
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	7637	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	10688

Parameter	Description
Auto-refresh	To refresh the Port Statistics information automatically.
Receive Total and Transmit Total	
Rx and Tx Packets	The number of received and transmitted (good and bad) packets
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.



Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Queue Counters	The number of received and transmitted packets per input and output queue.
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short1 frames received with valid CRC.
Rx Oversize	The number of long1 frames received with valid CRC.
Rx Fragments	The number of short1 frames received with invalid CRC.
Rx Jabber	The number of long2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Transmit Error Counters	
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.
1Short frames are frames that are smaller than 64 bytes. 2Long frames are frames that are longer than the configured maximum frame length for this port.	

4.1.5 Qos Statistics

The section displays the QoS queuing counters for a specific switch port. for all the different queues.

To display the queuing counters in the web interface:

1. Navigate to **Configuration > Port > QoS Statistics**.
2. Check the **Auto-refresh** check box for periodic page refresh.
3. Click **Refresh** to refresh the port statistics, or click **Clear** to clear all statistics on the ports.

Figure 25: Queuing Counters Overview

Queuing Counters

Auto-refresh ☐

Refresh

Clear

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	7655	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10732
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

Parameter	Description
Port	Indicates the port number.
Qn	Qn is the Queue number. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.
Auto-refresh	To refresh the Queuing Counters automatically.

4.1.6 SFP Information

The section displays the SFP module detail information if connected to the switch. The information includes: Connector type, Fiber type, wavelength, baud rate, and Vendor OUI etc.

To display the SFP information in the web interface:

Navigate to **Configuration > Port > SFP Information**

Figure 26: SFP Information Overview

SFP Information for Port 9B	
Connector Type	none
Fiber Type	none
Tx Central Wavelength	none
Bit Rate	none
Vendor OUI	none
Vendor Name	none
Vendor P/N	none
Vendor Revision	none
Vendor Serial Number	none
Date Code	none
Temperature	none
Vcc	none
Mon1 (Bias)	none
Mon2 (TX PWR)	none
Mon3 (RX PWR)	none

Parameter	Description
Connector Type	Display the connector type, for instance, UTP, SC, ST, LC and so on.
Fiber Type	Display the fiber mode, for instance, Multi-Mode, Single-Mode.
Tx Central Wavelength	Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.
Baud Rate	Display the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.
Vendor OUI	Display the Manufacturer's OUI code which is assigned by IEEE.
Vendor Name	Display the company name of the module manufacturer.
Vendor P/N	Display the product name by module manufacturer.
Vendor Rev (Revision)	Display the module revision.
Vendor SN (Serial Number)	Display the serial number assigned by the manufacturer.
Date Code	Display the date this SFP module was made.
Temperature	Display the current temperature of SFP module.
Vcc	Display the working DC voltage of SFP module.
Mon1 (Bias) mA	Display the Bias current of SFP module.
Mon2 (TX PWR)	Display the transmit power of SFP module.
Mon3 (RX PWR)	Display the receiver power of SFP module.

4.1.7 EEE

This section enables the user to inspect and configure the current EEE port settings.

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

EEE works by powering down circuits when there is no traffic. All circuits power up when a port gets data to transmit. 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 transmitting traffic. The devices can exchange information about the devices wakeup time using the LLDP protocol.

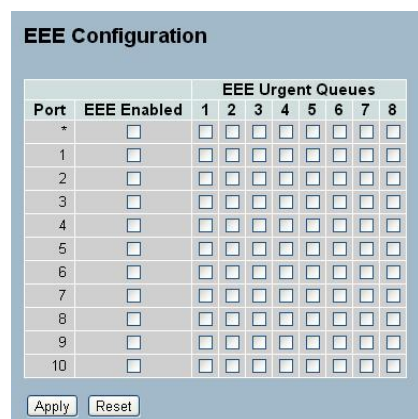
For maximizing the power saving, the circuit isn't started at once transmit data are ready for a port, but is instead queued until 3000 bytes of data are ready to transmit. For not introducing a large delay in case that data less then 3000 bytes transmits, data always transmits after 48 us, giving a maximum latency of 48 us + the wakeup time.

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 transmit, the circuits power up at once and reduces the latency to the wakeup time.

To configure the EEE Configuration via the web interface:

1. Navigate to **Configuration > Port > EEE**.
2. Enable EEE and Urgent Queues for the desired ports. The queues postpone the transmission until it is ready to transmit 3000 bytes.
3. Click **Apply** to save the setting. Click Reset to cancel changes and revert to previously saved values.

Figure 27: EEE Configuration



Port	EEE Enabled	EEE Urgent Queues							
		1	2	3	4	5	6	7	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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>

Apply Reset

Parameter	Description
Port	Indicates the port number.
EEE Enabled	Controls whether EEE is enabled for this switch port.
EE Urgent Queues	Queues set will activate transmtion of frames as soon as any data is available. Otherwise the queue will postpone the transmsion until 3000 bytes are ready to be transmitted.

4.2 ACL

ACLs are most common for using as packet filtering but also for selecting types of traffic to analyze, forward, or influence in some way. The ACLs are divided into EtherTypes - IPv4, ARP protocol, MAC, and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. While creating ACEs for ingress classification, users can assign a policy for each port, the policy number is 1-8, applied to any port. This makes it very easy to determine the type of ACL policy.

4.2.1 Ports

The section describes how to configure the ACL parameters (ACE) of each switch port. These parameters affect frames received on a port unless the frame matches a specific ACE

To configure the ACL ports via the web interface:

1. Navigate to **Configuration > ACL > Ports**.
2. Use the drop-down menu to set ACL parameters for each port.
3. Click **Apply** or click **Reset** to revert to previously saved values.
4. Click **Refresh** to refresh port counters or **Clear** to clear port counters.

Figure 28: ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	<>	<>	<>	Disabled	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
21	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
22	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
23	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
24	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
25	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
26	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

Parameter	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The 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 values are Disabled or the values 1 through 16. The default value is "Disabled".
Port Redirect	Select which port frames are redirected on. The values are Disabled or a specific port number. The default value is "Disabled".
Mirror	Specify the mirror operation of this port. The 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 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 are limited.
Shutdown	Specify the port shut down operation of this port. The 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 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.

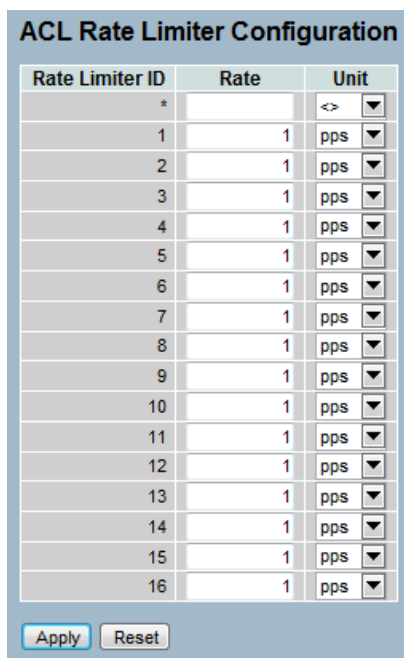
4.2.2 Rate Limiters

The section describes how to configure the switch's ACL Rate Limiter parameters. The Rate Limiter ID ranges from 1 to 16 and the rate is set in pps or kbps.

To configure ACL Rate Limiter via the web interface:

1. Navigate to **Configuration > ACL > Rate Limiter**.
2. Specify the rate ranging from 0 to 3276700.
3. Scroll to set the Unit to pps or kbps.
4. Click **Apply** or click **Reset** to revert to previously saved values.

Figure 29: ACL Rate Limiter Configuration



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

Apply Reset


Parameter	Description
Rate Limiter ID	The rate limiter ID for the settings.
Rate	The values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
Unit	Specify the rate unit. The values are: pps : packets per second. kbps : Kbits per second.

4.2.3 Access Control List

The section describes how to configure Access Control List rules. An Access Control List (ACL) is a sequential list of conditions that permit or deny that apply to IP addresses, MAC addresses, or other more specific criteria. The switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, copying matching packets to another port or to the system log, or shutting down a port.

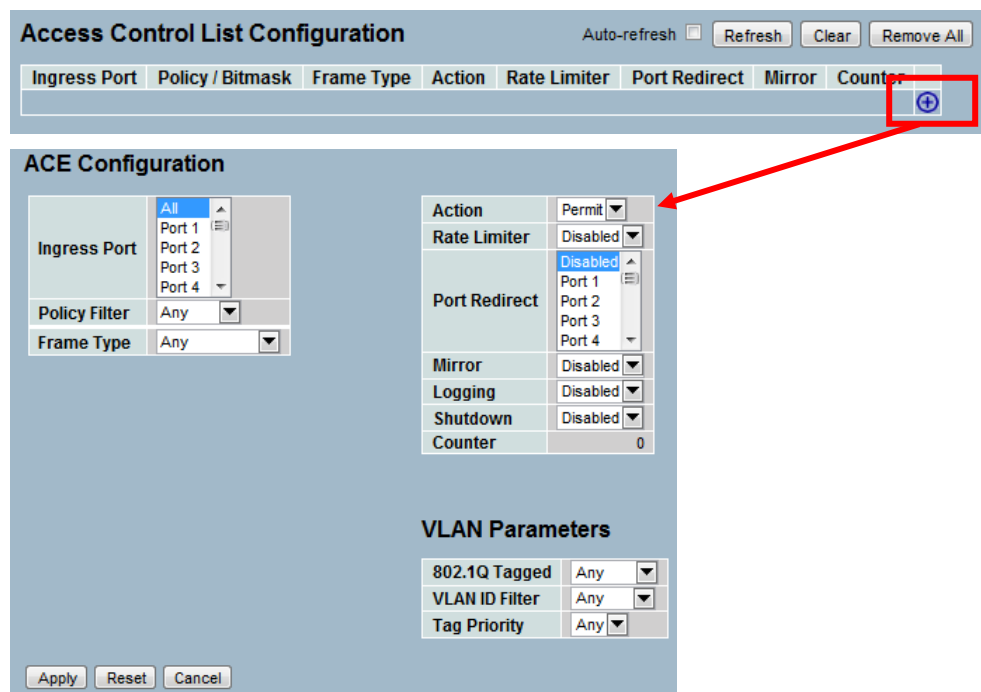
This page shows the Access Control List (ACL), which is made up of the ACEs defined on the switch. Each row describes the defined ACE. The maximum number of ACEs is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocols, cannot be edited or deleted, the order sequence cannot be changed and have the highest priority.

To configure Access Control List via the web interface:







1. Navigate to **Configuration > ACL > Access Control List**.
2. Click the  button to add a new ACL, or use the other ACL modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
3. Specific the parameters of the ACE.
4. Click **Apply** or click **Reset** to revert to previously saved values.

When editing an entry on the ACE Configuration page, note that the items displayed depend on various selections, such as Frame Type and IP Protocol type. Specify the relevant criteria to match for this rule and set the actions to take when matching a rule (such as Rate Limiter, Port Copy, Logging, and Shutdown).

Figure 30: ACL Rate Limiter Configuration



Parameter	Description
Ingress Port	<p>Select the ingress port for which this ACE applies.</p> <p>All: The ACE applies to all port.</p> <p>Port n: The ACE applies to this port number, where n is the number of the switch port.</p>
Policy Filter	<p>Specify the policy number filter for this ACE.</p> <p>Any: No policy filter is specified (policy filter status is "don't-care".)</p> <p>Specific: To filter a specific policy with this ACE, select this value. Two fields for entering policy value and bitmask appear.</p>
Frame Type	<p>Indicates the frame type of the ACE. Possible values are:</p> <p>Any: The ACE will match any frame type.</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 permitted for the ACE operation.</p> <p>Deny: The frame that hits this ACE is dropped.</p>
Rate Limiter	<p>Indicates the rate limiter number of the ACE. The range is 1 to 16. When set to Disabled, the rate limiter operation is disabled.</p>
Port Redirect	<p>Frames that hit the ACE are redirected to the port number specified here. The range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled.</p>
Mirror	<p>Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The 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>
Logging	<p>Indicates the logging operation of the ACE. Possible 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 are limited.</p>

Shutdown	Indicates the port shut down operation of the ACE. Possible values: Enabled: If a frame matches the ACE, the ingress port will be disabled. Disabled: Port shut down is disabled for the ACE.
Counter	The counter indicates the number of times the ACE was hit by a frame.
VLAN Parameters	
802.1Q Tagged	Specify whether frames can hit the action according to the 802.1Q tag. The values are: Any: Any value ("don't-care"). Enabled: Tagged frame only. Disabled: Untagged frame only. The default value is "Any".
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: To filter a specific VLAN ID with this ACE, select this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, enter a specific VLAN ID number. The range is 1 to 4094. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)
Modification Buttons	Modify each ACE (Access Control Entry) in the table using the following buttons:  : Inserts a new ACE before the current row.  : Edits the ACE row.  : Moves the ACE up the list.  : Moves the ACE down the list.  : Deletes the ACE.  : The lowest plus sign adds a new entry at the bottom of the ACE listings

4.2.4 ACL Status

The section describes how to display the ACL status by different ACL users. Each row describes the defined ACE. It is a conflict if a specific ACE does not apply to the hardware due to hardware limitations. The maximum number of ACEs is 256 on each switch.

To display the ACL status in the web interface:

1. Navigate to **Configuration > ACL > ACL status**.
2. Check the **Auto-refresh** button to refresh the page automatically periodically.
3. Click **Refresh** to refresh the ACL Status.

Figure 31: ACL Status

ACL Status										
						Combined	Auto-refresh <input type="checkbox"/>		Refresh	
User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
IP Management	All	ARP	Deny	Disabled	Disabled	Disabled	Yes	No	934	No
IP Management	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Disabled	Yes	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No
Reserved	All	EType	Permit	Disabled	Disabled	Disabled	No	No	0	No
Static	All	Any	Permit	Disabled	Disabled	Disabled	No	No	3410	No

Parameter	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress ports. Port: The ACE will match a specific ingress port
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The range is 1 to 16. When disabled,



	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 values are Disabled or a specific port number. When disabled, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. If Yes, the specific ACE is not applied to the hardware due to hardware limitations.

4.3 Aggregation

Use Aggregation to configure the settings of Link Aggregation. Users can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

4.3.1 Static Trunk

Ports using Static Trunk as the trunk method can select the unique Static GroupID to form a logical “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of the static trunk group may not know to aggregate together to form a “logical trunked port”. Allworx strongly recommends using Static Trunk on both ends of a link. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

To configure the Trunk Aggregation Hash mode and Aggregation Group via the web interface:

1. Navigate to **Configuration > Aggregation > Static Trunk**.
2. Check the hash code contributors to include.
3. Select the ports for the Group ID that would form a static trunk.
4. Click **Apply** or click **Reset** to revert to previously saved values.

Figure 32: Aggregation Mode Configuration

Aggregation Mode Configuration

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

Aggregation Group Configuration

Group ID	Port Members											
	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Normal	<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"/>
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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter		Description
Hash Code Contributors		
Source MAC Address		The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
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		
Locality		<p>Indicates the aggregation group type. This field is only valid for stackable switches.</p> <p>Global: The group members may reside on different units in the stack. The device supports two 8-port global aggregations.</p> <p>Local: The group members reside on the same unit. Each local aggregation may consist of up to 16 members.</p>
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 have the same speed in each group.

4.4 LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as the trunking method can select the unique LACP GroupID to form a logical “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

4.4.1 Configuration

This page enables the user to inspect and change the current LACP port configurations. An LACP trunk group with more than one ready member-port is a “real trunked” group. An LACP trunk group with only one or less than one ready member-port is not a “real trunked” group.

To configure the LACP parameters via the web interface:

1. Navigate to **Configuration > Aggregation > LACP > Configuration**.
2. Check the LACP Enabled box to enable LACP on the port.
3. Set the key to Auto or Specific. Auto is the default.
4. Set the role to Active or Passive. Default is Active.
5. Click **Apply** or click **Reset** to revert to previously saved values.

Figure 33: LACP Port Configuration

LACP Port Configuration

Port	LACP Enabled	Key		Role
*	<input type="checkbox"/>	<>		<>
1	<input type="checkbox"/>	Auto		Active
2	<input type="checkbox"/>	Auto		Active
3	<input type="checkbox"/>	Auto		Active
4	<input type="checkbox"/>	Auto		Active
5	<input type="checkbox"/>	Auto		Active
6	<input type="checkbox"/>	Auto		Active
7	<input type="checkbox"/>	Auto		Active
8	<input type="checkbox"/>	Auto		Active
9A	<input type="checkbox"/>	Auto		Active
10A	<input type="checkbox"/>	Auto		Active
9B	<input type="checkbox"/>	Auto		Active
10B	<input type="checkbox"/>	Auto		Active

Apply Reset

Parameter	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. LACP can form a maximum of 12 LLAGs per switch and 2 GLAGs per stack.
Key	The Key value incurred by the port, range 1-65535. The Auto setting will set the key based on 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 displays the LACP activity status. Active will transmit LACP packets each second, while Passive will wait for a LACP packets from a partner (speak if spoken to).

4.4.2 System Status

This section provides a status overview for all LACP instances

To display the LACP System status in the web interface:

1. Navigate to **Configuration > Aggregation > LACP > System Status**.
2. Check the **Auto-refresh** checkbox for automatic page refresh periodically.
3. Click **Refresh** to refresh the LACP System Status.

Figure 34: LACP System Status

LACP System Status				
Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
No ports enabled or no existing partners				

Parameter	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id displays as 'isid:aggr-id' and for GLAGs as 'aggr-id'.
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Local Ports	Displays which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".

4.4.3 Port Statistics

This section provides a Port Statistics overview for all LACP instances

To display the LACP Port status in the web interface:

1. Navigate to Configuration> Aggregation > LACP > Port Statistics.
2. Check the **Auto-refresh** checkbox for automatic page refresh periodically.
3. Click **Refresh** to refresh the LACP Statistics.

Figure 35: LACP Statistics

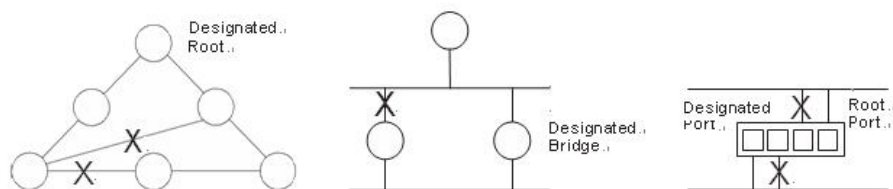
LACP Statistics				
Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Parameter	Description
Port	The switch port number.
LACP Received	Indicates the number of received LACP frames at each port.
LACP Transmitted	Indicates the number of sent LACP frames from each port.
Discarded	Displays how many unknown or illegal LACP frames have been discarded at each port.

4.5 Spanning Tree

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

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



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

4.5.1 Bridge Settings

The section describes how to configure the Spanning Tree Bridge and STP System settings. It enables configuring STP System settings used by all STP Bridge instances in the Switch Stack.

To configure the Spanning Tree Bridge Settings parameters via the web interface:

1. Navigate to **Configuration > Spanning Tree > Bridge Settings**.
2. Use the drop-down menus to select the parameters and specify other values in the Basic Settings.
3. Specify parameters in the Advanced settings.
4. Click **Apply** or click **Reset** if to want to revert to previously saved values.

Figure 36: STP Bridge Configuration

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

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

Apply Reset

Parameter	Description
Basic Settings	
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Bridge Priority	Controls the bridge priority. Lower numeric values have higher 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 state (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 MaxAge must be $\leq (\text{FwdDelay}-1)*2$.
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 BPDUs 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 BPDUs per second.
Advanced Settings	
Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.



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

4.5.2 MSTI Mapping

When implementing Spanning Tree protocol on the switch that the bridge instance. The CIST is not available for explicit mapping, as it receives the VLANs not explicitly mapped. Due to the reason that users need to set the list of VLANs mapped to the MSTI. Separate the VLANs with comma and/or space. Map a VLAN to one MSTI. Leave the unused MSTI empty (i.e., no mapped VLANs).

This section enables the user to inspect and change the current STP MSTI bridge-instance priority configurations.

To configure the Spanning Tree MSTI Mapping parameters via the web interface:

1. Navigate to **Configuration > Spanning Tree > MSTI Mapping**.
2. Specify the configuration identification parameters in the fields.
3. Specify the values in the VLANs Mapped field.
4. Click **Apply** or click **Reset** to cancel the changes and revert to previously saved values.

Figure 37: MSTI Configuration

Parameter		Description
Configuration Identification		
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 MSTIs (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		
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 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 have any VLANs).

4.5.3 MSTI Priorities

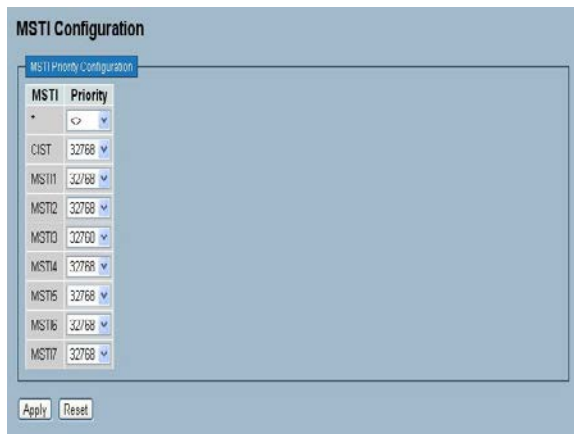
When implementing an Spanning Tree protocol on the switch that the bridge instance. The CIST is the default instance which is always active. For controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier

This section enables the user to inspect and change the current STP MSTI bridge-instance priority configurations.

To configure the Spanning Tree MSTI Priorities parameters via the web interface:

1. Navigate to **Configuration > Spanning Tree > MSTI Priorities**.
2. Set the priority for the MSTI Instances. Default is 32768.
3. Click **Apply** and click **Reset** to cancel the changes and revert to previously saved values.

Figure 38: MSTI Configuration



MSTI	Priority
CIST	32768
MST11	32768
MST12	32768
MST13	32768
MST14	32768
MST15	32768
MST16	32768
MST17	32768

Apply Reset

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

4.5.4 CIST Ports

When implementing a Spanning Tree protocol on the switch that the bridge instance users need to configure the CIST Ports. This section enables the user to inspect and change the current STP CIST port configurations.

To configure the Spanning Tree CIST Ports parameters via the web interface:

1. Navigate to **Configuration > Spanning Tree > CIST Ports**.
2. Use the drop-down menus and check boxes to set all parameters of CIST Aggregated Port Configuration.
3. Enable or disable the STP, then use the drop-down menus and check boxes to set all parameters of the CIST normal Port configuration.
4. Click **Apply** and click **Reset** to cancel the changes and revert to previously saved values.

Figure 39: STP CIST Port Configuration

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 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 type="checkbox"/>	<>	<>	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9A	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10A	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9B	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10B	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Apply Reset

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

Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (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 enables deriving operEdge from whether BPDUs are received on the port or not.
Restricted Role	If enabled, it 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, it 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 persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
BPDU	If enabled, it causes the port to disable itself upon receiving valid BPDUs. 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.

4.5.5 MSTI Ports

This section enables the user to inspect and change the current STP MSTI port configurations.

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. Select the MSTI instance before displaying actual MSTI port configuration options. It contains MSTI port settings for physical and aggregated ports.

To configure the Spanning Tree MSTI Port Configuration parameters via the web interface:

1. Navigate to **Configuration > Spanning Tree > MSTI Ports**.
2. Use the drop-down menu to select the MST1 or other MSTI port.
3. Click **Get** to set the parameters of the MSTI ports.
4. Use the drop-down menus to set all parameters of the MSTI Port configuration.
5. Click **Apply** or click **Reset** to cancel the changes and revert to previously saved values.

Figure 40: MSTI Port Configuration

MSTI Port Configuration

Select MSTI
MST1 ▼ Get

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 ▼
9A	Auto ▼	128 ▼
10A	Auto ▼	128 ▼
9B	Auto ▼	128 ▼
10B	Auto ▼	128 ▼

Apply Reset

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

4.5.6 Bridge Status

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

To display the STP Bridge status in the web interface:

1. Navigate to **Configuration > Spanning Tree > Bridge Status**.
2. Checking the **Auto-refresh** button automatically refreshes the page at periodic intervals.
3. Click **Refresh** to refresh the STP Bridge status.

Figure 41: STP Bridge Status

STP Bridges							Auto-refresh <input type="checkbox"/>	Refresh
MSTI	Bridge ID	Root			Topology Flag	Topology Change Last		
		ID	Port	Cost				
CIST	80:00:00:0A:DD:04:00:14	80:00:00:0A:DD:04:00:14	-	0	Steady	-		

Parameter	Description
MSTI	The Bridge instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flat	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Last	The time since last topology change occurred.

4.5.7 Port Status

This section displays the STP CIST port status.

To display the STP Port status in the web interface:

1. Navigate to **Configuration > Spanning Tree > Port Status**.
2. Checking the **Auto-refresh** button automatically refreshes the page at periodic intervals.
3. Click **Refresh** to refresh the port status page.

Figure 42: STP Port Status

STP Port Status				Auto-refresh <input type="checkbox"/>	Refresh
Port	CIST Role	CIST State	Uptime		
1	Non-STP	Forwarding	-		
2	Non-STP	Forwarding	-		
3	Non-STP	Forwarding	-		
4	Non-STP	Forwarding	-		
5	Non-STP	Forwarding	-		
6	Non-STP	Forwarding	-		
7	Non-STP	Forwarding	-		
8	Non-STP	Forwarding	-		
9	Non-STP	Forwarding	-		
10	Non-STP	Forwarding	-		
11	Non-STP	Forwarding	-		
12	Non-STP	Forwarding	-		
13	Non-STP	Forwarding	-		
14	Non-STP	Forwarding	-		

Parameter	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled.Non-STP.
Cist State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.
Uptime	The time since the bridge port was last initialized.

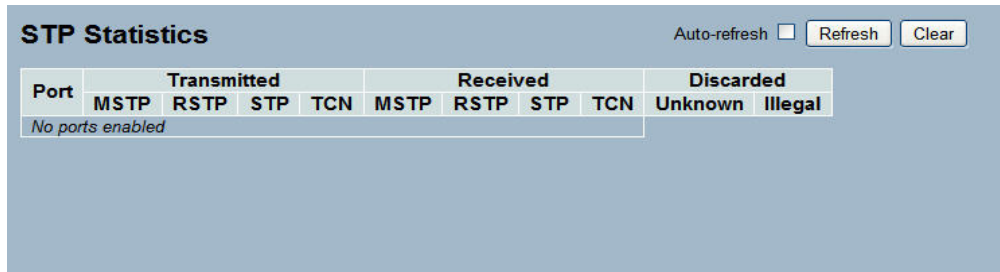
4.5.8 Port Statistics

After completing the STP configuration, display the STP Statistics. This section displays the STP Statistics counters of the bridge ports in the currently selected switch.

To display the STP Port statistics in the web interface:

1. Navigate to **Configuration > Spanning Tree > Port Statistics**.
2. Checking the **Auto-refresh** button automatically refreshes the page at periodic intervals.
3. Click **Refresh** to refresh the STP Bridges.

Figure 43: STP Statistics



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

Parameter	Description
Port	The switch port number of the logical STP port.
MSTP	The number of MSTP Configuration BPDUs received/transmitted on the port.
RSTP	The number of RSTP Configuration BPDUs received/transmitted on the port.
STP	The number of legacy STP Configuration BPDUs received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDUs received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDUs received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDUs received (and discarded) on the port.

4.6 **IGMP Snooping**

The function is used to enable the multicast groups to forward the multicast packets to the member ports and avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell a multicast packet from a broadcast packet and treats both all as broadcast packets.

A switch that supports IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packets only to members who have already joined the specified IP multicast group.

The IGMP Snooping discards the packets, if the user transmits multicast packets to the multicast group not built up in advance. IGMP proxy or snooping enabled on the switch enables it to connect to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

4.6.1 **Basic Configuration**

This section describes how to set the basic IGMP snooping on the switch.

To configure the IGMP Snooping parameters via the web interface:

1. Navigate to **Configuration > IGMP Snooping > Basic Configuration**.
2. Check the Snooping Enabled box to enable IGMP snooping globally on the switch.
3. Check the port that has to be set as the Router Port and enable/ disable the Fast Leave function on the ports.
4. Use the drop-down menu to set the Throttling parameter.
5. Click **Apply** or click **Reset** to cancel the changes and revert to previously saved values.

Figure 44: IGMP Snooping Configuration

IGMP Snooping Configuration

Global Configuration

Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Proxy Enabled	<input type="checkbox"/>

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
9A	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10A	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9B	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10B	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Parameter	Description
Snooping	Enable IGMP Snooping globally on the switch.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
IGMP SSM Range	It enables the SSM-aware hosts and routers run the SSM service model for groups in the address range.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
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 fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.6.2 VLAN Configuration

This section describes the VLAN configuration settings integrated with IGMP Snooping function. For each setting, the page displays 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 displays the first 20 entries from the beginning of the VLAN Table in ascending order of the VLAN IDs. . The "Start from VLAN" field enables the user to select the starting point in the VLAN Table.

To configure the IGMP Snooping VLAN Configuration via the web interface:

1. Navigate to **Configuration > IGMP Snooping > VLAN Configuration**.
2. Check/uncheck the Snooping Enabled checkbox to enable or disable Snooping on that VLAN.
3. Click the **Refresh** to update the data or click << or >> to display previous entry or next entry.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 45: IGMP Snooping VLAN Configuration

VLAN ID	Snooping Enabled
1	<input checked="" type="checkbox"/>

Parameter	Description
Snooping Enabled	Enable the Global IGMP Snooping.

4.6.3 Port Group Filtering

This section describes how to set the IGMP Port Group Filtering. In some network Application environments, as like the metropolitan or multiple-dwelling unit (MDU) installations, a user might want to control the multicast groups to which a user on a switch port can belong. It enables the user to control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan.

With this feature, users can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating users with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether to permit or deny access to the group. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the port forwards the IGMP report for normal processing.

IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

To configure IGMP Snooping Port Group Filtering via the web interface:

1. Navigate to **Configuration > IGMP Snooping > Port Group Filtering**.
2. Click Add new Filtering Group.
3. Select the port to enable the Port Group Filtering for and specify the Filtering Groups.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 46: IGMP Snooping Port Group Filtering Configuration

The figure shows two screenshots of the web interface for IGMP Snooping Port Group Filtering Configuration. The top screenshot shows the initial state with a red box highlighting the 'Add new Filtering Group' button. A red arrow points from this button to the bottom screenshot. The bottom screenshot shows the configuration form after clicking the button. It includes a 'Delete' checkbox, a 'Port' dropdown menu set to '1', and an empty 'Filtering Groups' text input field. Below these fields are 'Add new Filtering Group', 'Apply', and 'Reset' buttons.

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next Apply.
Port	Select port for which to enable the IGMP Snooping Port Group Filtering function.
Filtering Groups	The IP Multicast Group(s) that will be filtered.

4.6.4 Status

This section displays the IGMP Snooping status.

To display the IGMP Snooping status in the web interface:

1. Navigate to **Configuration > IGMP Snooping > Status**.
2. Check the **Auto-refresh** button to refresh the page at periodic intervals.
3. Click **Refresh** to refresh the IGMP Snooping Status or click **Clear** to clear the IGMP Snooping Status.

Figure 47: IGMP Snooping Status

IGMP Snooping Status									
Auto-refresh <input type="checkbox"/> 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
1	v3	v3	ACTIVE	0	0	0	0	0	0
Router Port									
Port	Status								
1	-								
2	-								
3	-								
4	-								
5	-								
6	-								
7	-								
8	-								
9A	-								
10A	-								
9B	-								
10B	-								

Parameter	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Current working Querier Version.
Host Version	Current working Host Version.
Querier Status	Displays the Querier status "ACTIVE" or "IDLE".
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.

4.6.5 Groups Information

Entries in the IGMP Group Table display on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group. The switch will use the last entry of the currently displayed table as a basis for the next lookup. When reaching the end the text "No more entries" displays.

To display the IGMP Snooping Group Information in the web interface:

1. Navigate to **Configuration > IGMP Snooping > Group Information**.
2. Check **Auto-refresh** to refresh the page at periodic intervals.
3. Click **Refresh** to refresh an entry of the IGMP Snooping Groups Information.
4. Click << or >> to move to previous or next entry.

Figure 48: IGMP Snooping Groups Information

Parameter	Description
Navigating the IGMP Group Table The "Start from VLAN", and "group" input fields enable the user to select the starting point in the IGMP Group Table. The switch will use the last entry of the currently displayed table as a basis for the next lookup. When reaching the end, the text "No more entries" displays.	
IGMP Group Table Columns	
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

4.6.6 IPv4 SSM information

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S, G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

SSM by INA reserves addresses in the range 232.0.0.0/8 (232.0.0.0 to 232.255.255.255). In the switch configure SSM for arbitrary IP multicast addresses also.

To display the IGMPv3 IPv4 SSM Information in the web interface:

1. Navigate to **Configuration > IGMP Snooping > IPv4 SSM Information**.
2. Check **Auto-refresh** to refresh the page at periodic intervals.
3. Click **Refresh** to refresh an entry of the IGMPv3 IPv4 SSM Information.
4. Click << or >> to move to previous or next entry.

Figure 49: IPv4 SSM Information

Parameter	Description
<p>Navigating the IGMPv3 Information Table</p> <p>Each page displays up to 99 entries from the IGMPv3 SSM (Source Specific Multicast) Information table, default being 20, selected through the "entries per page" field. When first visited, the web page displays the first 20 entries from the beginning of the IGMPv3 Information Table.</p> <p>The "Start from VLAN", and "group" fields enable the user to select the starting point in the IGMPv3 Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMPv3 Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.</p> <p>The switch will use the last entry of the currently displayed table as a basis for the next lookup. When reaching the end the text "No more entries" displays.</p>	
IGMPv3 Information Table Columns	
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.



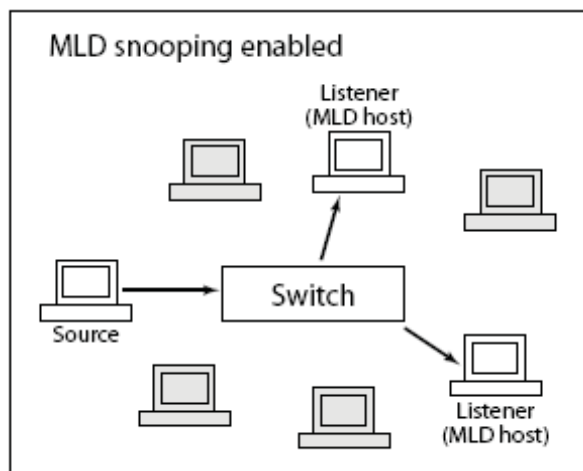
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the Type. It can be either Allow or Deny.

4.7 MLD Snooping

Curiously enough, a network node that acts as a source of IPv6 multicast traffic is only an indirect participant in MLD snooping—it just provides multicast traffic, and MLD doesn't interact with it. (Note, however, that in an application like desktop conferencing a network node may act as both a source and an MLD host; but MLD interacts with that node only in its role as an MLD host.)

A source node creates multicast traffic by sending packets to a multicast address. In IPv6, addresses with the first eight bits set (that is, "FF" as the first two characters of the address) are multicast addresses, and any node that listens to such an address will receive the traffic sent to that address. The source and destination systems running application software cooperate to determine what multicast address to use. (Note that this is a function of the application software, not of MLD.)

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts



4.7.1 Basic Configuration

This section describes how to configure the MLD Snooping basic configuration and the parameters.

To configure the MLD Snooping Configuration via the web interface:

1. Navigate to **Configuration > MLD Snooping > Basic Configuration**.
2. Check the Snooping Enabled checkbox to enable MLD snooping globally on the switch. Set the other global configuration parameters.
3. Check the boxes to set the port to join Router port and Fast Leave.
4. Set the Throttling mode to unlimited or 1 to 10.
5. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 50: MLD Snooping Basic Configuration

MLD Snooping Configuration

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

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
9A	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10A	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9B	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10B	<input type="checkbox"/>	<input type="checkbox"/>	unlimited

Parameter	Description
Snooping Enabled	Enable the Global MLD Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMCv6 traffic flooding. Note that disabling unregistered IPMCv6 traffic flooding may lead to failure of Neighbor Discovery.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	To enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

4.7.2 2 VLAN Configuration

When MLD snooping is enabled on a VLAN, the switch acts to minimize unnecessary multicast traffic. If the switch receives multicast traffic destined for a given multicast address, it forwards that traffic only to ports on the VLAN that have MLD hosts for that address. It drops that traffic for ports on the VLAN that have no MLD hosts

To configure the MLD Snooping VLAN Configuration via the web interface:

1. Navigate to **Configuration > MLD Snooping > VLAN Configuration**.
2. Check the Snooping Enabled checkbox for VLANs to enable snooping.
3. Click **Refresh** to refresh an entry of the MLD Snooping VLAN Configuration Information.
4. Click "<< or >>" to move to previous or next entry.

Figure 51: MLD Snooping VLAN Configuration

MLD Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled
1	<input checked="" type="checkbox"/>

Save Reset

Refresh |<< >>

Parameter	Description
VLAN ID	The VLAN ID of the entry.
Snooping Enabled	Enable the per-VLAN MLD Snooping. Select up to 64 VLANs.

4.7.3 Port Group Filtering

This section describes how to set the Port Group Filtering in the MLD Snooping function.

To configure the MLD Snooping Port Group Filtering via the web interface:

1. Navigate to **Configuration > MLD Snooping > Port Group Filtering**.
2. Click Add new Filtering Group.
3. Specify the Filtering Groups for each port.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 52: MLD Snooping Port Group Filtering

The figure consists of two screenshots of the web interface for MLD Snooping Port Group Filtering Configuration.

The top screenshot shows the configuration page with three tabs: **Delete**, **Port**, and **Filtering Groups**. The **Filtering Groups** tab is active. A red box highlights the **Add new Filtering Group** button. Below this button are **Apply** and **Reset** buttons.

The bottom screenshot shows the same page after clicking the **Add new Filtering Group** button. A table is displayed with the following structure:

Delete	Port	Filtering Groups
<input type="button" value="Delete"/>	1	<input type="text"/>

Below the table, there is an **Add new Filtering Group** button and **Apply** and **Reset** buttons.

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next apply.
Port	The logical port for the settings.
Filtering Groups	The IP Multicast Group that will be filtered.

4.7.4 Status

This section displays the MLD Snooping Status and information.

To display the MLD Snooping Status in the web interface:

1. Navigate to **Configuration > MLD Snooping > Status**.
2. Check the **Auto-refresh** box to refresh the page at periodic intervals.
3. Click **Refresh** to refresh or click Clear to clear the MLD Snooping Status Information.

Figure 53: 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
1	v2	v2	ACTIVE	0	0	0	0	0

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9A	-
10A	-
9B	-
10B	-

Parameter	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Current working Querier Version .
Host Version	Current working Host Version.
Querier Status	Displays the Querier status - "ACTIVE" or "IDLE".
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V1 Leaves Received	The number of Received V1 Leaves.

4.7.5 Group Information

This page displays the MLD Snooping Groups Information. The "Start from VLAN", and "group" input fields enable the user to select the starting point in the MLD Group Table

To display the MLD Snooping Group information in the web interface:

1. Navigate to **Configuration > MLD Snooping > Group Information**.
2. Check **Auto-refresh** to refresh the page at periodic intervals.
3. Click **Refresh** to refresh or click Clear to clear the MLD Snooping Group Information.

Figure 54: MLD Snooping Groups Information

Parameter	Description						
<p>Navigating the MLD Group Table</p> <p>Each page displays up to 99 entries from the MLD Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page displays the first 20 entries from the beginning of the MLD Group Table. The "Start from VLAN", and "group" input fields enable the user to select the starting point in the MLD Group Table.</p> <p>The "Start from VLAN", and "group" fields enable the user to select the starting point in the IGMPv3 Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next IGMPv3 Information Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.</p> <p>The switch will use the last entry of the currently displayed table as a basis for the next lookup. When reaching the end, the text "No more entries" displays.</p>							
<p>MLD Snooping Information Table Columns</p> <table> <tr> <td>VLAN ID</td><td>VLAN ID of the group.</td></tr> <tr> <td>Groups</td><td>Group address of the group displayed.</td></tr> <tr> <td>Port Members</td><td>Ports under this group.</td></tr> </table>		VLAN ID	VLAN ID of the group.	Groups	Group address of the group displayed.	Port Members	Ports under this group.
VLAN ID	VLAN ID of the group.						
Groups	Group address of the group displayed.						
Port Members	Ports under this group.						

4.7.6 IPv6 SSM Information

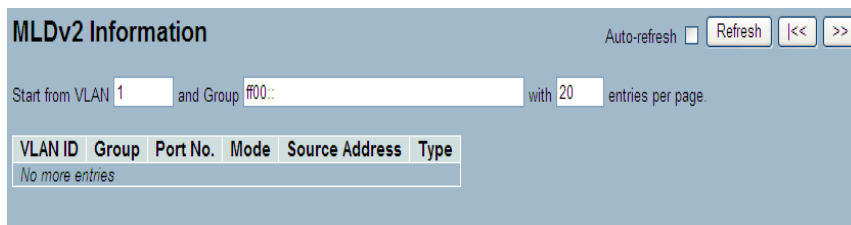
The MLDv2 Information Table is sorted first by VLAN ID, then by group, and then by Port No. It also treats different source addresses belong to the same group as single entry.

Each page displays up to 64 entries from the MLDv2 SSM (Source Specific Multicast) Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page displays the first 20 entries from the beginning of the MLDv2 Information Table. The "Start from VLAN", and "group" fields enable the user to select the starting point in the MLDv2 Information Table.

To display the MLDv2 IPv6 SSM Information in the web interface:

1. Navigate to **Configuration > MLD Snooping > IPv6 SSM Information**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the MLDv2 IPv6 SSM Information.
4. Click "<< or >>" to move to previous or next entry.

Figure 55: IPv6 SSM Information



Parameter		Description
MLDv2 Information Table Columns		
VLAN ID		VLAN ID of the group.
Groups		Group address of the group displayed.
Port		Switch port number.
Mode		Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address		IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type		Indicates the Type. It can be either Allow or Deny.

:

4.8 MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port.

When a subscriber selects a channel, the set-top box or the PC sends an IGMP join message to Switch A requesting to join the appropriate multicast. MVR source ports are uplink ports that send and receive multicast data to and from the multicast VLAN.

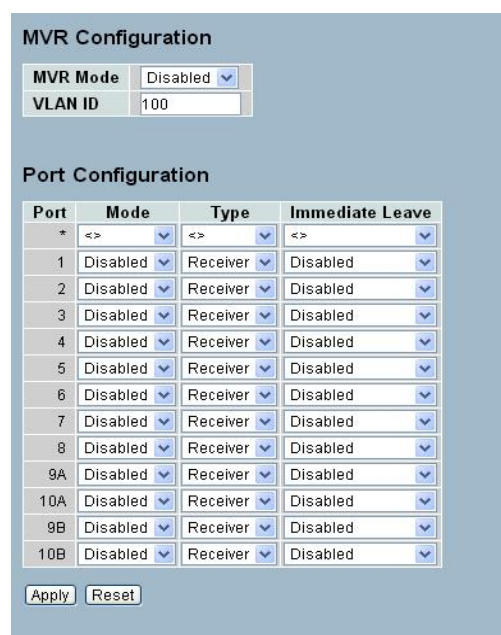
4.8.1 Configuration

The section describes the MVR basic configuration.

To configure MVR via the web interface:

1. Navigate to **Configuration > MVR > Configuration**.
2. Use the drop-down menu to enable or disable MVR. Set the VLAN ID and port details.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 56: MVR Configuration



Port	Mode	Type	Immediate Leave
*	<>	<>	<>
1	Disabled	Receiver	Disabled
2	Disabled	Receiver	Disabled
3	Disabled	Receiver	Disabled
4	Disabled	Receiver	Disabled
5	Disabled	Receiver	Disabled
6	Disabled	Receiver	Disabled
7	Disabled	Receiver	Disabled
8	Disabled	Receiver	Disabled
9A	Disabled	Receiver	Disabled
10A	Disabled	Receiver	Disabled
9B	Disabled	Receiver	Disabled
10B	Disabled	Receiver	Disabled

Parameter	Description
MVR Mode	Enable/Disable the MVR globally.
VLAN ID	Specify the Multicast VLAN ID.
Mode	Enable MVR on the port.
Type	Specify the MVR port type on the port.
Immediate Leave	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.

Type	Enable fast leave on the port.
------	--------------------------------

4.8.2 Port Group Allow

This section enables adding multicast groups.

To configure Port Allow Group via the web interface:

1. Navigate to **Configuration > MVR > Port Group Allow**.
2. Click **Add new Allow Group**.
3. Click **Apply** or Click **Reset** to revert to previously saved values. Click **Apply** and **Save Start** to save the change.

Figure 57: MVR Port Group Allow




Parameter	Description
Delete	Check to delete entry – the next apply deletes.
Port	Indicates the port number.
Allow Group	The allowed IP multicast groups.

4.8.3 Groups Information

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

To display the MVR Groups Information in the web interface:

1. Navigate to **Configuration > MVR > Groups Information**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the MVR Groups Information.
4. Click "<< or >>" to move to previous or next entry.

Figure 58: MVR Groups Information

Parameter		Description
MVR Group Table Columns		
VLAN ID		VLAN ID of the group.
Groups		Group ID of the group displayed.
Port Members		Ports under this group.

4.8.4 Statistics

This section displays the MVR Statistics on the switch.

To display the MVR Statistics Information in the web interface:

1. Navigate to **Configuration > MVR > Statistics**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the MVR Statistics
4. Click "<< or >>" to move to previous or next entry.

Figure 59: MVR Statistics Information

VLAN ID	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
100	0	0	0	0

Parameter	Description
VLAN ID	The Multicast VLAN ID.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.

4.9 LLDP

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

4.9.1 LLDP Configuration

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

To configure LLDP:

1. Navigate to **Configuration > LLDP > LLDP Configuration**.
2. Modify LLDP timing parameters, if required.
3. Set the required mode for transmitting or receiving LLDP messages.
4. Specify the information to include in the TLV field of advertised messages.
5. Click **Apply**.

Figure 60: LLDP Configuration


LLDP Configuration

LLDP Parameters

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

Port	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Enabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9A	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10A	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9B	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10B	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Parameter		Description
LLDP Parameters		
Tx Interval		The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold		Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.
Tx Delay		If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit		When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information is not valid anymore. Tx Reinit controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.
LLDP Port Configuration		
The LLDP port settings relate to the currently selected stack unit, as reflected by the page header.		
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 neighbor units is analyzed.</p> <p>Tx only: The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p> <p>Disabled: The switch will not send out LLDP information, and drops LLDP information received from neighbors.</p> <p>Enabled: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
CDP Aware		<p>The CDP operation is restricted to decoding incoming CDP frames (The switch does not 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 neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded; CDP frames are not displayed in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.</p> <p>CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.</p> <p>CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but</p>

	<p>only the first address displays in the LLDP neighbors table.</p> <p>CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.</p> <p>CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.</p> <p>Both CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities display as "others" in the LLDP neighbors' table.</p> <p>If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch.</p>
	<p>NOTE: When CDP awareness on a port is disabled the CDP information is not 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

4.9.2 LLDP Neighbors

This page provides a status overview for all LLDP neighbors.

To display LLDP neighbors in the web interface:

1. Navigate to **Configuration > LLDP > LLDP Neighbors**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to update manually the current page.

Figure 61: LLDP Neighbor Information

LLDP Neighbour Information						
						Auto-refresh <input type="checkbox"/> Refresh
Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
No LLDP neighbour information found						



NOTE: If the switch has not discovered any LLDP devices the table display "No LLDP neighbor information found".

Parameter	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilities	<p>System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:</p> <ol style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-)</p>
Management Address	Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

4.9.3 LLDP-MED Configuration

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

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

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

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

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

This page enables configuring LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

To configure LLDP-MED via the web interface:

1. Click **Configuration > LLDP > LLDP-MED Configuration**.
2. Modify the parameters according to requirement.
3. Click **Add new policy**. After defining the new policy, apply it to the ports.
4. Click **Apply**.

Figure 62: LLDP-MED Configuration

LLDPMED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude degrees North ▼
Longitude degrees East ▼
Altitude Meters ▼
Map Datum WGS84 ▼

Civic Address Location

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

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
<input type="checkbox"/>	0	Voice ▼	Tagged ▼	200	0	0

Parameter	Description
Fast start repeat count	<p>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 insufficient knowledge of the network policy.</p> <p>With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order to share LLDP-MED information as fast as possible to new neighbors.</p> <p>Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.</p> <p>It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism are 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</p>
Coordinates Location	
Latitude	<p>Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.</p> <p>It is possible to specify the direction to either North of the equator or South of the equator.</p>
Longitude	<p>Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.</p> <p>It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.</p>
Altitude	<p>Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits.</p> <p>It is possible to select between two altitude types (floors or meters).</p> <p>Meters: Representing meters of Altitude defined by the vertical datum specified.</p> <p>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.</p>
Map Datum	<p>The Map Datum is used for the coordinates given in these options:</p> <p>WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327,</p>

	<p>Prime Meridian Name: Greenwich.</p> <p>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).</p> <p>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.</p>
<p>Civic Address location</p> <p>IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).</p>	
Country Code	The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
County	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City district	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Main Street.
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, ½
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: 27913.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.

Room no.	Room number - Example: 450F.
Place Type	Place type - Example: Office.
Postal community name	Postal community name - Example: Leonia.
P.O. Box	Post office box (P.O. BOX) - Example: 12345.
Additional Code	Additional code - Example: 1320300003.
Emergency Call Service	Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.
Emergency Call Service	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
<p>Policies</p> <p>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.</p> <p>Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.</p> <p>The network policy attributes advertised are:</p> <ol style="list-style-type: none"> 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) <p>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:</p> <ol style="list-style-type: none"> 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) <p>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.</p> <p>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</p>	
Delete	Check to delete the policy. It will be deleted during the next apply.

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 signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. 3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
Tag	<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 be one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP	DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.
Adding a new policy	Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy.
Port Policies Configuration	Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.
Port	The port number to which the configuration applies.
Policy ID	The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.

4.9.4 LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each port detecting LLDP neighbor. This function applies to VoIP devices which support LLDP-MED.

To display LLDP-MED neighbors in the web interface:

1. Click **Configuration > LLDP > LLDP-MED Neighbors**.
2. Click **Auto-refresh** to refresh the page automatically at periodic intervals
3. Click **Refresh** to refresh the page manually.

Figure 63: LLDP-MED Neighbors



NOTE: If there are no LLDP-MED devices in the network, the table displays “No LLDP-MED neighbor information found”.

Parameter	Description
Port	The port on which the LLDP frame was received.
Device Type	<p>LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.</p> <p>LLDP-MED Network Connectivity Device Definition</p> <p>LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:</p> <ol style="list-style-type: none"> 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method
LLDP-MED Endpoint Device Definition	<p>LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.</p> <p>Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined below:</p> <p>Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support</p>

	all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).
LLDP-MED Generic Endpoint (Class I)	<p>The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.</p> <p>Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.</p>
LLDP-MED Media Endpoint (Class II)	<p>The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.</p> <p>Discovery services defined in this class include media-type-specific network layer policy discovery.</p>
LLDP-MED Communication Endpoint (Class III)	<p>The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.</p> <p>Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management..</p>
LLDP-MED Capabilities	<p>LLDP-MED Capabilities describe the neighbor unit's LLDP-MED capabilities. The possible capabilities are:</p> <ol style="list-style-type: none"> 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
Application Type	<p>Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.</p> <ol style="list-style-type: none"> 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances

	<p>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.</p> <p>2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.</p> <p>3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.</p> <p>4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.</p> <p>5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.</p> <p>6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</p> <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 - for use in network topologies that require a separate policy for the video signalling than for the video media.</p>
Policy	<p>Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. It can be either Defined or Unknown</p> <p>Unknown: The network policy for the specified application type is currently unknown.</p> <p>Defined: The network policy is defined.</p>
Tag	<p>TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. It can be either Tagged or Untagged.</p> <p>Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.</p> <p>Tagged: The device is using the IEEE 802.1Q tagged frame format.</p>
VLAN ID	<p>VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.</p>
Priority	<p>Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7) can be used.</p>
DSCP	<p>DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. It contains one of 64 code point values (0 through 63).</p>

4.9.5 EEE

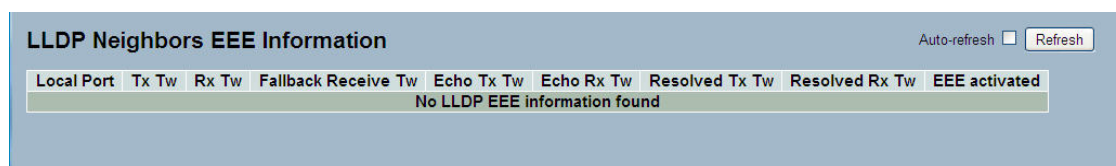
By using EEE, users achieve power savings at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange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

This page provides an overview of EEE information exchanged by LLDP.

To display LLDP EEE neighbors:

1. Click **LLDP > EEE**. The discovered EEE devices display.
2. Click **Refresh** for manual update web screen.
3. Click **Auto-refresh** for auto-update web screen.

Figure 64: LLDP Neighbors EEE Information



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



NOTE: If the network has no devices enabled EEE function, then the table displays "No LLDP EEE information found".

Parameter	Description
Local Port	The port for receiving or transmitting LLDP frames.
Tx Tw	The link partner's maximum time that transmit path can holdoff sending data after deassertion of LPI.
Rx Tw	The link partner's time that receiver would like the transmitter to holdoff to allow time for the receiver to wake from sleep.
Fallback Receive Tw	<p>The link partner's fallback receive Tw.</p> <p>A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.</p>
Echo Tx Tw	<p>The link partner's Echo Tx Tw value.</p> <p>The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner it can determine whether or not the remote link partner has received, registered and processed its most recent</p>



	values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.
Echo Rx Tw	The link partner's Echo Rx Tw value..
Resolved Tx Tw	The resolved Tx Tw for this link. Note : NOT the link parther The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
Resolved Rx Tw	The resolved Rx Tw for this link. Note : NOT the link parther The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).
Auto-refresh	To evoke the auto-refresh icon then the device will refresh the information automatically.
Upper right icon (Refresh)	Click refresh the LLDP Neighbours information manually.

4.9.6 Port Statistics

Two types of counters display. Global counters are counters that refer to the whole switch, while local counters refer to per port counters.

To display LLDP Statistics in the web interface:

1. Click **Configuration > LLDP > Port Statistics**.
2. Click **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.
4. Click **Clear** to clear all counters.

Figure 65: LLDP Port Statistics Information

Global Counters					Auto-refresh <input type="checkbox"/> Refresh Clear				
Neighbour entries were last changed at 2011-01-01 00:00:00 (4945 sec. ago)									
Total Neighbours Entries Added					0				
Total Neighbours Entries Deleted					0				
Total Neighbours Entries Dropped					0				
Total Neighbours 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	
9A	0	0	0	0	0	0	0	0	
10A	0	0	0	0	0	0	0	0	
9B	0	0	0	0	0	0	0	0	
10B	0	0	0	0	0	0	0	0	

Parameter	Description
Global Counters	
Neighbor entries were last changed	It displays the time when the last entry was deleted or added, and the time elapsed since the last change was detected.
Total Neighbor Entries Added	Displays the number of new entries added since switch reboot.
Total Neighbor Entries Deleted	Displays the number of new entries deleted since switch reboot.
Total Neighbor Entries Dropped	Displays the number of LLDP frames dropped due to the entry table being full.
Total Neighbor Entries Aged Out	Displays the number of entries deleted due to Time-To-Live expiring.
Local Counters	
The displayed table contains a row for each port.	



Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed and the Age-Out counter is incremented.

4.10 PoE

Use Power over Ethernet to transmit electrical power to remote devices over standard Ethernet cable. For example, use it for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to an external power supply.

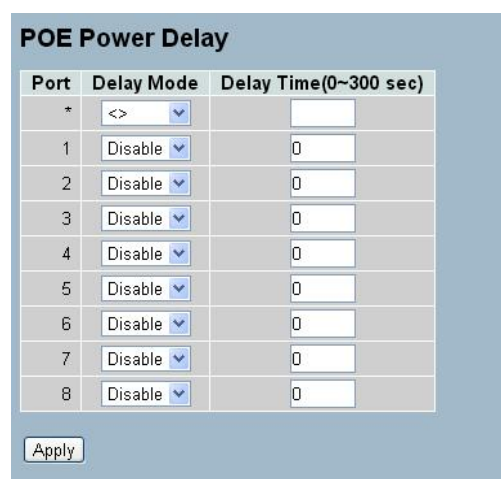
4.10.1 Configuration

This page enables the user to inspect and configure the current PoE port settings.

To configure Power over Ethernet via the web interface:

1. Navigate to **Configuration > PoE > Configuration**.
2. Enable/disable PoE mode for each port using the drop-down menu. Specify the priority and maximum power.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.


Figure 66: Power over Ethernet Configuration



Port	Delay Mode	Delay Time(0~300 sec)
*	<>	
1	Disable	0
2	Disable	0
3	Disable	0
4	Disable	0
5	Disable	0
6	Disable	0
7	Disable	0
8	Disable	0

Apply

Parameter	Description
Power Supply Configuration	
Primary Power Supply [W]	The switch can have PoE power supplies. It is used as power source. For being able to determine the amount of power the powered device may use, the amount of power the power sources can deliver must be defined.
Ethernet Port Configuration	
Port	This is the logical port number for this row.
PoE Mode	The PoE Mode represents the PoE operating mode for the port. Disabled: PoE disabled for the port. Enabled : Enables PoE IEEE 802.3af/at.
Priority	The Priority represents the port's priority. There are three levels of power priority - Low, High and Critical. The priority is used in the case where the remote devices require more power

	than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
Maximum Power 	It indicates the maximum power in watts that can be delivered to a remote device. NOTE: To set the Port support IEEE802.3at, then set the Maximum allowed value to 30W.

4.10.2 Status

This page enables the user to inspect the current status for all PoE ports. The section displays all ports' PoE Status.

To display PoE Status in the web interface:

1. Navigate to **Configuration > PoE > Status**.
2. Click **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Clicking **Refresh** manually refreshes the page.

Figure 67: Power over Ethernet Status

Power Over Ethernet Status Auto-refresh <input type="checkbox"/> Refresh							
Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8	0	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Parameter	Description
Local Port	This is the logical port number for this row.
PD Class	The PD class that the device attached port belongs to. The classification current describes the amount of power the PD will require during normal operation.
Power Requested	The Power Requested displays the requested amount of power the PD wants reserved.
Power Allocated	The Power Allocated displays the amount of power the switch has allocated for the PD.
Power Used	The Power Used displays the power the PD is currently using.
Current Used	The Current Used displays the current the PD is currently using.
Priority	The Priority displays the port's priority configured by the user (Allworx is typically 3 watts).
Port Status	The Port Status displays the port's status.

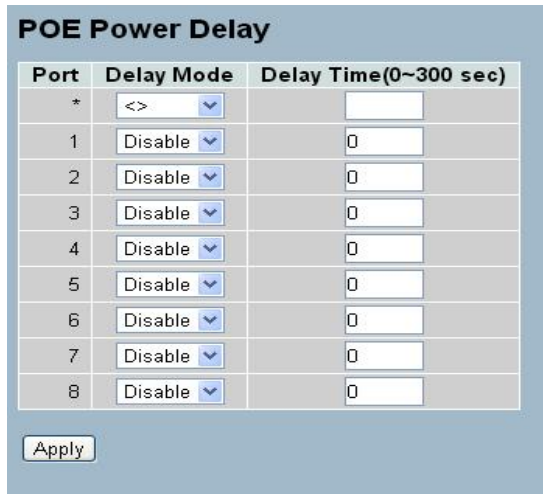
4.10.3 Power Delay

This page enables the user to set a time delay to provide power on a port after the rebooting the device.

To set the power delay via the web interface:

1. Navigate to **Configuration > PoE > Power Delay**.
2. Enable the Delay Mode and set the delay time.
3. Click **Apply**.

Figure 68: Power Delay



Port	Delay Mode	Delay Time(0~300 sec)
*	<>	
1	Disable	0
2	Disable	0
3	Disable	0
4	Disable	0
5	Disable	0
6	Disable	0
7	Disable	0
8	Disable	0

Apply

Parameter	Description
Port	Indicates the port number.
Delay Mode	To turn on/off the power delay function Enabled: Enable PoE power delay Disabled: Disable PoE power delay
Delay Time	Upon reboot, the PoE port with start providing power after waiting for the delay time to end. Value ranges from 0 – 300 sec.

4.10.4 Auto Checking

This page enables the user to set auto detect parameters to check the link status between the PoE port and the power device. If a fail connect is detected, the PD is rebooted automatically.

To configure Auto Checking via the web interface:

1. Navigate to **Configuration > PoE > Auto Checking**.
2. Specify the Auto Checking parameters for the ports.
3. Click **Apply**.

Figure 69: Auto Checking

POE Auto Checking

Ping Check Disable

Port	Ping IP Address	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
1	0.0.0.0	30	3	error=0 total=0	Nothing	15
2	0.0.0.0	30	3	error=0 total=0	Nothing	15
3	0.0.0.0	30	3	error=0 total=0	Nothing	15
4	0.0.0.0	30	3	error=0 total=0	Nothing	15
5	0.0.0.0	30	3	error=0 total=0	Nothing	15
6	0.0.0.0	30	3	error=0 total=0	Nothing	15
7	0.0.0.0	30	3	error=0 total=0	Nothing	15
8	0.0.0.0	30	3	error=0 total=0	Nothing	15

Apply

Parameter	Description
Ping Check	When enabled, the function detects the connection between the PoE port and the PD connected.
Port	Indicates the switch port number.
Ping IP Address	The PD's IP address to ping.
Interval Time	Time intervals at which switch sends a message to the PD. Range is 10 – 120 sec.
Retry Time	When the port is unable to ping the PD, it will retry again. After 3 failed attempts, it will trigger failure action. Range is 1-5.
Failure Log	Failure counter.
Failure Action	Nothing: Port continues to ping PD but no action is taken. Reboot Remote PD: Turn off PoE port power causing PD to reboot.

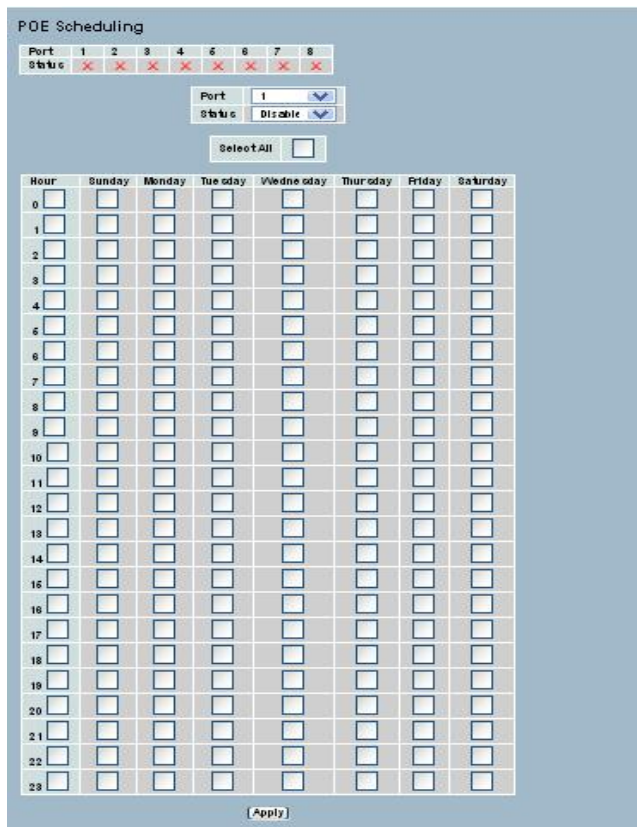
4.10.5 Scheduling

PoE scheduling enables the user to select what time of the day and week a PoE port would provide power to a connected power device.

To configure the PoE scheduling via the web interface:

1. Navigate to **Configuration > PoE > Scheduling**.
2. Enable PoE scheduling for desired ports.
3. Specify the days of the week and hours of the day to enable PoE.
4. Click Apply.

Figure 70: PoE Scheduling



PoE Scheduling

Port	1	2	3	4	5	6	7	8
Status	✗	✗	✗	✗	✗	✗	✗	✗

Port: Status: Select All: ☐

Hour	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0	<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"/>
2	<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"/>
4	<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"/>
6	<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"/>
8	<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"/>
10	<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"/>
12	<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"/>
14	<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"/>
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Apply]

Parameter	Description
Port	Indicates the switch port number.
Status	PoE Scheduling status Enabled: Enable PoE scheduling Disabled: Disable PoE scheduling
Hour	Time of the day to provide PoE on the selected port.

4.10.6 Filtering Database

Filtering Data Base Configuration gathers many functions, including MAC Table Information, Static MAC Learning, etc.

MAC table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for determining which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The network administrator configures the static entries, if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which displays the MAC address of the equipment sending the frame, and uses the SMAC address by the switch to automatically update the MAC table with these dynamic MAC addresses. The MAC table removes dynamic entries after not seeing the frame with the corresponding SMAC address after a configurable age time.

4.10.7 Configuration

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

To configure MAC Address Table via the web interface:

1. Navigate to **Configuration > Filtering Database > Configuration**.
2. Check the Disable Automatic Aging checkbox to disable the feature.
3. Specify the Aging Time.
4. Click **Apply**.

MAC Table Learning

1. Use the radio buttons to set the port members to Auto, Disable, or Secure.
2. Click **Apply**.

Static MAC Table Configuration

1. Click **Add new Static entry**.
2. Specify the VLAN ID, MAC address and select the port members.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 71: MAC Address Table Configuration

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging ☐

Aging Time seconds

MAC Table Learning

	Port Members											
	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<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"/>
Secure	<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"/>


Static MAC Table Configuration

	Port Members													
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Delete	<input type="text" value="1"/>	<input type="text" value="00-00-00-00-00-00"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Static MAC Table Configuration

	Port Members													
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9A	10A	9B	10B
Delete	<input type="text" value="1"/>	<input type="text" value="00-00-00-00-00-00"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Parameter	Description
Aging Configuration	<p>By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is called aging.</p> <p>Configure aging time by entering a value in seconds. The range is 10 to 1000000 seconds.</p> <p>Disable the automatic aging of dynamic entries by checking <input checked="" type="checkbox"/> Disable Automatic Aging.</p>
MAC Table Learning	<p>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:</p>
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped.

	<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>
<p>Static MAC Table Configuration</p> <p>The static MAC table can contain upto 64 entries. The maximum of 64 entries is for the whole stack, and not per switch.</p> <p>The MAC table is sorted first by VLAN ID and then by MAC address.</p>	
Delete	Check to delete the entry. It will be deleted during the next apply.
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.
Adding a New Static Entry	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click Apply.

4.10.8 Dynamic MAC Table

This page displays entries in the MAC Table. The MAC Table contains up to 8192 entries and sorts first by VLAN ID, and then by MAC address.

To display MAC Address Table in the web interface:

Navigate to **Configuration > Filtering Database > Dynamic MAC Table**.

Figure 72: Dynamic MAC Address Table Information

MAC Address Table			Auto-refresh <input type="checkbox"/> Refresh Clear << >>															
Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.																		
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9A	10A	9B	10B			
Static	200	00-0A-DD-04-00-14	✓															
Dynamic	200	00-14-22-C5-6C-56	✓	✓														
Static	200	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	200	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	200	33-33-FF-04-00-14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	200	33-33-FF-A8-01-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameter	Description
Type	Indicates whether the entry is a static or dynamic entry.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	The ports that are members of the entry.

4.11 VLAN

Use the management VLAN to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 200, but users can designate any VLAN as the management VLAN using the Management VLAN window. Only one management VLAN can be active at a time.

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

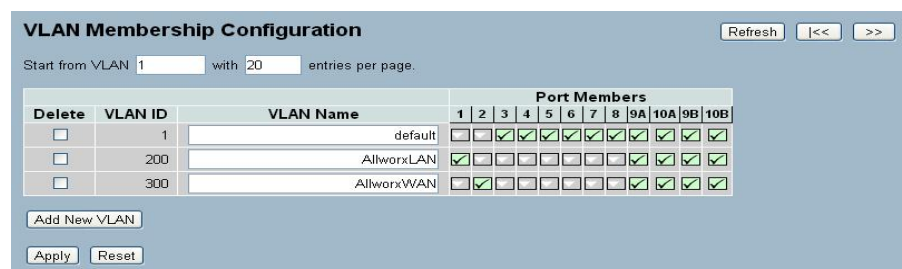
4.11.1 VLAN Membership

Users can monitor and modify the VLAN membership configuration for the selected stack switch unit, which supports up to 4096 VLANs. This page enables for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

To configure VLAN membership configuration via the web interface:

1. Navigate to **Configuration > VLAN > VLAN Membership**.
2. Click **Add New VLAN** to add a new VLAN. Modify the VLAN ID and name. Add or remove ports by selecting the port members.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 73: VLAN Membership Configuration



VLAN Membership Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members																							
			1	2	3	4	5	6	7	8	9A	10A	9B	10B												
<input type="checkbox"/>	1	default	<input type="checkbox"/>	<input 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 type="checkbox"/>	200	AllworxLAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>												
<input type="checkbox"/>	300	AllworxWAN	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>												

Add New VLAN

Apply Reset

Parameter	Description
Delete	To delete a VLAN entry, check this box. The entry will be deleted on the selected switch in the stack. If none of the ports of this switch are members of a VLAN then the delete checkbox is greyed out (unable to delete the entry during the next Apply).
VLAN ID	Indicates the ID of this particular VLAN.
VLAN Name	Indicates the name of the VLAN. VLAN Name can only contain alphabets or numbers. VLAN name should contain atleast one alphabet.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box. To remove or exclude the port from the VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding New VLAN	<p>Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.</p> <p>Enables the VLAN on the selected stack switch unit when clicking on Apply. The VLAN is thereafter present on the other stack switch units, but with no port members. The check box is greyed out when VLAN is displayed on other stacked switches, but user can add member ports to it.</p>

A VLAN without any port members on any stack unit will be deleted when clicking **Apply**.

4.11.2 Ports

After adding ports to VLANs, modify the port-type, egress rules, and PVID settings in the VLAN port configuration page.

The function in VLAN Tag Rule Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can select ingress filtering rules to each port. There are two ingress filtering rules to apply to the switch. The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. The Ingress Filtering Rule 2 is “drop untagged frame”. Users can also select the Role of each port as Access, Trunk, or Hybrid.

To configure VLAN Port configuration via the web interface:

1. Navigate to **Configuration > VLAN > Ports**.
2. Specify the port parameters.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 74: VLAN Port Configuration


Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>	<input type="checkbox"/>	<>	<>	
1	C-port	<input type="checkbox"/>	All	Access	200
2	C-port	<input type="checkbox"/>	All	Access	300
3	Unaware	<input type="checkbox"/>	All	Hybrid	1
4	Unaware	<input type="checkbox"/>	All	Hybrid	1
5	Unaware	<input type="checkbox"/>	All	Hybrid	1
6	Unaware	<input type="checkbox"/>	All	Hybrid	1
7	Unaware	<input type="checkbox"/>	All	Hybrid	1
8	Unaware	<input type="checkbox"/>	All	Hybrid	1
9A	C-port	<input type="checkbox"/>	All	Trunk	1
10A	C-port	<input type="checkbox"/>	All	Trunk	1
9B	C-port	<input type="checkbox"/>	All	Trunk	1
10B	C-port	<input type="checkbox"/>	All	Trunk	1

Apply Reset

Parameter	Description
Ethertype for Custom S-ports	This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports. Custom EtherType enables the user to change the EtherType value on a port to any value to support network devices that do not use the standard 0x8100 EtherType field value on 802.1Q-tagged or 802.1p-tagged frames.
Port	Indicates the port number.
Port Type	Port can be one of the following types: Unaware, Customer port(C-port), Service

	<p>port(S-port), Custom Service port(S-custom-port)</p> <p>If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.</p>
Ingress Filtering	<p>Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled.</p>
Frame Type	<p>Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.</p>
Port VLAN ID 	<p>Configures the VLAN identifier for the port. The values are 1 through 4095. The default value is 1.</p> <p>NOTE: The port must be a member of the same VLAN as the Port VLAN ID.</p>

4.11.3 Switch Status

This page displays the status of all VLANs configured on the switch. The drop-down menu on the top of the page enables displaying only specific VLANs.

To display VLAN membership status in the web interface:

1. Navigate to **Configuration > VLAN > Switch Status**.
2. Select the view from the drop-down list.

Figure 75: VLAN Membership Status for Static User

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



Parameter	Description
VLAN USER (scroll to select one kind VLAN user as below:)	
VLAN User module uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configurations such as PVID and UVID. Currently we support the following VLAN user types:	
CLI/Web/SNMP : These are referred to as static.	
NAS : NAS provides port-based authentication, which involves communication between a Supplicant, Authenticator, and an Authentication Server.	
MVRP : Multiple VLAN Registration Protocol (MVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.	
GVRP : GARP VLAN Registration Protocol (GVRP) allows dynamic registration and deregistration of VLANs on ports on a VLAN bridged network.	
Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones.	
MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.	
MSTP : The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment	
VLAN ID	Indicates the ID of this particular VLAN.
VLAN Membership	The VLAN Membership Status Page displays the current VLAN port members for all VLANs configured by a selected VLAN User. When ALL VLAN Users are selected, it displays this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member.

4.11.4 Port Status

This page displays the VLAN status by port.

To display VLAN Port Status in the web interface:

1. Navigate to **Configuration > VLAN > Port Status**.
2. Select an option from the drop-down list.

Figure 76: VLAN Port Status for Static User

Port	PVID	Port Type	Ingress Filtering	Frame Type	Tx Tag	UVID	Conflicts
1	1	UnAware	Disabled	All	Untag This	1	No
2	1	UnAware	Disabled	All	Untag This	1	No
3	1	UnAware	Disabled	All	Untag This	1	No
4	1	UnAware	Disabled	All	Untag This	1	No
5	1	UnAware	Disabled	All	Untag This	1	No
6	1	UnAware	Disabled	All	Untag This	1	No
7	1	UnAware	Disabled	All	Untag This	1	No
8	1	UnAware	Disabled	All	Untag This	1	No
9A	1	UnAware	Disabled	All	Untag This	1	No
10A	1	UnAware	Disabled	All	Untag This	1	No
9B	1	UnAware	Disabled	All	Untag This	1	No
10B	1	UnAware	Disabled	All	Untag This	1	No

Parameter	Description
Port	The logical port for the settings contained in the same row.
PVID	Displays the VLAN identifier for that port. The values are 1 through 4095. The default value is 1.
Port Type	<p>Displays the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port.</p> <p>If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.</p>
Ingress Filtering	Displays the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.
Frame Type	Displays whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Tx Tag	Displays egress filtering frame status whether tagged or untagged.
UVID	Displays UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
Conflicts	<p>Displays conflicts that exist or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur:</p> <ul style="list-style-type: none"> • Functional Conflicts between features. • Conflicts due to hardware limitation. • Direct conflict between user modules.

4.11.5 Private VLANs

The private VLAN does not permit communication between ports in that private VLAN.

4.11.5.1 Private VLANs Membership Section

Monitor and modify the Private VLAN membership configurations for the switch, add or delete Private VLANs, and add or delete Port members of each Private VLAN on this page. 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.

To configure Private VLANs via the web interface:

1. Navigate to **VLANs > Private VLANs > Private VLAN Membership**.
2. Click **Add new Private VLAN**.
3. Specify the Private VLAN ID and Port Members
4. Click **Apply**.

Figure 77: Private VLAN Membership Configuration



Private VLAN Membership Configuration		Port Members															
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9A	10A	9B	10B				
<input type="checkbox"/>	1	<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"/>				

Add New Private VLAN

Apply Reset

Parameter	Description
Delete	To delete a private VLAN entry, check this box. The entry will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Private VLAN	Click to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed.

4.11.5.2 Port Isolation

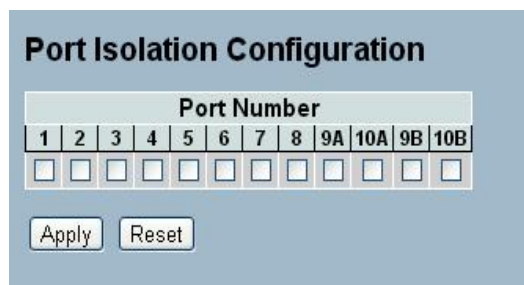
Port Isolation provides for an apparatus and method to isolate ports on layer 2 switches on the same VLAN to restrict traffic flow. The apparatus comprises a switch having said plurality of ports, each port configured as a protected port, or a non-protected port. An address table memory stores an address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

Use this page to 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.

To configure Port Isolation via the web interface:

1. Navigate to Configuration > **VLAN** > **Private VLANs** > **Port Isolation**.
2. Select the ports that have to be isolated.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 78: Port Isolation Configuration



Port Number															
1	2	3	4	5	6	7	8	9A	10A	9B	10B				
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Reset

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

4.11.6 MAC-based VLAN

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

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

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

4.11.6.1 Configuration

This page enables adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page displays only static entries.

To configure MAC address-based VLANs via the web interface:

1. Navigate to **Configuration > VLAN > MAC-based VLAN > Configuration**.
2. Click **Add new entry** and specify the MAC address and VLAN ID.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 79: MAC-based VLAN Membership Configuration

MAC-based VLAN Membership Configuration

Delete	MAC Address	VLAN ID	Port Members															
			1	2	3	4	5	6	7	8	9A	10A	9B	10B				
Currently no entries present																		

Add new entry **Apply** **Reset**

MAC-based VLAN Membership Configuration **Refresh** **<<** **>>**

Delete	MAC Address	VLAN ID	Port Members															
			1	2	3	4	5	6	7	8	9A	10A	9B	10B				
Delete	00-00-00-00-00-00	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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				

Add new entry **Apply** **Reset**

Parameter	Description
Delete	To delete a MAC-based VLAN entry, check this box and click apply. The entry will be deleted on the selected switch 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.
Add new entry	Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. Do not use broadcast or multicast MAC addresses. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled on the selected stack switch unit when clicking Apply . A MAC-based VLAN without any port members on any stack unit will be deleted when clicking Apply .

4.11.6.2 Status

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

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

To display MAC-based VLANs configured in the web interface:

1. Navigate to **Configuration > VLAN > MAC-based VLAN > Status**.
2. Specify the view: Static NAS Combined.

Figure 80: MAC-based VLAN Membership Status for User Static

Parameter	Description
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	Port members of the MAC-based VLAN entry.

4.11.7 Protocol -based VLAN

The switch supports Ethernet LLC and SNAP protocols.

LLC

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

SNAP

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

4.11.7.1 Protocol to Group

This page enables adding new protocols to Group Name (unique for each Group) mapping entries as well as enables seeing and deleting already mapped entries for the selected stack switch/unit switch.

To configure Protocol -based VLANs via the web interface:

1. Navigate to **Configuration > VLAN > Protocol -based VLAN**.
2. Click **Add new entry** and specify the frame type and group name.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 81: Protocol to Group Mapping Table

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Add new entry



Apply Reset

Protocol to Group Mapping Table Refresh

Delete	Frame Type	Value	Group Name
Delete	Ethernet	Etype: 0x0800	

Add new entry

Apply Reset

Parameter	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 Apply.
Frame Type	<p>Frame Type can have one of the following values:</p> <ol style="list-style-type: none"> 1. Ethernet 2. LLC 3. SNAP 0. <p> NOTE: On changing the Frame type field, valid value of the following text field varies depending on the new frame type 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 are the criteria for the 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> <ol 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> <ol 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 ranging 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 which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).</p> <p> NOTE: Do not use special characters or underscore (_)in Group Name field.</p>
Add new entry	Click to add a new entry in mapping table. An empty row is added to the table; configure the Frame Type, Value, and the Group Name as needed.

4.11.7.2 Group to VLAN

This section enables mapping an already configured Group Name to a VLAN for the selected stack switch unit.

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

1. Navigate to **Configuration > VLAN > Protocol-based VLAN > Group to VLAN**.
2. Click **Add new entry** and specify the Group Name and VLAN ID. Select the ports.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 82: Group Name to VLAN Mapping Table

Parameter	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 Apply.
Group Name	A valid Group Name is a string of 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). Do not use special characters. The Group name to map to a VLAN must be present in Protocol to Group mapping table and must not be reused by other existing mapping entry on this page.
VLAN ID	Indicates the ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Add new entry	Click to add a new entry in mapping table. An empty row is added to the table. The Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095.

4.12 Voice VLAN

Voice VLAN is a 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 traffic, ensuring the transmission priority of voice traffic and voice quality.

4.12.1 Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, so that the switch can classify and schedule network traffic. Allworx recommends that there are two VLANs on a port - one for voice, one for data.

To configure Voice VLAN via the web interface:

1. Navigate to **Configuration > Voice VLAN > Configuration**.
2. Enable the Voice VLAN mode.
3. Specify the VLAN ID, Aging Time, and Traffic Class.
4. Specify Port Mode, Security, and Discovery Protocol for each port in the Port Configuration section.
5. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.


Figure 83: Voice VLAN Configuration

Voice VLAN Configuration

Mode	Enabled
VLAN ID	200
Aging Time	86400 seconds
Traffic Class	7 (High)

Port Configuration

Port	Mode	Security	Discovery Protocol
*	Forced	<>	LLDP
1	Forced	Disabled	LLDP
2	Forced	Disabled	LLDP
3	Forced	Disabled	LLDP
4	Forced	Disabled	LLDP
5	Forced	Disabled	LLDP
6	Forced	Disabled	LLDP
7	Forced	Disabled	LLDP
8	Forced	Disabled	LLDP
9A	Disabled	Disabled	LLDP
10A	Disabled	Disabled	LLDP
9B	Disabled	Disabled	LLDP
10B	Disabled	Disabled	LLDP

Parameter	Description
Mode	<p>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:</p> <p>Enabled: Enable Voice VLAN mode operation.</p> <p>Disabled: Disable Voice VLAN mode operation.</p>
VLAN ID	<p>Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system. The range is 1 to 4095.</p>
Aging Time	<p>Indicates the Voice VLAN secure learning aging time. The 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 in the [age_time; 2 * age_time] interval.</p>
Traffic Class	<p>Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will belong to this class.</p>
Port Mode	<p>Indicates the Voice VLAN port mode.</p> <p>When the port mode is not equal disabled, we must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.</p> <p>Possible port modes are:</p> <p>Disabled: Disjoin from Voice VLAN.</p> <p>Auto: Enable auto detect mode. It detects whether there is a VoIP phone attached to the specific port and configures the Voice VLAN members automatically.</p> <p>Forced: Force join to Voice VLAN.</p>
Port Security	<p>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:</p> <p>Enabled: Enable Voice VLAN security mode operation.</p> <p>Disabled: Disable Voice VLAN security mode operation.</p>
Port Discovery Protocol	<p>Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. Enable the 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:</p> <p>OUI: Detect telephony device by OUI address.</p> <p>LLDP: Detect telephony device by LLDP.</p> <p>Both: Both OUI and LLDP</p>
	<p>Note: If using is a phone model 9224 handset, do the following steps:</p> <p>Connect the phone to the switch. The phone fails to boot up.</p> <p>Press the button below the <i>Config</i> softkey and navigate to Network Settings. Select the option by pressing the ✓ key.</p>

	<p>Set the VLAN mode to <i>Enabled</i> and navigate down to the Phone VLAN settings. Set the phone VLAN to 200 and press EXIT. Select YES when prompted to save configuration.</p> <p>Reboot the phone. The phone will now boot successfully and load new firmware. Select YES to load firmware to flash.</p> <p>Once the phone boots up select CONFIG and navigate down to Set Factory Defaults. Select YES to save configuration changes. The phone will reboot and now will have the default VLAN mode set to Auto Config (desired setting).</p>
--	---

4.12.2 OUI

This section describes how to configure Voice VLAN OUI table. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.

To configure Voice VLAN OUI Table via the web interface:

1. Navigate to **Configuration > Voice VLAN > OUI**.
2. Specify Telephony OUI and Description.
3. Click **Apply**.

Figure 84: 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

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next apply.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The description of the OUI address. Normally, it describes which vendor telephony device it belongs to. The string length is 0 to 32.
Add New entry	Click to add a new entry in Voice VLAN OUI table. An empty row is added to the table and the Telephony OUI and Description can be set.

4.13 GARP

The Generic Attribute Registration Protocol (GARP) provides a generic framework whereby devices in a bridged LAN, e.g. end stations and switches, can register and de-register attribute values, such as VLAN Identifiers, with each other. In doing so, the attributes propagate to devices in the bridged LAN, and these devices form a reachability tree that is a subset of an active topology. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

A GARP participation in a switch or an end station consists of a GARP application component and a GARP Information Declaration (GID) component associated with each port on the switch. The GARP Information Propagation (GIP) component carries out the propagation of information between GARP participants for the same application in a bridge. Protocol exchanges take place between GARP participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP application concerned.

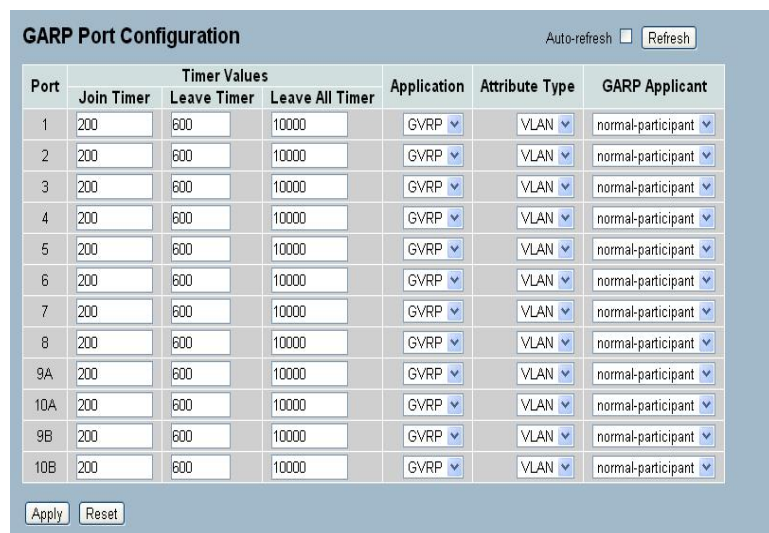
4.13.1 Configuration

This page enables configuring the basic GARP settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

To configure GARP Port Configuration via the web interface:

1. Navigate to **Configuration > GARP > Configuration**.
2. Specify GARP parameters for all the ports.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 85: GARP Port Configuration



Port	Timer Values			Application	Attribute Type	GARP Applicant
	Join Timer	Leave Timer	Leave All Timer			
1	200	600	10000	GVRP	VLAN	normal-participant
2	200	600	10000	GVRP	VLAN	normal-participant
3	200	600	10000	GVRP	VLAN	normal-participant
4	200	600	10000	GVRP	VLAN	normal-participant
5	200	600	10000	GVRP	VLAN	normal-participant
6	200	600	10000	GVRP	VLAN	normal-participant
7	200	600	10000	GVRP	VLAN	normal-participant
8	200	600	10000	GVRP	VLAN	normal-participant
9A	200	600	10000	GVRP	VLAN	normal-participant
10A	200	600	10000	GVRP	VLAN	normal-participant
9B	200	600	10000	GVRP	VLAN	normal-participant
10B	200	600	10000	GVRP	VLAN	normal-participant

Apply Reset

Parameter	Description
Port	<p>The Port column displays the list of ports on the switch. There are 4 settings which can be configured on a per port basis.</p> <ul style="list-style-type: none"> • Timer Values • Application • Attribute Type • GARP Applicant
Timer Values	<p>To set the GARP join timer, leave timer and leave all timers in micro-seconds. Three different timers can be configured on this page:</p> <p>Join Timer :The default value for Join timer is 200ms.</p> <p>Leave Timer : The range of values for Leave Time is 600-1000ms. The default value for Leave Timer is 600ms.</p> <p>Leave All Timer : The default value for Leave All Timer is 10000ms</p>
Application	Currently only supported application is GVRP.
Attribute Type	Currently only supported Attribute Type is VLAN.
GARP Applicant	<p>This configuration is used to configure the Applicant state machine behaviour for GARP on a particular port locally.</p> <ul style="list-style-type: none"> • Normal-participant: In this mode the Applicant state machine will operate normally in GARP protocol exchanges. • Non-participant: In this mode the Applicant state machine will not participate in the protocol operation. <p>The default configuration is normal participant</p>

4.13.2 Statistics

This section displays the GARP port statistics for all ports. The port statistics relate to the currently selected stack unit, as reflected by the page header.

To display GARP Port statistics in the web interface:

1. Navigate to **Configuration > GARP > Statistics**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 86: GARP Port Statistics



Port	Peer MAC	Failed Count
1	--	--
2	--	--
3	--	--
4	--	--
5	--	--
6	--	--
7	--	--
8	--	--
9A	--	--
10A	--	--
9B	--	--
10B	--	--

Parameter	Description
Port	The Port column displays the list of all ports for which per port GARP statistics are shown.
Peer MAC	Peer MAC is MAC address of the neighbor Switch from which the GARP frame is received.
Failed Count	Number of GARP Join packets received by the switch that failed to join a VLAN.
Attribute Type	Currently only supported Attribute Type is VLAN.
GARP Applicant	<p>This configuration is used to configure the Applicant state machine behaviour for GARP on a particular port locally.</p> <ul style="list-style-type: none"> Normal-participant: In this mode the Applicant state machine will operate normally in GARP protocol exchanges. Non-participant: In this mode the Applicant state machine will not participate in the protocol operation. <p>The default configuration is normal participant</p>

4.14 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to maintain the group membership information of the VLANs automatically and dynamically. GVRP provides the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with the attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintains the contents of Dynamic VLAN Registration Entries for each VLAN and propagate the information to other GVRP-aware devices to setup and update the knowledge database, the set of VLANs associated with current, active members, and the ports to reach these members.

4.14.1 Configuration

This page enables configuring the basic GVRP settings for all switch ports. The settings relate to the currently selected stack unit, as reflected by the page header.

To configure GVRP Port settings via the web interface:

1. Navigate to **Configuration > GVRP > Configuration**.
2. Specify the GVRP mode and port Parameters.
3. Click **Apply**.

Figure 87: GVRP Global Configuration

Global Configuration

GVRP Mode Disable ▾

Port Configuration

Port	GVRP Mode	GVRP rrole
1	Disable ▾	Disable ▾
2	Disable ▾	Disable ▾
3	Disable ▾	Disable ▾
4	Disable ▾	Disable ▾
5	Disable ▾	Disable ▾
6	Disable ▾	Disable ▾
7	Disable ▾	Disable ▾
8	Disable ▾	Disable ▾
9A	Disable ▾	Disable ▾
10A	Disable ▾	Disable ▾
9B	Disable ▾	Disable ▾
10B	Disable ▾	Disable ▾

Apply Reset

Parameter	Description
GVRP Mode	<p>GVRP Mode is a global setting. Select Enable to enable the GVRP globally. In a stack, this configuration command sends message to all the slaves connected in stack.</p> <p>Default value of Global GVRP Mode is 'Disable'</p>
Port	<p>The Port column displays the list of configurable ports per port GVRP settings. There are 2 configuration settings to configure on per port bases.</p> <ul style="list-style-type: none"> GVRP Mode GVRP role <p>GVRP Mode</p> <p>This configuration is to enable/disable GVRP Mode on a particular port locally.</p> <ul style="list-style-type: none"> Disable: Select to Disable GVRP mode on this port. Enable: Select to Enable GVRP mode on this port. <p>The default value is 'disable'.</p> <p>GVRP role</p> <p>This configuration is used to configure restricted role on an interface.</p> <ul style="list-style-type: none"> Disable: Select to Disable GVRP role on this port. Enable: Select to Enable GVRP role on this port. <p>The default configuration is 'disable'</p>

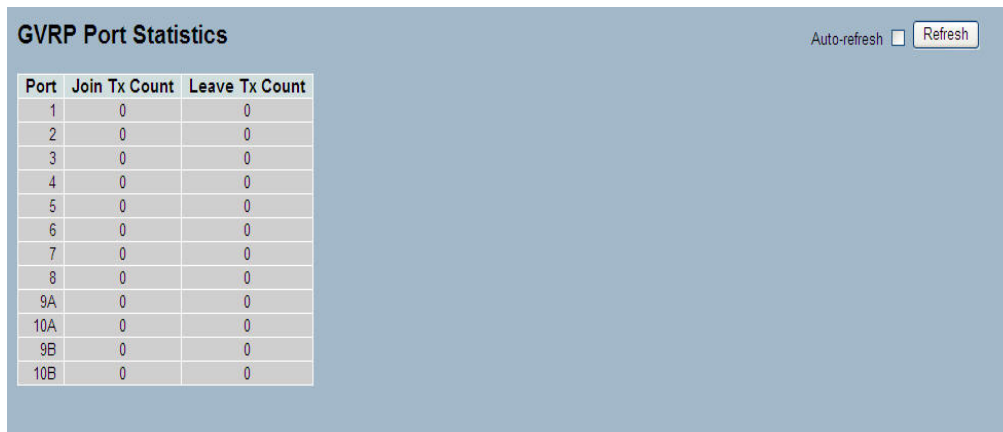
4.14.2 Statistics

This section displays the GVRP Port statistics for all switch ports.

To display GVRP Port statistics in the web interface:

1. Navigate to **Configuration > GVRP > Statistics**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 88: GVRP Port Statistics



Port	Join Tx Count	Leave Tx Count
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9A	0	0
10A	0	0
9B	0	0
10B	0	0

Parameter	Description
Port	The Port coulmn displays the list of ports to see port counters and statistics.
Join Tx Count	Number of GVRP Join packets sent by the switch
Leave Tx Count	Number of GVRP Leave packets sent by the switch

4.15 QoS

The switch supports four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

The switch offers high flexibility in the classification of incoming frames to a QoS class. The QoS classification looks for information up to Layer 4, including IPv4 and IPv6 DSCP, IPv4 TCP/UDP port numbers, and user priority of tagged frames. The QoS control list (QCL) implements the QoS classification mechanism. The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific QoS class.

The switch also supports advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frame. The ingress super priority queue allows traffic recognized as CPU traffic to be received and queued for transmission to the CPU even when all the QoS class queues are congested.

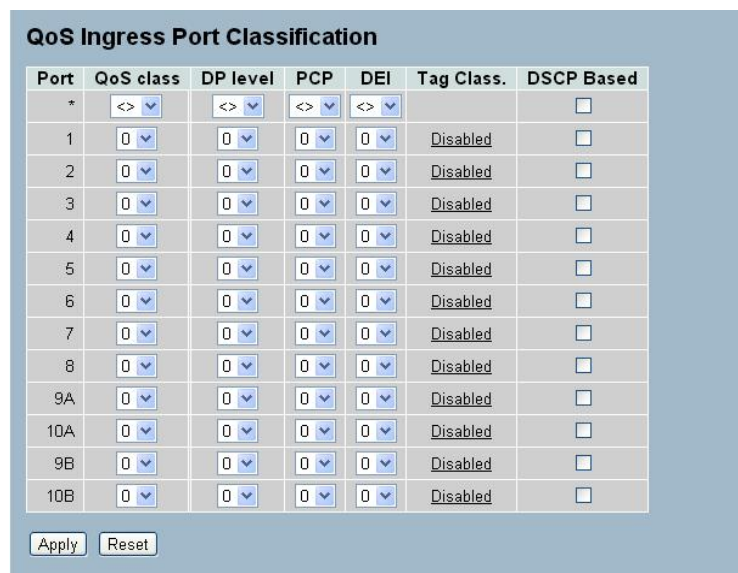
4.15.1 Port Classification

The section enables configuring the basic QoS Ingress Classification settings for all switch ports.

To configure the QoS Port Classification parameters via the web interface:

1. Navigate to **Configuration > QoS > Port Classification**.
2. Use the drop-down menu to set the various port parameters.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 89: QoS Configuration



Port	QoS class	DP level	PCP	DEI	Tag Class	DSCP Based
*	<>	<>	<>	<>		<input type="checkbox"/>
1	0	0	0	0	Disabled	<input type="checkbox"/>
2	0	0	0	0	Disabled	<input type="checkbox"/>
3	0	0	0	0	Disabled	<input type="checkbox"/>
4	0	0	0	0	Disabled	<input type="checkbox"/>
5	0	0	0	0	Disabled	<input type="checkbox"/>
6	0	0	0	0	Disabled	<input type="checkbox"/>
7	0	0	0	0	Disabled	<input type="checkbox"/>
8	0	0	0	0	Disabled	<input type="checkbox"/>
9A	0	0	0	0	Disabled	<input type="checkbox"/>
10A	0	0	0	0	Disabled	<input type="checkbox"/>
9B	0	0	0	0	Disabled	<input type="checkbox"/>
10B	0	0	0	0	Disabled	<input type="checkbox"/>

Apply Reset

Parameter	Description
Port	The port number for which the configuration applies.
QoS class	Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.
DP level	Controls the default Drop Precedence level, i.e., the DP level for frames not classified in any other way.
PCP	Controls the default PCP for untagged frames.
DEI	Controls the default DEI for untagged frames.
Tag Class	Displays the classification mode for tagged frames on this port. Disabled: Use default QoS class and DP level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping.
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.

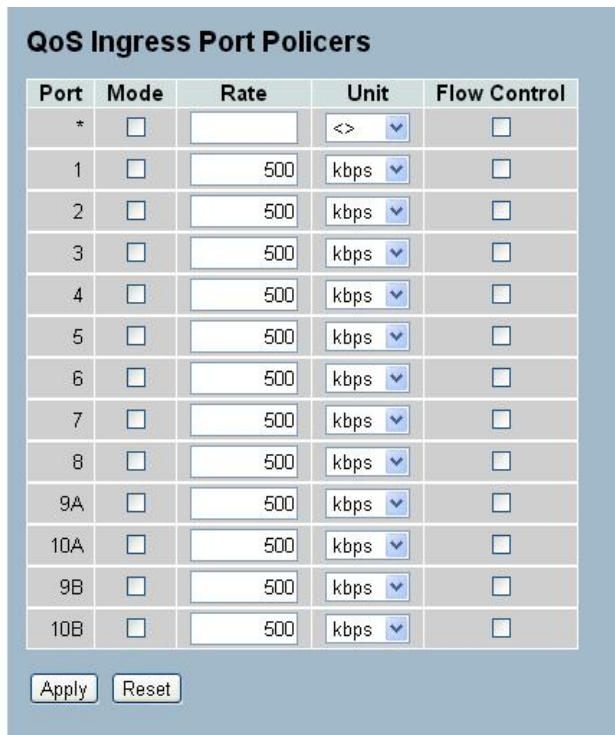
4.15.2 Port Policing

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

To configure the QoS Port Policing via the web interface:

1. Navigate to **Configuration > QoS > Port Policing**.
2. Check the Mode checkbox to enable policing on a port. Set the rate in kbps, Mbps, fps, or kfps.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 90: QoS Ingress Port Policing Configuration



Port	Mode	Rate	Unit	Flow Control
*	<input type="checkbox"/>		<>	<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"/>
9A	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
10A	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
9B	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
10B	<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

Apply Reset

Parameter	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Check/uncheck to enable/disable port policing for the port.
Rate	To set the Rate limit value for this port, the default is 500.
Unit	Scroll to select the unit of rate - includes kbps, Mbps, fps and kfps. The default is kbps.

4.15.3 Port Schedulers

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

To configure the QoS Port Schedulers via the web interface:

1. Navigate to **Configuration > QoS > Port Schedulers**.
2. Click on the port number to set the parameters for the port.

Figure 91: QoS Egress Port Schedules

QoS Egress Port Schedulers

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

Click the Port index to set the QoS Egress Port Schedulers

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Enable	Rate	Unit	Excess
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>

STRICT

Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps

Apply Reset Cancel

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

Enable	Rate	Unit	Excess
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input checked="" type="checkbox"/>	500	kbps	<input type="checkbox"/>

Weight	Percent
17	17%
17	17%
17	17%
17	17%
17	17%
17	17%
17	17%

DRR

STRICT

Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps

Apply Reset Cancel

If selecting weighted mode, the parameters have to be set accordingly



Parameter	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Mode	Displays the scheduling mode for this port.
Weight (Qn)	Displays the weight for this queue and port.
Scheduler Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this 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 1-1000 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 allowing the queue 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	Displays 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 1-1000 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".

4.15.4 Port Shaping

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

To configure the QoS Port Shapers via the web interface:

1. Navigate to **Configuration > QoS > Port Shaping**.
2. Click on the port number to set the parameters for that port.

Figure 92: QoS Egress Port Shaper

Click the Port index to set the QoS Egress Port Shapers

Port	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9A	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10A	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9B	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10B	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Strict Priority

Queue Shaper

Enable	Rate	Unit	Excess
Q0	500	kbps	
Q1	500	kbps	
Q2	500	kbps	
Q3	500	kbps	
Q4	500	kbps	
Q5	500	kbps	
Q6	500	kbps	
Q7	500	kbps	

Port Shaper

Enable	Rate	Unit
	500	kbps

Apply Reset Cancel

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: Weighted

Queue Shaper

Enable	Rate	Unit	Excess
Q0	500	kbps	
Q1	500	kbps	
Q2	500	kbps	
Q3	500	kbps	
Q4	500	kbps	
Q5	500	kbps	
Q6	500	kbps	
Q7	500	kbps	

Queue Scheduler

Weight	Percent
17	17%
17	17%
17	17%
17	17%
17	17%
17	17%
17	17%

Port Shaper

Enable	Rate	Unit
	500	kbps

Apply Reset Cancel

If selecting weighted mode, the parameters have to be set accordingly

Parameter	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Shapers (Qn)	ShoDisplaysws "disabled" or actual queue shaper rate - e.g. "800 Mbps".
Shapers (Port)	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".
Scheduler Mode	Controls whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port.
Queue Shaper Enable	Controls whether the queue shaper is enabled for this queue on this 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 1-1000 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 allowing the queue 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 1-1000 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".

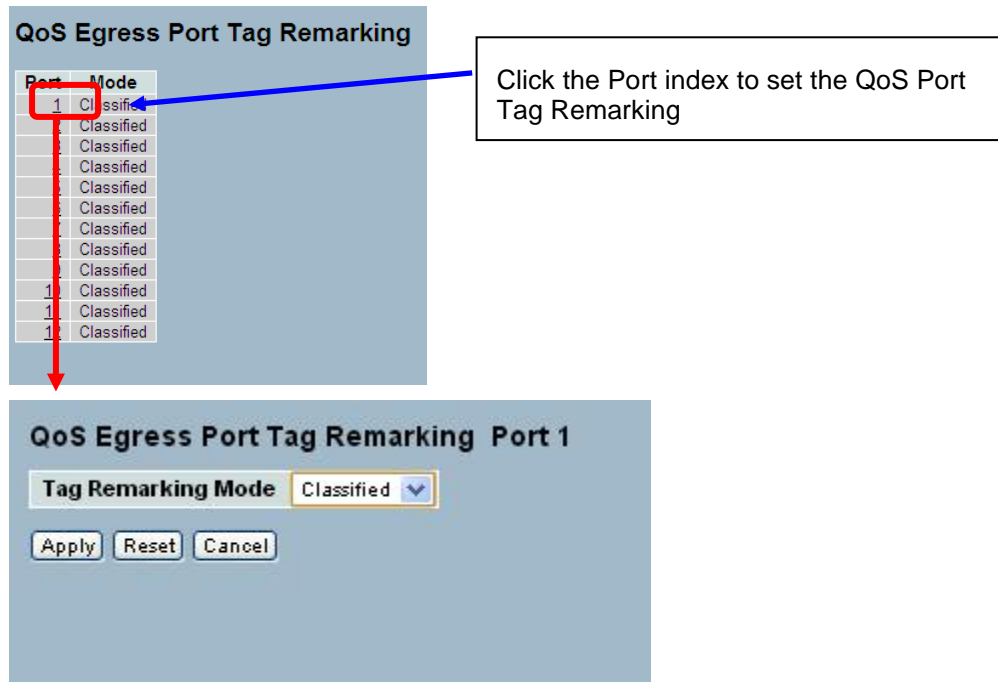
4.15.5 Port Tag Remarking

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

To configure the QoS Port Tag Remarking via the web interface:

1. Navigate to **Configuration > QoS > Port Tag Remarking**.
2. Click on the port number to set parameters for that port.

Figure 93: Port Tab Remarking



Parameter	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Tag Remarking Mode	<p>Scroll to select the tag remarking mode for this port.</p> <p>Classified: Use classified PCP/DEI values.</p> <p>Default: Use default PCP/DEI values.</p> <p>Mapped: Use mapped versions of QoS class and DP level.</p>

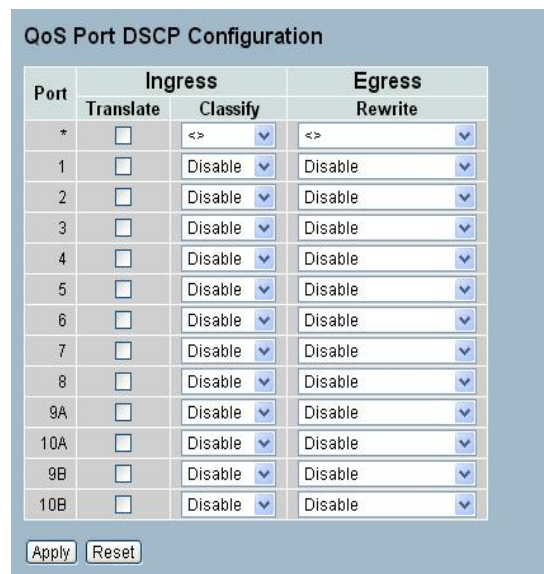
4.15.6 Port DSCP

This section describes how to set the QoS Port DSCP configuration.

To configure the QoS Port DSCP parameters via the web interface:

1. Navigate to **Configuration > QoS > Port DSCP**.
2. Check the Translate checkbox to enable the Ingress Translate and enable/disable the Classify and Egress Rewrite parameters using the drop-down menu.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 94: QoS Port DSCP Configuration



Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<>	<>
1	<input type="checkbox"/>	Disable	Disable
2	<input type="checkbox"/>	Disable	Disable
3	<input type="checkbox"/>	Disable	Disable
4	<input type="checkbox"/>	Disable	Disable
5	<input type="checkbox"/>	Disable	Disable
6	<input type="checkbox"/>	Disable	Disable
7	<input type="checkbox"/>	Disable	Disable
8	<input type="checkbox"/>	Disable	Disable
9A	<input type="checkbox"/>	Disable	Disable
10A	<input type="checkbox"/>	Disable	Disable
9B	<input type="checkbox"/>	Disable	Disable
10B	<input type="checkbox"/>	Disable	Disable

Apply Reset

Parameter	Description
Port	The Port column displays the list of ports to configure dscp ingress and egress settings.
Ingress	<p>Change the ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <p>Translate : To Enable the Ingress Translation</p> <p>Classify: Classification for a port has 4 different values</p> <ul style="list-style-type: none"> • Disable: No Ingress DSCP Classification. • DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. • Selected: Classify only selected DSCP to enable classification as specified in DSCP Translation window for the specific DSCP. • All: Classify all DSCP
Egress	<p>Port Egress Rewriting can be one of below parameters</p> <ul style="list-style-type: none"> • Disable: No Egress rewrite. • Enable: Rewrite enable without remapping. <p>Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.</p>

4.15.7 DSCP-Based QoS

This section describes how to configure the DSCP-Based QoS mode.

To configure the DSCP –Based QoS settings via the web interface:

1. Navigate to **Configuration > QoS > DSCP-Based QoS**.
2. Check the Trust checkbox to turn on DSCP Trust.
3. Use the drop-down menu to select the QoS Class and DPL parameters
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 95: DSCP-Based QoS Ingress Classification Configuration

DSCP-Based QoS Ingress Classification Auto-refresh ☐ [Refresh](#)

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

[Apply](#) [Reset](#)

Parameter	Description
DSCP	Maximum number of supported DSCP values is 64.
Trust	Click if the DSCP value is trusted.
QoS Class	QoS Class value can range from 0-7.
DPL	Drop Precedence Level (0-3)

4.15.8 DSCP Translation

This section describes how to the QoS DSCP Translation settings. Do the DSCP translation in Ingress or Egress.

To configure the DSCP Translation parameters via the web interface:

1. Navigate to **Configuration > QoS > DSCP Translation**
2. Use the drop-down menu to set the Ingress Translate and Egress Remap parameters.
3. Check the Classify checkbox to enable DSCP classification.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 96: DSCP Translation Configuration

Parameter	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges is 0 to 63.
Ingress	<p>Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map.</p> <p>There are two configuration parameters for DSCP Translation –</p> <ul style="list-style-type: none"> • Translate: DSCP at Ingress side translates to any of (0-63) DSCP values. • Classify : Click to enable Classification at Ingress side
Egress	<p>Configurable parameters for Egress side –</p> <ul style="list-style-type: none"> • Remap DP0: Select the DSCP value from select menu to remap. DSCP value ranges from 0 to 63 • Remap DP1: Select the DSCP value from select menu to remap. DSCP value ranges from 0 to 63. • Remap: Select the DSCP value from the menu to remap. DSCP values range from 0 to 63

4.15.9 DSCP Classification

This section describes to teach user to configure DSCP classification. It enables mapping DSCP value to a QoS Class and DPL value.

To configure the DSCP Classification parameters via the web interface:

1. Navigate to **Configuration > QoS > DSCP Classification**.
2. Use the drop-down menu to select the DSCP classification values.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 97: DSCP Classification Configuration

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Apply Reset

Parameter	Description
QoS Class	Available QoS Class values range from 0 to 7. QoS Class (0-7) can be mapped to a DSCP value .
DPL	Drop Precedence Level (0-1) can be configured for all available QoS Classes
DSCP	Select DSCP value (0-63) from DSCP menu to map to corresponding QoS Class and DPL value

4.15.10 QoS Control List Configuration

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

To configure the QoS Control List parameters via the web interface:


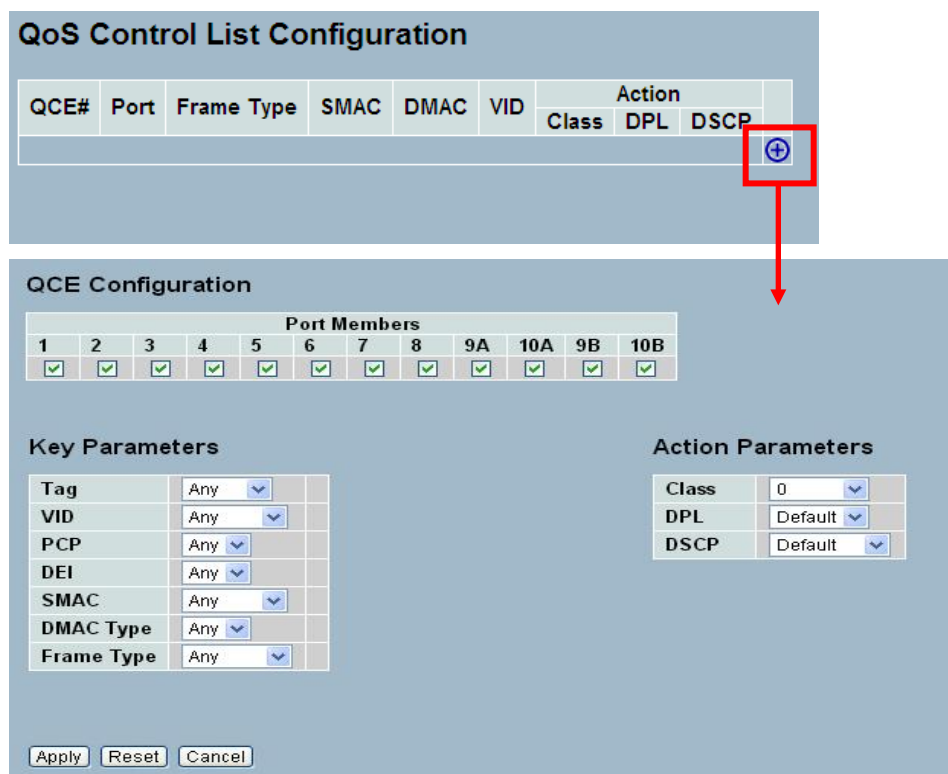







1. Navigate to **Configuration > QoS > QoS Control List**.
2. Click the  sign to add a new QoS Control List
3. Set the parameters for the QCE and apply it to a port by checking the box (es) for the port(s).
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 98: QoS Control List Configuration



Parameter	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: <ul style="list-style-type: none"> Any: The QCE will match all frame types. Ethernet: Only allows Ethernet frames (with Ether Type 0x600-0xFFFF). LLC: Only allows (LLC) frames. SNAP: Only allows (SNAP) frames IPv4: The QCE will match only IPV4 frames.

	<ul style="list-style-type: none"> IPv6: The QCE will match only IPV6 frames
SMAC	Displays the OUI field of Source MAC address, i.e. first three octets (byte) of MAC address.
DMAC	<p>Specify the type of Destination MAC addresses for incoming frame. Possible values are:</p> <ul style="list-style-type: none"> Any: Allows all types of Destination MAC addresses. Unicast: Only allows Unicast MAC addresses. Multicast: Only allows Multicast MAC addresses. Broadcast: Only allows Broadcast MAC addresses. <p>The default value is 'Any'</p>
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'.
Conflict (Not present in Web UI)	<p>Displays QCE status. 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 resource required by the QCE and pressing 'Refresh' button.</p> <p>PCP and DEI</p>
Action	<p>Indicates the action that is taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>There are three action fields: Class, DPL and DSCP.</p> <ul style="list-style-type: none"> Class: Classified QoS Class; if a frame matches the QCE it goes in the queue. DPL: Drop Precedence Level; if a frame matches the QCE then DP level will be set to value displayed in the DPL column. DSCP: If a frame matches the QCE, then the DSCP classification includes the value displayed in the DSCP column.
Modification Buttons	<p>Modify each QCE (QoS Control Entry) in the table using the following buttons:</p> <p>: Inserts a new QCE before the current row.</p> <p>: Edits the QCE.</p> <p>: Moves the QCE up the list.</p> <p>: Moves the QCE down the list.</p> <p>: Deletes the QCE.</p> <p>: The lowest plus sign adds a new entry at the bottom of the QCE listings</p>
Port Members	Check the checkbox button to make any port a member of the QCL entry. By default all ports will be checked.
Key Parameters	Key configurations are described as below:

	<p>Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'</p> <p>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</p> <p>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'</p> <p>DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'</p> <p>SMAC Source MAC address: 24 MS bits (OUI) or 'Any'</p> <p>DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'</p> <p>Frame Type 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> <ul style="list-style-type: none"> Any: Allow all types of frames. Ethernet: Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any'; default value is 'Any'. 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 Address: Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' SNAP : PID: Valid PID(a.k.a. Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any' 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 converting Mask to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. <p>DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43</p> <p>IP Fragment IPv4 frame fragmented option: yes no any</p> <p>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p> <ul style="list-style-type: none"> IPv6 :Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'



	<p>Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits</p> <p>DSCP Diffserv Code Point value(DSCP): It can be specific value, range of value or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43</p> <p>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p>
Action Configuration	<p>Class QoS Class: "class (0-7)", default- basic classification</p> <p>DP Valid DP Level can be (0-3)", default- basic classification</p> <p>DSCP Valid dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43)</p>

4.15.11 QCL Status

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

To display the QoS Control List Status in the web interface:

1. Navigate to **Configuration > QoS > QCL Status**.
2. Use the drop-down menu to select the view, and then check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 99: QoS Control List Status

QoS Control

List Status

Combined

Auto-refresh

Resolve Conflict

Refresh

User	QCE#	Frame Type	Port	Action	Class	DP	DSCP	Conflict
Static	2	Any	2,4,7,8,10A-10B	Class 2	Default	Default	No	
Static	1	Any	5-10B	Class 0	Default	Default	No	

Parameter	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of incoming frame. Possible frame types are: <ul style="list-style-type: none"> Any: The QCE matches all frame types. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF). LLC: Only (LLC) frames. LLC: Only (SNAP) frames. IPv4: The QCE matches only IPV4 frames. IPv6: The QCE matches only IPV6 frames
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on an ingress frame if parameters configured are matched with the frame's content. <p>There are three action fields: Class, DPL and DSCP.</p> <ul style="list-style-type: none"> Class: Classified QoS Class; if a frame matches the QCE it goes in the queue. DPL: Drop Precedence Level; if a frame matches the QCE then DP level will be set to value displayed in the DPL column. DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed in the DSCP column
Conflict	Displays QCE status. It is possible that resources required to add a QCE may not be available. If so, a 'Yes' conflict status displays, otherwise it is always 'No'. To resolve the conflict release the resource required by the QCE and press 'Refresh' button.

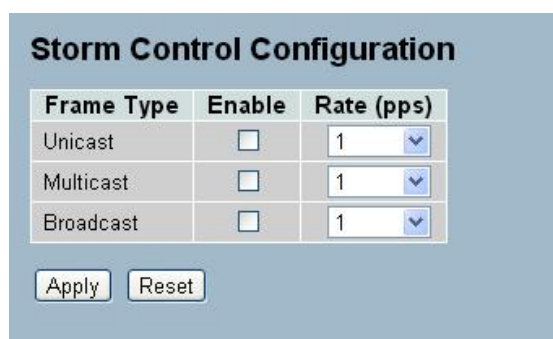
4.15.12 Storm Control

This section enables the user to configure the Storm control for the switch. 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

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

1. Navigate to **Configuration > QoS > Storm Control**.
2. Enable Storm Control for the port and set the rate limits for the frame types.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 100: Storm Control Configuration



Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Apply Reset

Parameter	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	<p>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. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K. , 1024K, 2048K, 4096K, 8192K, 16384K or 32768K.</p> <p>1 kpps is actually 1002.1 pps</p>

4.16 sFlow Agent

Monitor and modify the sFlow Collector configuration for the switch here. The switch supports up to 1 Collector. This page enables configuring sFlow collector IP type, sFlow collector IP Address and Port Number.

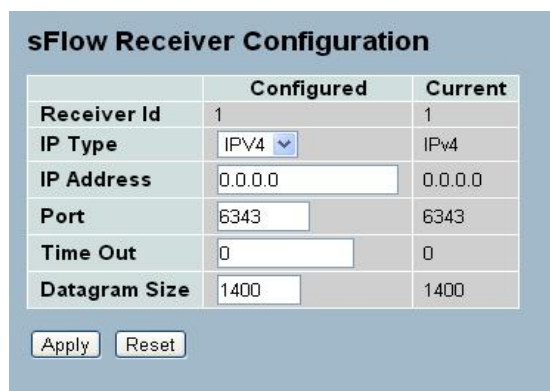
4.16.1 Collector

The "Current" field displays the currently configured sFlow Collector. The "Configured" field displays the new Collector settings configured by the administrator.

To configure the sFlow Agent via the web interface:

1. Navigate to **Configuration > sFlow Agent > Collector**.
2. Set the parameters for the Collector.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 101: sFlow Collector Configuration UI shows sFlow Receiver ID



The screenshot shows the 'sFlow Receiver Configuration' web interface. It features a table with two columns: 'Configured' and 'Current'. The rows represent different configuration parameters: Receiver Id, IP Type, IP Address, Port, Time Out, and Datagram Size. Each row has input fields for the 'Configured' column and a read-only field for the 'Current' column. Below the table are 'Apply' and 'Reset' buttons.

	Configured	Current
Receiver Id	1	1
IP Type	IPv4	IPv4
IP Address	0.0.0.0	0.0.0.0
Port	6343	6343
Time Out	0	0
Datagram Size	1400	1400

Apply Reset

Parameter	Description
Collector Id: UI displays Receiver ID	The "Collector ID" input fields enable the user to select the Collector ID. Indicates the ID of this particular sFlow Collector. Currently one ID is supported as one collector is supported.
ID Type	A drop down list to select the type of IP of Collector is displayed. By default, it is IPv4.
IP Address	The address of a reachable IP should be entered. This IP is used to monitor the sFlow samples sent by sFlow Agent(the switch). By default, the IP is set to 0.0.0.0
Port	A port to listen to the sFlow Agent has to be configured for the Collector. The accepted value is within the range of 1-65535. A port number not used by other protocols can to be configured.By default, the port number is 6343.
Time Out	The duration during which the collector receives samples. Once it expires, the sampler stops sending the samples. It is through the management the value is set before it expires. The accepted value is within the range of 0-2147483647. By default it is set to 0.
Datagram Size	It is the maximum UDP datagram size to send out the sFlow samples to the receiver. The range is 200 -1500 bytes. The default is 1400 bytes.

4.16.2 Sampler

This page displays the sFlow sampler, and it is available to edit. There is a random sample average of 1 out of N packets/operations. This type of sampling does not provide a 100% accurate results, but it does provide a result with quantifiable accuracy.

To configure the sFlow Agent via the web interface:


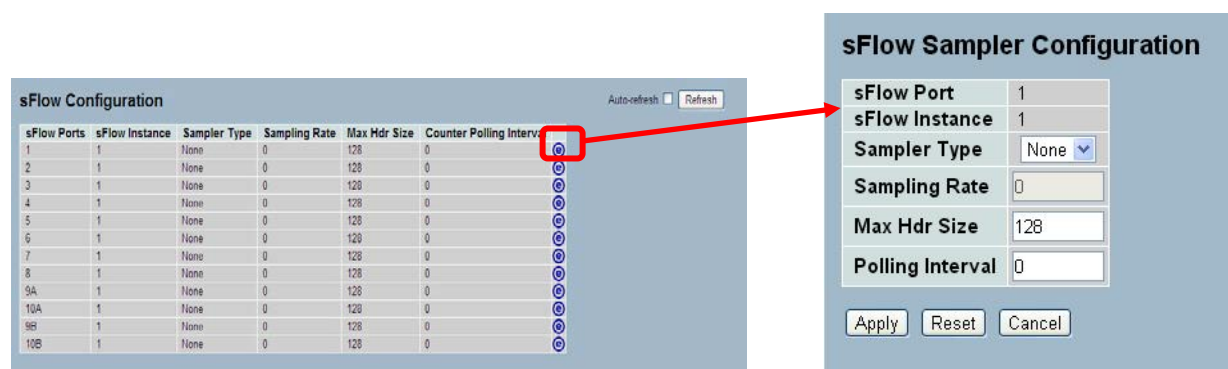
1. Navigate to **Configuration > sFlow Agent > Sampler**.
2. Click the  symbol to edit the sFlow sampler parameters
3. Select the Sample Type and set the other parameters.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 102: sFlow Sampler Configuration



Parameter	Description
sFlow Ports	List of the port numbers on which sFlow is configured.
sFlow Instance	Configured sFlow instance for the port number.
Sampler Type	Configured sampler type on the port. It can one of the following types: None, Rx, Tx or All. By default, the value is "None"By default, the IP is set to 0.0.0.0
Sampling Rate	Configured sampling rate on the ports.
Max Hdr Size	Configured size of the header of the sampled frame.
Polling Interval	Configured polling interval for the sampling.

4.17 Loop Protection

With the loop protection feature enabled, configure the switch to shut down a port if detecting a loop in the edge of the network. An undetected loop can cause a broadcast storm.

4.17.1 Configuration

To configure loop protection general and port settings via the web interface:

1. Navigate to **Configuration > Loop Protection > Configuration**.
2. Specify the global loop protection settings, and then specify loop protection settings for each port.
3. Click **Apply** or Click **Reset** to revert to previously saved values.

Figure 103: Loop Protection

The screenshot shows the web interface for configuring loop protection. The 'General Settings' tab is selected, displaying the 'Global Configuration' section. In this section, 'Enable Loop Protection' is set to 'Disable', 'Transmission Time' is 5 seconds, and 'Shutdown Time' is 180 seconds. Below this, the 'Port Configuration' tab is visible, showing a table with columns for Port, Enable, Action, and Tx Mode. The table lists ports 1 through 10B, all with 'Enable' checked, 'Shutdown Port' as the action, and 'Enable' as the Tx Mode. 'Apply' and 'Reset' buttons are at the bottom.

Parameter	Description
Enable Loop Protection	Enable/disable loop protection globally on the switch
Transmission Time	The interval between each loop protection PDU sent on each port. Valid values are 1 – 10 seconds.
Shutdown Time	The period for which a port will be kept in disabled state in the event a loop is detected. Valid values are 0 – 604800 seconds. A value of 0 will keep the port disabled until next device reboot.
Port	Indicates the port number
Enable	To enable loop protection on the port
Action	The action performed when a loop is detected. Options are Shutdown Port, Shutdown Port and Log or Log Only
Tx Mode	Controls whether the port is actively generating loop protection PDUs or is just passively looking for PDUs.

4.17.2 Status

This page displays the loop protection status.

Figure 104: Loop Protection Status

Loop Protection Status						
Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9A	Shutdown	Enabled	0	Down	-	-
10A	Shutdown	Enabled	0	Down	-	-
9B	Shutdown	Enabled	0	Down	-	-
10B	Shutdown	Enabled	0	Down	-	-

Parameter	Description
Port	Indicates the switch port number.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current status of the port.
Loop	Whether a loop is currently detected on the port.
Time of last loop	The time the last loop was detected on the port.

4.18 Single IP

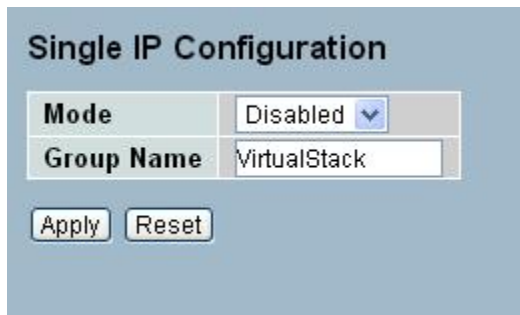
The Single IP feature enables management of a switch stack, consisting up to 32 PowerFlex switches, using a single IP. Each Single IP group consists of a Master switch with all other switches in the group set as Slaves. The Master Switch acts as an agent to manage all switches in the group. Access the Slave switches from the Master switch.

4.18.1 Configuration

To configure Single IP via the web interface:

1. Navigate to **Configuration > Single IP > Configuration**.
2. Specify the Single IP mode and Group name.
3. Click **Apply** or Click **Reset** to revert to previously saved values.

Figure 105: Single IP Configuration



Parameter	Description
Mode	<p>Possible modes are:</p> <p>Disable: Disable Single IP mode</p> <p>Master: Enable Single IP Management and set the switch as the Master switch</p> <p>Slave: Enable Single IP Management and set the switch as a Slave switch</p>
Group Name	Name of the Single IP group upto 64 characters in length.

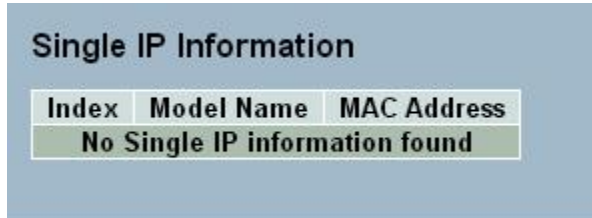
4.18.2 Information

This page displays the active Slave switch information.

To view the Slave switch information via the web interface:

Navigate to **Configuration > Single IP > Information**.

Figure 106: Single IP Information



Parameter	Description
Index	The ID of the active Slave switch
Model Name	Displays the model name of the Slave switch
MAC Address	Displays the MAC address of the Slave switch

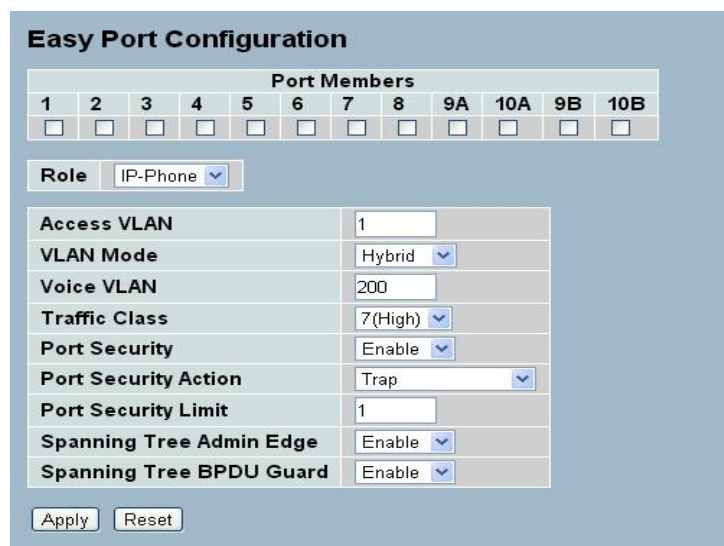
4.19 Easy Port

Easy Port provides a convenient way to save and share common configurations, to enable features and settings based on the location of a switch in the network, and for mass configuration deployments across the network. Users can easily implement devices such as Voice over IP phones, Wireless Access Points, etc.

To configure Easy Port via the web interface:

1. Navigate to **Configuration > Easy Port**.
2. Use the drop-down menu to set the role for the device and set the parameters for the role.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 107: Easy Port Configuration



Easy Port Configuration

Port Members											
1	2	3	4	5	6	7	8	9A	10A	9B	10B
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Role: IP-Phone

Access VLAN	<input type="text" value="1"/>
VLAN Mode	Hybrid
Voice VLAN	<input type="text" value="200"/>
Traffic Class	7(High)
Port Security	Enable
Port Security Action	Trap
Port Security Limit	<input type="text" value="1"/>
Spanning Tree Admin Edge	Enable
Spanning Tree BPDU Guard	Enable

Apply Reset

Parameter	Description
Port Members	To select which Port to enable the Easy Port function for.
Role	Select the type of device to connect and implement the Easy Port settings for .
Access VLAN	To set the Access VLAN ID.
VLAN Mode	Select the VLAN mode - Access, Trunk or Hybrid.
Voice VLAN	Set the Voice VLAN ID for VoIP phones.
Traffic Class	Select the traffic class for the data stream priority. The value range is 0 (Low) to 7 (High). For example, if voice traffic has higher priority, set the Traffic Class value as 7.
Port Security	Enable or disable the Port Security function on the port. If turning on the function, then set the Port Security limit the number of devices that can access the port (via MAC address).
Port Security Action	To set the action when a port security violation occurs. The options are Trap, Shutdown, Trap and Shutdown.



Port Security Limit	To set the Port security limit, the default is 1.
Spanning Tree Admin Edge	Enable or disable the Spanning Tree Admin Edge function on the Easy Port.
Spanning Tree BPDU Guard	Enable or disable the Spanning Tree BPDU Guard function on the Easy Port.

4.20 Mirroring

Users can mirror traffic from any source port to a target port for real-time analysis, and then attach a traffic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

For example, assuming that Port A and Port B are Monitoring Port and Monitored Port respectively, the traffic received by Port B is copied to Port A for monitoring.


To configure the Mirroring via the web interface:

1. Navigate to **Configuration > Mirroring**.
2. Set the Monitoring and Monitored ports and the modes – RX only, TX only or enabled (both RX and TX). By default, the ports disable mirroring.
3. Click **Save** to save the setting or click Reset to cancel changes and revert to previously saved values.

Figure 108: Mirror Configuration



Parameter	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.	
Port	Indicates the port number.
Mode	Select mirror mode. Rx only: Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored.

	<p>Tx only: Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored.</p> <p>Disabled: Neither frames transmitted nor frames received are mirrored.</p> <p>Enabled: Frames received and frames transmitted are mirrored on the mirror port</p> <p>NOTE: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.</p>
---	--

4.21 Trap Event Severity

Use the function to set an Alarm trap and get the Event log. Use the Trap Events Configuration function to enable the switch to send out the trap information while pre-defined trap events occur.

To configure the Trap Event Severity via the web interface:

1. Navigate to **Configuration > Trap Event Severity Configuration**.
2. Select the Group name and Severity Level
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 109: Trap Event Severity Configuration

Group Name	Severity Level
ACL	Info
ACL Log	Debug
Access Mgmt	Info
Auth Failed	Warning
Cold Start	Warning
Config Info	Info
Firmware Upgrade	Info
Import Export	Info
LACP	Info
Link Status	Warning
Login	Info
Logout	Info
Loop Protect	Info
Mgmt IP Change	Info
Module Change	Notice
NAS	Info
Password Change	Info
Poe Auto Check	Warning
Port Security	Info
VLAN	Info
Warm Start	Warning

Apply Reset

Parameter	Description
Group Name	The field for which to generate Trap Events.
Severity Level	Select the event type. The options are “Emerg, Alert, Crit, Error, Warning, Notice, Info and Debug”,

4.22 SMTP Configuration

The SMTP configuration enables configuring the switch to generate an email when a trap event occurs. Up to 6 email recipients can be set,

To configure the SMTP settings via the web interface:

1. Navigate to **Configuration > SMTP Configuration**.
2. Select the Severity Level and set the parameters.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 110: SMTP Configuration

The screenshot shows the 'SMTP Configuration' web page. It has a light blue header with the title. Below is a form with the following fields: 'Mail Server' (text input), 'User Name' (text input), 'Password' (text input), 'Severity Level' (dropdown menu showing 'Info'), 'Sender' (text input), 'Return Path' (text input), 'Email Address 1' through 'Email Address 6' (six text input fields). At the bottom left are two buttons: 'Apply' and 'Reset'.

Parameter	Description
Mail Server	Specify the IP Address of the Email server.
Username	Specify the username on the mail server.
Password	Specify the password on the mail server.
Sender	To set the mail sender name.
Return-Path	To set the mail return-path as sender's mail address.
Email Address 1-6	Email addresses to send the alarm message to.

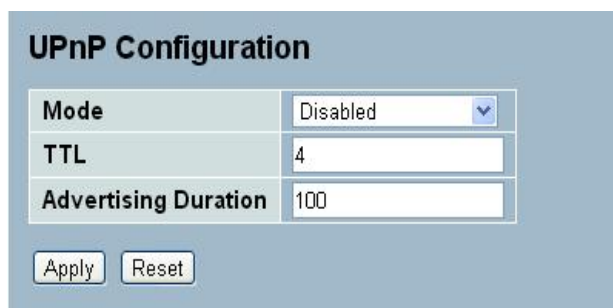
4.23 UPnP

Universal Plug and Play (UPnP) enables devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of networking components.

To configure the UPnP settings via the web interface:

1. Navigate to **Configuration > UPnP**
2. Specify the mode, TTL and Advertising Duration.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 111: UPnP Configuration



Parameter	Description
Mode	Indicates the UPnP operation mode. Possible modes are: Enabled: Enable UPnP operation mode. Disabled: Disable UPnP operation mode. When enabled, two ACEs are automatically added to trap UPnP related packets to CPU. The ACEs are automatically removed when the mode is Disabled.
TTL	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
Advertising Duration	The duration tells the control point (s) how often it should receive an SSDP advertisement message from the switch.

5 Security

This chapter describes the security configuration tasks of the switch including IP Source Guard, ARP Inspection, DHCP Snooping, AAA, etc.

5.1 IP Source Guard

This section describes how to configure the IP Source Guard parameters.

5.1.1 Configuration

To configure IP Source Guard via the web interface:

1. Navigate to **Security > IP Source Guard > Configuration**.
2. Set the mode to Enabled to enable the IP Source Guard on the switch globally.
3. Set the port mode and Maximum Dynamic Clients for each port.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 112: UPNP Configuration

IP Source Guard Configuration

Mode: Disabled

☐ Translate dynamic to static

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
9A	Disabled	Unlimited
10A	Disabled	Unlimited
9B	Disabled	Unlimited
10B	Disabled	Unlimited

Parameter	Description
Mode	Enable or disable IP Source Guard globally on the switch. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Select ports on which to enable IP Source Guard. It has to be enabled both globally and at port level for it to take effect.
Max Dynamic Clients	Specify the maximum number of dynamic clients to learn on the 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 forward IP packets that are matched in static entries on the specific port.

5.1.2 2 Static Table

This section describes how to configure the Static IP Source Guard Table parameters.

To configure Static IP Source Guard Table via the web interface:

1. Navigate to **Security > IP Source Guard > Static Table**.
2. Click **Add new entry**.
3. Specify the Port, VLAN ID, IP Address, and MAC address in the entry. UI has no MAC address field.
4. Click **Apply**.

Figure 113: Static IP Source Guard Table

The figure consists of two screenshots of the 'Static IP Source Guard Table' web interface. The top screenshot shows the 'Add new entry' button highlighted with a red box, with a red arrow pointing to the bottom screenshot. The bottom screenshot shows the form with the following fields: 'Delete' (button), 'Port' (dropdown menu with '1' selected), 'VLAN ID' (text input), 'IP Address' (text input), and 'MAC address' (text input). Below these fields are the 'Add new entry', 'Save', and 'Reset' buttons.

Parameter	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 entry.
IP Address	Allowed Source IP address.
IP Mask	Allowed Source IP mask.
MAC address	Allowed Source MAC address.
Add new entry	Click to add a new entry to the Static IP Source Guard table. Specify the Port, VLAN ID, IP address, and IP Mask for the new entry. Click Apply.

5.1.3 Dynamic Table

This section displays to configure the Dynamic IP Source Guard Table.

To display the Dynamic IP Source Guard Table in the web interface:

1. Navigate to **Security > IP Source Guard > Dynamic Table**.
2. Specify the Start from port, VLAN ID, IP Address, and entries per page.
3. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
4. Click **Refresh** to refresh the page manually.
5. Click << or >> to go to the previous or next page.

Figure 114: Dynamic Table

Parameter	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the IP traffic is permitted.
IP Address	User IP address of the entry
MAC address	Source MAC address.

5.2 *ARP Inspection*

This section describes how to configure the ARP Inspection parameters of the switch.

5.2.1 Configuration

To configure ARP Inspection via the web interface:

1. Navigate to **Security > ARP Inspection > Configuration**.
2. Select Enabled to globally enable ARP Inspection and set the mode for each port.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 115: ARP Inspection Configuration

ARP Inspection Configuration

Mode: Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9A	Disabled
10A	Disabled
9B	Disabled
10B	Disabled

Apply Reset

Parameter	Description
Mode	Enable or disable ARP Inspection globally on the switch.
Port Mode Configuration	Enable or disable ARP Inspection for each port. It has to be enabled both globally and at each port level for it to take effect on the port.

5.2.2 Static Table

This section describes how to configure the Static ARP Inspection Table parameters.

To configure the Static ARP Inspection Table via the web interface:

1. Navigate to **Security > ARP Inspection > Static Table**.
2. Click **Add new entry**.
3. Specify the Port, VLAN ID, IP Address and MAC address for the entry.
4. Click **Apply**.

Figure 116: Static ARP Inspection Table

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the entry.
VLAN ID	The vlan ID for the entry.
MAC Address	Allowed Source MAC address in ARP request packets.
IP Address	Allowed Source IP address in ARP request packets.
Add new Entry	Click to add a new entry to the Static ARP Inspection table. Buttons:

5.2.3 Dynamic Table

This section displays the Dynamic ARP Inspection Table. 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.

To display Dynamic ARP Inspection Table in the web interface:

1. Specify the Start from port, VLAN ID, MAC Address, IP Address, and entries per page.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.

Click **Refresh** to refresh the page manually.

Figure 117: Dynamic ARP Inspection Table

Dynamic ARP Inspection Table

Auto-refresh ☐ Refresh |<< >>

Start from Port 1, VLAN 1, MAC address 00-00-00-00-00-00 and IP address 0.0.0.0 with 20 entries per page.

Port	VLAN ID	MAC Address	IP Address
No more entries			

Parameter	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.

5.3 DHCP Snooping

This section describes how to configure the DHCP Snooping parameters. DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

5.3.1 Configuration

To configure DHCP Snooping via the web interface:

1. Navigate to **Security > DHCP Snooping > Configuration**.
2. Set the Snooping Mode as "Enabled".
3. Set the mode of the port to "Trusted".
4. Click **Apply**.

Figure 118: DHCP Snooping Configuration

DHCP Snooping Configuration

Snooping Mode: Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Untrusted
9A	Untrusted
10A	Untrusted
9B	Untrusted
10B	Untrusted

Apply Reset

Parameter	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	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.

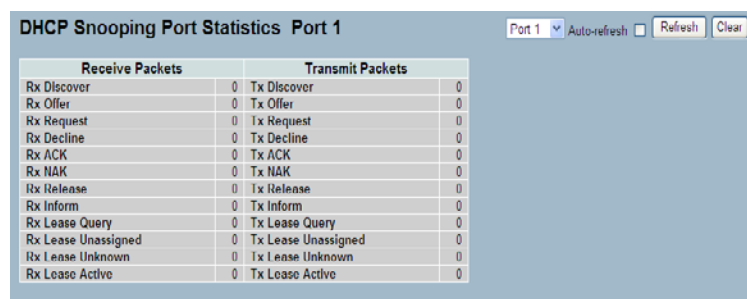
5.3.2 Statistics

This section displays the DHCP Snooping Statistics of the switch. The statistics show only packet counters when enabling DHCP snooping mode and disabling relay mode and it does not count the DHCP packets for DHCP client.

To display the DHCP Snooping Statistics in the web interface:

1. Navigate to **Security > DHCP Snooping > Statistics**.
2. Specify the port to display the statistics.
3. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
4. Click **Refresh** to refresh the page manually.

Figure 119: DHCP Snooping Port Statistics



Receive Packets		Transmit Packets	
Rx Discover	0	Tx Discover	0
Rx Offer	0	Tx Offer	0
Rx Request	0	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	0
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0

Parameter	Description
Rx and Tx Discover	Number of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	Number of offer (option 53 with value 2) packets received and transmitted.
Rx and Tx Request	Number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	Number of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	Number of ACK (option 53 with value 5) packets received and transmitted.
Rx and Tx NAK	Number of NAK (option 53 with value 6) packets received and transmitted.
Rx and Tx Release	Number of release (option 53 with value 7) packets received and transmitted.
Rx and Tx Inform	Number of inform (option 53 with value 8) packets received and transmitted.
Rx and Tx Lease Query	Number of lease query (option 53 with value 10) packets received and transmitted.
Rx and Tx Lease Unassigned	Number of lease unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Lease Unknown	Number of lease unknown (option 53 with value 12) packets received and transmitted.
Rx and Tx Lease Active	Number of lease active (option 53 with value 13) packets received and transmitted.

5.4 DHCP Relay

This section describes how to forward DHCP requests to another specific DHCP server via DHCP relay. The DHCP servers may be on another network.

5.4.1 Configuration

This section describes how to configure DHCP Relay settings including:

- Relay Mode (Enabled or Disabled)
- Relay Server IP setting
- Relay Information Mode (Enabled or Disabled)
- Relay Information Mode Policy (Replace, Keep and Drop)

To configure DHCP Relay via the web interface:

1. Navigate to **Security > DHCP Relay > Configuration**.
2. Enable the DHCP Relay mode, and then specify the Relay Server IP address.
3. Enable the Relay Information Mode, and then specify the Relay Information Policy setting.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 120: UPnP Configuration DHCP Relay Configuration

DHCP Relay Configuration

Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Replace

Apply Reset

Parameter	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, if not located in the same subnet domain. The DHCP broadcast messages will not be flooded for security considerations. Disabled: Disable DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address.
Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to the DHCP server and removes it from a DHCP message when transferring it to the DHCP client. It only works when DHCP relay operation mode is enabled. Disabled: Disable DHCP relay information mode operation

Relay Information Policy	<p>Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if agent receives a DHCP message that already contains relay agent information it will enforce the policy. It only works when the DHCP relay information operation mode is enabled. 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 packet when a DHCP message that already contains relay information is received.</p>
--------------------------	--

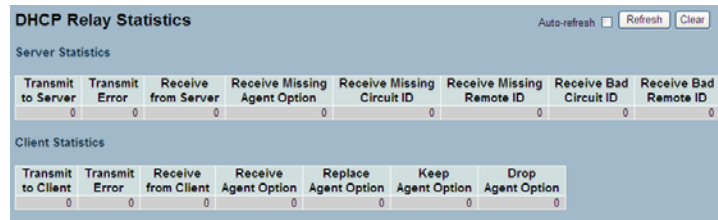
5.4.2 Statistics

This section displays the DHCP Relay Statistics of the switch. The statistics show both the Server and Client packet counters when enabling DHCP Relay mode.

To display the DHCP Snooping Statistics in the web interface:

1. Navigate to **Security > DHCP Relay > Statistics**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 121: DHCP Relay Statistics



DHCP Relay Statistics							
Auto-refresh <input type="checkbox"/> Refresh Clear							
Server Statistics							
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0
Client Statistics							
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option	
0	0	0	0	0	0	0	

Parameter	Description
Transmit to Server	Number of packets that are relayed from client to server.
Transmit Error	Number of packets that resulted in errors while being sent to clients.
Receive from Server	Number of packets received from server.
Receive Missing Agent Option	Number of packets received without agent information options.
Receive Missing Circuit ID	Number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	Number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	Number of packets of Circuit ID option not matching known Circuit ID.
Receive Bad Remote ID.	Number of packets of Remote ID option not matching known Remote ID.
Client Statistics	
Transmit to Client	Number of relayed packets from server to client.
Transmit Error	Number of packets that resulted in error while being sent to servers.
Receive from Client	Number of received packets from server.
Receive Agent Option	Number of received packets with relay agent information option.
Replace Agent Option	Number of packets replaced with relay agent information option.
Keep Agent Option	Number of packets when the relay agent information was retained.
Drop Agent Option	Number of dropped and received packets w/ relay agent information.

5.5 NAS

This section describes how to configure the NAS parameters of the switch. Use the NAS server to connect users to a variety of resources including Internet access, conference calls, printing documents on shared printers, etc.

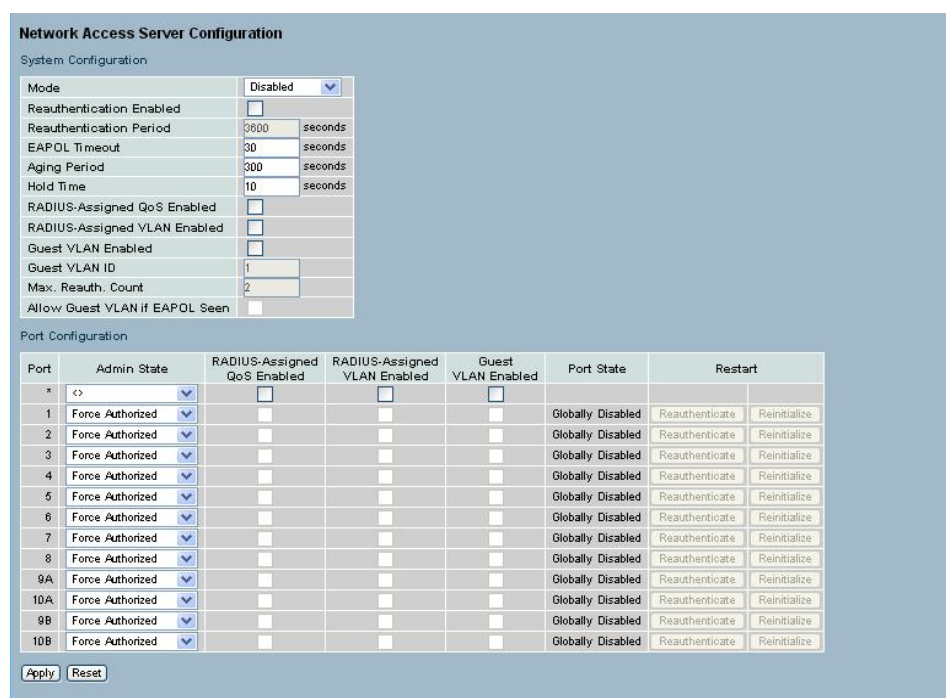
5.5.1 Configuration

This section describes how to configure NAS settings of IEEE 802.1X, MAC-based authentication system, and port settings.

To configure NAS settings via the web interface:

1. Navigate to **Security > NAS > Configuration**.
2. Select Enabled to enable NAS globally on the switch.
3. Check Reauthentication Enabled.
4. Set Reauthentication Period (Default is 3600 seconds).
5. Set EAPOL Timeout (Default is 30 seconds).
6. Set Aging Period (Default is 300 seconds).
7. Set Hold Time (Default is 10 seconds).
8. Enable RADIUS-Assigned QoS and VLAN.
9. Checked Guest VLAN Enabled.
10. Specify Guest VLAN ID.
11. Specify Max. Reauth. Count.
12. Check Allow Guest VLAN if EAPOL Seen.
13. Click **Apply**.

Figure 122: Network Access Server Configuration



Network Access Server Configuration

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
9A	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10A	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
9B	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10B	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Apply Reset

Parameter	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports can forward 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 does not 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>Determine the time for retransmission of Request Identity EAPOL frames.</p> <p>Valid values are in the range 1 to 255 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> <ul style="list-style-type: none"> • Single 802.1X • Multi 802.1X • MAC-Based Auth. <p>When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.</p> <p>If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.</p> <p>For ports in MAC-based Auth. mode, reauthentication does not 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	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> • • Single 802.1X • • Multi 802.1X • • MAC-Based Auth. <p>If a client is denied access - either because the RADIUS server denies the</p>

	<p>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. When unchecked, RADIUS-server assigned VLAN is disabled on all ports</p>
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>
Port Configuration The port parameters are as described below:	
Port	The port number for which the configuration applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available.
Force Authorized	In this mode, the switch will send one EAPOL Success frame when the port link comes up, and allows any client on the port network access without authentication.
Force Unauthorized	In this mode, the switch sends one EAPOL Failure frame when the port link comes up, and denies network access to any client on the port.
Port-based 802.1X	<p>In the 802.1X-world, the user is called the supplicant, the switch is the authenticator and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, because it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.</p> <p>When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant</p>
	<p>NOTE: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead).</p> <p>Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant and since the server has not yet failed (because the X seconds has not expired), the same server will be contacted</p>

	<p>upon the next backend authentication server request from the switch. This scenario loops forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.</p>
Single 802.1X	<p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though each is really are not authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is not an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant has access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.</p>
Multi 802.1X	<p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This enables other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though each is really are not authenticated. To overcome this security breach, use the Multi 802.1X variant.</p> <p>Multi 802.1X is not an IEEE standard, but features many of the same characteristics as port-based 802.1X. Multi 802.1X is like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.</p> <p>In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.</p> <p>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>
MAC-based Auth.	<p>Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string of the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-case hexadecimal digits. The switch only supports the MD5-Challenge</p>

	<p>authentication method, so the RADIUS server must be configured accordingly.</p> <p>When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.</p> <p>The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients do not need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>
RADIUS-Assigned QoS Enabled	<p>When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it is invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X <p>RADIUS attributes used in identifying a QoS Class:</p> <p>Refer to the written documentation for a description of the RADIUS attributes needed in order to successfully identify a QoS Class. The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.</p> <p>Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:</p> <p>All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '3', which translates into the desired QoS Class in the range [0; 3]</p>
RADIUS-Assigned VLAN Enabled	<p>When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.</p>

	<p>If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it is invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).</p> <p>This option is only available for single-client modes, i.e.</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X <p>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p>RADIUS attributes used in identifying a VLAN ID:</p> <p>RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:</p> <ul style="list-style-type: none"> • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. • The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): <ul style="list-style-type: none"> • Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). • Value of Tunnel-Type must be set to "VLAN" (ordinal 13). • Value of Tunnel-Private-Group-ID must be a string of ASCII characters in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1 - 4095].
Guest VLAN Enabled	<p>When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.</p> <p>This option is only available for EAPOL-based modes, i.e.:</p> <ul style="list-style-type: none"> • Port-based 802.1X • Single 802.1X • Multi 802.1X <p>For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.</p> <p>Guest VLAN Operation:</p> <p>When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The</p>

	<p>interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.</p> <p>Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port have access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.</p> <p>While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.</p>
Port State	<p>The current state of the port. It can undertake one of the following values:</p> <p>Globally Disabled: NAS is globally disabled.</p> <p>Link Down: NAS is globally enabled, but there is no link on the port.</p> <p>Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.</p> <p>Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p>X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p>
Restart	<p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.</p> <p>Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.</p>

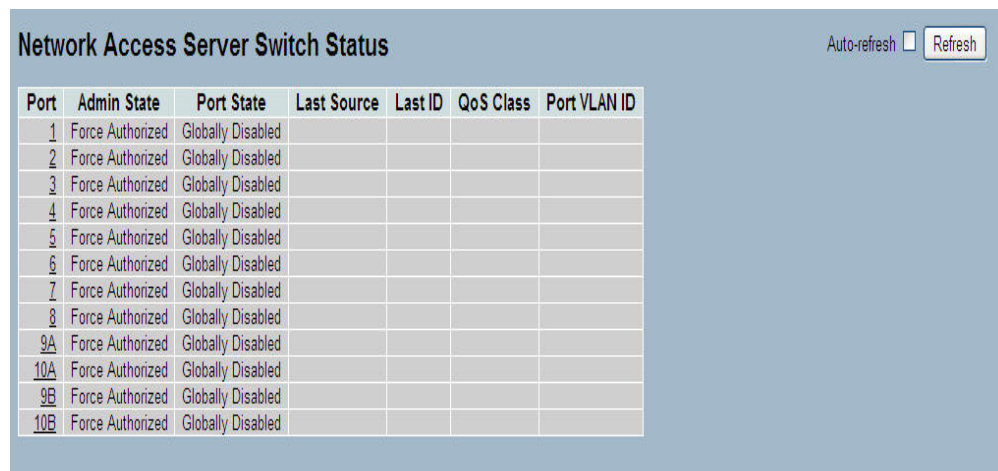
5.5.2 Switch Status

This section displays each port's NAS status. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

To display the NAS Switch Status via the web interface:

1. Navigate to **Security > NAS > Switch Status**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 123: Network Access Server Switch Status



Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled				
2	Force Authorized	Globally Disabled				
3	Force Authorized	Globally Disabled				
4	Force Authorized	Globally Disabled				
5	Force Authorized	Globally Disabled				
6	Force Authorized	Globally Disabled				
7	Force Authorized	Globally Disabled				
8	Force Authorized	Globally Disabled				
9A	Force Authorized	Globally Disabled				
10A	Force Authorized	Globally Disabled				
9B	Force Authorized	Globally Disabled				
10B	Force Authorized	Globally Disabled				

Parameter	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	<p>The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS.</p> <p>If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID</p>

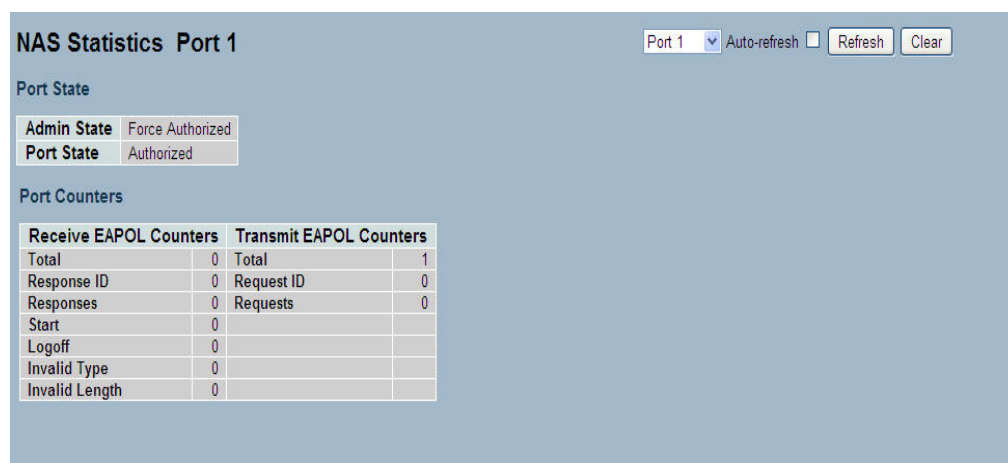
5.5.3 Port Status

This section provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication.

To view the NAS Port Status in the web interface:

1. Navigate to **Security > NAS > Port Status**.
2. Specify Port for which to display NAS statistics.
3. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
4. Check **Refresh** to refresh the page manually.

Figure 124: NAS Statistics



NAS Statistics Port 1 Port 1 Auto-refresh ☐ Refresh Clear

Port State

Admin State	Force Authorized
Port State	Authorized

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Parameter	Description
Port State	
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. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.
Port Counters	
EAPOL Counters	These supplicant frame counters are available for the following administrative states: <ul style="list-style-type: none"> Force Authorized



	<ul style="list-style-type: none">• Force Unauthorized• Port-based 802.1X• Single 802.1X• Multi 802.1X If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.
Backend Server Counters	<p>These backend (RADIUS) frame counters are available for the following administrative states:</p> <ul style="list-style-type: none">• Port-based 802.1X• Single 802.1X• Multi 802.1X• MAC-based Auth.
Last Supplicant/Client Info	<p>Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:</p> <ul style="list-style-type: none">• Port-based 802.1X• Single 802.1X• Multi 802.1X• MAC-based Auth.
Selected Counters	
Selected Counters	<p>The Selected Counters table is visible when the port is in one of the following administrative states:</p> <ul style="list-style-type: none">• Multi 802.1X• MAC-based Auth. <p>The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.</p>
Attached MAC Addresses	
Identity	<p>Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.</p> <p>Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.</p> <p>This column is not available for MAC-based Auth</p>
MAC Address	<p>For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client.</p> <p>Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.</p>
VLAN ID	



This column holds the VLAN ID that the corresponding client has currently secured through the Port Security module.	
State	The client can either be authenticated or unauthenticated. In the authenticated state, it can forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server has not successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

5.6 AAA

This section shows how to use an AAA (Authentication, Authorization, and Accounting) server to provide access control to the network. The AAA server can be a TACACS+ or RADIUS server.

5.6.1 Configuration

This section describes how to configure AAA setting of TACACS+ or RADIUS server.

To configure the RADIUS and TACACS+ server settings:

1. Navigate to **Security > AAA > Configuration**.
2. Click **Apply** after setting the parameters or click Reset to cancel changes and revert to previously saved values.

To configure the Common Configuration parameters via the web interface:

1. Set Timeout (Default is 15 seconds).
2. Set Dead Time (Default is 300 seconds).

To configure TACACS+ Authorization and Accounting parameters via the web interface:

1. Select Enabled in the Authorization.
2. Select Enabled in the Failback to Local Authorization.
3. Select Enabled in the Account.

To configure RADIUS Authentication Server parameters via the web interface:

1. Check Enabled to enable the server.
2. Specify IP address or Hostname of the RADIUS server.
3. Specify Authentication Port for RADIUS server (Default is 1812).
4. Specify secret key shared with the RADIUS server.

To configure RADIUS Accounting Server parameters via the web interface:

1. Check Enabled to enable the server.
2. Specify IP address or Hostname of the RADIUS server.
3. Specify Accounting Port for RADIUS server (Default is 1813).
4. Specify secret key shared with the RADIUS server.

To configure TACACS+ Authentication Server parameters via the web interface:

1. Check Enabled to enable the server.
2. Specify IP address or Hostname of the TACACS+ Server.
3. Specify Authentication Port for TACACS+ Server (Default is 49).
4. Specify secret key shared with the TACACS+ server.

Figure 125: Common Server Configuration



The screenshot shows a web interface titled "Authentication Server Configuration". Under the "Common Server Configuration" section, there are two rows of configuration fields:

Common Server Configuration		
Timeout	15	seconds
Dead Time	300	seconds

Figure 126: TACACS+ Accounting Configuration

TACACS+ Authorization and Accounting Configuration

Authorization	Disabled ▼
Fallback to Local Authorization	Disabled ▼
Accounting	Disabled ▼

Figure 127: RADIUS Authentication Configuration

RADIUS Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

Figure 128: RADIUS Accounting Configuration

RADIUS Accounting Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

Figure 129: TACACS+ Authentication Configuration

TACACS+ Authentication Server Configuration

#	Enabled	IP Address/Hostname	Port	Secret
1	<input type="checkbox"/>		49	
2	<input type="checkbox"/>		49	
3	<input type="checkbox"/>		49	
4	<input type="checkbox"/>		49	
5	<input type="checkbox"/>		49	

Apply Reset

Parameter	Description
Timeout	<p>The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.</p> <p>If the server does not reply within this timeframe, it will be considered dead and continue with the next enabled server (if any).</p> <p>RADIUS servers use the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead</p>
Dead Time	<p>The Dead Time, which can be set to a number between 0 and 3600 seconds, 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.</p> <p>Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.</p>
RADIUS Authentication Server Configuration	
#	The RADIUS Authentication Server number for which the configuration below applies. Upto 5 servers can be configured.
Enabled	Enable the RADIUS Authentication Server by checking this box.
IP Address/Hostname	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.
RADIUS Account Server Configuration	
#	The RADIUS Accounting Server number for which the configuration below applies. Upto 5 servers can be configured.
Enabled	Enable the RADIUS Accounting Server by checking this box.
IP Address/Hostname	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch.
TACACS+ Authentication Server Configuration	



#	The TACACS+ Authentication Server number for which the configuration below applies. Upto 5 servers can be configured.
Enabled	Enable the TACACS+ Authentication Server by checking this box.
IP Address/Hostname	The IP address or hostname of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.
Port	The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
Secret	The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch.

5.6.2 RADIUS Overview

This section shows an overview of the RADIUS Authentication and Accounting server statistics.

To view the RADIUS server statistics in the web interface:

1. Navigate to **Security > AAA > RADIUS Details**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 130: RADIUS Authentication Server Status Overview

RADIUS Authentication Server Status Overview			Auto-refresh <input type="checkbox"/> Refresh
#	IP Address	Status	
1	0.0.0.0:1812	Disabled	
2	0.0.0.0:1812	Disabled	
3	0.0.0.0:1812	Disabled	
4	0.0.0.0:1812	Disabled	
5	0.0.0.0:1812	Disabled	

RADIUS Accounting Server Status Overview		
#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Parameter	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	<p>The current state of the server. This field takes one of the following values:</p> <p>Disabled: The server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running.</p> <p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.</p> <p>Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled</p>
RADIUS Accounting Servers	
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
State	The current state of the server. This field takes one of the following values:



	<p>Disabled: The server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running.</p> <p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p>Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled</p>
Auto-refresh	The page will be automatically refreshed at periodic intervals.
Upper right icon (Refresh)	Click to manually refresh the page.

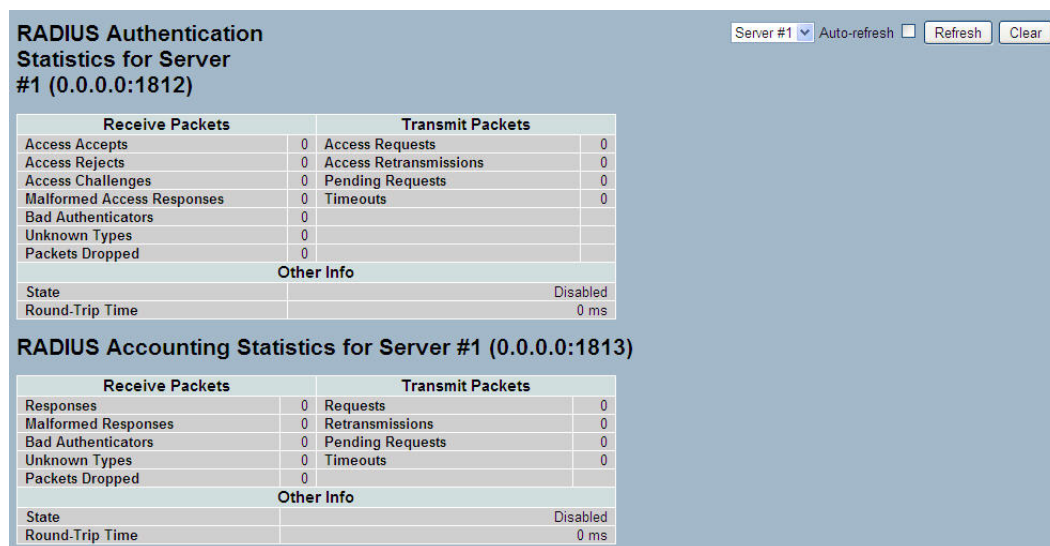
5.6.3 RADIUS Details

This section displays detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB.

To view the RADIUS Details in the web interface:

1. Navigate to **Security > AAA > RADIUS Details**.
2. Specify server with the statistics to view.
3. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
4. Click **Refresh** to refresh the page manually.

Figure 131: RADIUS Authentication and Accounting Statistics



Parameter	Description
RADIUS Authentication Statistics	
Rx Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server
Rx Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server
Rx Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server
Rx Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx Unknown Types	The number of RADIUS packets that were received with unknown types from

	the server on the authentication port and dropped.
Rx Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx Access Requests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx Timeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Other Info	
State	<p>State Shows the state of the server. It takes one of the following values:</p> <p>Disabled: The selected server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running.</p> <p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.</p> <p>Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</p>
Round-trip Time	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.
RADIUS Accounting Servers	
Rx Responses	The number of RADIUS packets (valid or invalid) received from the server.
Rx Malformed Responses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx Bad Authenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx Unknown Types	The number of RADIUS packets of unknown types that were received from the



	server on the accounting port.
Rx Packets Dropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx Requests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx Retransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx Pending Requests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx Timeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Other Info	
State	<p>Shows the state of the server. It takes one of the following values:</p> <p>Disabled: The selected server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running.</p> <p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p>Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</p>
Round-trip Time	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

5.7 Port Security

This section enables configuring the Port Security settings to restrict input to an interface by limiting and identifying MAC addresses.

5.7.1 Limit Control

To configure Limit Control globally via the web interface:

1. Navigate to **Security > Port Security > Limit Control**.
2. Select Enabled to enable Port Security globally.
3. Check Aging Enabled.
4. Set Aging Period (Default is 3600 seconds).

To configure Limit Control for each port via the web interface:

1. Select Enabled to enable Port Security for desired ports.
2. Specify the maximum number of MAC addresses in the "Limit" field
3. Set Action (Trap, Shutdown, Trap & Shutdown). This is the action taken on the port when a security violation occurs.
4. Click Apply or click Reset to cancel changes and revert to previously saved values.

Figure 132: Port Security Limit Control Configuration

Port Security Limit Control Configuration

System Configuration


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

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<>		<>		
1	Disabled	4	None	Disabled	Reopen
2	Disabled	4	None	Disabled	Reopen
3	Disabled	4	None	Disabled	Reopen
4	Disabled	4	None	Disabled	Reopen
5	Disabled	4	None	Disabled	Reopen
6	Disabled	4	None	Disabled	Reopen
7	Disabled	4	None	Disabled	Reopen
8	Disabled	4	None	Disabled	Reopen
9A	Disabled	4	None	Disabled	Reopen
10A	Disabled	4	None	Disabled	Reopen
9B	Disabled	4	None	Disabled	Reopen
10B	Disabled	4	None	Disabled	Reopen

Apply Reset

Parameter	Description
System Configuration	
Mode	Indicates if Limit Control is globally enabled or disabled on the switch.. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period .
Aging Period	<p>If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, there may be other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.</p> <p>The Aging Period can be set to a number between 10 and 10,000,000 seconds.</p> <p>To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host can 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 can forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.</p>
Port Configuration	
Port	The port number to which the configuration applies.
Mode	Controls whether Limit Control is enabled on this port. Both port mode 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	<p>The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.</p> <p>The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be guaranteed, if the remaining ports have already used all available MAC addresses.</p>
Action	<p>If Limit is reached, the switch can take one of the following actions:</p> <p>None: Do not allow more than Limit MAC addresses on the port, but take no further action.</p> <p>Trap: If Limit + 1 MAC addresses are 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 everytime the limit gets exceeded.</p> <p>Shutdown: If Limit + 1 MAC addresses are seen on the port, shut down the port.</p>

	<p>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:</p> <ul style="list-style-type: none"> • Reboot the switch • Disable and re-enable Limit Control on the port Click the Reopen button. <p>Trap & Shutdown: If Limit + 1 MAC addresses are seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.</p>
State	<p>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:</p> <p>Disabled: Limit Control is either globally disabled or disabled on the port.</p> <p>Ready: The limit is not yet reached. This can be shown for all actions.</p> <p>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.</p> <p>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.</p>
Re-open	<p>If a port is shutdown by this module, 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.</p> <p> NOTE: Clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.</p>

5.7.2 Switch Status

This section shows the Port Security status on the switch. 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 pass 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 even one user module decides to block it, blocking continues 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.

To view the Port Security Switch Status in the web interface:

1. Navigate to **Security > Port Security > Switch Status**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 133: Port Security Switch Status

Port Security Switch Status

Auto-refresh

Refresh

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	-	-
9A	----	Disabled	-	-
10A	----	Disabled	-	-
9B	----	Disabled	-	-
10B	----	Disabled	-	-

Parameter	Description
User Module Legend	The legend shows all user modules that may request Port Security services.
User Module Name	The full name of a module that may request Port Security services.
Abr	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.
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 Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

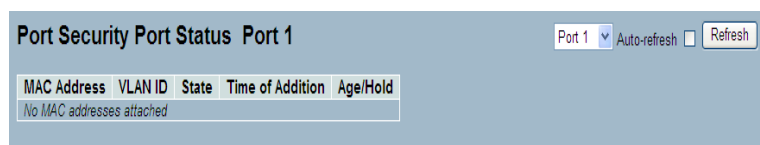
5.7.3 Port Status

This section 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 user module decides to block it, blocking continues until that user module decides otherwise.

To view the Port Security Port Status in the web interface:

1. Navigate to **Security > Port Security > Port Status**.
2. Specify the Port to view the status.
3. Check **Auto-refresh** to refresh the page automatically at periodic intervals
4. Click **Refresh** to refresh the page manually.

Figure 134: Port Security Port Status



Parameter	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 cannot transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
Age/Hold	<p>If at least one user module has decided to block this MAC address, it stays 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.</p> <p>If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) displays.</p>

5.8 Access Management

This section enables configuring access management on the switch including HTTP/HTTPS, SNMP, and TELNET/SSH. Users can manage the Switch over an Ethernet LAN, or over the Internet.

5.8.1 Configuration

This section enables configuring access management table of the Switch. Sixteen is the maximum entry number. If the application's type matches any one of the access management entries, it enables access to the switch.

To configure Access Management via the web interface:

1. Navigate to **Security > Access Management > Configuration**.
2. Select Enabled mode to enable global access management on the switch.
3. Click **Add new entry**, and then specify the Start IP Address, End IP Address.
4. Check Access Management method(s) (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
5. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 135: Access Management Configuration

Parameter	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.
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 via HTTP/HTTPS interface if the host IP address falls in the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch via SNMP interface if the host IP address falls in the IP address range provided in the entry.
TELNET/SSH	Indicates that the host can access the switch via TELNET/SSH interface if the host IP address falls in the IP address range provided in the entry.

5.8.2 Statistics

This section enables configuring detailed statistics of the Access Management settings including HTTP, HTTPS, SSH, TELNET, and SSH.

To view the Access Management statistics in the web interface:

1. Navigate to **Security > Access Management > Statistics**.
2. Check **Auto-refresh** to refresh the page automatically at periodic intervals.
3. Click **Refresh** to refresh the page manually.

Figure 136: Access Management Statistics

Access Management Statistics				Auto-refresh <input type="checkbox"/>	Refresh	Clear
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			

Parameter	Description
Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discarded packets from the interface when access management mode is enabled.

5.9 SSH

This section enables configuring SSH (Secure SHell) on the switch to securely access it. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

To configure SSH via the web interface:

1. Navigate to **Security > SSH**.
2. Select **Enabled** in the mode to enable SSH.
3. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 137: SSH Configuration



SSH Configuration

Mode: Enabled

Apply Reset

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

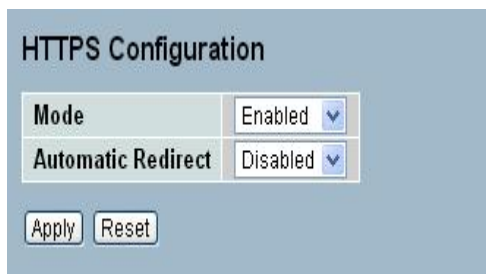
5.10 HTTPS

This section enables configuring HTTPS to access the Switch securely. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

To configure a HTTPS Configuration in the web interface:

1. Navigate to **Security > HTTPS**.
2. Select Enabled in the mode to enable HTTPS.
3. Enable Automatic Redirect.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 138: HTTPS Configuration



HTTPS Configuration

Mode: Enabled

Automatic Redirect: Disabled

Apply Reset

Parameter	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. Automatically redirect web browser to HTTPS when HTTPS mode is enabled. Possible modes are: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation

5.11 Auth Method

This page enables setting the authentication method when accessing the switch via one of the management client interfaces.

To configure Authentication Method via the web interface:

1. Navigate to **Security > Authentication Method**.
2. Specify the authentication method (none, local, RADIUS, TACACS+) for each client (console, Telnet, SSH, Web).
3. Check Fallback, if applicable.
4. Click **Apply** or click **Reset** to cancel changes and revert to previously saved values.

Figure 139: Auth Method Configuration

Client	Authentication Method	Fallback
console	local	<input type="checkbox"/>
telnet	local	<input type="checkbox"/>
ssh	local	<input type="checkbox"/>
web	local	<input type="checkbox"/>

Apply Reset

Parameter	Description
Client	The management client for which the configuration applies.
Automatic Method	<p>Authentication Method can be set to one of the following values:</p> <ul style="list-style-type: none"> • none: authentication is disabled and login is not possible. • local: use the local user database on the switch for authentication. • RADIUS: use a remote RADIUS server for authentication. • tacacs+ : use a remote TACACS+ server for authentication.
Fallback	<p>Enable fallback to local authentication by checking this box.</p> <p>If none of the configured authentication servers are alive, the local user database is used for authentication.</p> <p>This is only possible if the Authentication Method is set to a value other than 'none' or 'local'</p>

6 Maintenance

This chapter describes the entire switch Maintenance configuration tasks including Restart Device, Firmware upgrade, Save/Restore, Import/Export and Diagnostics.

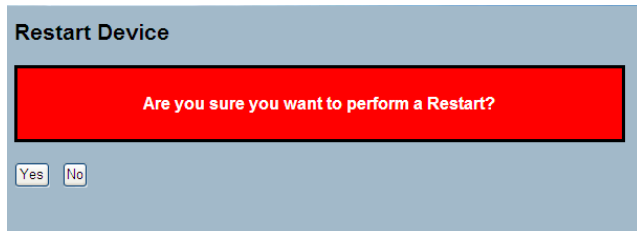
6.1 *Restart Device*

This section describes how to restart switch for any maintenance needs. Any configuration files or scripts saved in the switch should still be available afterwards.

To restart the switch via the web interface:

1. Navigate to **Maintenance > Restart Device**.
2. Click **Yes** or **No**.

Figure 140: Restart Device



Parameter	Description
Restart Device	Restart the switch from this page. After restart, the switch will boot normally.

6.2 Firmware

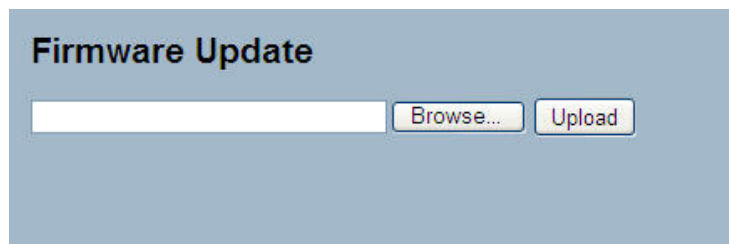
This section describes how to upgrade Firmware.



6.2.1 Firmware Upgrade

To perform a Firmware Upgrade via the web interface:

1. Navigate to **Maintenance > Firmware > Firmware Upgrade**.
2. Click **Choose File** and browse to the file in the local device.
3. Click **Upload**.

Figure 141: Firmware update



Parameter	Description
Choose File	Click the Choose File button to locate the path to the file in the local device.
Upload	<p>Click the "Upload" button. The switch will start to upload the firmware.</p> <p> NOTE: This page facilitates an update of the firmware controlling the switch. After the software image is uploaded a page announces that the firmware is initiated. After about a minute, the firmware is updated and the switch will restart automatically.</p> <p> 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.</p>

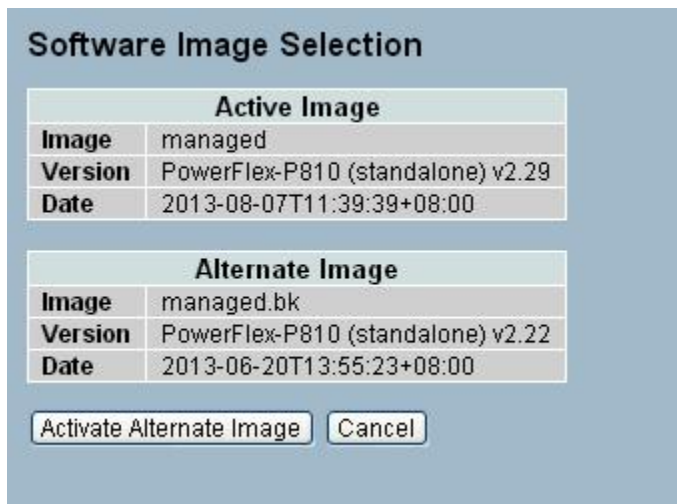
6.2.2 Firmware Selection

This page provides information about the active and backup firmware images and enables reverting to alternate image if required.

To activate alternate firmware image via the web interface:

1. Navigate to **Maintenance > Firmware > Firmware Selection**.
2. Click Activate Alternate Image.

Figure 142: Firmware Selection



The screenshot displays the 'Software Image Selection' web interface. It features two tables: 'Active Image' and 'Alternate Image'. The 'Active Image' table shows 'managed' as the image, 'PowerFlex-P810 (standalone) v2.29' as the version, and '2013-08-07T11:39:39+08:00' as the date. The 'Alternate Image' table shows 'managed.bk' as the image, 'PowerFlex-P810 (standalone) v2.22' as the version, and '2013-06-20T13:55:23+08:00' as the date. At the bottom, there are two buttons: 'Activate Alternate Image' and 'Cancel'.

Active Image	
Image	managed
Version	PowerFlex-P810 (standalone) v2.29
Date	2013-08-07T11:39:39+08:00

Alternate Image	
Image	managed.bk
Version	PowerFlex-P810 (standalone) v2.22
Date	2013-06-20T13:55:23+08:00

6.3 Save / Restore

This section describes how to save and restore the Switch configuration including resetting the switch to Factory Defaults.

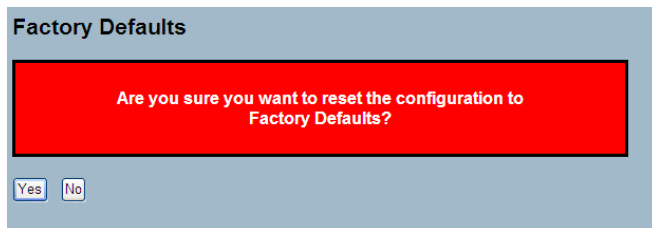
6.3.1 Factory Defaults

This section describes how to reset the Switch configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

To set the switch to Factory Defaults Configuration via the web interface:

1. Navigate to **Maintenance > Save/Restore > Factory Defaults**.
2. Click **Yes**.
3. Check the "Restore Default Configuration without changing current IP address" checkbox to restore all other settings except the current IP settings to factory defaults. This prevents losing connectivity to the switch once it reboots.

Figure 143: Factory Defaults – to be updated



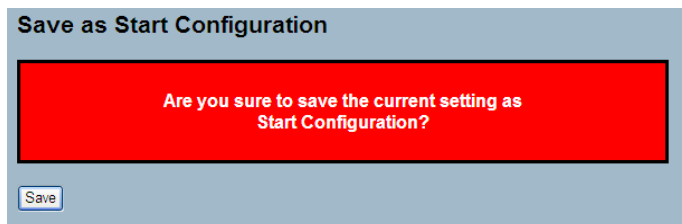
6.3.2 Save Start

This section enables saving the current running configuration to the start-up configuration. Any current configuration files will be saved in XML format.

To save current configuration to start-up configuration via the web interface:

1. Navigate to Maintenance > **Save/Restore > Save Start**.
2. Click **Save**.

Figure 144: Save as Start Configuration



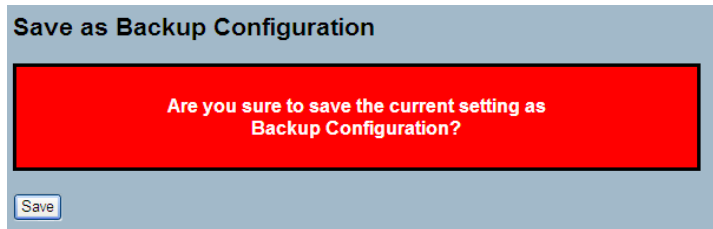
6.3.3 Save User

This section describes how to save current configuration to backup configuration. Any current configuration files will be saved in XML format.

To save current configuration to backup configuration via the web interface:

1. Navigate to **Maintenance > Save/Restore > Save User**.
2. Click **Save**.

Figure 145: Save as Backup Configuration



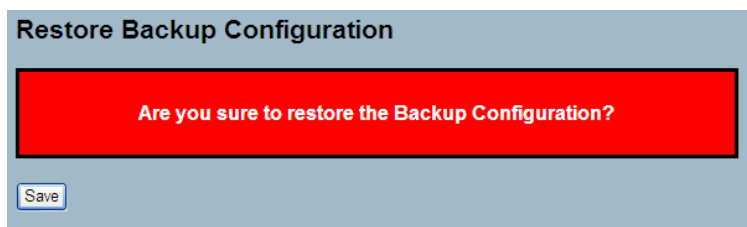
6.3.4 Restore User

This section describes how to restore backup configuration to the switch. Any current configuration files will be restored in XML format.

To restore backup configuration via the web interface:

1. Navigate to **Maintenance > Save/Restore > Restore User**.
2. Click **Save**

Figure 146: Restore Backup Configuration



6.4 Export / Import

This section describes how to export and import the Switch configuration.

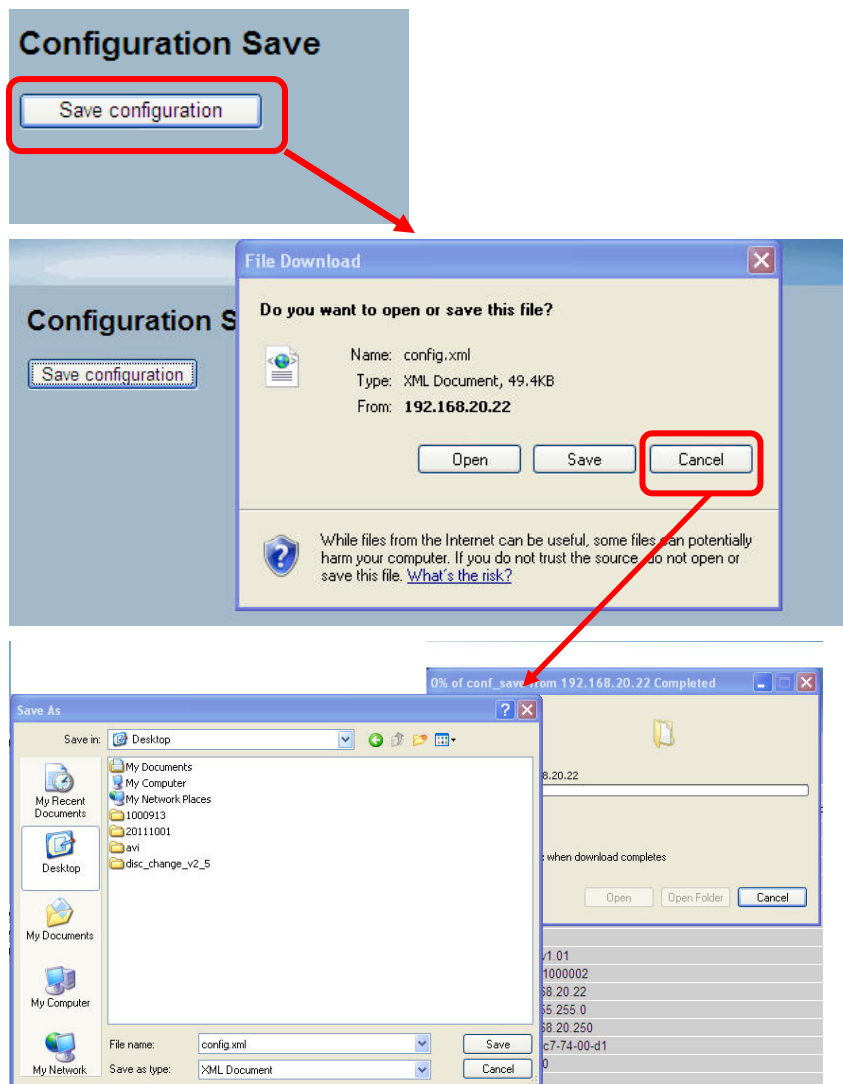
6.4.1 Export Config

This section describes how to export the Switch Configuration for maintenance needs. Any current configuration files will be exported as an XML file.

To export config file via the web interface:

1. Navigate to **Maintenance > Export/Import > Export Config**
2. Click Save configuration.
3. Save the file in the local device.

Figure 147: Export Configuration



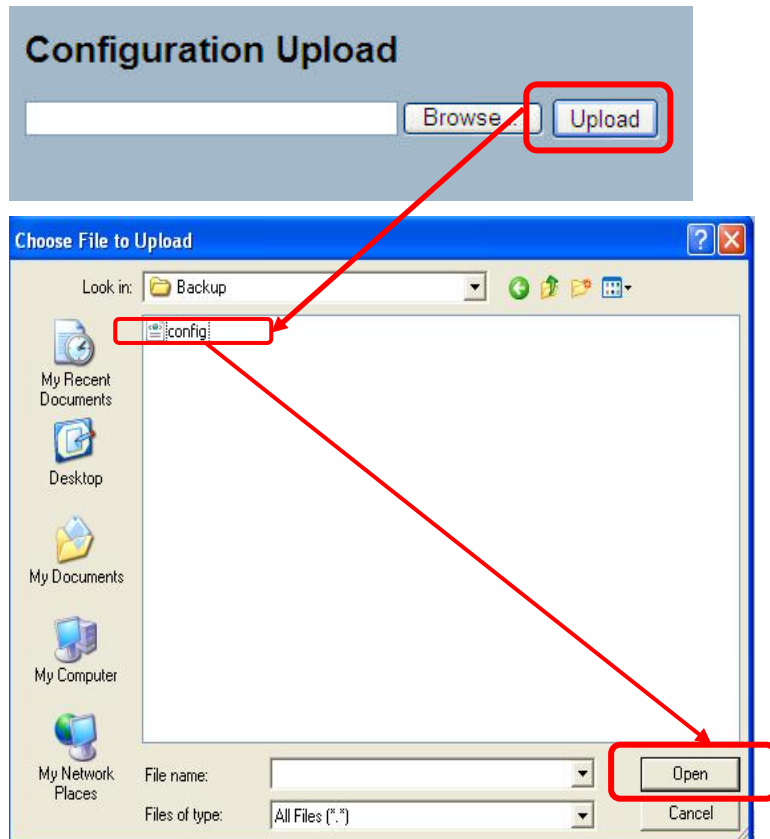
6.4.2 Import Config

This section describes how to import the Switch configuration.

To import config file to the switch via the web interface:

1. Navigate to **Maintenance > Export/Import > Import Config**.
2. Click **Choose File** to select the config file from the local device.
3. Click **Upload**

Figure 148: Import Config – Update figure



6.5 *Diagnostics*

This section provides a set of basic system diagnosis. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

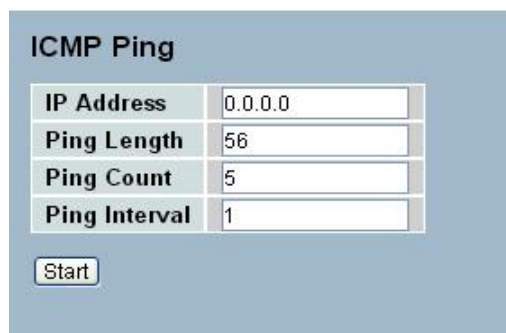
6.5.1 Ping

This section enables issuing ICMP PING packets to troubleshoot IPv4 connectivity issues.

To send an ICMP PING via the web interface:

1. Navigate to **Maintenance > Diagnostics > Ping**.
2. Specify the IP Address to ping.
3. Specify the Ping length, Count and Interval.
4. Click **Start**.

Figure 149: ICMP Ping – Update figure



The screenshot shows a web interface titled "ICMP Ping". It contains four input fields arranged vertically, each with a label and a text box. Below the fields is a "Start" button.

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

Start

After clicking Start, 5 ICMP packets transmit, and display the sequence number and roundtrip time upon reception of a reply. 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

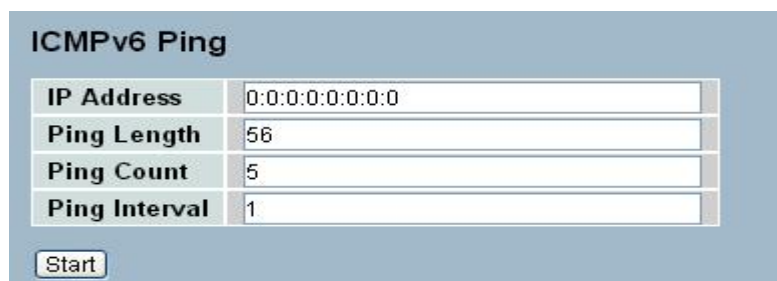
6.5.2 Ping6

This section enables issuing ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

To send an ICMPv6 PING via the web interface:

1. Navigate to **Maintenance > Diagnostics > Ping6**.
2. Specify the IPv6 address to ping.
3. Specify the ping Length, Count and Interval.
4. Click **Start**.

Figure 150: ICMPv6 Ping – Update figure



ICMPv6 Ping	
IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

After clicking Start, 5 ICMPv6 packets transmit, and then display the sequence number and roundtrip time upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 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

6.5.3 VeriPHY

This section is used for running the VeriPHY Cable 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 the cable diagnostics results display 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.

To run a VeriPHY Cable Diagnostics via the web interface:

1. Navigate to **Maintenance > Diagnostics > VeriPHY**.
2. Specify the Port to generate cable statistics. Select **All** to run the diagnostics for all ports.
3. Click **Start**.

Figure 151: VeriPHY

VeriPHY Cable Diagnostics

Port All

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--

Parameter	Description
Port	The port for requiring VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair

7 Glossary of Web-based Management

Term	Definition
A	
ACE	<p>An acronym for Access Control Entry describing access permission associated with a particular ACE ID.</p> <p>The three ACE frame types are Ethernet Type, ARP, and IPv4, and two ACE actions permit and deny. The ACE also contains many detailed, different parameter options available for individual application.</p>
ACL	<p>An acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.</p> <p>Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.</p> <p>ACL implementations can be complex, for example, when prioritizing the ACEs for the various situation. In networking, the ACL refers to a list of service ports or network services available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, similar to firewalls.</p> <p>There are 3 web-pages associated with the manual ACL configuration:</p> <p>ACL Access Control List: The web page shows the ACEs prioritized, highest (top) to lowest (bottom). The default table is empty. An ingress frame only gets hit on one ACE even though there are more matching ACEs. The first matching ACE takes action (permit/deny) on that frame and an associated counter increments. An ACE associations include Policy, 1 ingress port, or any ingress port (the whole switch). If creating an ACE Policy, then associate that Policy with a group of ports under the "Ports" web-page. There are number of parameters to configure with an ACE. Read the Web page help text for further information for each. The maximum number of ACEs is 64.</p> <p>ACL Ports: Use the ACL Ports configuration to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Create the Traffic Policy under the "Access Control List" - page. Users can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. Each only applies if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port increments. See the Web page help text for each specific port property.</p> <p>ACL Rate Limiters: Under this page configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per second. Under "Ports" and "Access Control List" web-pages users can assign a Rate Limiter ID to the ACE(s) or ingress port(s).</p>
AES	<p>An acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.</p>
APS	<p>An acronym for Automatic Protection Switching. Use this protocol to secure bidirectional switching in the two ends of a protection group, defined in G.8031.</p>

Term	Definition
Aggregation	<p>Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.</p> <p>(Also Port Aggregation, Link Aggregation)</p>
ARP	<p>An acronym for Address Resolution Protocol. It is a protocol used to convert an IP address into a physical address, such as an Ethernet address. ARP permits a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.</p>
ARP Inspection	<p>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. Use this feature to block such attacks. Only valid ARP requests and responses can go through the switch device.</p>
Auto-Negotiation	<p>The process where two different devices establish the mode of operation and share the speed settings by those devices for a link.</p>
C	
CC	<p>An acronym for Continuity Check. It is a MEP functionality able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.</p>
CCM	<p>An acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.</p>
CDP	<p>An acronym for Cisco Discovery Protocol.</p>
D	
DEI	<p>An acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.</p>
DES	<p>An acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.</p> <p>Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.</p>
DHCP	<p>An acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.</p> <p>DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.</p> <p>The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). IP address pool management is done by the server and not by a human network administrator.</p> <p>Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the</p>

Term	Definition
	task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.
DHCP Relay	<p>Forwards and transfers DHCP messages between the clients and the server when not on the same subnet domain.</p> <p>The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.</p> <p>The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.</p> <p>The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.</p>
DHCP Snooping	Blocks intruders 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.
DNS	An acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.
DoS	An acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.
Dotted Decimal Notation	<p>Refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.</p> <p>An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.</p>
DSCP	An acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.
E	
EEE	An abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

Term	Definition
EPS	An abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.
Ethernet Type	Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.
F	
FTP	An acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
Fast Leave	Multicast snooping Fast Leave processing permits the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.
H	
HTTP	<p>An acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).</p> <p>HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when entering a URL in the browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.</p> <p>Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle it when arriving. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.</p>
HTTPS	<p>An acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.</p> <p>HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.</p> <p>HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange</p>

Term	Definition
I	
ICMP	An acronym for Internet Control Message Protocol. A protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.
IEEE 802.1X	An IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.
IGMP	An acronym for Internet Group Management Protocol. A communications protocol used to manage the membership of Internet Protocol multicast groups. by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. Online video and gaming use IGMP, and enable a more efficient use of resources when supporting these uses.
IGMP Querier	A router sends IGMP Query messages onto a particular link. This router is called the Querier.
IMAP	<p>An acronym for Internet Message Access Protocol. A protocol for email clients to retrieve email messages from a mail server. The protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.</p> <p>The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves email messages on the server rather than downloading the messages to the computer. To remove messages from the server, use the mail client to generate local folders, copy messages to the local hard drive, and then delete and expunge the messages from the server.</p>
IP	<p>An acronym for Internet Protocol used for communicating data across an internet network.</p> <p>IP is a "best effort" system, which means there is no assurance that a packet of information sent over reaches its destination in the same condition. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and uses this IP address to identify the device uniquely among all other devices connected to the extended network.</p> <p>The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number reduces drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.</p>

Term	Definition
IPMC	An acronym for IP MultiCast.
IP Source Guard	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.
L	
LACP	An IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, permits bundling several physical ports together to form a single logical port.
LLC	The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.
LLDP	An IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol(LLDP) specified in this standard permits 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)
LLDP-MED	An extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).
LOC	An acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. EPS can use as a switch criteria.
M	
MAC Table	Bases the switching of frames on the DMAC address contained in the frame. The switch builds a table that maps MAC addresses to switch ports to know which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports. The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

Term	Definition
MEP	An acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).
MD5	An acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.
Mirroring	<p>For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)</p> <p>Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port</p>
MLD	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.
MVR	<p>Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.</p> <p>The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested the multicast streams. (Wikipedia)</p>
N	
NAS	An acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.
NetBIOS	<p>An acronym for Network Basic Input/Output System. It is a program that permits applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).</p> <p>The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.</p>
NFS	<p>An acronym for Network File System. It permits hosts to mount partitions on a remote system and use as a local file systems.</p> <p>NFS enables the system administrator to store resources in a central location on the network, providing authorized users continuous access, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network</p>

Term	Definition
NTP	An acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.
O	
OAM	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.
Optional TLVs	A LLDP frame contains multiple TLVs. For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.
OUI	An acronym for Organizationally Unique Identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. Users can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.
P	
PCP	An acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.
PD	An acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.
PHY	An abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).
PING	ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected. ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.
PoE	PoE is aAn acronym for Power Over Ethernet. Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.
Policer	A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.
POP3	An acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

Term	Definition
	<p>POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations enable users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.</p> <p>An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. Consider IMAP as a remote file server.</p> <p>POP and IMAP deal with the receiving of e-mail. Do not with the Simple Mail Transfer Protocol (SMTP). Send e-mail with SMTP, and a mail handler receives it on the recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.</p>
Private LAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
PTP	An acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.
Q	
QCE	<p>An acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.</p> <p>There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application</p>
QCL	<p>An acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.</p> <p>Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.</p>
QL	In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.
QoS	<p>An acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.</p> <p>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.</p> <p>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</p>
R	
RARP	An acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

Term	Definition
RADIUS	An acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization, and accounting management for people or computers to connect and use a network service.
RDI	An acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.
RSTP	In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.
S	
SHA	An acronym for Secure Hash Algorithm designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.
Shaper	Limits the bandwidth of transmitted frames. It is located after the ingress queues.
SMTP	An acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.
SNAP	An acronym for SubNetwork Access Protocol. SNAP is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.
SNMP	An acronym for Simple Network Management Protocol, part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP permits diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.
SNTP	An acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.
SPROUT	Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.
SSID	Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising the SSIDs, and can

Term	Definition
	select one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).
SSH	An acronym for Secure SHell. It is a network protocol that permits exchanging data using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).
SSM	In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.
STP	An acronym for Spanning Tree Protocol. STP is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.
Switch ID	Switch IDs (1-16) are used to uniquely identify the switches within a stack. The Switch ID of each switch shows on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.
SyncE	An abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588)
T	
TACACS+	An acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.
Tag Priority	A 3-bit field storing the priority level for the 802.1Q frame.
TCP	<p>An acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.</p> <p>The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.</p> <p>The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.</p> <p>Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).</p>

Term	Definition
TELNET	<p>An acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.</p> <p>TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if entering commands directly on the server console</p>
TFTP	<p>An acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.</p>
U	
UDP	<p>An acronym for User Datagram Protocol. It is a communications protocol that uses Internet Protocol (IP) to exchange the messages between computers.</p> <p>UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because of very small data units to exchange may prefer UDP to TCP.</p> <p>UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.</p> <p>Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP)</p>
User Priority	<p>A 3-bit field storing the priority level for the 802.1Q frame. Also known as PCP.</p>
V	
VLAN	<p>An acronym for Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:</p> <p>VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.</p> <p>VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.</p> <p>Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged</p>

Term	Definition
	frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag
VLAN ID	A 12-bit field specifying the VLAN to which the frame belongs.
Voice VLAN	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.



Toll Free 1-866-ALLWORX • 585-421-3850

www.allworx.com

Version: 1. Revised October 7, 2013