AS Series Gigabit Managed L3 Lite PoE+ Switches

AS5010-P
AS5026-P
AS5048-P
AS5128-P
AS5152-P

User Manual

Version: 1.0.2 August 2016

About this Guide

Purpose

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

Audience

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

Warranty

The AS series comes with a limited lifetime warranty. For full Alloy warranty terms and conditions please follow the link below:
https://www.alloy.com.au/support/warranty/

Conventions

The following conventions are used throughout this guide to show information:

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to a potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Compliances and Safety Statements

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

European Community (CE) Electromagnetic Compatibility Directive

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

RFI Emission: - Limit according to EN 55022:2010 AS/NZS CISPR 22:2009, Class A

- Limit for harmonic current emission according to EN 61000-3-2:2006+A1:2009+A2:2009

- Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3:2008

Immunity: - Product family standard according to EN 55024:2010

- Electrostatic Discharge according to IEC 61000-4-2:2008

- Radio-frequency electromagnetic field according to IEC 61000-4-3:2006+A1:2007+A2:2010

- Electrical fast transient/burst according to IEC 61000-4-4:2010

- Surge immunity test according to IEC 61000-4-5:2005

- Immunity to conducted disturbances, Induced by radio-frequency fields: IEC 61000-4-6:2008

- Power frequency magnetic field immunity test according to IEC 61000-4-8:2009

- Voltage dips, short interruptions and voltage variations immunity test according to IEC 61000-4-11:2004

LVD: - EN60950-1:2006+A11:2009+A1:2010EMC:

Australian RCM Compliance.

This equipment is compliant with the required Australian RCM standards.

PLEASE READ THE FOLLOWING SAFETY INFORMATION CAREFULLY BEFORE INSTALLING THE SWITCH:

WARNING: Installation and removal of the unit must be carried out by qualified personnel only.

- This guide is intended for use by network administrators who are responsible for setting up and installing network equipment; consequently, it assumes a basic working knowledge of LANs (Local Area Networks).

- The unit must be connected to an earthed (grounded) outlet to comply with international safety standards.

- Do not connect unit to an A.C outlet (power supply) without an earth (ground) connection.

- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN 60320/IEC 320 appliance inlet.

- The socket outlet must be near to the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.

- This unit operates under SELV (Safety Extra Low Voltage) conditions according to IEC 60950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

SAFETY PRECAUTIONS

Read the following information carefully before operating the device. Please follow the following precaution items to protect the device from risks and damage caused by fire and electric power:

- Use the power adapter that is included with the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburdened power outlet or damaged cords and plugs may cause electric shock or fire. Check the power cords regularly, if you find any damage, replace it at once.
- Proper space for heat dissipation is necessary to avoid any damage caused by device overheating. The ventilation holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these ventilation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid placing the device in direct sunshine.
- Do not put this device close to a place which is damp or wet. Do not spill any fluid on this device.
- Please follow the instructions in the user manual/quick install guide carefully to connect the device to your PC or other electronic product. Any invalid connection may cause a power or fire risk.

Do not place this device on an unstable surface or support.

CAUTION: Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- If you are connecting a device mounted outdoors to this switch, please ensure you have installed an additional lightning arrestor between this device and the outdoor equipment.

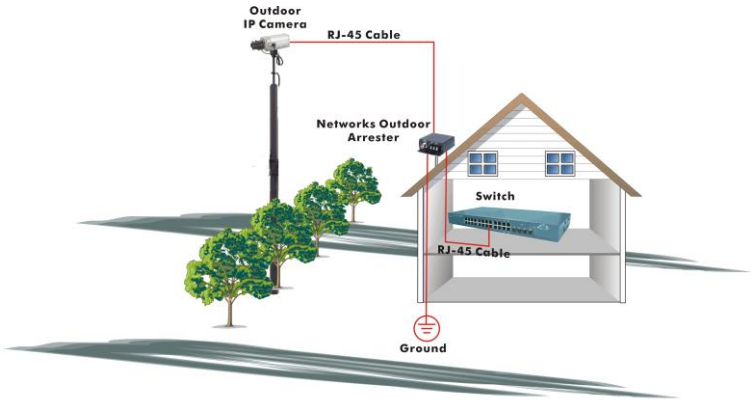


Fig. Additional arrester installed between outdoor device and this switch

NOTE: The switch is an indoor device; if it will be used in outdoor environment or connects with some outdoor device, then it must use a lightning arrester to protect the switch

WARNING:

- Self-demolition of Product is strictly prohibited. Damage caused by self-demolition will result in voiding the switches warranty.
- Do not place product in outdoor locations.
- Before installation, please make sure input power supply and product specifications are compatible to each other.
- To reduce the risk of electric shock. Disconnect all AC or DC power cords and RPS cables to completely remove power from the unit.
- Before importing / exporting configuration please make sure the firmware version is always the same.

Revision History

Document Part Number	Publish Date	Comments
AS5-0116-01	January 2016	Original Document

1. Introduction

Overview of AS Series Layer 3 Lite Managed PoE+ Switches

AS series switch models offer flexible port configurations, with combinations of 1000Base-T 10/100/1000mbps RJ-45, paired 1000Base-T/SFP arrays (with the SFP slot supporting 100Mbps or 1Gbps SFP modules), unpaired SFP slots (also supporting 100Mbps or 1Gbps SFP modules), and SFP+ slots for 100Mb, 1Gbps or 10Gbps SFP modules. Port densities range from 10 to 52 ports.

All SFP Ports support both 100M and 1000M SFP modules allowing easy upgrade paths for existing cabling and network infrastructure.

All AS series switches provide IEEE 802.3af and the latest 802.3at 'PoE+' Power over Ethernet. With all standalone RJ-45 ports supporting PoE+, devices such as IP Phones and Wireless Access Points can now be connected directly to the network with data and power supplied over a single UTP cable, reducing deployment and maintenance costs and making it much easier to install devices exactly where they are required. With support of 802.3at PoE+, up to 30 watts of power can be supplied per port, so power hungry devices such as Pan Tilt Zoom IP Security Cameras can be connected directly to the network.

The AS switches comply with the latest IEEE 802.3az Energy Efficient Green Ethernet standard to minimise power usage, with features such as Link Detection and Cable Length Detection. Link Detection automatically turns the power off/on to individual ports depending on link/idle traffic status. Cable Length Detection adjusts the signal strength based on the length of the cable – when using shorter cables, the power consumption is reduced.

All of the Alloy AS Series switches feature Alloy's latest user friendly responsive Web GUI, allowing ease of configuration on all devices including PC, Tablet and Phones. Alloy have also included a bundle of unique features including a built in Device Management System (DMS), advanced PoE features and support for Alloy's Android and iOS Apps.

Switch Features

- Managed Layer 2+ and Layer 3 Lite GbE Connectivity
- Built in Device Management System (DMS)
- High performance
- Enterprise-class security features
- PoE Port configuration and scheduling
- 802.3at high power PoE plus standard
- IEEE 802.3az EEE Energy Efficient Ethernet standard for green Ethernet
- Dual Speed SFP ports supporting both 100M and 1000M SFP Modules
- Limited Lifetime Warranty

Product Model Overview

Part Number	Description
AS5010-P	10 Port Layer 3 Lite Managed PoE+ Switch with 10x 10/100/1000Mbps Ports + 2x Paired 100M/1Gb SFP Ports
AS5026-P	26 Port Layer 3 Lite Managed PoE+ Switch with 26x 10/100/1000Mbps Ports + 2x Paired 100M/1Gb SFP Ports
AS5048-P	48 Port Layer 3 Lite Managed PoE+ Switch with 48x 10/100/1000Mbps Ports + 4x Paired 100M/1Gb SFP Ports
AS5128-P	28 Port Layer 3 Lite Managed PoE+ Switch with 24x 10/100/1000Mbps Ports + 4x 1Gb/10GbE SFP Ports
AS5152-P	52 Port Layer 3 Lite Managed PoE+ Switch with 48x 10/100/1000Mbps Ports + 4x 1Gb/10GbE SFP Ports

Reset Button

To reset the switch to factory default please follow the procedure below. By factory defaulting the switch you will lose all current configuration settings including the IP Address settings and any changes to the username and password.

1) Locate the reset button on the front panel of the switch.
2) Hold down the reset button for 10 seconds and then release. You should see all LED's on switch go hard on.
3) Switch will now reboot with factory configuration.

Overview of the Web Management Interface

The AS series switches contain an embedded web server and management software that can be used to manage and monitor switch functions. Without configuration of these management functions the switch will act as a simple unmanaged switch. However, by utilizing the advanced features contained in the management software the switch can be used to improve the overall performance of your network.

The web-based management interface allows you to configure and monitor your switch via a standard web browser. From the web browser you can configure all switch features, such as VLAN's, Port Aggregation, QoS and ACL's.

Using a Web Browser to Access the Switch

You can use a web browser to access the switches web management interface. Please ensure you have a PC connected to the switch on the same network range and are able to ping the switches IP Address. You must be able to ping the IP Address of the switch to access its web management interface.

The default values of the AS Series switches are listed in the table below:

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

To connect to the web based management interface:

1. Configure your computer with a static IP address in the 192.168.1.x subnet, for example 192.168.1.10, with a subnet mask of 255.255.255.0.

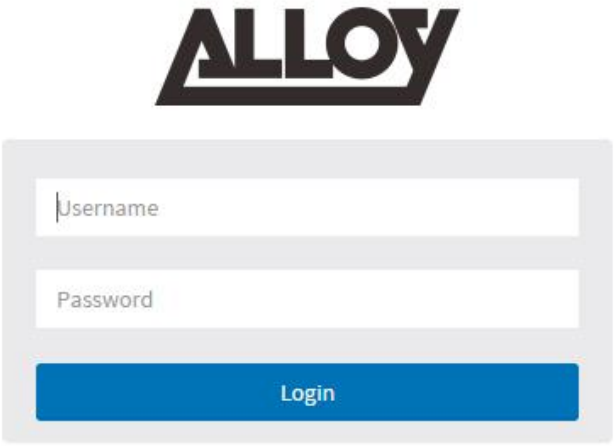
2. Connect an Ethernet cable from your computer to any port on the switch.

3. Open a web browser on your computer, for example Google Chrome.

4. Enter the default IP Address in the web browser address bar.
   The default IP Address is http://192.168.1.1
   The login screen will be displayed.

5. Enter the user name and password.
   The default admin user name is **admin** and the default password is blank. (No password)

6. Click the login button.
   The web management interface will be displayed.



NOTE: The AS series switches support management interfaces on both IPv4 and IPv6 IP Addresses.

The switch allows a total of two admin users to log into the web interface simultaneously. The admin who makes the last changes will take effect on the system.

2. Configuration

Initial Switch Configuration

Alloy suggest that the following system configuration changes should be completed before installation of your switch.

To complete initial configuration of your switch:

1. Configure your computer with a static IP address in the 192.168.1.x subnet, for example 192.168.1.10, with a subnet mask of 255.255.255.0.

2. Connect an Ethernet cable from your computer to any port on the switch.

3. Open a web browser on your computer, for example Google Chrome.

4. Enter the default IP Address in the web browser address bar.
   The default IP Address is http://192.168.1.1
   The login screen will be displayed.

5. Enter the user name and password.
   The default admin user name is **admin** and the default password is blank. (No password)

6. Click the login button.
   The web management interface will be displayed.

7. Select **Configuration > Security > Switch > Users.**

8. Click on **Admin**, enter the new admin password for the admin account into the **Password** field.
   Re-enter the same password in the **Password (again)** field.
   Click **Apply** to confirm your settings change.
   You will now be automatically logged out of the switch, please re-login with your new authentication details.

9. Select **Configuration > System > Information.**

10. Enter the **System Contact**, the name of the contact person for this switch.
    You can use a system contact up to 128 character in length. The default is blank.

11. Enter the **System Name**, the name to identify this switch.
    You can use a system name up to 128 character in length. The default is the switches model number.

12. Enter the **System Location**, the physical location of the switch.
    You can use a system location up to 128 character in length. The default is blank.
    Click **Apply** to confirm your settings change.

13. Select **Configuration > System > NTP.**

14. Change **Mode** to enabled.

15. Enter a network time server into **Server 1**.
    Example time server address, au.pool.ntp.org

16. You can enter up to 5 NTP Server addresses for redundancy.
    Click **Apply** to confirm your settings change.

System Configuration

Information

Enter the contact information of the network administrator in charge of configuring this switch.

1. Select **Configuration > System > Information.**
2. Enter the **System Contact**, the name of the contact person for this switch.
   You can use a system contact up to 128 characters in length. The default is blank.
3. Enter the **System Name**, the name to identify this switch.
   You can use a system name up to 128 characters in length. The default is the switches model number.
4. Enter the **System Location**, the physical location of the switch.
   You can use a system location up to 128 characters in length. The default is blank.
   Click **Apply** to confirm your settings change.

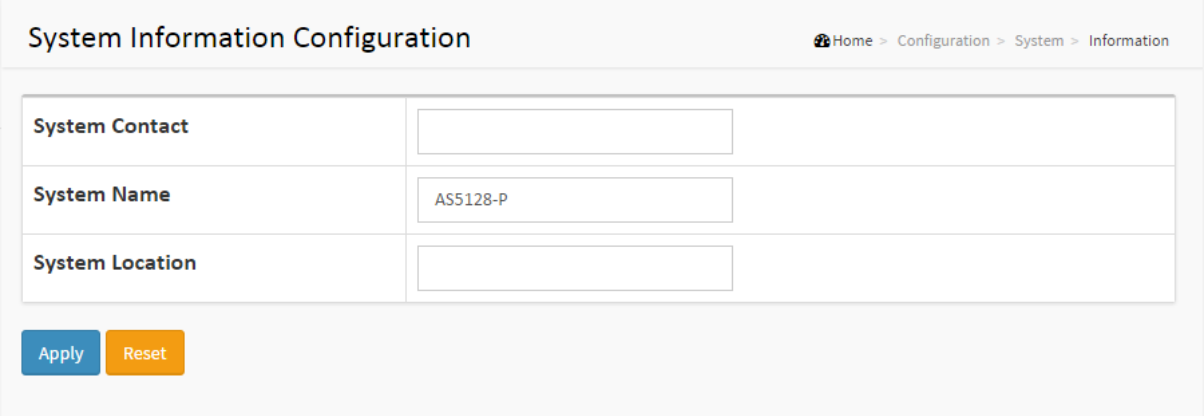


Fig. System Information

Parameter	Description
System Contact	Enter the **System Contact**, the name of the contact person for this switch. You can use a system contact up to 128 character in length. The default is blank.
System Name	Enter the System Name, the name to identify this switch. You can use a system name up to 128 characters in length. The default is the switches model number.
System Location	Enter the System Location, the physical location of the switch. You can use a system location up to 128 characters in length. The default is blank.

IP

Configure the IP Address of the switch, DNS Server settings and IP Routes.
The maximum number of interfaces supported is 128 and the maximum number of routes is 32.

Information

To configure the System IP parameters via the Web Interface:

1. Select **Configuration > System > IP.**
2. Select the required mode, **Host** or **Router**. In **Host** mode, IP traffic between interfaces will not be routed. In **Router** mode traffic is routed between all interfaces.
3. Enter how you would like the switch to obtain its DNS Server settings, when set to **Configured**, enter the appropriate DNS Server address for your network.
4. Enable or Disable the DNS proxy setting for the switch.
5. To edit default IP Address assigned to VLAN 1, tick the **Enable** checkbox under **IPv4 DHCP** to obtain an IP Address from a DHCP Server, otherwise enter an **IP Address** and the **Subnet Mask length** under the **IPv4** section. Alternatively, if you are using IPv6 IP Addressing, enter the **IPv6 Address** and **Subnet Mask Length** under the **IPv6** section.
6. If adding an additional interface click the **Add Interface** button, enter the required **VLAN ID** and enter IP Address information as in step 5.
7. When you add a new interface the IP Route for that interface will be added automatically. If you need to add an additional Static Route, click the **Add Route** button and enter the **Network Address**, **Subnet Mask Length**, **Gateway Address** and **Next Hop VLAN** parameters.
8. Click **Apply** to confirm your settings change.

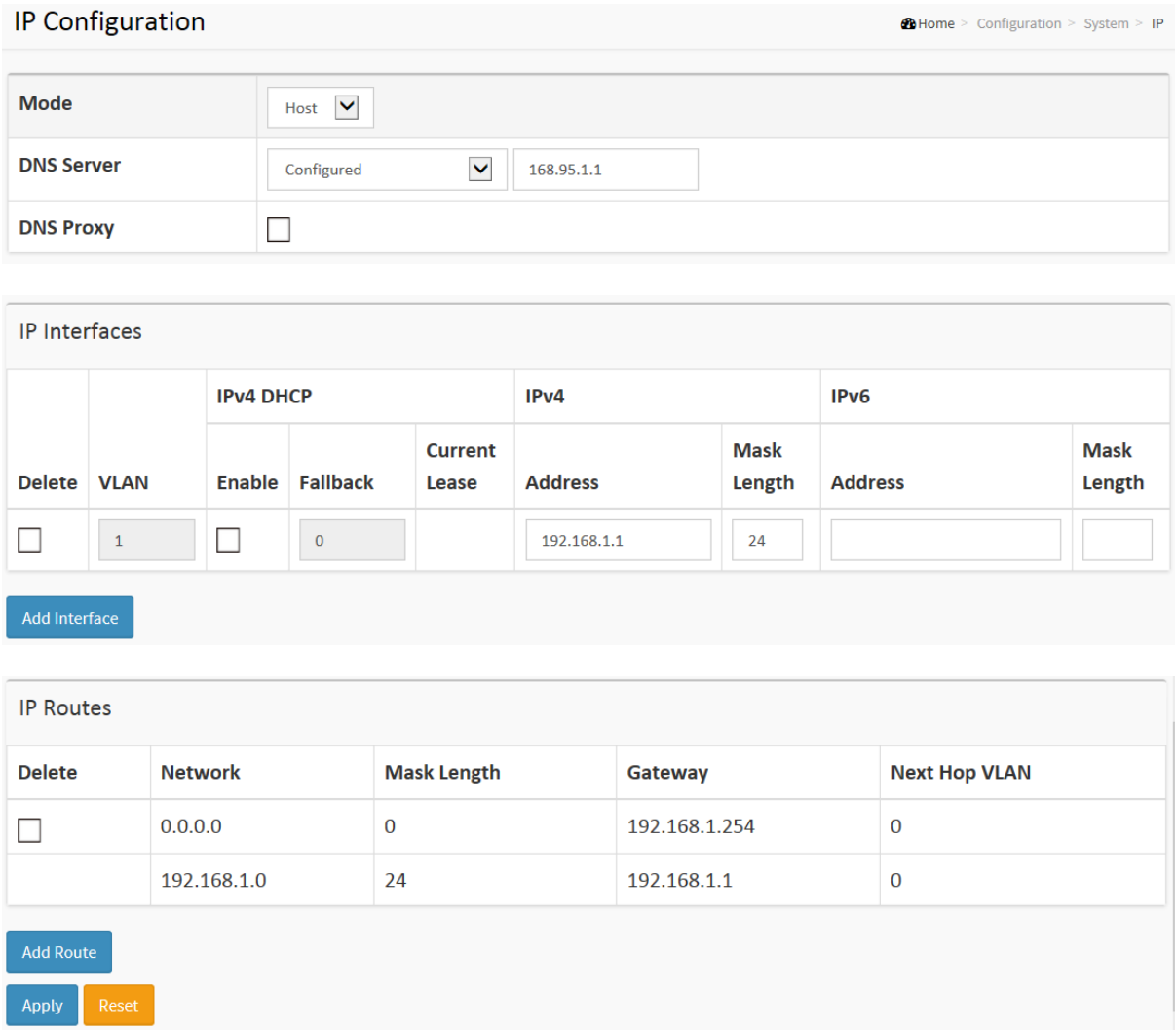


Fig. IP Configuration

Parameter	Description
IP Configuration	
Mode	Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
DNS Server	This setting controls the DNS name resolution done by the switch. The following modes are supported: • From any DHCP interfaces The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used. • No DNS server No DNS server will be used.

	• Configured Manually provide the IP address of the DNS Server in dotted decimal notation. • From this DHCP interface Specify from which DHCP-enabled interface a provided DNS server should be preferred.
DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network.
IP Interfaces	
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
IPv4 DHCP Enabled	Enable the DHCP client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IPv4 DHCP Fallback Timeout	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
IPv4 DHCP Current Lease	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv4 Mask	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.
IPv6 Address	The IPv6 address of the interface. An IPv6 address is a 128-bit record represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can

	also represent a legally valid IPv4 address. For example, ::192.1.2.34. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.
IP Routes	
Delete	Select this option to delete an existing IP route.
Network	The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.
Mask Length	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN (Only for IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.
Buttons	**Add Interface -** Click to add a new IP interface. A maximum of 8 interfaces is supported. **Add Route -** Click to add a new IP route. A maximum of 32 routes is supported. **Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

NTP

NTP (Network Time Protocol) is used to sync the time between devices on your network.
When syncing the time to your predefined time server please ensure you have configured your time zone first.
The default time zone is +8 hours.

Information

To configure the NTP parameters via the Web Interface:

1. Select **Configuration > System > NTP.**
2. From the drop down list under **Mode** select to **enable** or **disable** NTP.
3. Enter up to 5 **NTP Server** addresses. These can be local time servers on your network or internet based time server. If using an Internet based time server, please ensure the switch has access to the internet.
4. Click **Apply** to save settings and sync the time with the configured time server(s).
   Please note switch will not update time to the time server automatically, you must hit **Apply** button to re-sync.

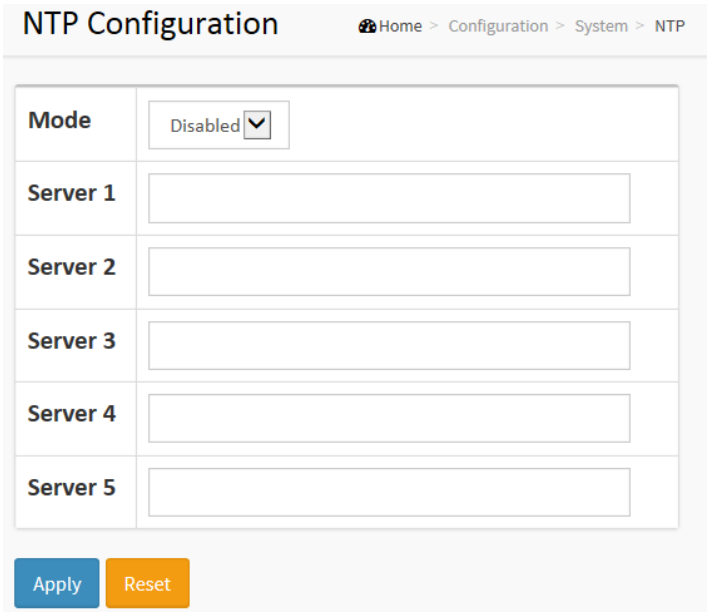


Fig. NTP Configuration

Parameter	Description
Mode	Possible modes are: Enabled: Enable NTP client mode operation.

	Disabled: Disable NTP client mode operation.
Server 1 to 5	Enter up to 5 Time Server addresses. These can be host names or IPv4 or IPv6 Addresses.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

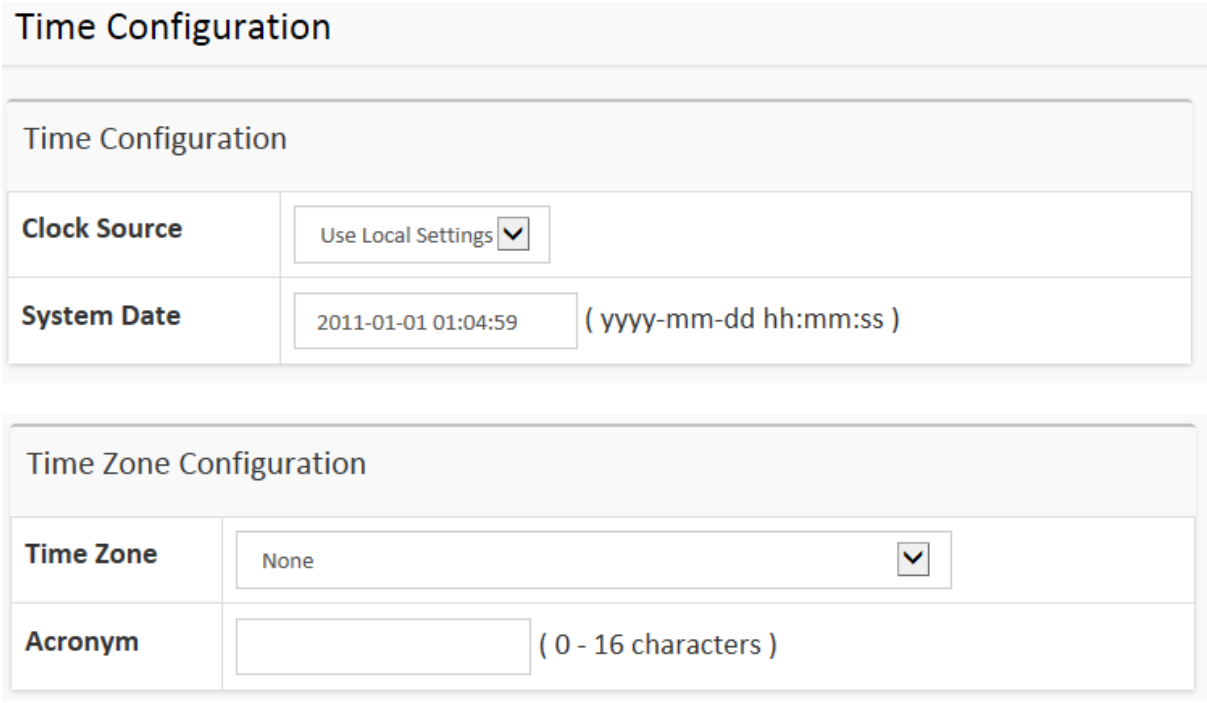
Time

The system time on the switch can be configured manually or via NTP.

Information

To configure the Time parameters via the Web Interface:

1. Select **Configuration > System > Time.**
2. Select the required Clock Source, options are **Use Local Settings** or **Use NTP Server**.
3. If **Use Local Settings** is selected enter the time and date in the **System Date** section in format yyyy-mm-dd hh:mm:ss.
4. When using Local Settings or NTP the **Time Zone Configuration** will also need to be set. Select the appropriate Time Zone for your location. Please note when using NTP please ensure the Time Zone Setting is configured correctly before syncing with a NTP Server. An optional **Acronym** can also be entered to describe the time zone being used.
5. If your location implements **Day Light Saving Time**, you can enable this and select whether or not the start and end dates and times are recurring.
6. When enabled enter the **Start** and **End** dates and times for Day light Saving.
7. Click **Apply** to confirm your settings change.



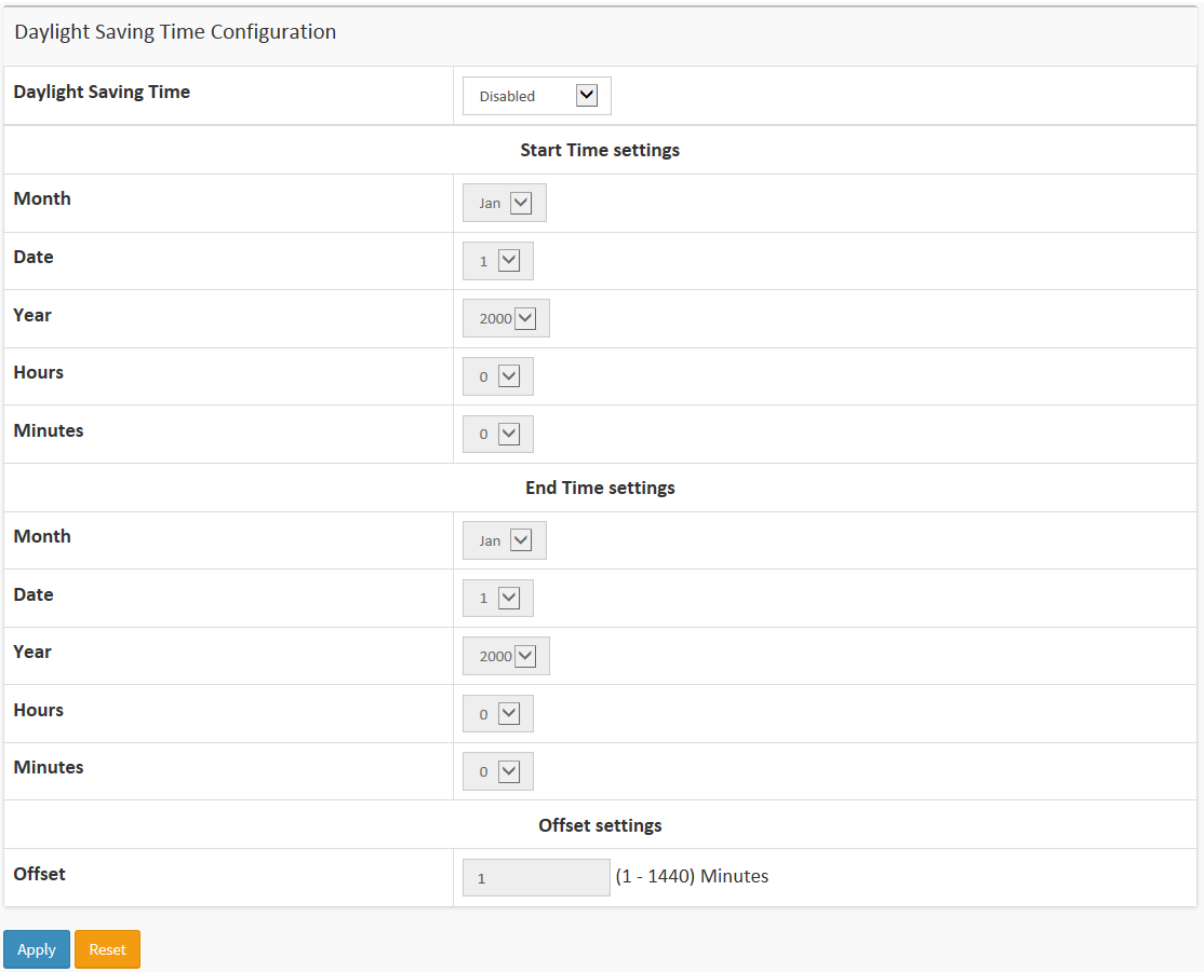


Fig. Time Configuration

Parameter	Description
Time Configuration	
Clock Source	Two modes of setting the system time are available. Use Local Time: Configure local time manually. Use NTP Server: Use NTP Server to provide system time.
System Date	Shows the current time of the system. The year of the system date is limited from 2011 to 2037.
Time Zone Configuration	
Time Zone	Lists various Time Zones worldwide. Select appropriate Time Zone for your region.
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. Limit of 16 characters.
Daylight Saving Time Configuration	
Daylight Saving	This is used to offset the time forward or back one hour during Daylight Saving

Time	Time. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for a single time configuration. Default: Disabled
Start Time Settings	Week - Select the starting week number. Day - Select the starting day. Month - Select the starting month. Hours - Select the starting hour. Minutes - Select the starting minute.
End Time Settings	Week - Select the ending week number. Day - Select the ending day. Month - Select the ending month. Hours - Select the ending hour. Minutes - Select the ending minute.
Offset Settings	Enter the number of minutes to add/remove during Daylight Saving Time. Range: 1 to 1440.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Log

The switch supports syslog, for exporting system logs to a third party logging software tool.

Information

To configure the Log Setting parameters via the Web Interface:

1. Select **Configuration > System > Log.**
2. Select to **enable** or **disable** the Syslog function from the Server Mode drop down box.
3. Enter the IP Address or FQDN of your Syslog server.
4. Click **Apply** to confirm your settings change.

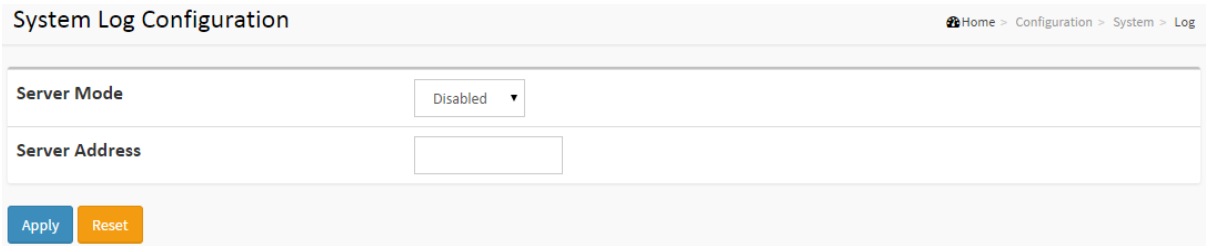


Fig. System Log Configuration

Parameter	Description
Server Mode	Select to enable or disable the Syslog function. When enabled, the syslog messages will be sent to the configured syslog server. The syslog protocol is based on UDP communication and uses UDP port 514. When enabled The syslog packet will always be sent even if the Syslog server address does not exist. Possible modes are: Enabled: Enable Syslog. Disabled: Disable Syslog.
Server Address	Enter the IPv4 IP address or host name of the syslog server.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Green Ethernet

Port Power Savings

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

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

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

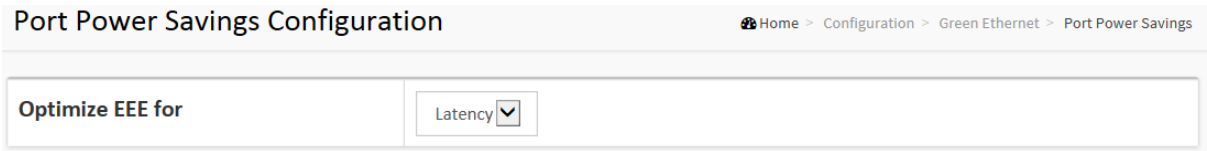
For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic.

Information

To configure the Green Ethernet Port Power Setting parameters via the Web Interface:

1. Select **Configuration > Green Ethernet > Port Power Savings.**
2. From the **Optimize EEE for** drop down box select whether to optimize power savings for **Latency** or for **Power Savings**.
3. Check the tick box next to the corresponding port to enable **ActiPHY** power savings.
4. Check the tick box next to the corresponding port to enable **PerfectReach** power savings.
5. Check the tick box next to the corresponding port to enable **EEE** power savings.
6. Click **Apply** to confirm your settings change.



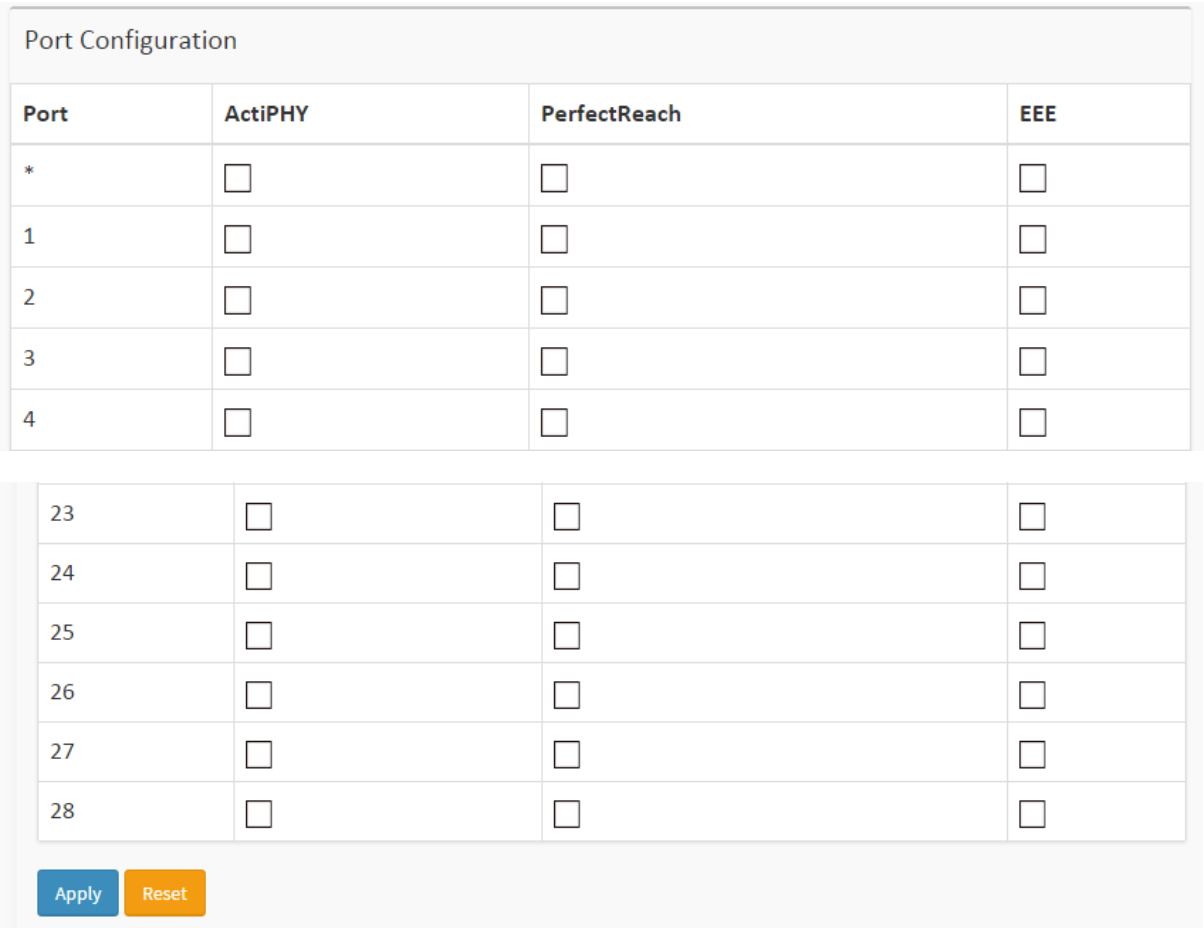


Fig. Port Power Savings Configuration

Parameter	Description
Optimize EEE for	The switch can be set to optimize EEE for either best power saving or least traffic latency.
Port	The switch port number.
ActiPHY	Tick this box to enable Link down power savings. This feature can be enabled on a per port basis. ActiPHY works by lowering the power for a port when there is no link. The port is powered up for a short moment in order to determine if cable is inserted.
PerfectReach	Tick this box to enable Cable Length power savings. This feature can be enabled on a per port basis. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
EEE	Tick this box to enable EEE power savings. This feature can be enabled on a per port basis. For maximizing power savings, the circuit isn't started when data is ready to be transmitted, instead its queued until a burst of data is ready to be transmitted. This will add some traffic latency.

Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Ports Configuration

Ports

Ports settings such disabling and enabling ports, forcing link speed and setting duplex settings as well as the current port status can be shown in this section.

Information

To configure the Port Configuration Setting parameters via the Web Interface:

1. Select **Configuration > Ports Configuration > Ports.**
2. If you are required to force the link speed of a particular port, select the speed from the drop down box under **Speed - Configured** for the appropriate port(s).
3. If Flow Control is required on a particular port check the tick box under **Flow Control – Configured** for the appropriate port(s).
4. The **Maximum Frame Size** can be selected on a per port basis. Enter the maximum frame size required.
5. If the port is receiving Excessive Collisions each port can be configured to **discard** packets or have the port **restart** backoff algorithm. These options can be selected from the drop down box under Excessive **Collision Mode**.
6. Click **Apply** to confirm your settings change.

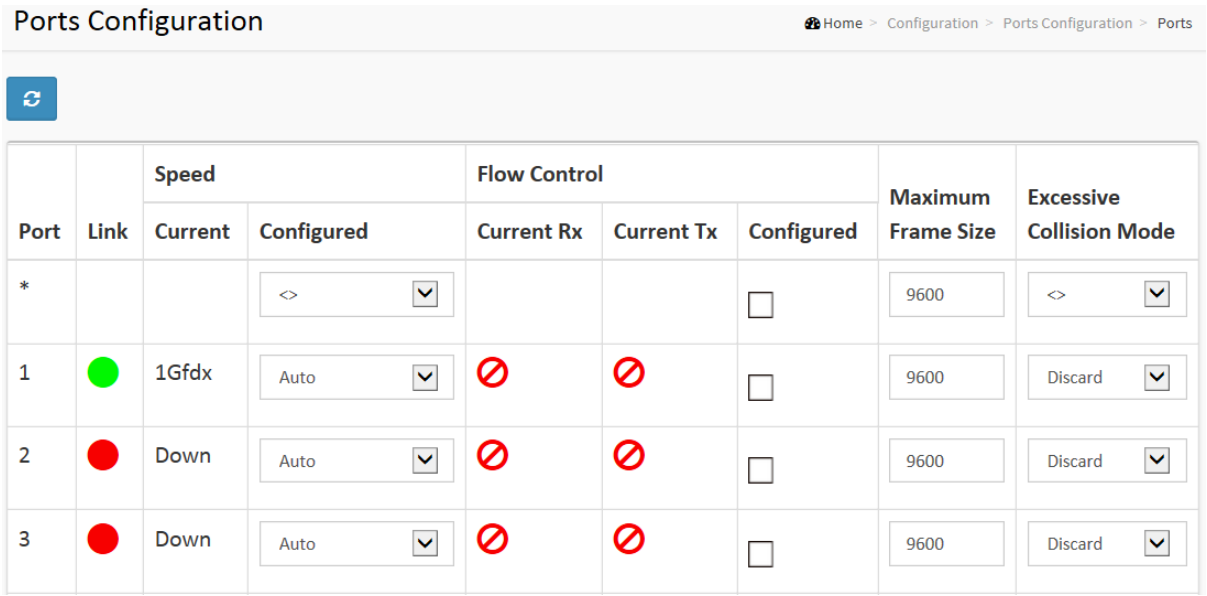


Fig. Ports Configuration

Parameter	Description
Port	The switch port number.
Link	Provides the current link status of the port. Red – Link disconnected Orange – 100Mb Link Active Green – 1Gb Link Active Blue – 10Gb Link Active
Speed - Current	Provides the current link speed of the port.
Speed - Configured	Allows you to set the speed of any given port. Only speeds supported by the port are shown. Disabled - Disables the switch port. Auto - Port will auto negotiate the speed with the link partner and will select the highest speed that is compatible with the link partner. 10Mbps HDX - Forces the port to 10Mbps half duplex mode. 10Mbps FDX - Forces the port to 10Mbps full duplex mode. 100Mbps HDX - Forces the port to 100Mbps half duplex mode. 100Mbps FDX - Forces the port to 100Mbps full duplex mode. 1Gbps FDX - Forces the port to 1Gbps full duplex SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Copper port is set in Auto mode. 100-FX - SFP port in 100-FX speed. Copper port disabled. 100-FX_AMS - Port in AMS mode. SFP port in 100-FX speed. Copper port in Auto mode.

	1000-X - SFP port in 1000-X speed. Copper port disabled. 1000-X_AMS - Port in AMS mode. SFP port in 1000-X speed. Copper port in Auto mode. Ports in AMS mode with 1000-X speed has Copper port preferred. Ports in AMS mode with 100-FX speed has fibre port preferred.
Flow Control	When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. Maximum frame size is 9600. Maximum frame size is 10056. (AS5048-P, AS5128-P & AS5152-P Only)
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart backoff algorithm after 16 collisions.
Buttons:	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.
Upper right icon	
Refresh	Used to refresh current port link status.

Port description for Switch

Allows you to add a descriptive name to individual ports.

Information

To configure the Port Description Settings via the Web Interface:

1. Select **Configuration > Ports Configuration > Ports Description.**
2. Enter a descriptive name for each port.
3. Click **Apply** to confirm your settings change.

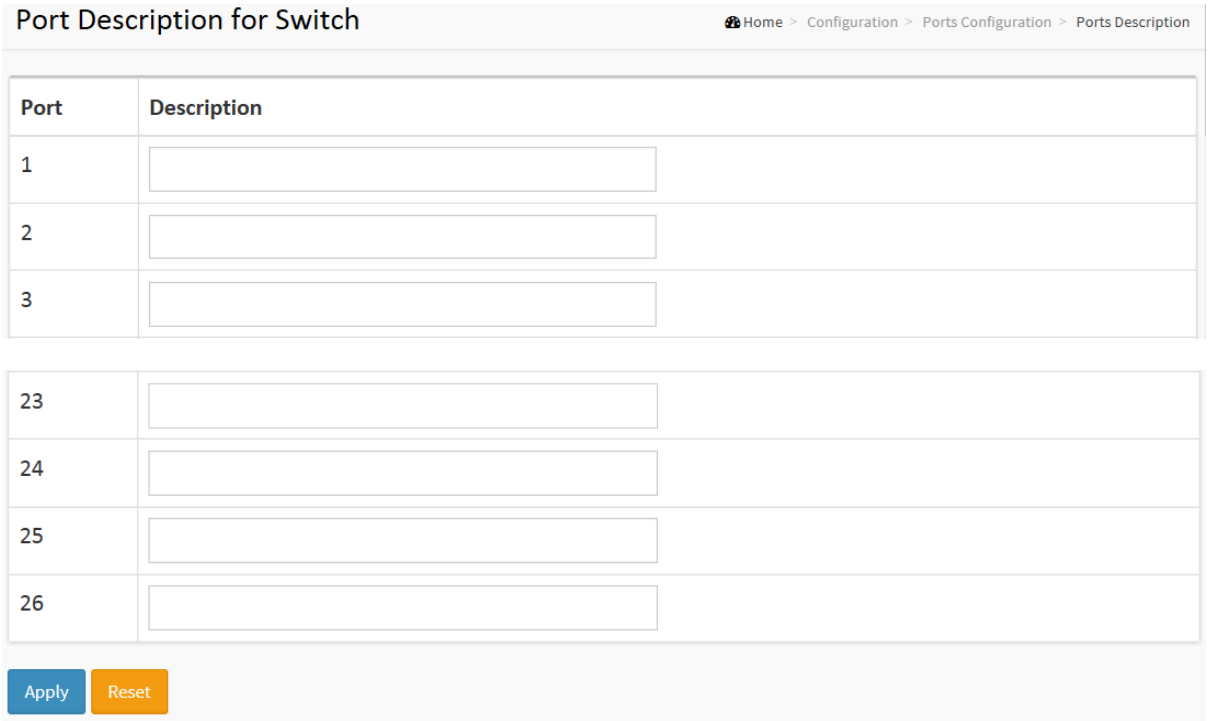


Fig. Port Description for Switch

Parameter	Description
Port	The switch port number.
Description	Enter a descriptive name in Alphanumeric characters. Maximum 47 characters.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

DHCP

Server

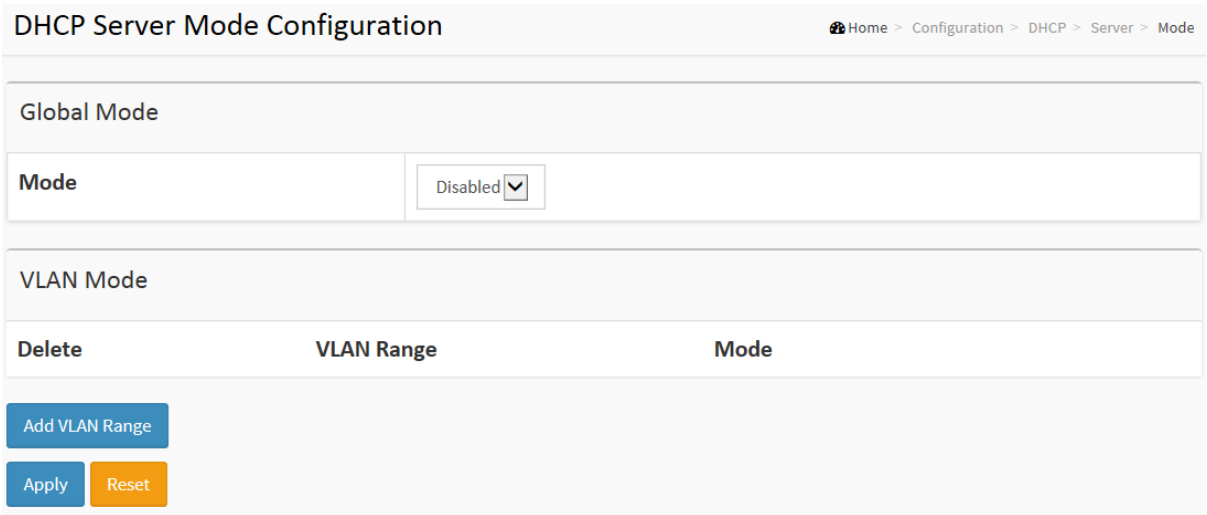
Mode

Use this section to enable or disable the DHCP Server function on the switch. You can also select whether DHCP will be enable or disable per VLAN ID.

Information

To configure the DHCP Server Setting parameters via the Web Interface:

1. Select **Configuration > DHCP > Server > Mode.**
2. Select to **enable** or **disable** DHCP Server from the **Mode** drop down box.
3. If you have multiple VLAN's on your network and you need to enable or disable the DHCP Server function per VLAN, select **Add VLAN Range**.
4. Enter the VLAN ID Range and select **enable** or **disable** from the **Mode** drop down box.
5. Click **Apply** to confirm your settings change.



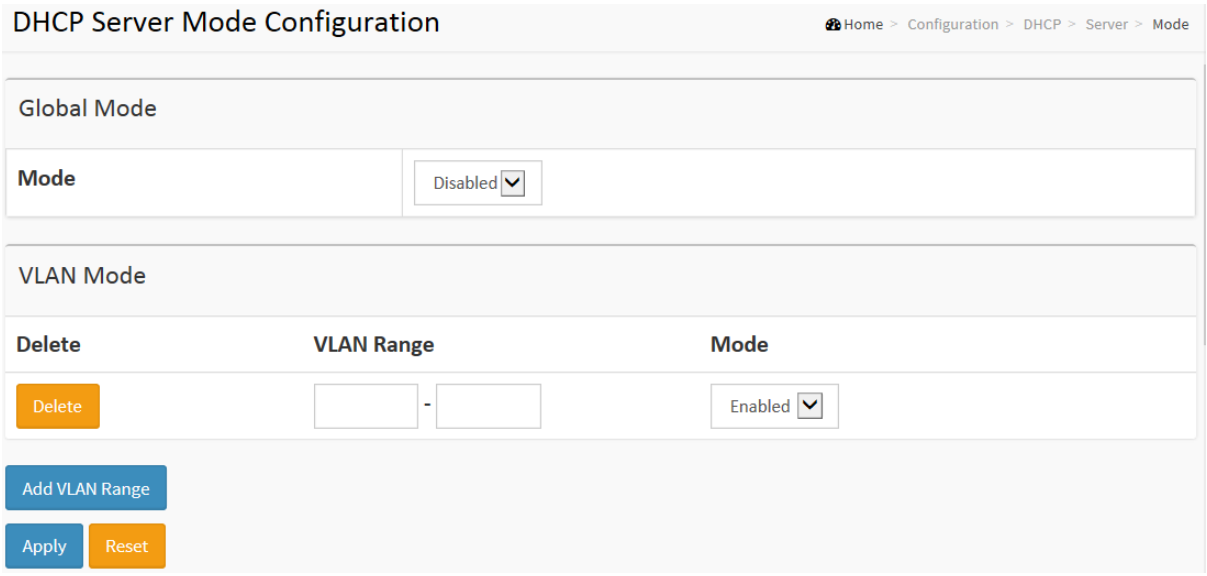


Fig. DHCP Server Mode Configuration

Parameter	Description
Mode	Used to enable or disable the DHCP Server function. Enabled: Enables DHCP Server Disabled: Disables DHCP Server
VLAN Range	Add the VLAN range that you would like to enable or disable the DHCP Server function. The first VLAN ID must be lower than the second VLAN ID. If you want to add a single VLAN enter the VLAN ID into either the first of second box.
Mode	Used to enable or disable the DHCP Server function per VLAN. Enabled: Enables DHCP Server Disabled: Disables DHCP Server
Buttons	
Add VLAN Range	Click to add new VLAN range.
Apply	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

Excluded IP

Use this section is used to exclude certain IP Addresses from your DHCP Pool. These addresses will not be issued to DHCP clients.

Information

To configure the DHCP Excluded IP Setting parameters via the Web Interface:

1. Select **Configuration > DHCP > Server > Excluded IP.**
2. Select **Add IP Range** and the required IP Address or IP Address range to exclude.
3. Click **Apply** to confirm your settings change.

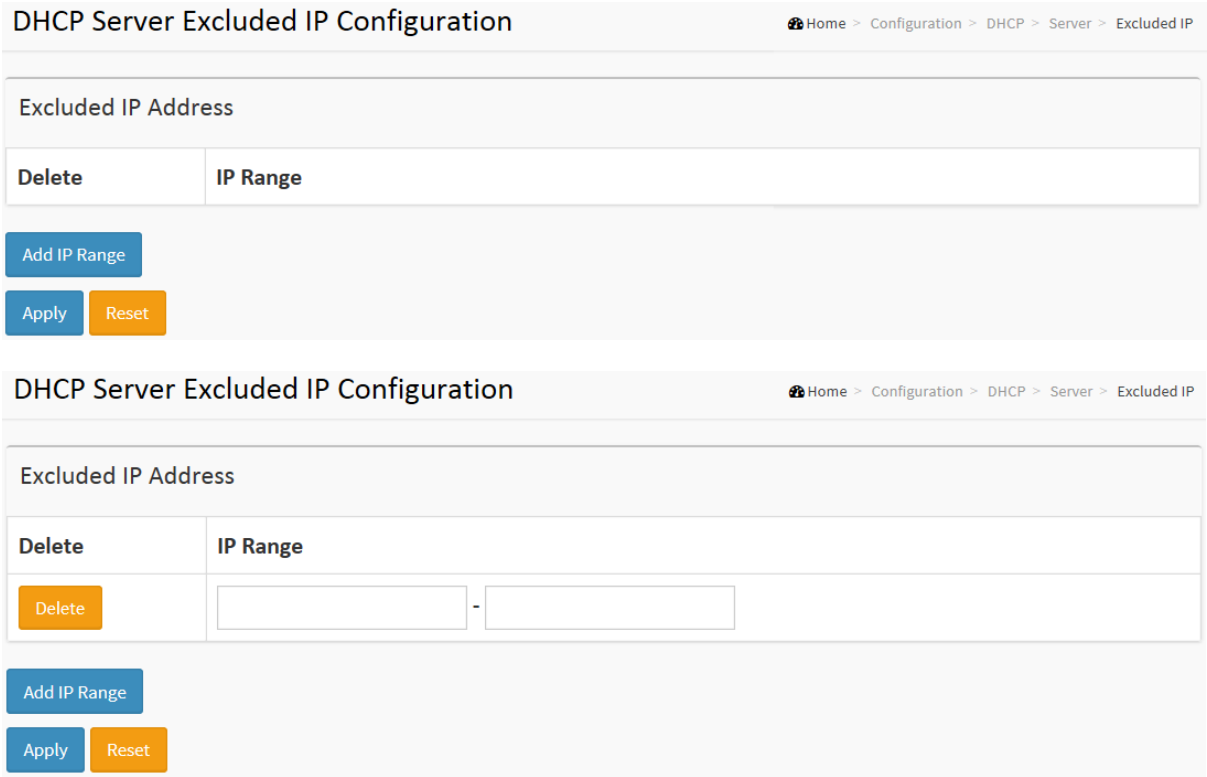


Fig. DHCP Server Excluded IP Configuration

Parameter	Description
IP Range	Defines the IP Address or IP Address range to exclude from the DHCP Server Pool.
Buttons	**Add IP Range** - Click to add new excluded IP range. **Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved

	values.

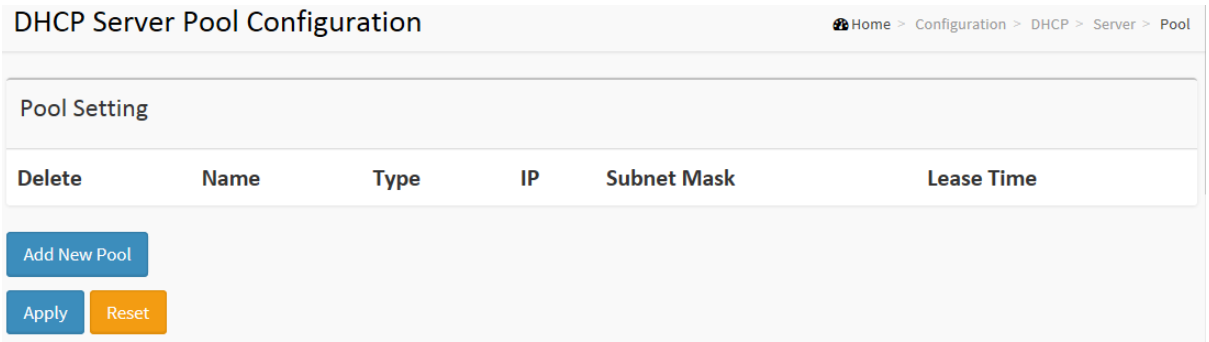
Pool

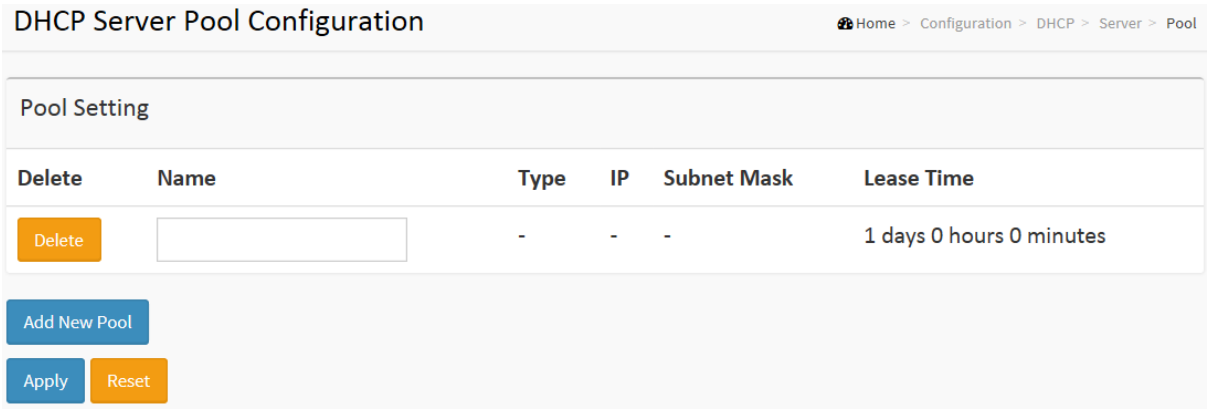
Use this section to add a DHCP pool or pools of IP Addresses to allocate to your DHCP clients.

Information

To configure the DHCP Pool Settings parameters via the Web Interface:

1. Select **Configuration > DHCP > Server > Pool.**
2. Select **Add New Pool** and enter a name for the DHCP Pool, then click **Apply**.
3. Select the type of DHCP Pool you would like to add. Options are **Host** and **Network**. Select Host for a single IP Address or Network for a complete IP Subnet.
4. Enter the required **IP Address** or Address Range and the **Subnet Mask**. E.g. 192.168.1.0, 255.255.255.0
5. Enter the required DHCP **Lease Time** in Days, hours or Minutes.
6. Complete the remaining **DHCP Options** based on your requirements.
7. Click **Apply** to confirm your settings change.





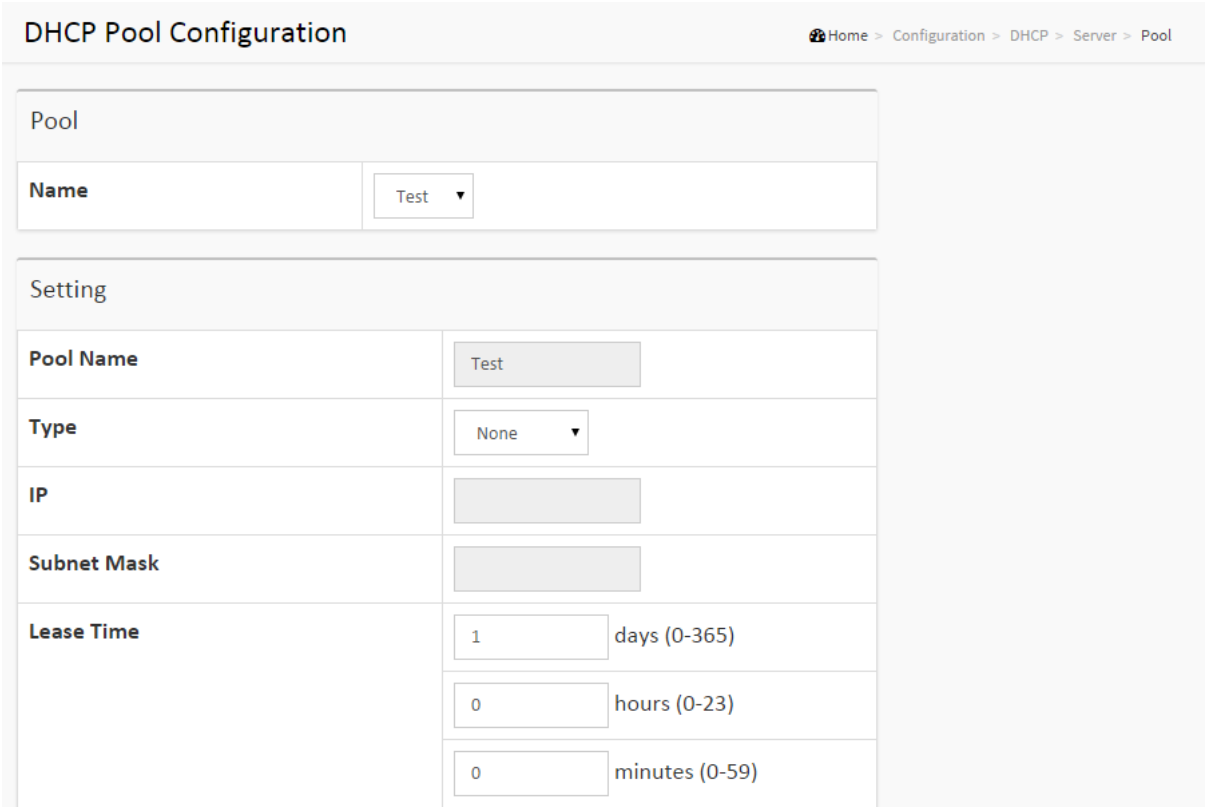


Fig. DHCP Server Pool Configuration

Parameter	Description
Pool Setting	
Delete	Tick check box next to DHCP Pool you would like to delete and click Apply button.
Name	The name of the DHCP Pool.
Type	Displays the type of DHCP Pool configured, Host or Network.
IP	IP Address of the Host or Subnet Address of the DHCP Pool.
Subnet Mask	Subnet Mask of the DHCP Pool address.
Lease Time	The current configured Lease Time for the DHCP Pool.
Add New Pool	
Name	The descriptive name of the DHCP Pool.
DHCP Pool Settings	
Name	Select the name of the DHCP Pool from the drop box that you would like to change settings for.

Pool Name	The name of the current pool you are configuring.
Type	Host or Network. Select Host for a single IP Address or Network for a complete IP Subnet.
IP	The IP Address or IP Subnet Address for the DHCP Pool. E.g. 192.168.0.0
Subnet Mask	The Subnet Mask for the DHCP Pool. E.g. 255.255.255.0
Lease Time	The amount of time that the IP Address will be held by the DHCP Client. Time can be set in Days, Hours and/or Minutes.
Domain Name	The domain name that will be included with the DHCP Settings provided to the DHCP client. E.g. alloy.com.au
Broadcast Address	The broadcast address of the IP Address Subnet that will be included with the DHCP Settings provided to the DHCP client. E.g. 192.168.0.255
Default Router	The Default Route or Default Gateway that will be included with the DHCP Settings provided to the DHCP client. E.g. 192.168.0.254
DNS Server	The DNS Server Address(es) that will be included with the DHCP Settings provided to the DHCP client.
TFTP Server	An optional DHCP Server option that provides a TFTP Server address to the DHCP client. This could be used to provide a configuration server address for an IP Phone to download its provisioning file.
Boot File	An optional DHCP Server option that provides a Boot File to the DHCP client. This could be used to provide the name of a configuration file for an IP Phone to download its provisioning file.
NTP Server	An optional DHCP Server option that provides a NTP Server Address to the DHCP client. E.g. au.pool.ntp.org
NetBIOS Node Type	An optional DHCP Server option that provides a NetBIOS Node Type to the DHCP client. NetBIOS provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network. Options are None, B-node, P-node, M-node and H-node. B-node: Broadcast P-node: Peer (WINS only) M-node: Mixed (Broadcast then WINS) H-node: Hybrid (WINS, then Broadcast)
NetBIOS Scope	An optional DHCP Server option that provides a NetBIOS Scope to the DHCP client. The Scope ID is a character string which is appended to the NetBIOS name for all NetBIOS over TCP/IP communications. It provides a method to isolate a collection of computers that only communicate with each other.
NetBIOS Name	An optional DHCP Server option that provides a NetBIOS Name Server to the

Server	DHCP client.
NIS Domain Name	An optional DHCP Server option that provides a NIS Domain Name to the DHCP client. Network Information System (NIS) is designed to centralize administration of UNIX®-like systems such as Solaris™, HP-UX, AIX®, Linux, NetBSD, OpenBSD, and FreeBSD.
NIS Server	An optional DHCP Server option that provides a NIS Server Address to the DHCP client.
Client Identifier	An optional DHCP Server option that provides a Client Identifier to the DHCP client.
Hardware Address	An optional DHCP Server option that provides a Hardware Address to the DHCP client.
Client Name	An optional DHCP Server option that provides a Client Name to the DHCP client.
Vendor 1 – 8 Class Identifier	DHCP Option 60 can be used to send vendor specific options to granularly control configuration. Enter the vendor ID here to identify the vendor products you want to send specific information to.
Vendor 1 – 8 Specific Information	DHCP Option 43 is used to send particular configuration options to a specific vendor's product. Enter the required information here.
Buttons	**Add New Pool:** Click to add new DHCP Pool. **Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Snooping

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients.

Information

To configure the DCHP Snooping parameters via the Web Interface:

1. Select **Configuration > DHCP > Snooping.**
2. **Enable** or **Disable** DHCP Snooping from the **Snooping Mode** drop down box.
3. Each port can be configured as **Trusted** or **Untrusted**. Set to trusted when you have a DHCP Server connected to that port. Set all other ports to untrusted.
4. Click **Apply** to confirm your settings change.

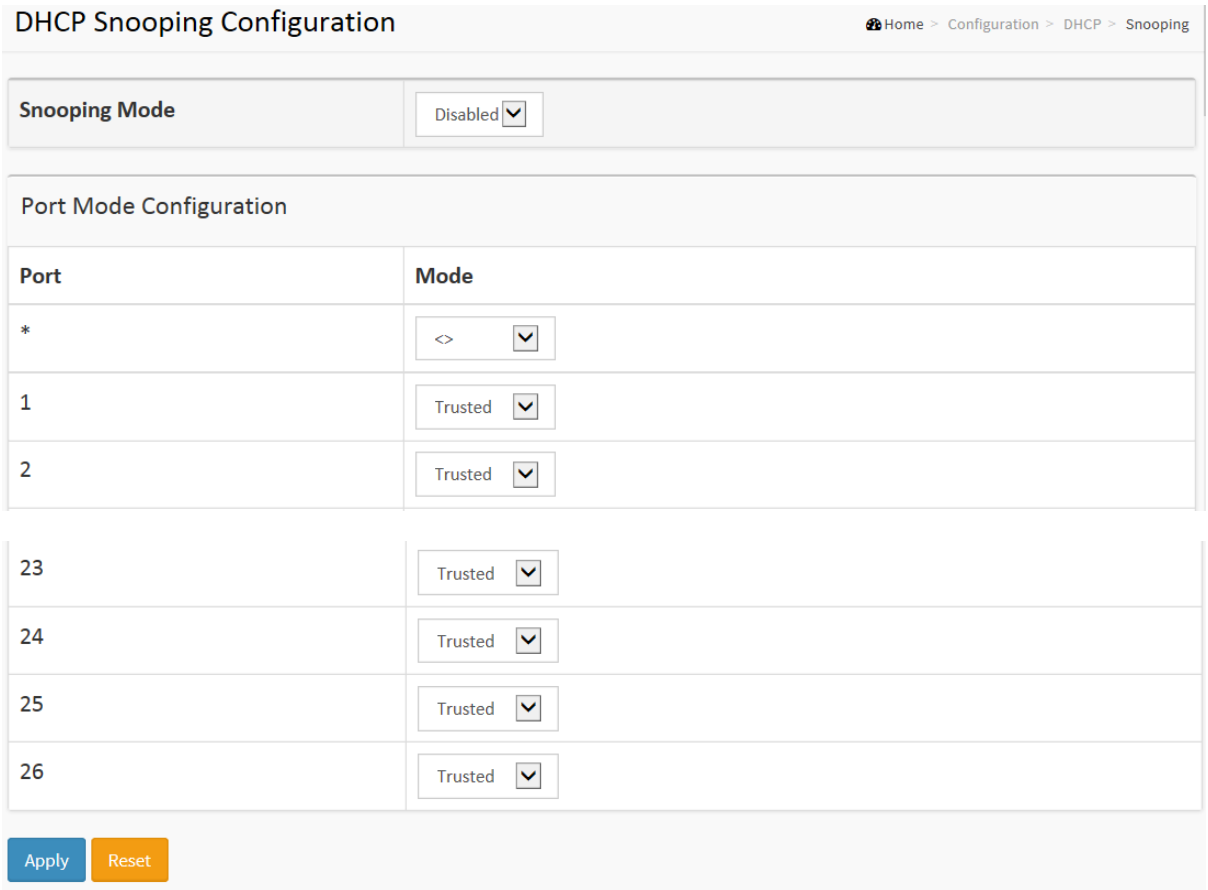


Fig. DHCP Snooping Configuration

Parameter	Description
Snooping Mode	Used to enable or disable DHCP Snooping on the switch. Enabled: Enable DHCP snooping. When DHCP snooping is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. Disabled: Disable DHCP snooping.
Port Mode Configuration	
Port	The switch port number.
Mode	Used to set trusted or untrusted mode of the switch. Trusted: Configures the port as a trusted source of DHCP messages. Untrusted: Configures the port as an untrusted source of DHCP messages.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet.

Information

To configure the DHCP Relay parameters via the Web Interface:

1. Select **Configuration > DHCP > Relay.**
2. Select to **enable** or **disable** the **DHCP Relay** function.
3. Enter the **Relay Server** IP Address.
4. Select to **enable** or **disable** the **Relay Information Mode**.
5. Select to either **Keep**, **Drop** or **Replace** the **DHCP Relay Information**.
6. Click **Apply** to confirm your settings change.

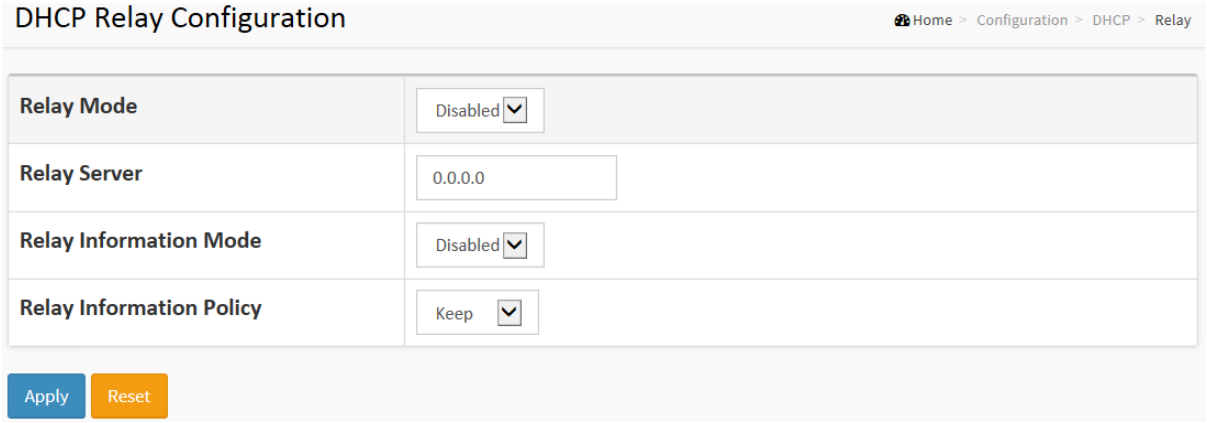


Fig. DHCP Relay Configuration

Parameter	Description
Relay Mode	Used to enable or disable the DHCP Relay function on the switch. Enabled: Enable DHCP relay. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. Disabled: Disable DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address.

Relay Information Mode	Used to enable or disable the DHCP Relay information function on the switch. Enabled: Enable DHCP relay information. When DHCP relay information is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to the DHCP client. It only works when DHCP relay operation mode is enabled. Disabled: Disable DHCP relay information mode operation.
Relay Information Policy	When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are: Replace: Replace the original relay information when a DHCP message that already contains it is received. Keep: Keep the original relay information when a DHCP message that already contains it is received. Drop: Drop the package when a DHCP message that already contains relay information is received.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Security

Switch

Users

Use this section to create additional users who will have access to the management of the switch. The privilege levels for these users can also be set here.

Information

Configure the Users security levels of the AS Switch under this section.

1. Select **Configuration > Security > Switch > Users.**
2. Click **Add New User** button to add additional user.
3. Enter the **Username** and the **Password** into the spaces provided.
4. Set the appropriate **Privilege Level** for the user from the drop down box.
5. Click **Apply** to confirm your settings change.

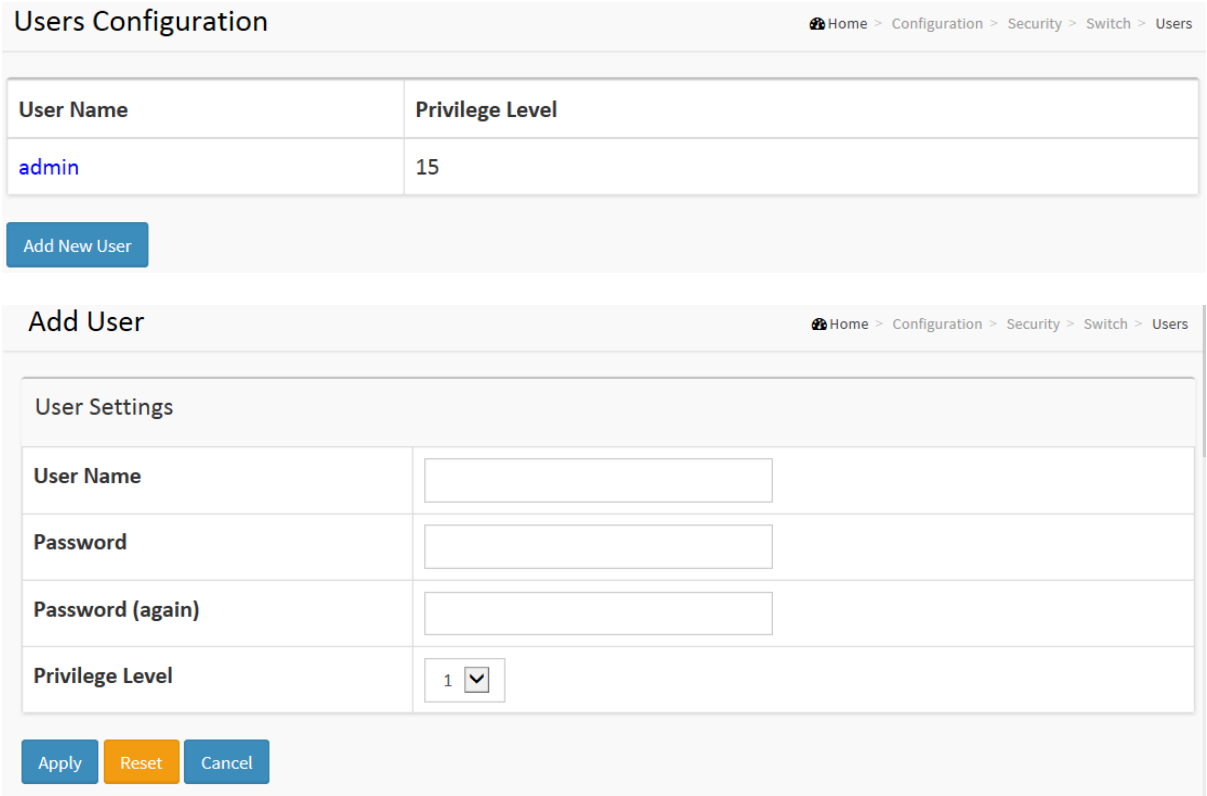


Fig. Users Configuration

Parameter	Description
Username	The name identifying the user. This is also a link to Add/Edit User.
Password	The password for the new user. Password length is 0 to 255 characters and only ASCII characters from 32 to 126 are allowed.
Password (again)	Repeat the same password as you entered in the Password field.
Privilege Level	Used to set the privilege level of the user. Privilege levels range from 1 to 15. Each privilege level can be configured in the **Configuration > Security > Switch > Privilege Levels** section. Standard privilege levels are as follows: Privilege Level 5: Read Only Access (Guest Account) Privilege Level 10: Read/Write Access (Standard User) Privilege Level 15: Read/Write and System Maintenance Access (Administrator)
Buttons	**Add New User:** Click to add New User. **Delete User**: Click to Delete the current user. **Cancel:** Click to undo any changes made locally and return to the Users section. **Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Privilege Levels

This section is used to assign privileges to particular functions of the switch.

Information

To configure the Security Privilege Level parameters via the Web Interface:

1. Select **Configuration > Security > Switch > Privilege Levels.**
2. Specify each of the **Privilege Levels** assigned to the particular switch function. Privilege levels can be configured from 1 through to 15.
   If you assign privilege level 5 to Configuration Read-only on switch function VLAN's, then any user that has a privilege set to 5 will have Read-only access to the VLAN functions of the switch.
3. Click **Apply** to confirm your settings change.

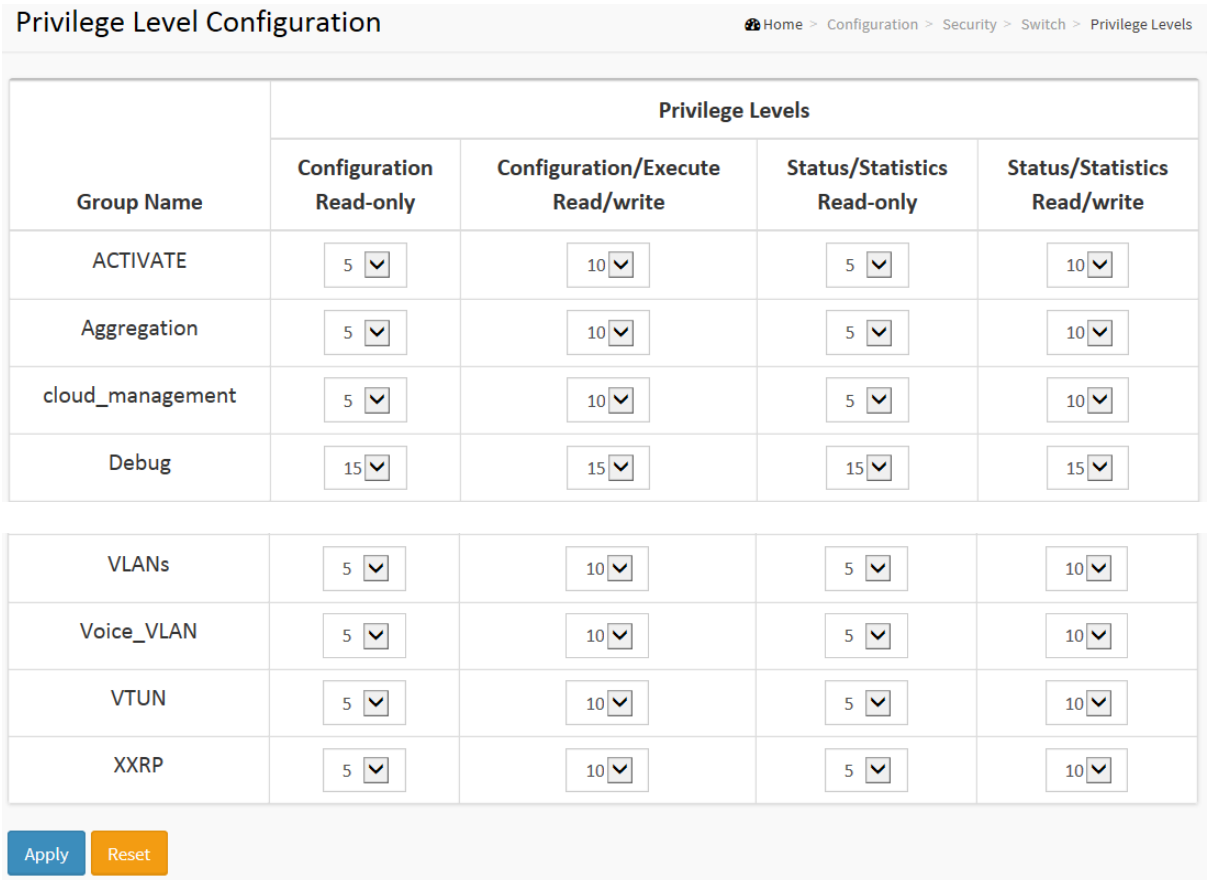


Fig. Privilege Level Configuration

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

	them contain more than one. The following description defines these privilege level groups in detail: System: Contact, Name, Location, Timezone, Daylight Saving Time, Log. Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard. IP: Everything except 'ping'. Port: Everything except 'VeriPHY'. Diagnostics: 'ping' and 'VeriPHY'. Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance. Debug: Only present in CLI.
Privilege Levels	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 User Privileges should be the same or greater than the authorization Privilege level to have the access to that group.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Auth Method

This section is used to set the authentication method for all configuration access types. Here you can set how the user is authenticated for Console, Telnet, SSH, HTTP or HTTPS access.

Information

To configure the Security Auth Method parameters via the Web Interface:

1. Select **Configuration > Security > Switch > Auth Method.**
2. Next to the corresponding configuration type select the authentication method you require. Options are No, Local, Radius and TACACS. Each configuration method can have two alternative methods for authentication in the case that initial method fails.
3. Select each alternative authentication method if required.
4. If you need to change the default port for the configuration method this can be done in the **Service Port** section.
5. Click **Apply** to confirm your settings change.

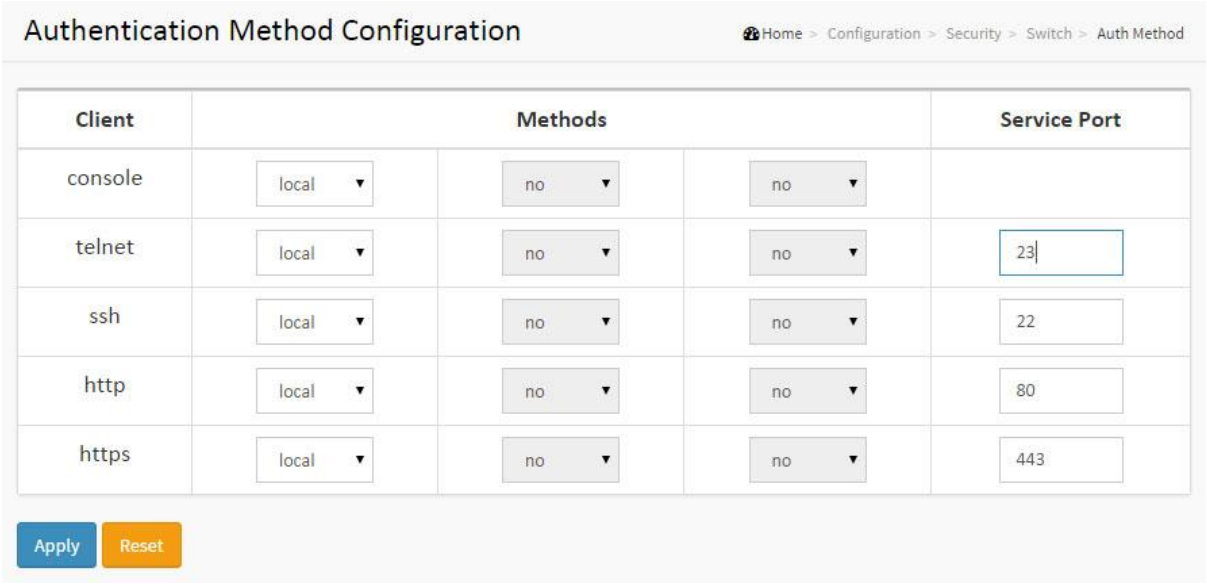


Fig. Authentication Method Configuration

Parameter	Description
Client	The management client for which you will select your authentication method. Management Client options are Console, Telnet, SSH, HTTP and HTTPS.
Methods	The authentication method you require for each management client type. Each configuration method can have two alternative methods for authentication in the case that initial method fails. Options are: No: 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.
Service Port	This allows you to change the default port number used by each of the management options. For example if you want to change the default port number of SSH from 22 to 2222, this can be done here.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

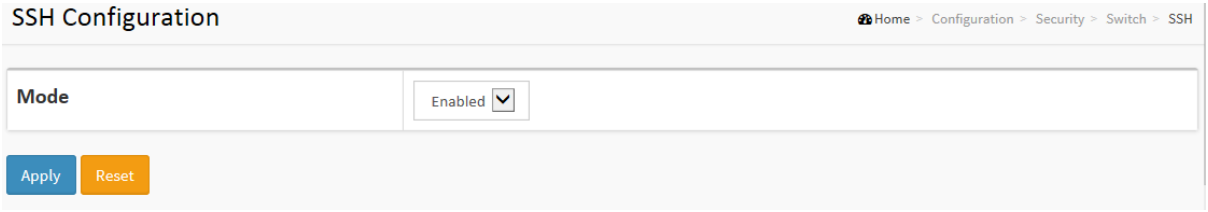
SSH

This section is used to enable or disable the SSH management option. SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Information

To configure the Security SSH parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SSH.**
2. From the drop down box select to **enable** or **disable** the SSH function.
3. Click **Apply** to confirm your settings change.



Parameter	Description
Mode	Used to enable or disable the SSH function.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

HTTPS

This section is used to enable or disable the HTTPS management option. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

Information

To configure the Security HTTPS Level parameters via the Web Interface:

1. Select **Configuration > Security > Switch > HTTPS.**
2. From the drop down box select to **enable** or **disable** the HTTPS function.
3. Select to enable or disable the **Automatic Redirect** function, which will automatically redirect a HTTP request to HTTPS.
4. Click **Apply** to confirm your settings change.

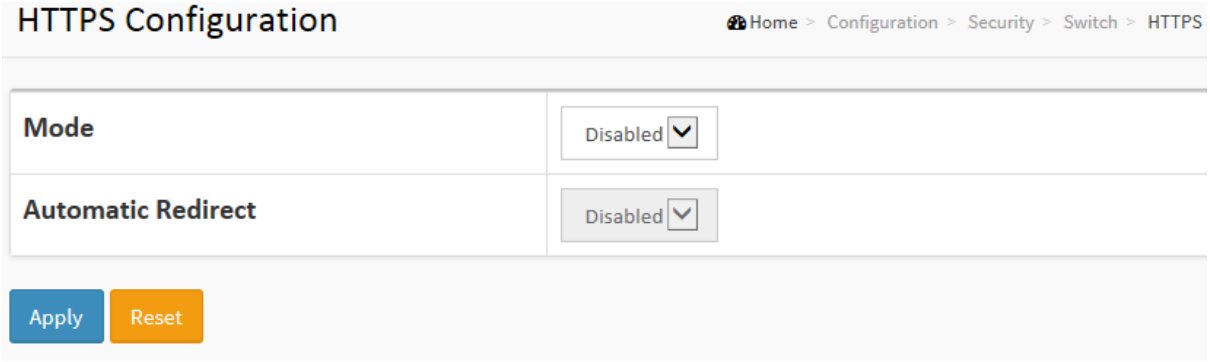


Fig. HTTPS Configuration

Parameter	Description
Mode	Used to enable or disable the HTTPS function.
Automatic Redirect	Used to enable or disable the Automatic Redirect function, which will automatically redirect a HTTP request to HTTPS.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Access Management

This section is used to limit who can access the management interfaces of the switch. This is set via IP Address or IP Address range and can be restricted based on the type of connection, including HTTP/HTTPS, SNMP and Telnet/SSH.

Information

To configure the Security Access Management parameters via the Web Interface:

1. Select **Configuration > Security > Switch > Access Management.**
2. From the drop down box select to enable or disable the **Access Management** function.
3. Click on **Add New Entry** button to allow access to a single IP or an entire IP range.
4. Enter required information including **VLAN ID**, start and ending **IP Address**.
5. Select the type of management access you would like to grant/limit access to.
6. Click **Apply** to confirm your settings change.

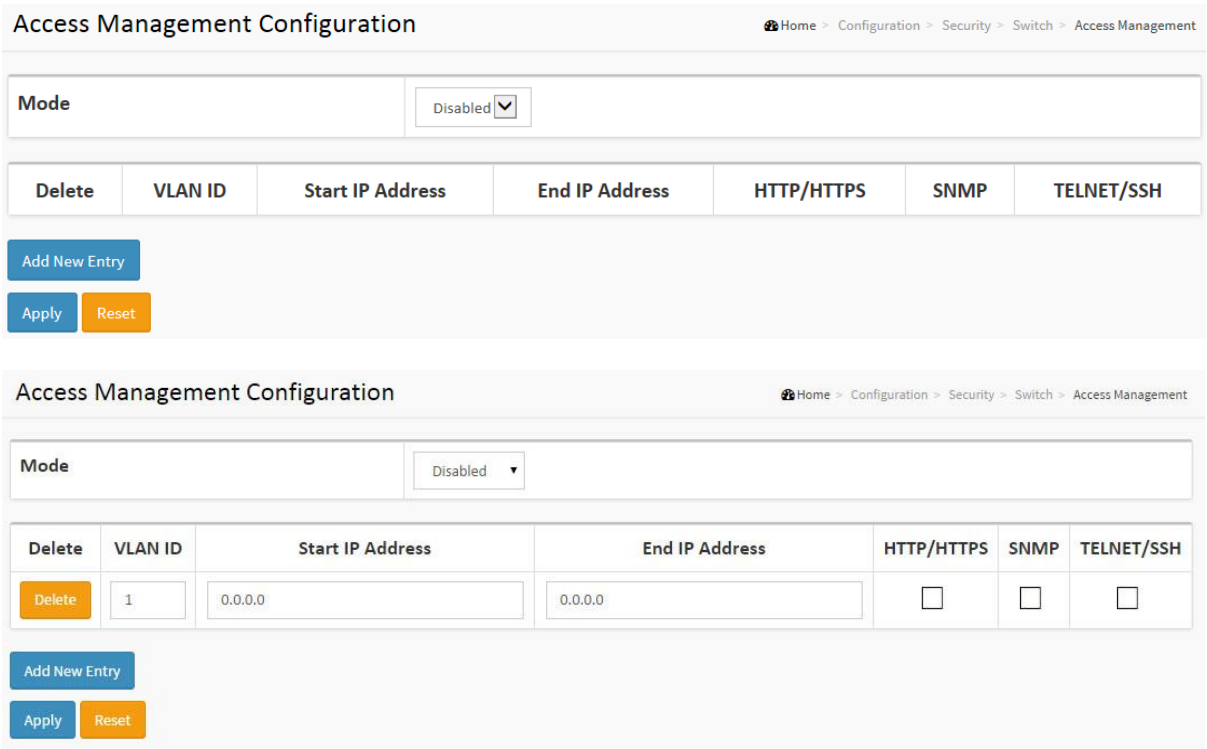


Fig. Access Management Configuration

Parameter	Description
Mode	Used to enable or disable the Access Management function.
VLAN ID	Enter the required VLAN ID that will have access to the management.

Start IP Address	Enter the IP Address that will have access to the management.
End IP Address	If allowing an IP Address range, enter the last IP Address in the range that will have access to the management.
HTTP/HTTPS	Check this box to allow access to the HTTP/HTTPS management.
SNMP	Check this box to allow access to the SNMP management.
Telnet/SSH	Check this box to allow access to the Telnet/SSH management.
Add New Entry	Click to add a new access management entry.
Delete	Click to Delete the currently configured Access Management entry.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage a Managed device equipped with a SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax.

System

This section describes how to configure SNMP on the switch. This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name.

Information

To configure the SNMP Security parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > System.**
2. From the drop down box select to enable or disable the **SNMP** function.
3. Select the required **SNMP version** that your system supports.
4. Enter your configured **Read** and **Write Community** names in the spaces provided.
5. Click **Apply** to confirm your settings change.

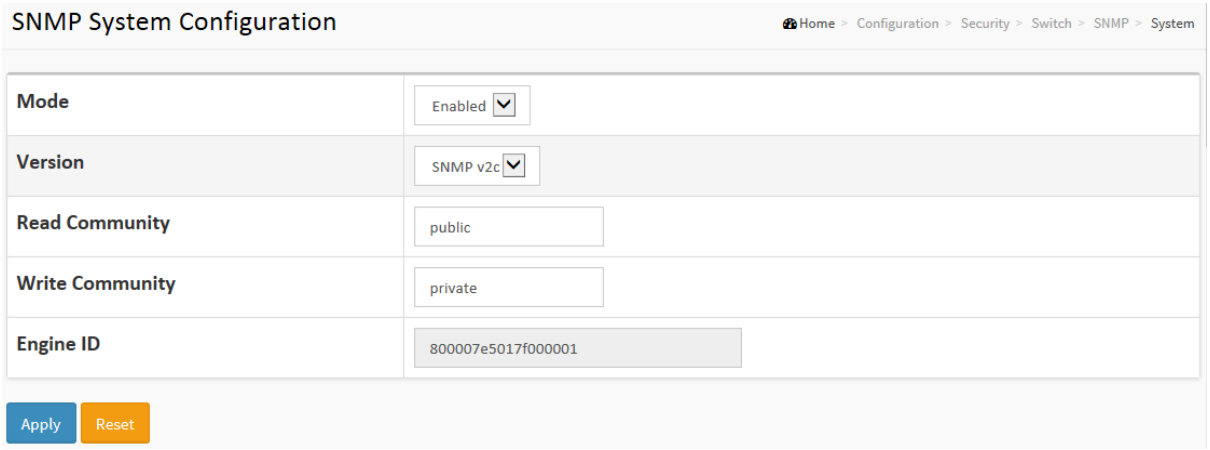


Fig. SNMP System Configuration

Parameter	Description
Mode	Used to enable or disable the SNMP function.
Version	Indicates the SNMP version supported. Possible versions are: SNMP v1: Set SNMP supported version 1. SNMP v2c: Set SNMP supported version 2c. SNMP v3: Set SNMP supported version 3.
Read Community	Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. This field is only applicable when SNMP version is SNMPv1 or SNMPv2c is used. If using SNMP version 3, the community string will be associated with the

	SNMPv3 communities table. It provides more flexibility than a SNMPv1 or SNMPv2c community string. In addition to the community string, a particular range of source addresses can be used to restrict source subnet.
Write Community	Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. This field is only applicable when SNMP version is SNMPv1 or SNMPv2c is used. If using SNMP version 3, the community string will be associated with the SNMPv3 communities table. It provides more flexibility than a SNMPv1 or SNMPv2c community string. In addition to the community string, a particular range of source addresses can be used to restrict source subnet.
Engin ID	Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

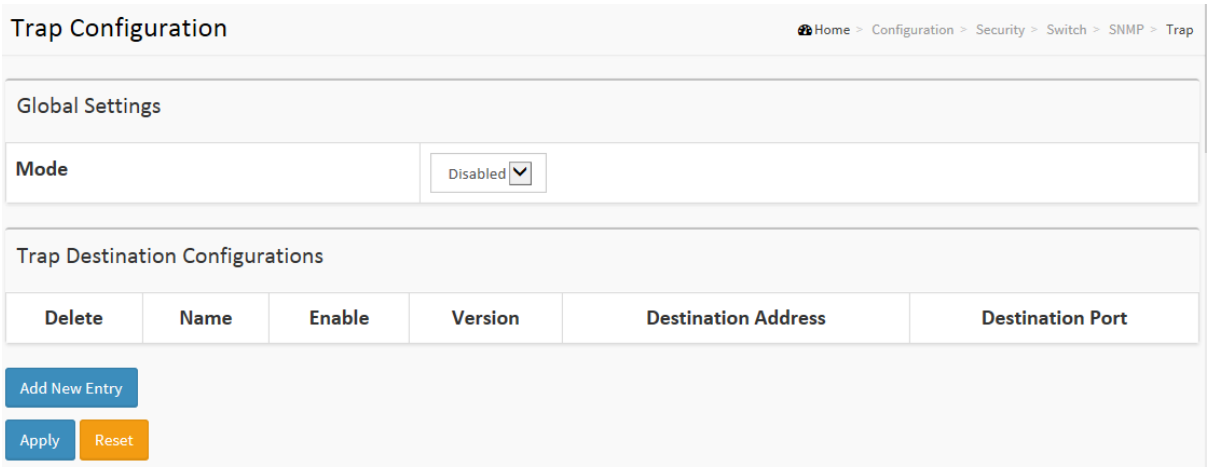
Trap

SNMP Traps are used to alert administrators when certain events have occurred. This section is used to create Trap Destinations/Managers, all configured SNMP trap event alerts will be sent to the Trap Destinations.

Information

To configure the SNMP Trap parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Trap.**
2. Click **Add New Entry** to create a new SNMP Trap on the switch.
3. Give the Trap a name in the **Trap Config Name** field.
4. Select to enable of disable the trap from the **Trap Mode** drop down box.
5. Select the required SNMP version you are using from the **Trap Version** drop down box.
6. Enter the **Trap Community Name**, **Trap Destination Address** and **Trap Destination Port** in the fields provided.
7. Select to enable or disable the **Trap Inform Mode** and enter the **Trap Inform Timeout** and **Trap Inform Retry Times** in the fields provided.
8. Enable or Disable the **Trap Probe Security Engine ID**, enter the **Trap Security Engine ID** and select the **Trap Security Name** from the fields provided. These options are only available when using SNMPv3.
9. Click **Apply** to confirm your settings change.



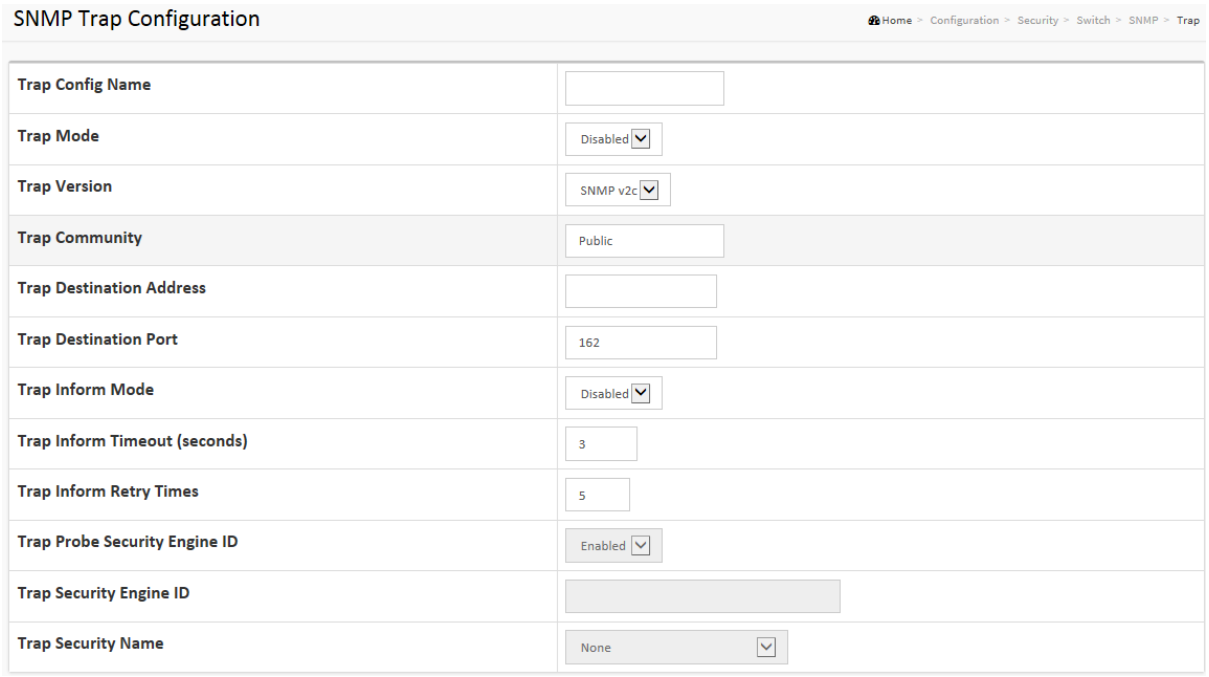


Fig. SNMP Trap Configuration

Parameter	Description
Mode	Used to enable or disable the SNMP Traps.
Trap Config Name	The Trap Configuration Name. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.
Trap Mode	Used to enable or disable the Trap Destination.
Trap Version	Select the required SNMP version required for your infrastructure. Possible versions are: SNMPv1: Set SNMP trap to version 1. SNMPv2c: Set SNMP trap to version 2c. SNMPv3: Set SNMP trap to version 3.
Trap Community	Indicates the community access string used when sending SNMP trap packets. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
Destination Address	The SNMP Trap destination address. Allows IPv4 and IPv6 IP Addresses as well as valid host names.
Destination Port	Indicates the SNMP trap destination port. The SNMP Agent will send SNMP messages via this port, the port range is 1~65535. Default Port is 162.
Trap Inform Mode	Used to enable or disable the Trap Inform Mode.
Trap Inform Timeout	The SNMP trap inform timeout.

(seconds)	The allowed range is 0 to 2147 seconds.
Trap Inform Retry Times	The SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps using USM for authentication and privacy. A unique engine ID for these traps is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps using USM for authentication and privacy. A unique security name is needed when traps are enabled.
Add New Entry	Click to add a new Trap Destination.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Communities

This function is used to configure SNMPv3 communities.

Information

To configure the SNMP Community parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Communities.**
2. If using the default public and private community names enter the required **Source IP Address** and **Subnet Mask**.
3. Alternatively click **Add New Entry** to add a new community name, along with required **Source IP Address** and **Subnet Mask**.
4. Click **Apply** to confirm your settings change.

Fig. SNMPv3 Community Configuration

Parameter	Description
Delete	Tick the check box next to the entry you want to delete and click the Apply button.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as the security name and map to a SNMPv1 or SNMPv2c community string.
Source IP	The SNMP access Source Address. This can be used in conjunction with the Source Mask to limit where SNMP information is sent and received from. It can be limited to a single IP Address or an entire subnet.
Source Mask	Indicates the SNMP access source address mask.
Add New Entry	Click to add a new SNMPv3 Community string.
Buttons	**Apply** – Click to save changes.

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

Users

This function is used to configure SNMPv3 Users.

Information

To configure the SNMP User parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Users.**
2. Click **Add New Entry**.
3. Enter the appropriate **Engine ID** and **User Name**.
4. Select the required **Security level**, Authentication and Privacy, Authentication and No Privacy or No Authentication and No Privacy.
5. If using Authentication, select the required **Authentication Protocol** and enter a password.
6. If using Privacy, select the required **Privacy Protocol** and enter a password.
7. Click **Apply** to confirm your settings change.

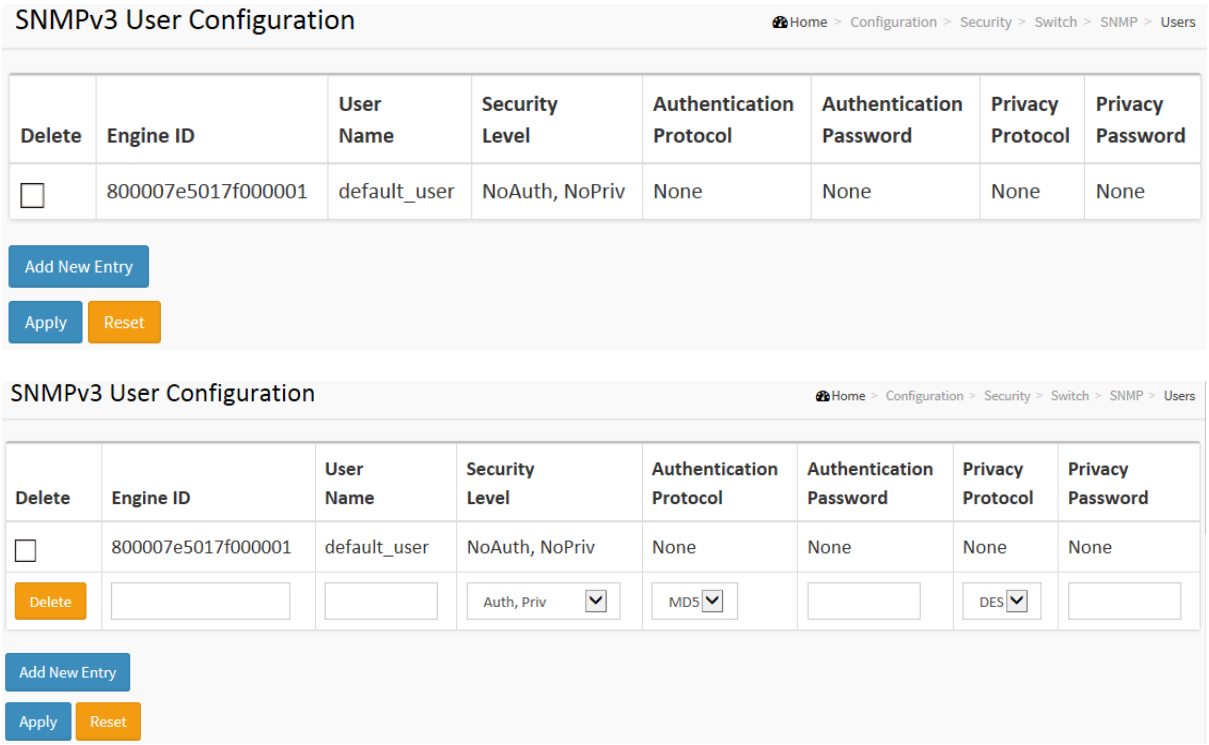


Fig. SNMPv3 User Configuration

Parameter	Description
Delete	Tick the check box next to the entry you want to delete and click the Apply button.

Engine ID	An octet string identifying the engine ID for this user. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User Name	A string identifying the user name for this user. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model for this user. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy. The security level cannot be modified if an entry already exists. If you need to modify a security level the user will need to be deleted and recreated.
Authentication Protocol	Indicates the authentication protocol for this user. Possible authentication protocols are: None: No authentication protocol. MD5: An optional flag to indicate that this user uses MD5 authentication protocol. SHA: An optional flag to indicate that this user uses SHA authentication protocol. The security level cannot be modified if an entry already exists. If you need to modify a security level the user will need to be deleted and recreated.
Authentication Password	Enter a password for Authentication. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol for this user. Possible privacy protocols are: None: No privacy protocol. DES: An optional flag to indicate that this user uses DES authentication protocol.
Privacy Password	Enter a password for Privacy. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.
Add New Entry	Click to add a new SNMPv3 User.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved

	values.

Groups

This function is used to configure SNMPv3 Groups. Max Group Number: v1: 2, v2: 2, v3:10.

Information

To configure the SNMP Security parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Groups.**
2. If you would like to change the name of the default groups do so under the **Group Name** section.
3. If you are adding a new group click the **Add New Entry** button and select the required **Security Model**, **Security Name** and **Group Name**.
4. Click **Apply** to confirm your settings change.

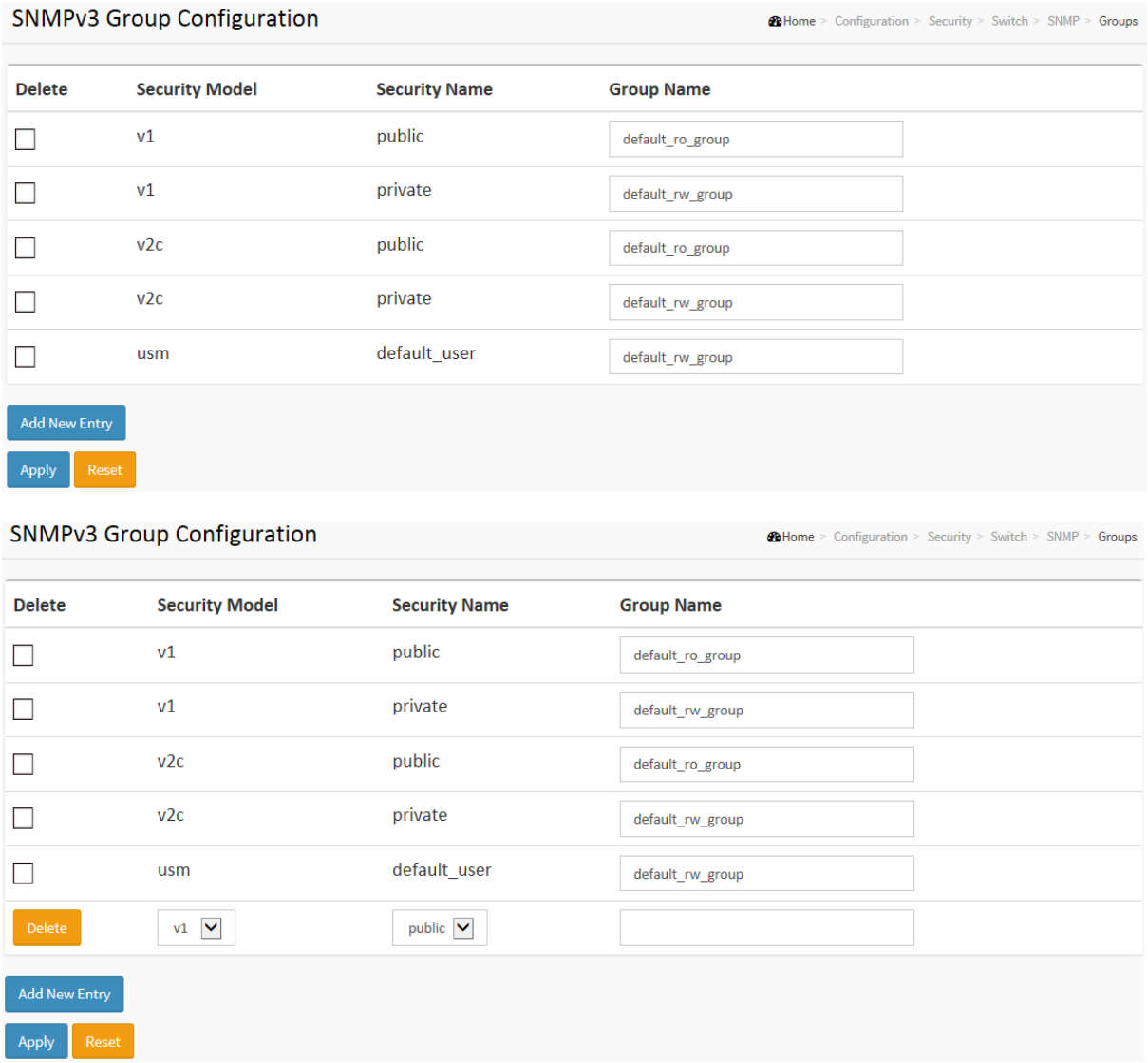


Fig. SNMPv3 Group Configuration

Parameter	Description
Delete	Tick the check box next to the entry you want to delete and click the Apply button.
Security Model	Indicates the security model for this group. 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 group. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Group Name	A string identifying the group name. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Add New Entry	Click to add a new SNMPv3 Group.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Views

This function is used to configure SNMPv3 Views. Maximum View Entries: 28.

Information

To configure the SNMP Viewing parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Views.**
2. Click on **Add New Entry** button to add a new view.
3. Enter the **View Name**, **View Type** and the **OID Subtree**.
4. Click **Apply** to confirm your settings change.

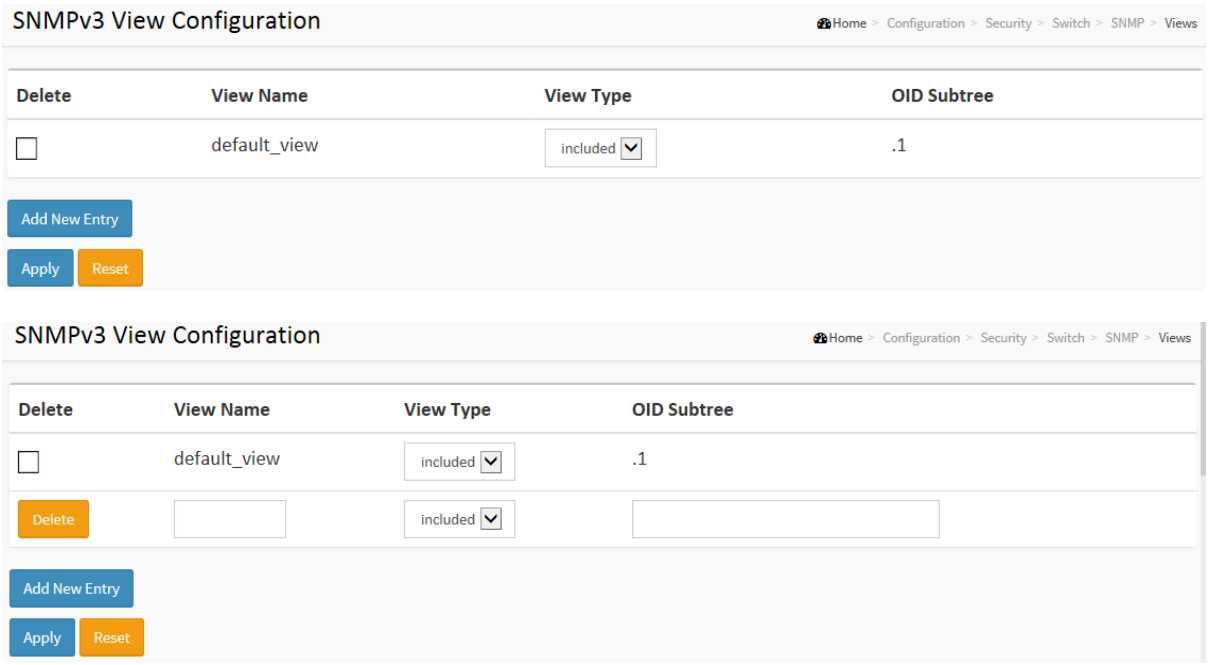


Fig. SNMPv3 View Configuration

Parameter	Description
Delete	Tick the check box next to the entry you want to delete and click the Apply button.
View Name	A string identifying the view name for this entry. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type for this entry. Possible view types are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep

	the 'excluded' view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).
Add New Entry	Click to add a new SNMPv3 View.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Access

This function is used to configure SNMPv3 Access. Maximum Access entries: 14

Information

To configure the SNMP Access parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Access.**
2. For the default entries the **Read View Name** and **Write View Name** can be selected from the drop down boxes.
3. To add a new Access Configuration click the **Add New Entry** button.
4. Select the Read Only or Read/Write from the **Group Name** drop down box.
5. Select the required **Security Model** and the appropriate **Security Level**.
6. Select the **Read View Name** and **Write View Name** from the drop down boxes provided.
7. Click **Apply** to confirm your settings change.

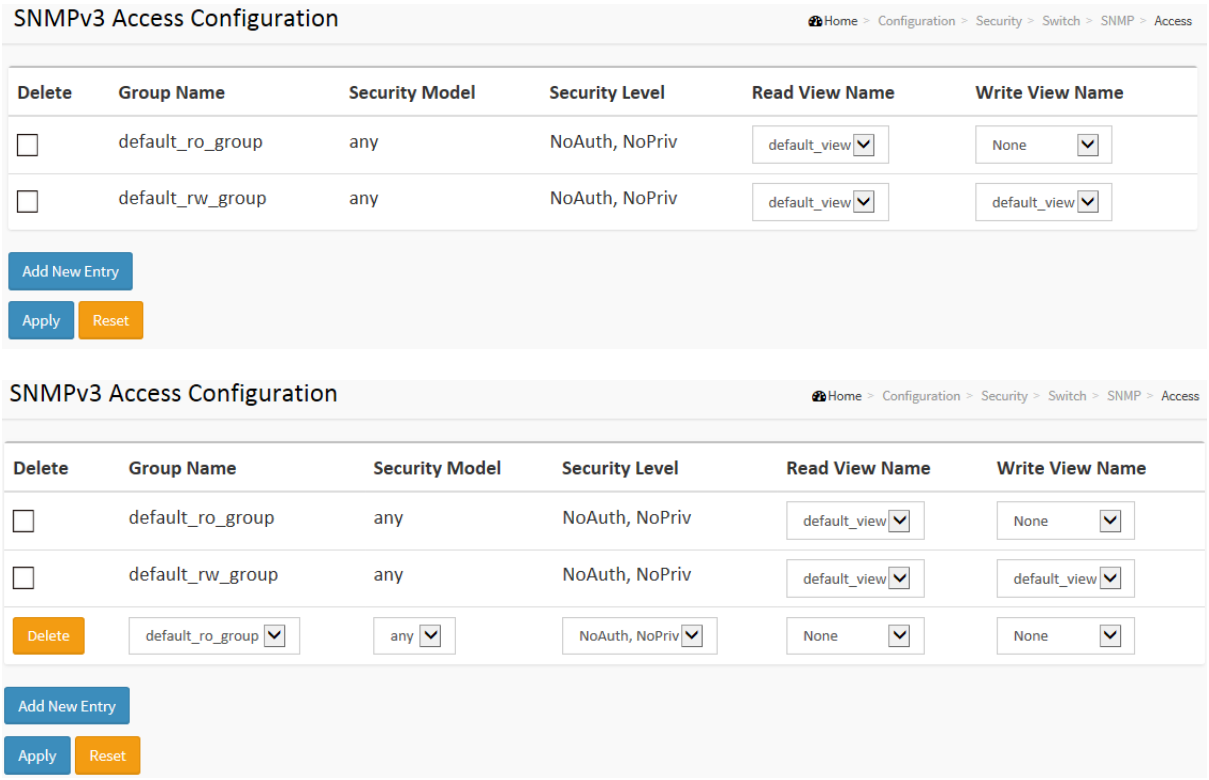


Fig. SNMPv3 Access Configuration

Parameter	Description

Delete	Tick the check box next to the entry you want to delete and click the Apply button.
Group Name	A string identifying the group name for this entry. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model for this entry. 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 level for this entry. Possible security models are: NoAuth, NoPriv: No authentication and no privacy. Auth, NoPriv: Authentication and no privacy. Auth, Priv: Authentication and privacy.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Add New Entry	Click to add a new SNMPv3 Access Configuration.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Trap Event Severity

This page displays the current trap event severity configurations. These options can also be configured here.

Information

To configure the SNMP Trap Event parameters via the Web Interface:

1. Select **Configuration > Security > Switch > SNMP > Trap Severity Configuration.**
2. Select an SNMP Trap number and click the number to add the trap information. Up to 6 traps can be configured.
3. If you have any Trap entries that you would like to delete, click on the delete button next to the Trap that you would like to delete.
4. Click the Save button to apply changes

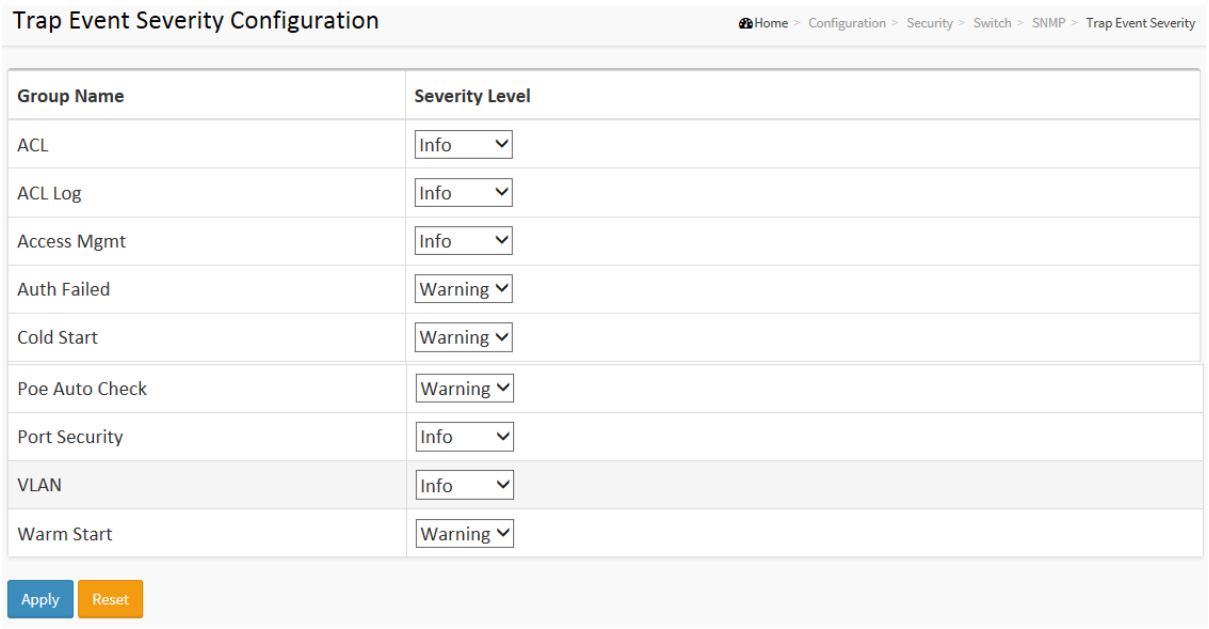


Fig: The Trap Event Severity Configuration

Parameter	Description
Group Name	The name identifying the severity group.
Severity Level	Every group has an severity level. The following level types are supported: <0> Information: Information messages. <1> Warning: Warning conditions. <2> Error: Error conditions.

Buttons	**Apply** – Click to save changes. **Reset -** Click to undo any changes made locally and revert to previously saved values.

RMON

An RMON implementation typically operates in a client/server model. Monitoring devices contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients.

Statistics

Configure RMON Statistics table on this page.

Information

To configure the RMON Statistic parameters via the Web Interface:

1. Click **Configuration** > **Security** > **Switch** > **RMON** > **Statistics**
2. Select Add New Entry to add a new Statistic
3. Specify the ID Parameters
4. Click **Apply** to Save ot **Reset** to revert unsaved settings.

Fig: The RMON Statics Configuration

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

	stored in RMON. The range is from 1 to 3600, default value is 50.
Buckets Granted	The number of data shall be saved in the RMON.

History

Configure RMON History table on this page.

Information

To configure the RMON History parameters via the Web Interface:

1. Click **Configuration** > **Security** > **Switch** > **RMON** > **History**
2. Select Add New Entry to add a new Entry
3. Specify the ID Parameters
4. Click **Apply** to Save ot **Reset** to revert unsaved settings.

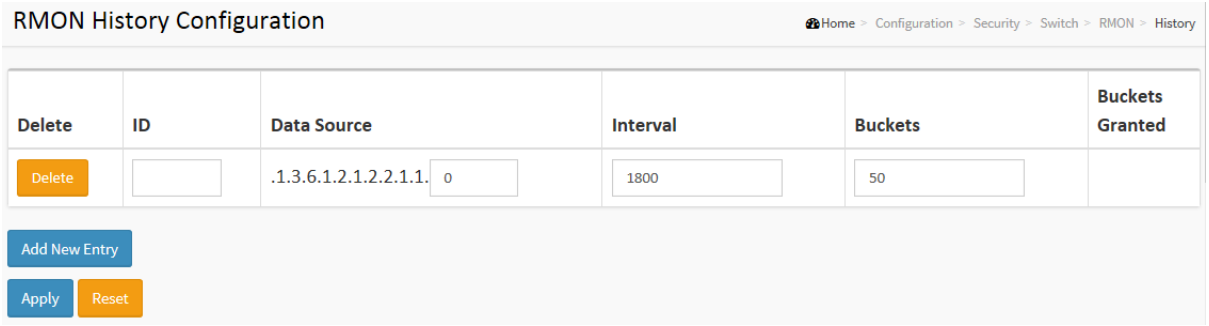


Fig: The RMON History Configuration

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

Alarm

Configure RMON Alarm table on this page.

Information

To configure the RMON Alarm parameters via the Web Interface:

1. Click >**Configuration** > **Security** > **Switch** > **RMON** > **Alarm**
2. Select **Add New Entry** to add a new Entry
3. Specify the ID Parameters
4. Click **Apply** to Save or **Reset** to revert unsaved settings.

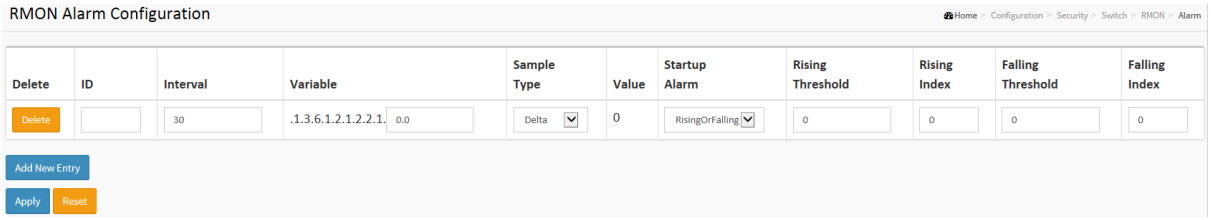


Fig: The RMON Alarm Configuration

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	Indicates the particular variable to be sampled, the possible variables are: **InOctets**: The total number of octets received on the interface, including framing characters. **InUcastPkts**: The number of uni-cast packets delivered to a higher-layer protocol. **InNUcastPkts**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. **InDiscards**:

	The number of inbound packets that are discarded even the packets are normal. **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol. **OutOctets**: The number of octets transmitted out of the interface , including framing characters. **OutUcastPkts**: The number of uni-cast packets that request to transmit. **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. **OutDiscards**: The number of outbound packets that are discarded event the packets is normal. **OutErrors**: The The number of outbound packets that could not be transmitted because of errors. **OutQLen**: The length of the output packet queue (in packets)
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Absolute**: Get the sample directly. **Delta**: Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **RisingTrigger** alarm when the first value is larger than the rising threshold. **FallingTrigger** alarm when the first value is less than the falling threshold. **RisingOrFallingTrigger** alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling Index	Falling event index (1-65535).

Event

Configure RMON Event table on this page.

Information

To configure the RMON Event parameters via the Web Interface:

1. Click Configuration > Security > SNMP > RMON> Event
2. Select **Add New Entry** to add a new Entry
3. Specify the ID Parameters
4. Click **Apply** to Save or **Reset** to revert unsaved settings.

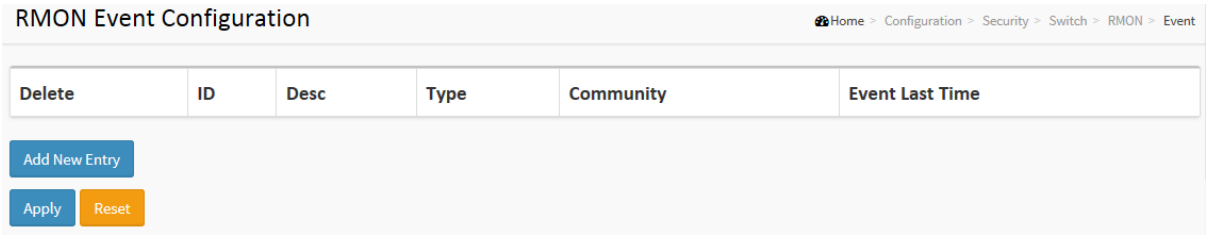


Fig: The RMON Event Configuration

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

	event.

Network

The AS Series switches supports Port Security function allowing the administrator to specify the amount of MAC addresses allowed to be accessed by an individual port.

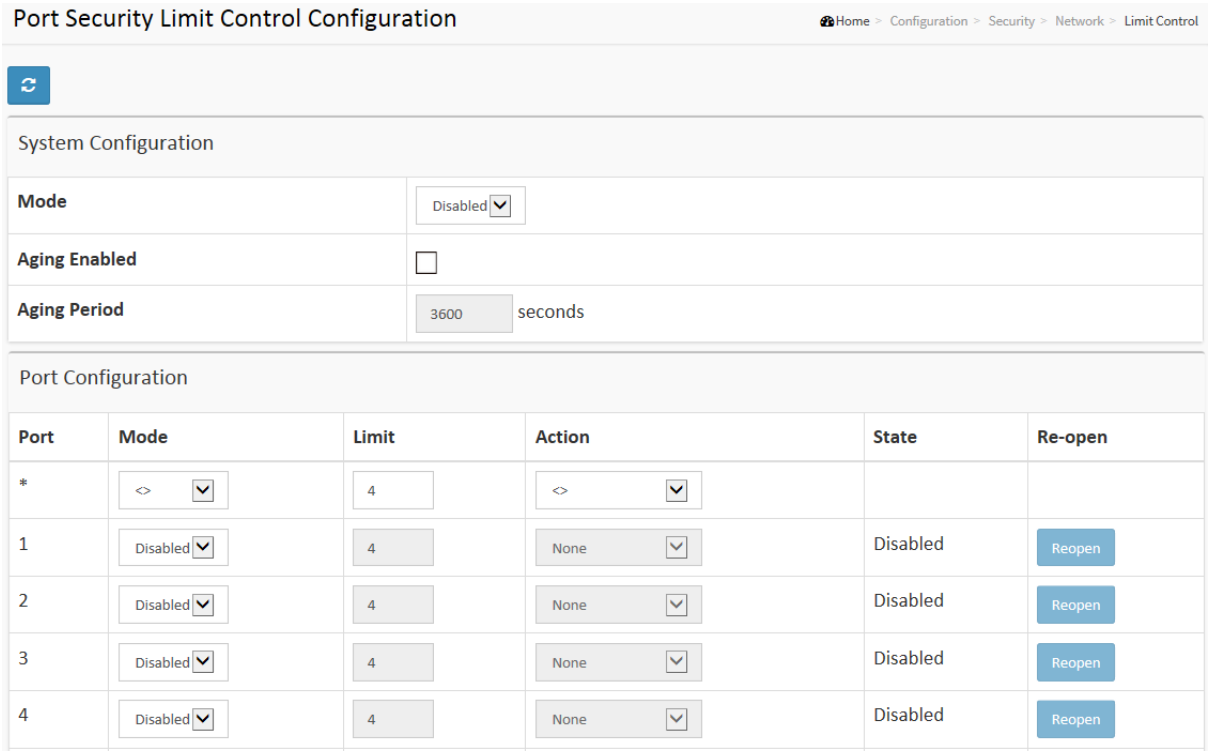
Limit Control

This section is used to configure the amount of MAC Addresses allowed to by the port and you can also specify the action taken once this configured threshold has been reached

Information

To configure the Network Limit Control Security parameters via the Web Interface:

1. Click **Configuration** > **Security** > **Switch** > **Limit Control**
2. Specify the appropriate system settings for your configuration.
3. Enable per port settings based on your requirements.
4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



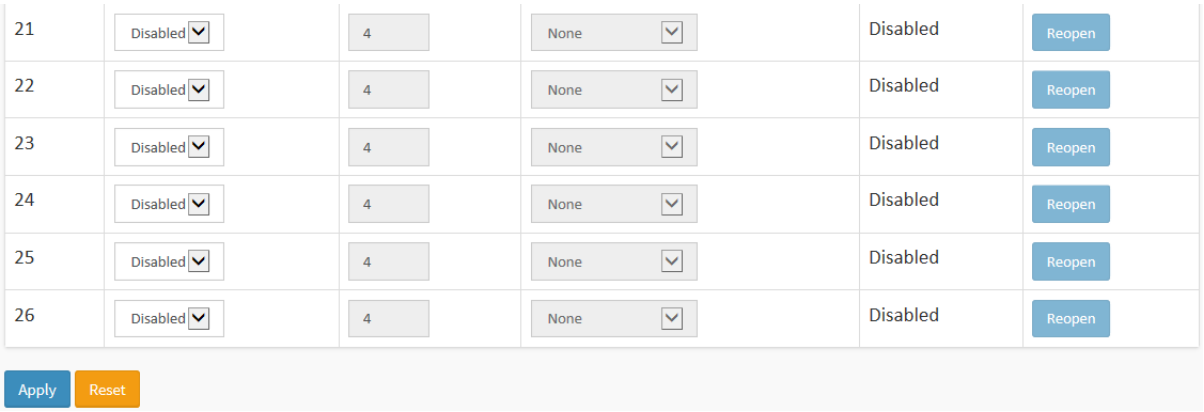


Fig: The Port Security Limit Control Configuration

System Configuration

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

Port Configuration

Parameter	Description
Port	Physical port of the switch.
Mode	Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.
Action	If Limit is reached, the switch can take one of the following actions: None: Do not allow more than Limit MAC addresses on the port, but take no further action. **Trap**: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded. **Shutdown**: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1) Reboot the switch. 2) Disable and re-enable Limit Control on the port or the switch. 3) Click the Reopen button. **Trap & Shutdown**: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
State	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: **Disabled:** Limit Control is either globally disabled or disabled on the port. **Ready:** The limit is not yet reached. This can be shown for all actions. **Limit Reached:** Indicates that the limit is reached on this port. This state can

	only be shown if Action is set to None or Trap. **Shutdown:** Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.
Re-open Button	If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shut down in the Action section. **NOTE: T**hat clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

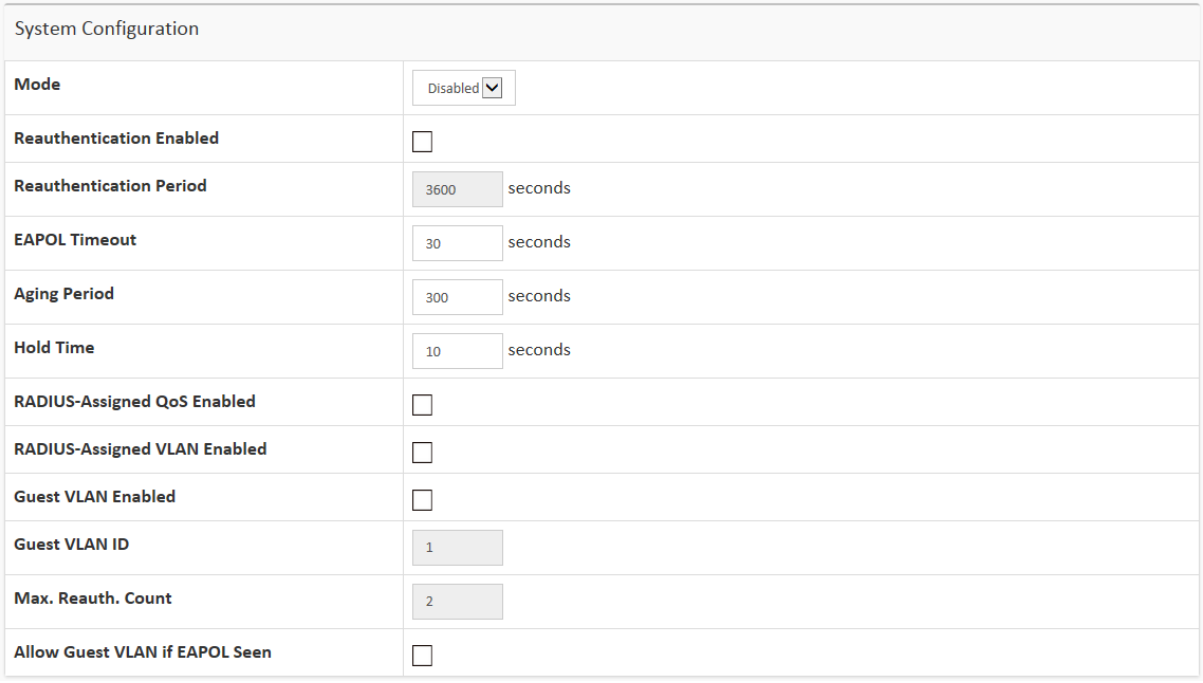
NAS

The AS Series switches supports aNAS (Network Access Server) function which allows users connection to a variety of resources, including the internet. Particular settings can be applied to this user based on authentication to a RADIUS Server. Functions such as 802.1x and Mac based Authentication can be used to authenticate users onto the network allowing them access to these shared resources.

Information

To configure the Network Access Server parameters via the Web Interface:

1. Click Configuration > Security > Network > NAS
2. Enable and configure the system wide parameters for the NAS server.
3. Configure the required settings for each of the ports that will utilize the NAS function.
4. Click the Apply button to save your changes or the Reset button to revert to previous settings.



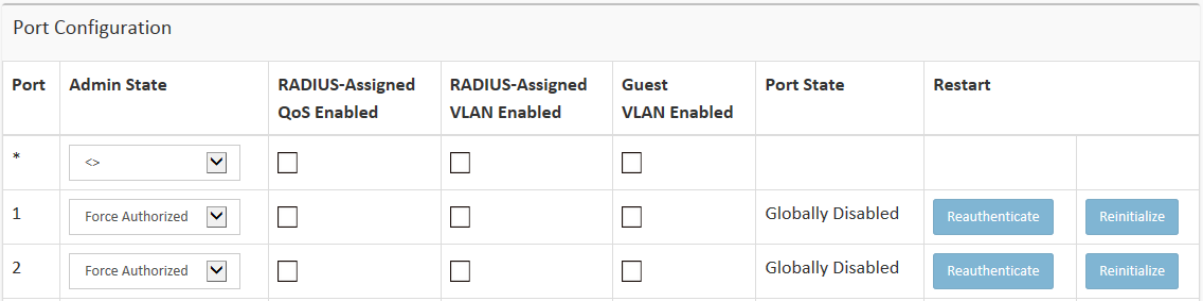


Fig: The Network Access Server Configuration

Parameter	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentcation Enabled	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
Aging Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If 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. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between

	the switch and the client, so this will not detect Whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • Single 802.1X • Multi 802.1X • MAC-Based Auth. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request 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. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
RADIUS-Assigned QoS Enabled	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description) The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-

	assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.
Guest VLAN Enabled	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.
Guest VLAN ID	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].
Max Reauth Count	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.
Port Configuration	The table has one row for each port on the selected switch and a number of columns, which are,
Port	Physical port of the switch.
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 any client on the port will be allowed network access without authentication.

Force Unauthorized	In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.
Port-based 802.1X	In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant **NOTE**: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.
Single 802.1X	In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is really not an IEEE

	standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.
Multi 802.1X	In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does 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. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.
MAC-based Auth	Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS

	server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 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 don't 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.
RADIUS-Assigned QoS Enabled	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X RADIUS attributes used in identifying a QoS Class: 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. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range

	'0' - '3', which translates into the desired QoS Class in the range [0; 3].
RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
Guest VLAN Enabled	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: • Port-based 802.1X • Single 802.1X • Multi 802.1X For trouble-shooting VLAN assignments, use the

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

	and will not cause the clients to get temporarily unauthorized. **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

ACL

The AS Series switches access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced 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. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number range from 1-8. However each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

Ports

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

Information

To configure the ACL Port Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **ACL** > **Ports**
2. Configure the required ACL settings for each of the ports.
3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

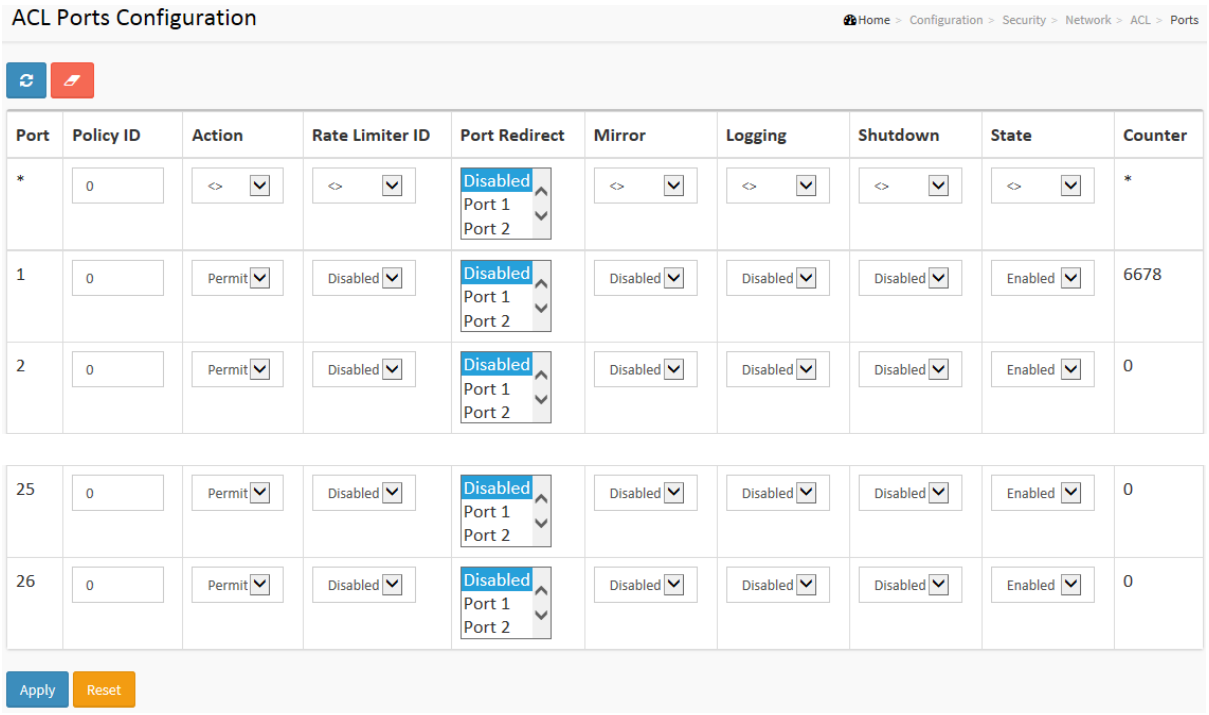


Fig: The ACL Ports Configuration

Parameter	Description
Port	Physical port of the switch.
Policy ID	Select the Policy to apply to this port. The allowed vales are 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted (Permit) or denied (Deny). The default value is Permit.
Rate Limiter ID	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is Disabled.
Port Redirect	Select which port frames are copied on. The allowed values are Disabled or a specific port number. The default value is Disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: **Enabled:** Frames received on the port are mirrored. **Disabled:** Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Specify the logging operation of this port. The allowed values are: **Enabled:** Frames received on the port are stored in the System Log. **Disabled:** Frames received on the port are not logged. The default value is Disabled. Please note that the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of this port. The allowed values are: **Enabled:** If a frame is received on the port, the port will be disabled. **Disabled:** Port shut down is disabled. The default value is Disabled.
State	Used to enable or disable the selected port. The allowed values are: **Enabled:** Enables the port and allows packets to be sent and received. **Disabled:** Disables the port. The default value is Enabled.
Counter	Displays the amount of frames that match this ACE.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

Rate Limiters

The section describes how to configure the ACL Rate Limiting Parameters. Up to 16 different rate limits can be set and applied to individual ports. Rate Limits can be set in either pps (Packets Per Second) or Kbps (Kilo Bits Per Second). Only 1 rate limit can be applied to each port.

Information

To configure the ACL Port Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **ACL** > **Rate Limiters**
2. Configure up to 16 Rate Limiters, using either pps or Kbps.
3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

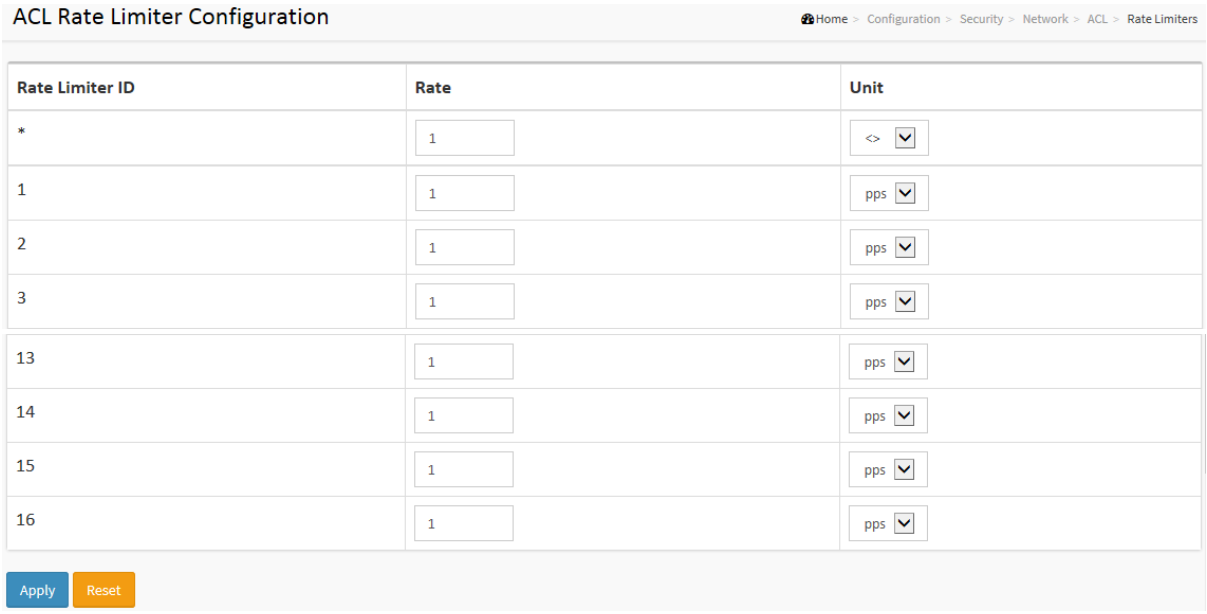


Fig: The ACL Rate Limiter Configuration

Parameter	Description
Rate Limiter ID	The Rate Limiter ID, from 1 through to 16.
Rate	Enter the required rate that you want to limit traffic flow to. If you are using Kbps, rates must be set in increments of 100.
Unit	Select to limit traffic in units of either pps (Packets Per Second) or Kbps (Kilo Bits Per Second).
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved

	values.

Access Control Lists

The section describes how to configure Access Control List rules. An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted. Other actions can also be invoked when a matching packet is found, including rate limiting, mirroring, redirecting 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 ACE's defined on this switch. Each row describes the ACE that is defined. The maximum number of ACE's is 256 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACE's used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority for these entries is the highest.

Information

To configure the Access Control List Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **ACL** > **Access Control Lists**
2. Click the  icon to add a new ACL or use the other ACL modification buttons, to edit or remove an existing ACL entry.
3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

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

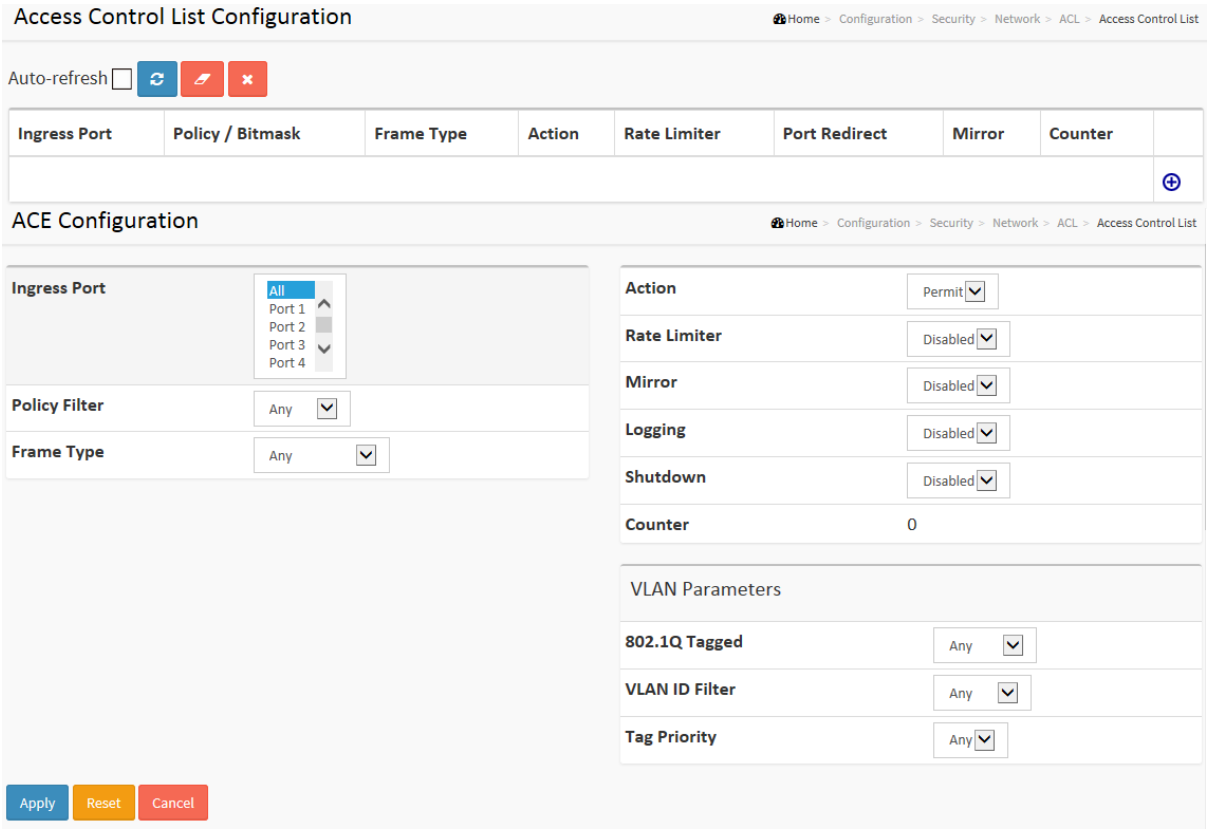


Fig: The ACL Rate Limiter Configuration

Parameter	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: **Any:** The ACE will match any ingress port. **Policy:** The ACE will match ingress ports with a specific policy (Policy must be created in the Ports Section before it will appear in the list). **Port:** The ACE will match a specific ingress port.
Policy / Bitmask	Indicates the Policy or Bitmask that the filter will match.
Frame Type	Indicates the frame type of the ACE. Possible values are: **Any:** The ACE will match any frame type. **Ethernet Type:** The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP:** The ACE will match ARP/RARP frames. **IPv4:** The ACE will match all IPv4 frames.
Action	Indicates the forwarding action of the ACE.

	Permit: Frames matching the ACE may be forwarded and learned. **Deny:** Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Copy	Indicates the port copy operation of the ACE. Frames matching the ACE are copied to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port copy operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: **Enabled:** Frames received on the port are mirrored. **Disabled:** Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Indicates the logging operation of the ACE. Possible values are: **Enabled:** Frames matching the ACE are stored in the System Log. **Disabled:** Frames matching the ACE are not logged. Please note that the System Log memory size and logging rate is limited.
Shutdown	Indicates the port shut down operation of the ACE. Possible values are: **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. Modification Buttons: You can modify each ACE (Access Control Entry) in the table using the following buttons:  : Inserts a new ACE before the current row.  : Edits the ACE row.  : 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.

Mac Parameter

Parameter	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. Any: No SMAC filter is specified. (SMAC filter status is "don't-care".) Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care".) MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

IP Source Guard

The AS Series switches support IP Source Guard. IP Source Guard can be used to help secure your switch from IP based spoofing attacks.

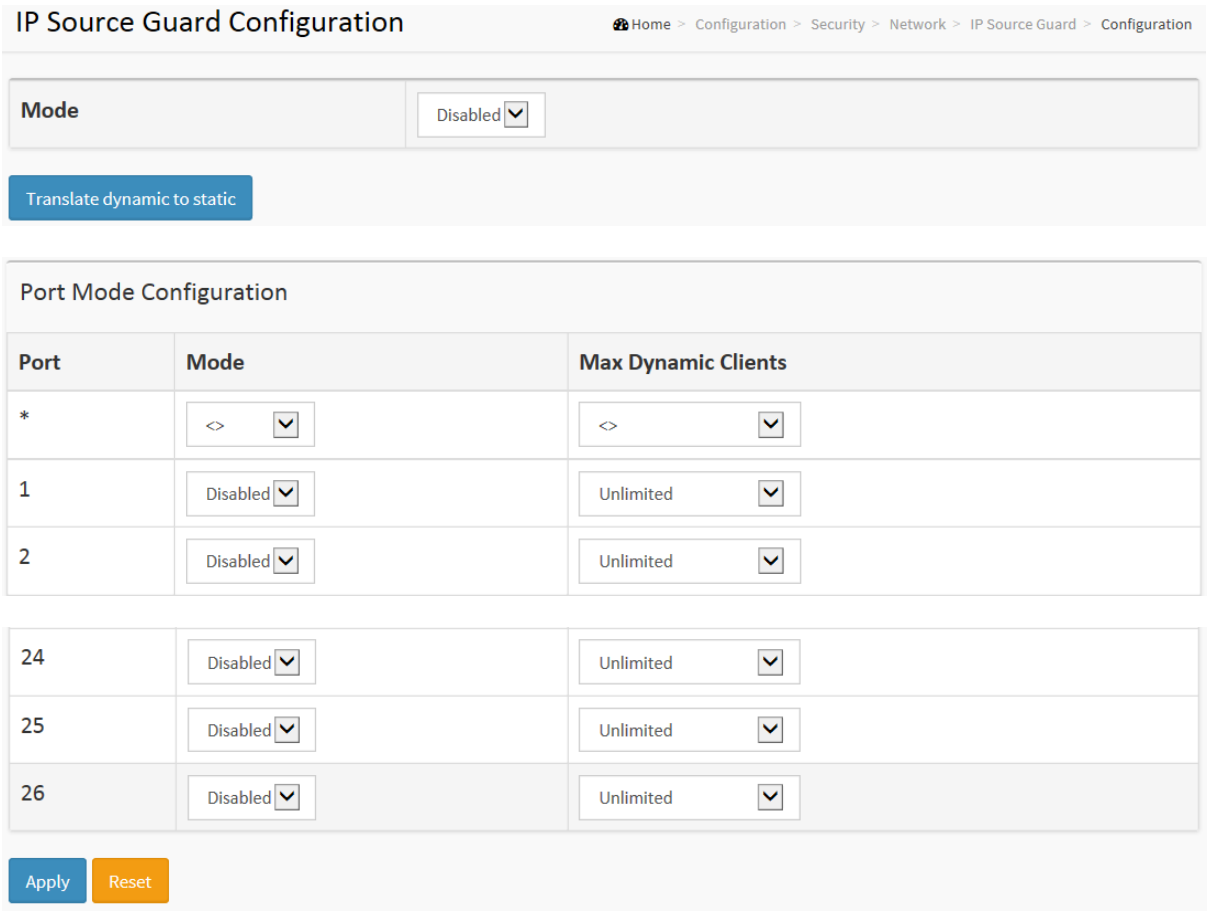
Configuration

This section is used to configure the IP Source Guard settings for the AS switch.

Information

To configure the IP Source Guard Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > IP **Source Guard** > **Configuration**
2. Select to enable or disable the IP Source Guard feature.
3. Select to enable or disable this function on each individual port.
4. Select the amount of Dynamic Clients allowed to be learnt by the port.
5. Click the Apply button to save your changes or the Reset button to revert to previous settings.



Parameter	Description
Mode of IP Source Guard Configuration	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.
Max Dynamic Clients	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

Static Table

This section is used to enter Static IP addresses into the AS switch.

Information

To configure the IP Source Guard Static Table Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **IP Source Guard** > **Static Table**
2. Click on Add New Entry.
3. Specify the Port, VLAN ID, IP Address and MAC Address.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

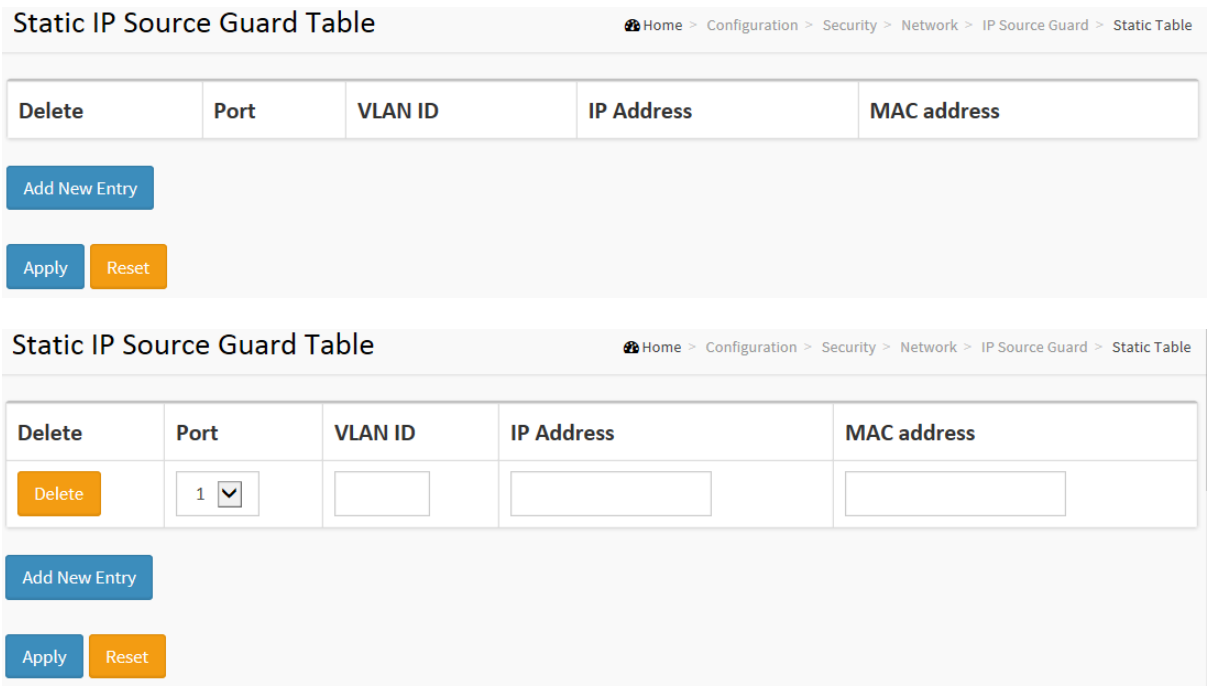


Fig: The Static IP Source Guard Table

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Port	Port: Physical port of the switch.
VLAN ID	The VLAN ID of the static entry.
IP Address	The IP Address of the static entry.

MAC Address	The MAC Address of the static entry.
Adding New Entry	Click to add a new static entry.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

ARP Inspection

The AS Series switches supports ARP Inspection. This allows the switch to intercept and examine all ARP request and response packets in a subnet and discard those packets with invalid IP to MAC address bindings.

Port Configuration

This section describes how to configure ARP Inspection setting including
Mode (Enabled and Disabled)
Port (Enabled and Disabled)

Information

To configure the ARP Inspection Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > ARP **Inspection** > **Port Configuration**
2. Select to enable or disable the ARP Inspection feature.
3. Select to enable or disable this function on each individual port.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

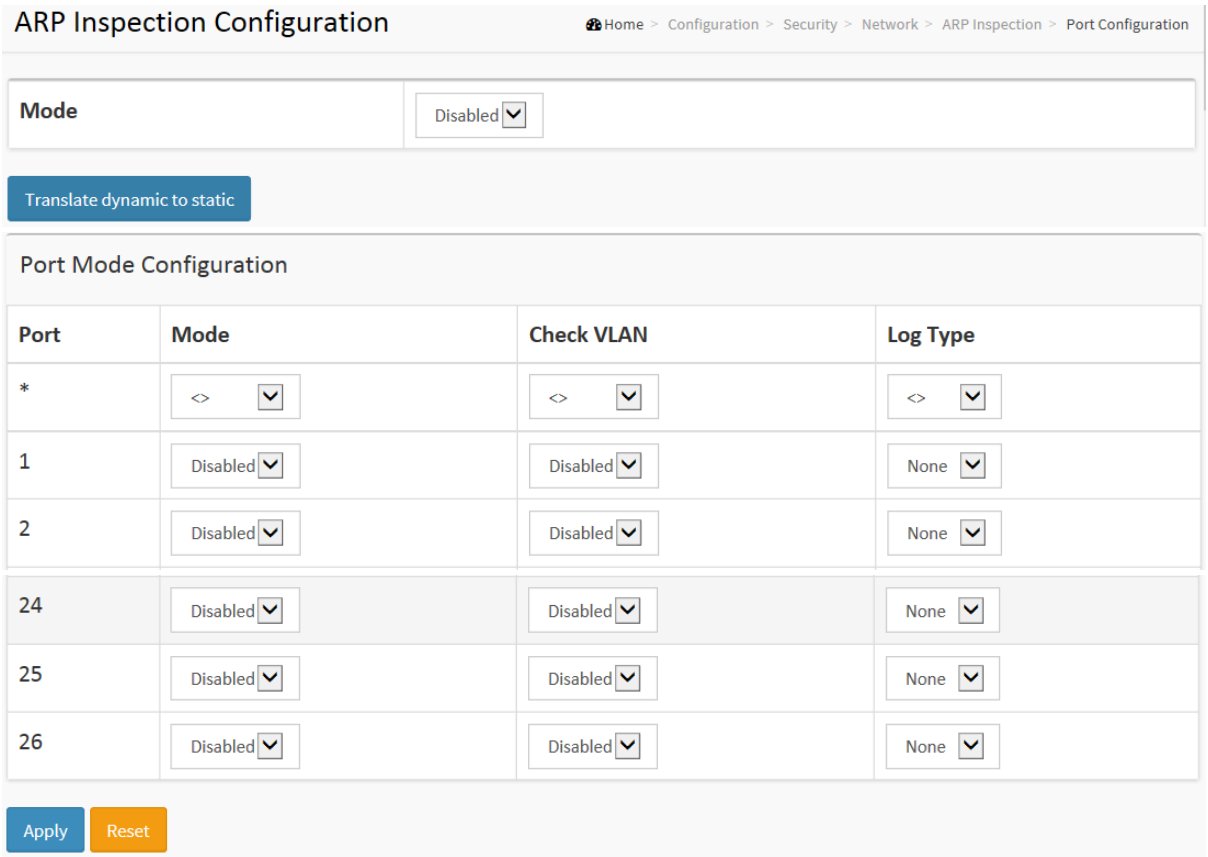


Fig: The ARP Inspection Configuration

Parameter	Description
Mode of ARP inspection Configuration	Enable the Global ARP Inspection or disable the Global ARP Inspection.
Port Mode Configuration	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are: **Enabled**: Enable ARP Inspection operation. **Disabled**: Disable ARP Inspection operation. If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: **Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation. Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

VLAN Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the entries per page input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

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

Information

To configure the ARP Inspection VLAN Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **ARP Inspection** > **VLAN Configuration**
2. To add a new entry select the **Add New Entry** button
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

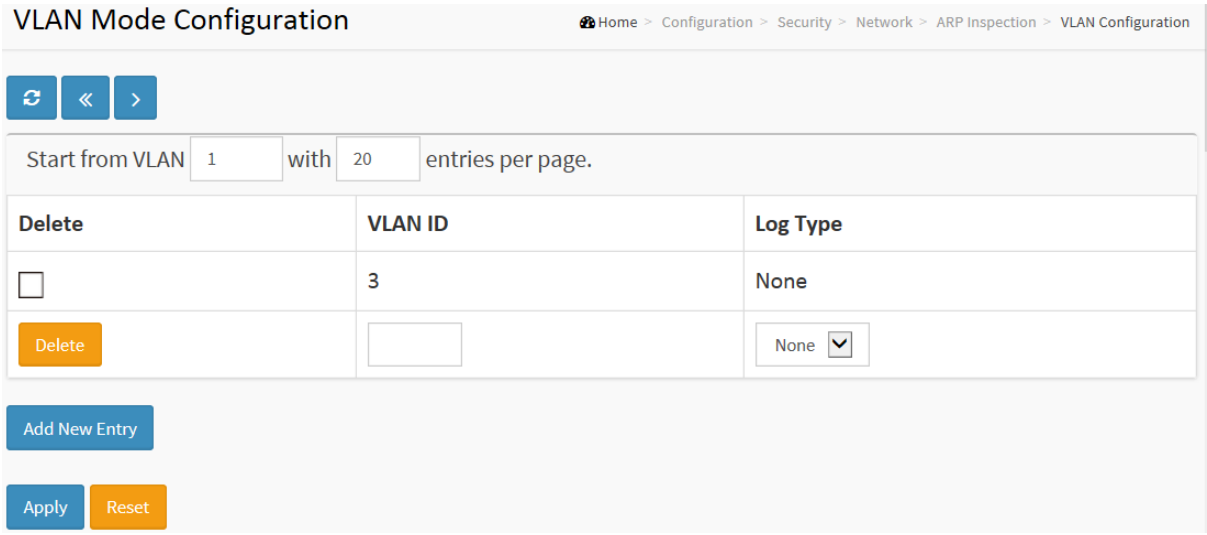


Fig: The VLAN Mode Configuration

Parameter	Description
VLAN mode Configuration	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on

	per VLAN setting. Possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.
Buttons	**Add New Entry**: Click to add a new VLAN to the ARP Inspection VLAN table. **Apply**: Click to save changes. **Reset:** Click to undo any changes made locally and revert to previously saved values.

Static Table

This section is used to enter Static ARP entries into the AS switch.

Information

To configure the Static Table ARP Inspection Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **ARP Inspection** > **Static Table**
2. Click on **Add New Entry**.
3. Specify the **Port**, **VLAN ID**, **IP Address** and **MAC Address**.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

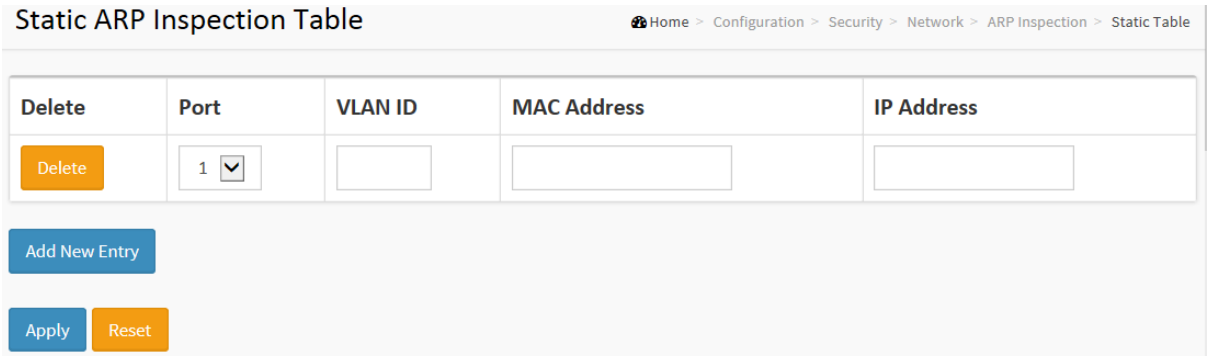


Fig: The Static ARP Inspection Table

Parameter	Description
Delete	Check the tick box next to the required entry and press the Apply button.
Port	Physical port of the switch.
VLAN ID	The VLAN ID of the static entry.
MAC Address	The MAC Address of the static entry.
IP Address	The IP Address of the static entry.
Adding new entry	Click to add a new static entry.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Dynamic Table

This section is used to view the dynamic ARP Inspection entries.

Information

To configure the Dynamic Table ARP Inspection Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **ARP Inspection** > **Dynamic Table**
2. To filter the entries you can select the Start from Port, VLAN ID and or IP Address.
3. If you want to auto-refresh the information you will need to check the Auto-Refresh tick box.
4. Click Refresh to manually refresh the information.
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

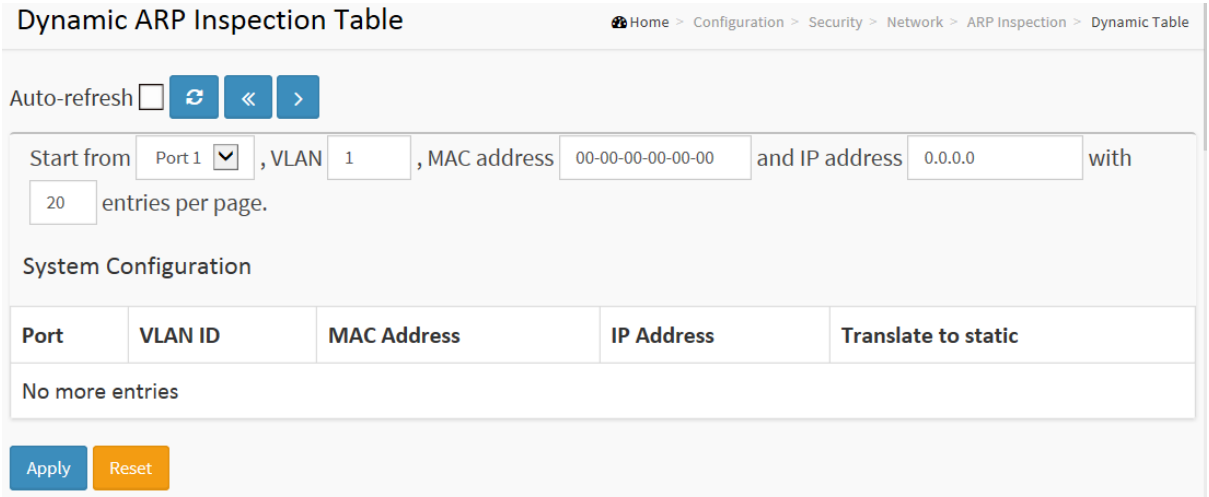


Fig: The Dynamic ARP Inspection Table

Parameter	Description
Port	Physical port of the switch.
VLAN ID	VLAN ID of the IP traffic that's permitted.
MAC Address	MAC Address of the dynamic entry.
IP Address	IP Address of the dynamic entry.
Translate to Static	Select the checkbox to translate the entry to static entry.
Buttons	**Apply** – Click to save changes.

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

AAA

The AS Series switches supports AAA (Authentication, Authorization, Accounting) to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

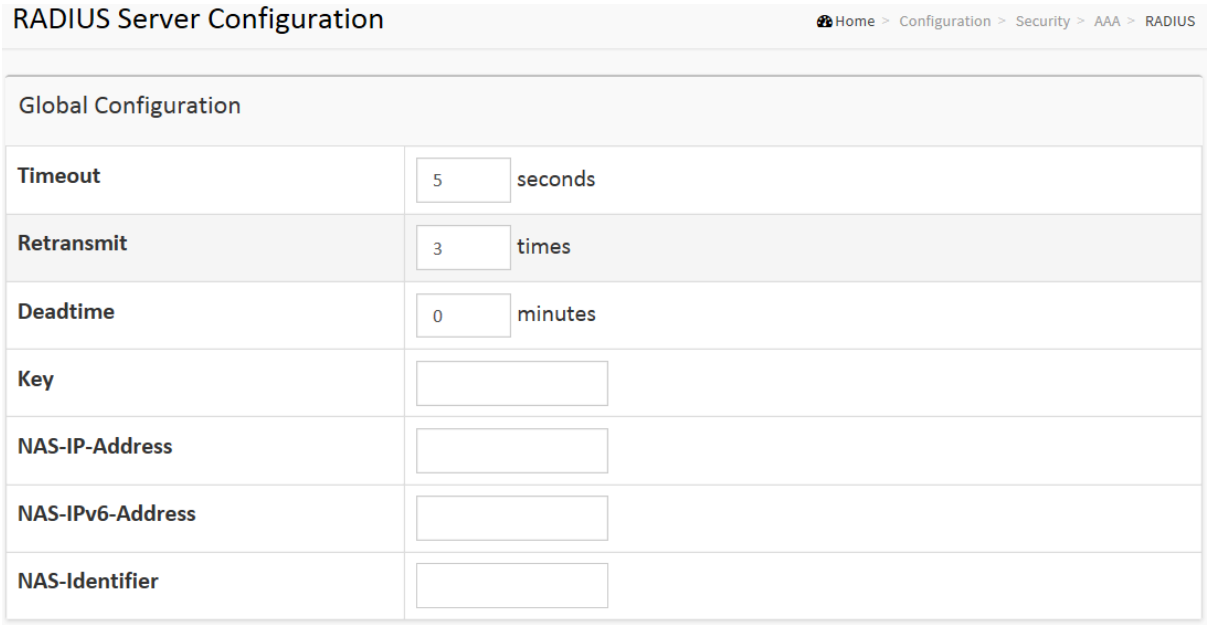
RADIUS

This section allows you to configure the RADIUS Server information.

Information

To configure the RADIUS Server Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **AAA** > **RADIUS**
2. Enter in the Global Configuration Settings such as Timeout, Retransmit times, Deadtime minutes, Key, NAS-IP-Address and NAS Identifier
3. To add a new server configuration, click the Add New Server Button and add the server configuration parameters.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.



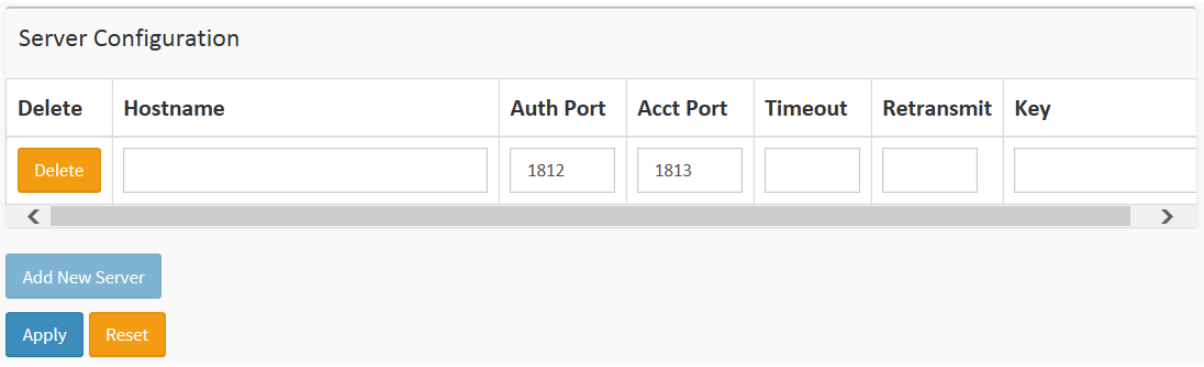


Fig: The RADIUS Authentication Server Configuration

Global Configuration

These setting are common for all of the RADIUS servers.

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

Server Configuration

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

Parameter	Description
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.
Adding a New Server	Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The button can be used to undo the addition of the new server.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

TACACS+

This page allows you to configure the TACASC+ Servers on the AS Series Switches.

Information

To configure the TACACS+ Server Configuration via the Web Interface:

1. Click **Configuration** > **Security** > **Network** > **AAA** > **TACACS+**
2. Enter in the Global Configuration Parameters such as Timeout, Deadtime and Key information
3. To add a new server, Click the Add New Server Button
4. Enter in the Server information you wish to add.
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

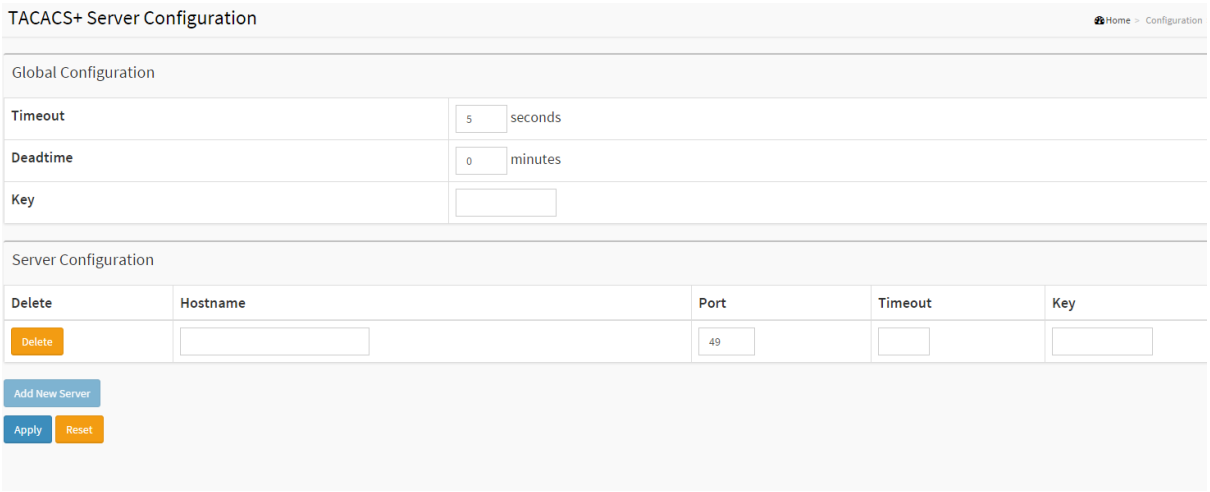


Fig: The TACACS+ Server Configuration

Global Configuration

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

Parameter	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

	Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

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

Parameter	Description
Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+ server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.
Adding a New Server	Click to add a new TACACS+ server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported. The button can be used to undo the addition of the new server.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Aggregation

The AS Series switches support two types of link aggregation, Static Trunk and LACP. Static Trunk is a non-protocol based aggregation method where the connections are determined via source and destination MAC Addresses. LACP is an IEEE standardized protocol used to aggregate ports. Because it is an IEEE standard LACP trunking or aggregation can be used across multi-vendor equipment.
By Aggregating ports between two devices this allows the bandwidth to be increased. For example if we aggregate 3 Gigabit Ports, the link between the two devices is increased to a 3Gb.

Static

This section is used to configure the static trunk settings. Here you will determine the method used to create the static trunk and also create your aggregation groups.

Ports using Static Trunk as their trunk method can choose their unique Static Group ID to form a logic “trunked port”. The benefit of using the 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 your static trunk group may not know that they should be aggregated together to form a “logical trunked port”. Using Static Trunk on both ends of a link is strongly recommended. Both devices must be configured to use the same speed and duplex settings.

Information

To configure the Static Aggregation Setting parameters via the Web Interface:

1. Click **Configuration** > **Aggregation** > **Static**
2. Select the type of method used to initiate the trunk.
3. Create the trunk group using the radio buttons in the table. Each Group ID is an individual trunk group, add the required ports into the desired trunk group.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

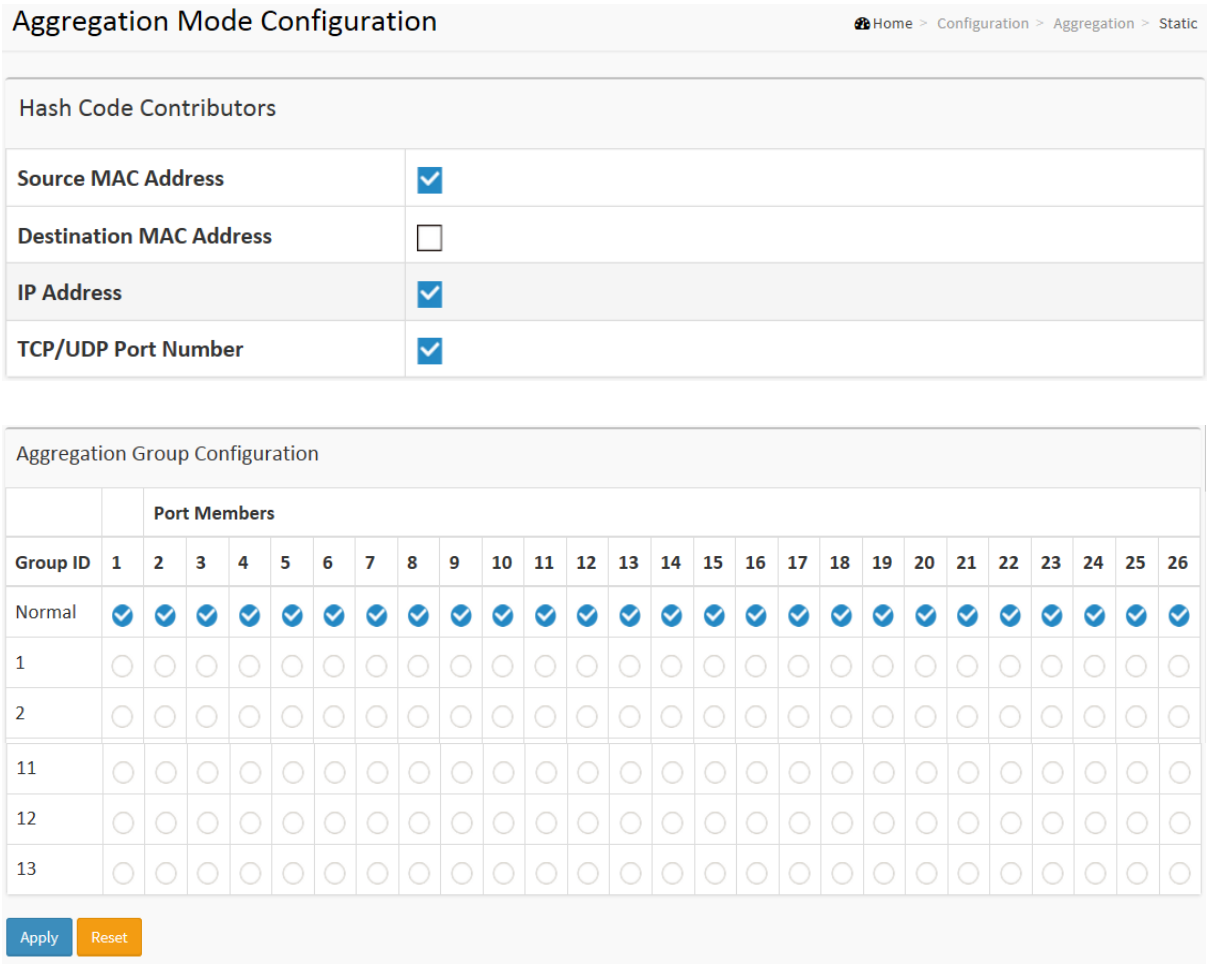


Fig: The Aggregation Mode Configuration

Hash Code Contributors

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

Parameter	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Buttons	**Apply** – Click to save changes. **Reset -** Click to undo any changes made locally and revert to previously saved values.

LACP

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP Group ID 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 other trunking methods, such as static trunking.

Information

To configure the LACP Aggregation Setting parameters via the Web Interface:

1. Click **Configuration** > **Aggregation** > **LACP**
2. Tick the **LACP Enabled** check box next to the port(s) you want to enable.
3. Select to either assign a Key automatically or manually assign a key. If you are manually assigning a key enter the key into the space provided.
4. Select the Role that you wish the port to play, either Active or Passive.
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

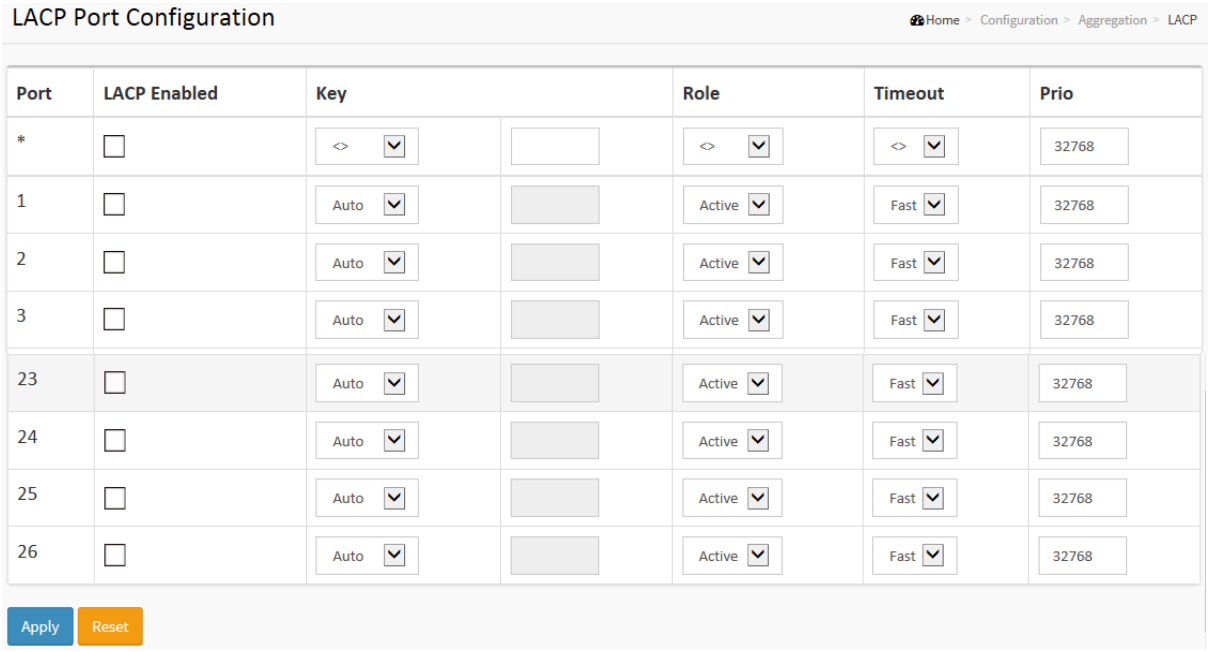


Fig: The LACP Port Configuration

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.
Key	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

Loop Protection

The AS Series switches support a Loop protection mechanism. Loop Protection can be used in environments that have devices that do not support the spanning tree protocol. If the switch receives a packet containing its own MAC address the port will be locked.

Information

To configure the Loop Protection Setting parameters via the Web Interface:

1. Click > **Configuration** > **Aggregation** > **Loop Protection**
2. Select the required Action to take when a loop is detected and select whether to enable or disable TX Mode.
3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

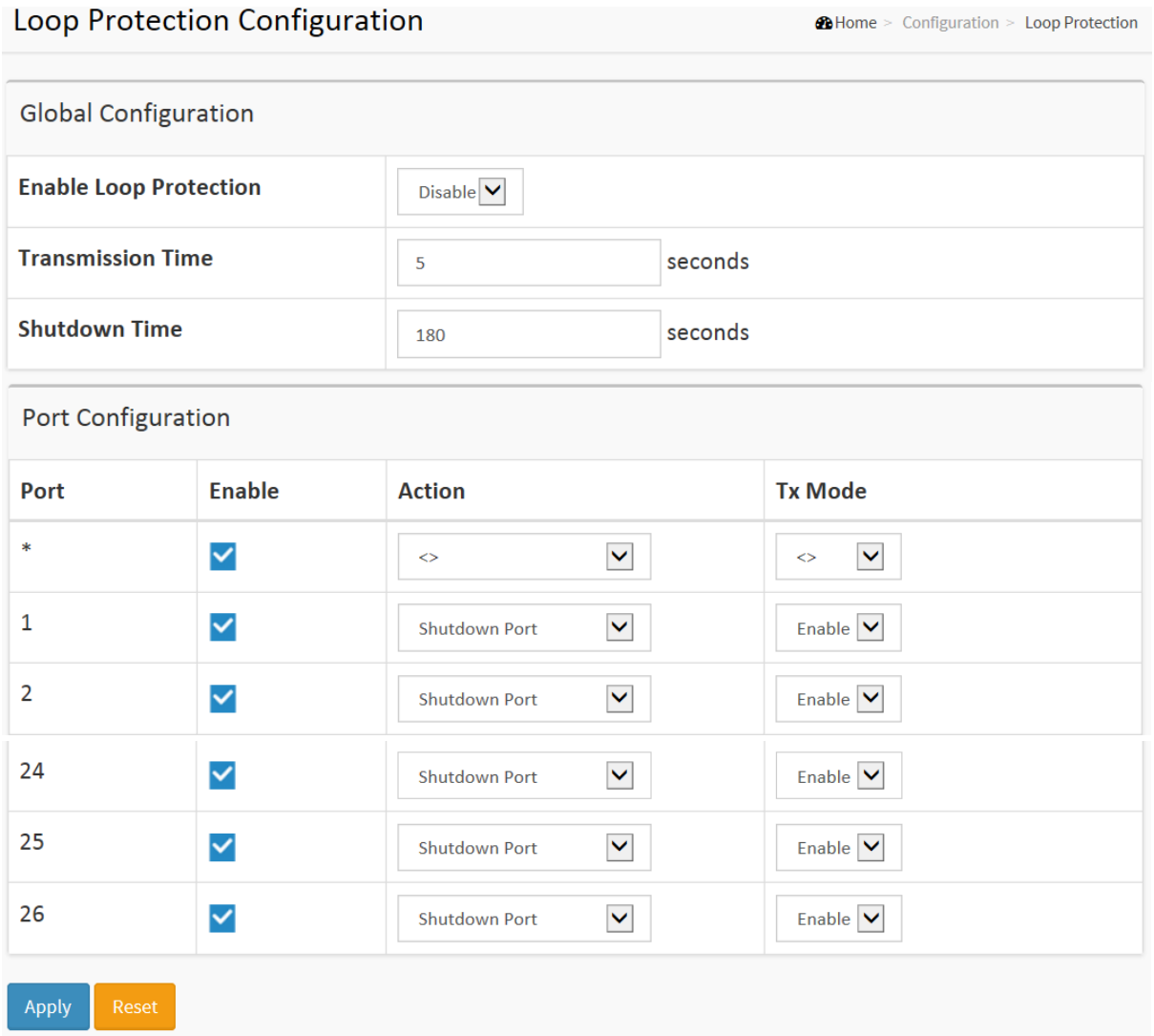


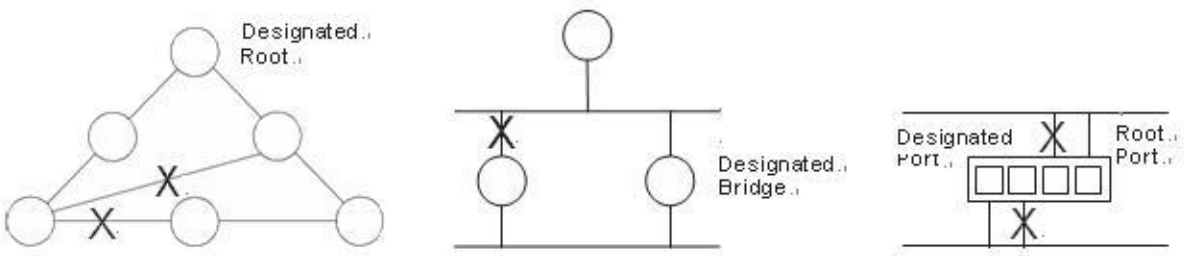
Fig: The Loop Protection Configuration.

Parameter	Description
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).
Port No	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port
Action	Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

Spanning Tree

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

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



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

STP can run in one of three modes: STP, RSTP or MSTP. A device running RSTP is compatible with other devices running STP; a device running MSTP is compatible with other devices running RSTP or STP. By default, on a device in MSTP mode each port automatically detects the mode of the device connected to it (MSTP, RSTP or STP), and responds in the appropriate mode by sending messages (BPDUs) in the corresponding format. Ports on a device in RSTP mode can automatically detect and respond to connected devices in RSTP and STP mode. Particular ports can also be forced to only operate in a particular mode (spanning-tree force-version command).

STP

The Spanning Tree Protocol (STP) is the original protocol defined by IEEE standard 802.1D-1988. It creates a single spanning tree over a network.

STP mode may be useful for supporting applications and protocols whose frames may arrive out of sequence or duplicated, for example NetBeui.

RSTP

Rapid Spanning Tree Protocol (RSTP) also creates a single spanning tree over a network. Compared with STP, RSTP provides for more rapid convergence to an active spanning tree topology. RSTP is defined in IEEE standard 802.1D-2004.

MSTP

The Multiple Spanning Tree Protocol (MSTP) addresses the limitations in the previous spanning tree protocols, STP and RSTP, within networks that use multiple VLANs with topologies that employ alternative physical links. It supports multiple spanning tree instances on any given link within a network, and supports large networks by grouping bridges into regions that appear as a single bridge to other devices.

MSTP is defined in IEEE standard 802.1Q-2005. The protocol builds on, and remains compatible with, the previous IEEE standards defining STP and RSTP.

Bridge Setting

This section is used to configure the spanning tree bridge settings, allowing full configuration of all spanning tree parameters. Here you can select what Spanning Tree Protocol you would like the switch to use, STP, RSTP or MSTP.

Information

To configure the Spanning Tree Bridge Setting parameters via the Web Interface:

1. Click **Configuration** > **Spanning Tree** > **Bridge Setting**
2. Select the required STP protocol and configure the appropriate basic and advanced STP parameters.
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

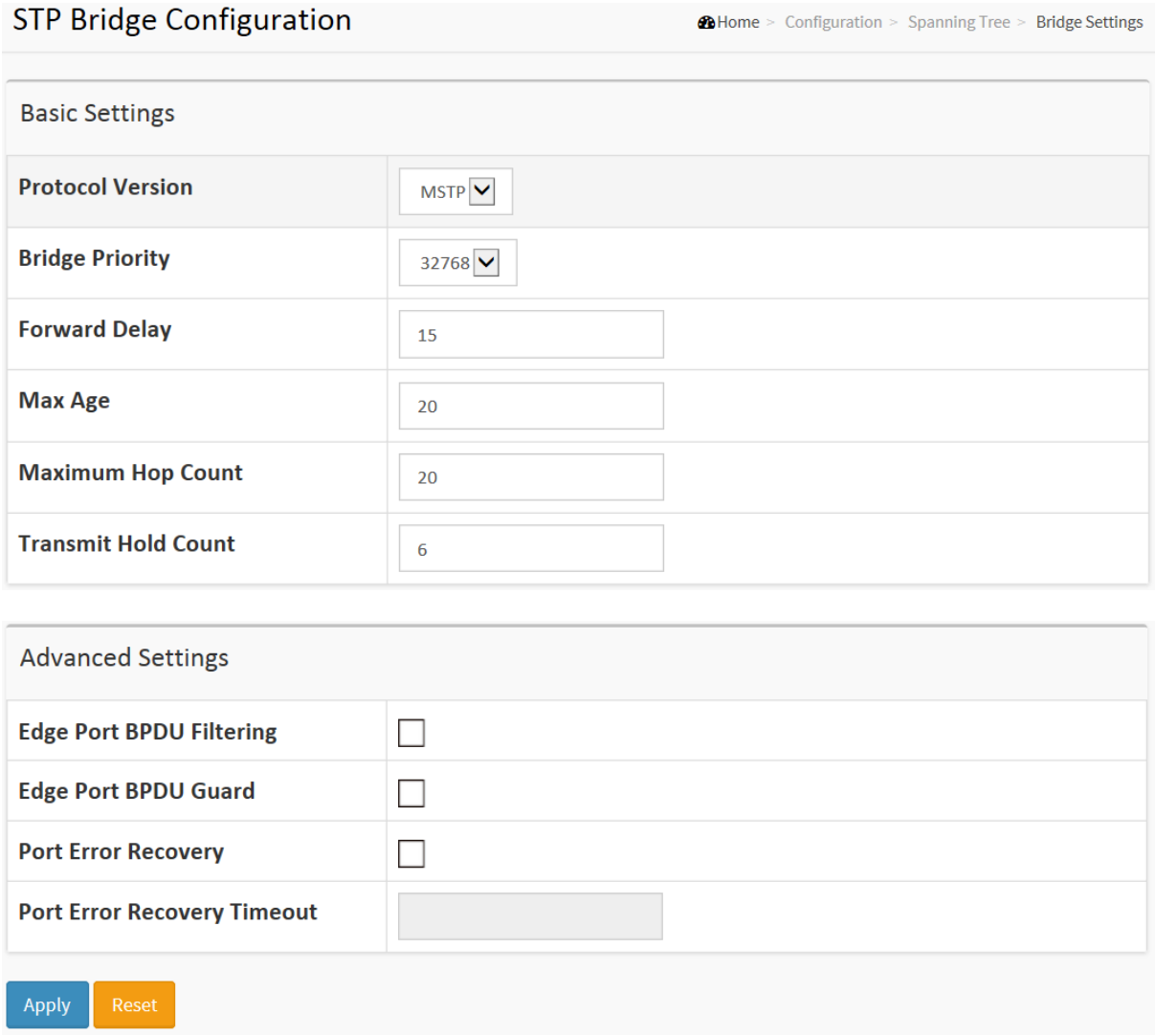


Fig: The STP Bridge Configuration

Basic Settings

Parameter	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.

Advanced Settings

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

Recovery Timeout	values are between 30 and 86400 seconds (24 hours).
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

MSTI Mapping Information

To configure the Spanning Tree MSTI Mapping parameters via the Web Interface:

1. Click **Configuration** > **Spanning Tree** > **MSTI Mapping**
2. Enter in a name for the configuration
3. Enter the required VLAN's into the configured MSTI(s).
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

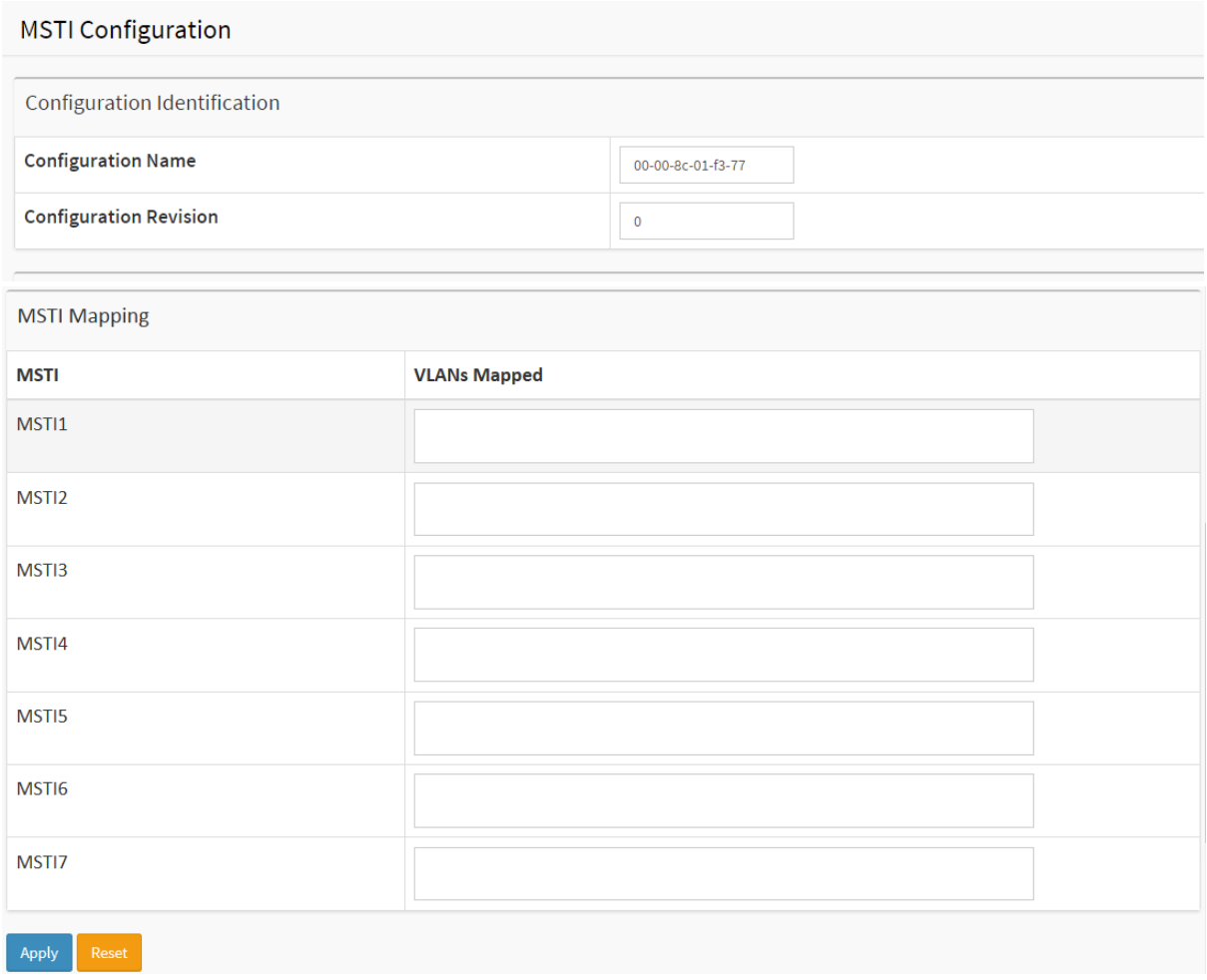
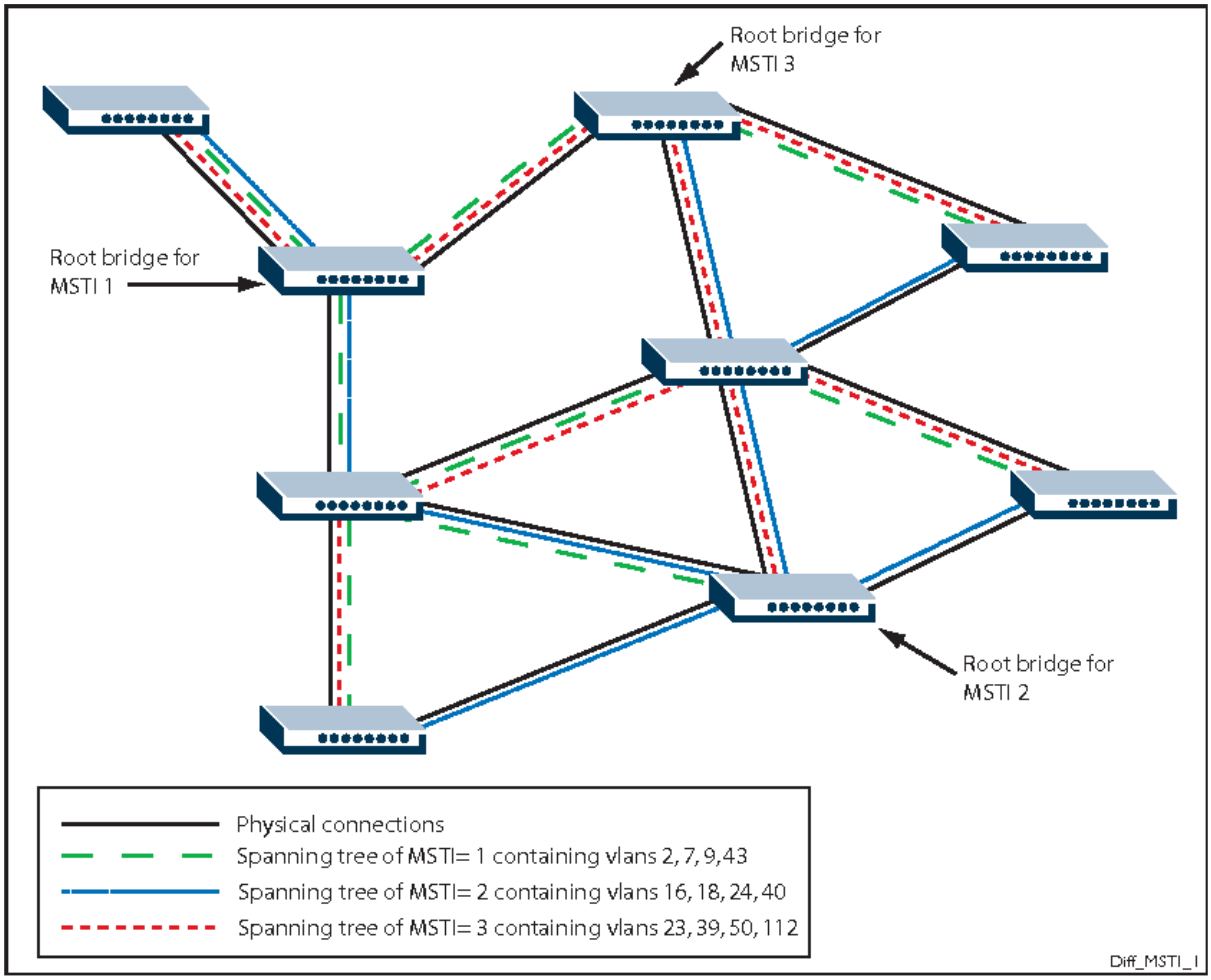


Fig: The MSTI Configuration



Example MSTI Configuration

Configuration Identification

Parameter	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTi	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

MSTI Priorities

This section is used to manually change the priority of the STP bridge instances. The CIST (Common and Internal Spanning Tree) is the default Bridge Instance when using MSTP and is always active. Any VLAN that has not been assigned to a MIST is assigned to the CIST. The lower the priority value, the higher the priority the bridge has.

Information

To configure the Spanning Tree MSTI priorities parameters via the Web Interface:

1. Click **Configuration** > **Spanning Tree** > **MSTI Priorities**
2. Configure the Priority for each MSTI. The lower Numeric Value the higher the priority.
3. Select Apply to save or Reset to revert any unsaved settings.

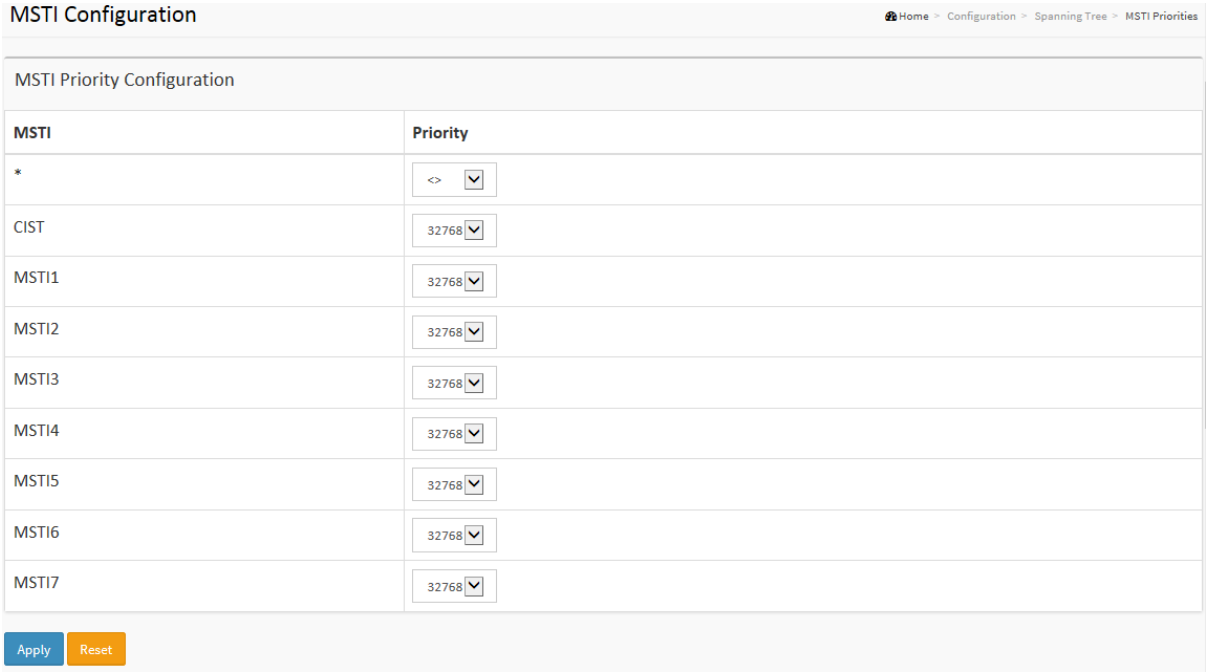


Fig: The MSTI Configuration

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 better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

CIST Ports

This section is used to configure individual STP Parameters for each port. Here you can enable and disable STP on individual ports, configure the ports as AdminEdge ports, give certain ports higher priority than others and much more.

Information

To configure the Spanning Tree CIST Ports parameters via the Web Interface:

1. Click **Configuration** > **Spanning Tree** > **CIST Ports**
2. Configure the **CIST Aggregated Port** Configuration Settings
3. Configure the **CIST Normal Port** settings, you can set each port individually or all at once if required.
4. Click the **Apply** button to save your changes or **the** Reset button to revert to previous settings.

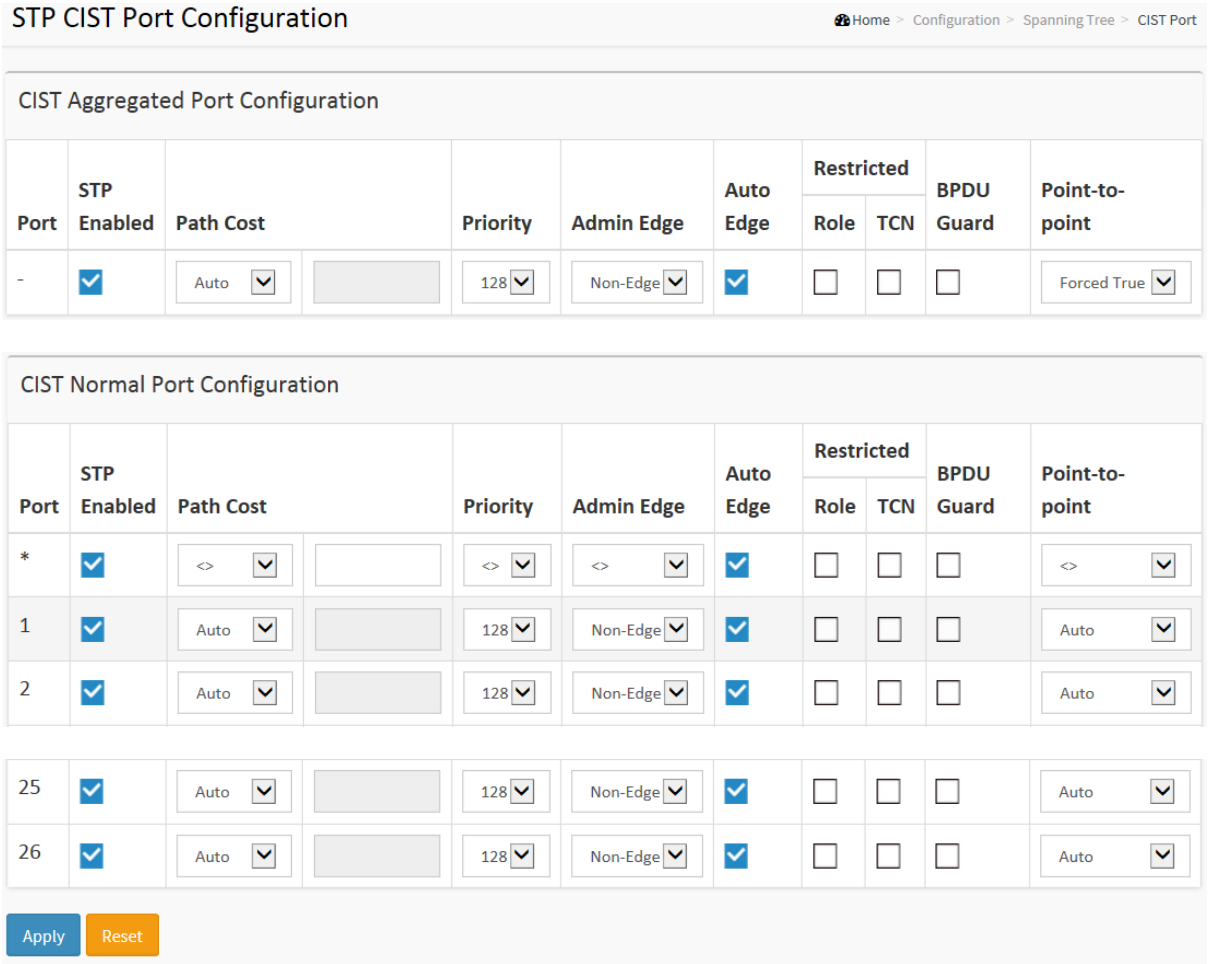


Fig: The STP CIST Port Configuration

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 favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
operEdge (State flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.
AdminEdge	Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point to Point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

MSTI Ports

This section is used to configure MSTI Port parameters. An MSTI Port is a virtual port and each MSTI has its own virtual port. The MSTI must be configured before the individual port configuration options can be applied. This section is much the same as the CIST Port settings but configuration done here is for each MSTI rather than the CIST.

Information

To configure the Spanning Tree CIST Ports parameters via the Web Interface:

1. Click **Configuration** > **Spanning Tree** > **MSTI Ports**
2. Select the MSTI you would like to configure and press the GET button.
3. Now you can configure the appropriate port settings for the MSTI.
4. Repeat for all MSTIs.
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

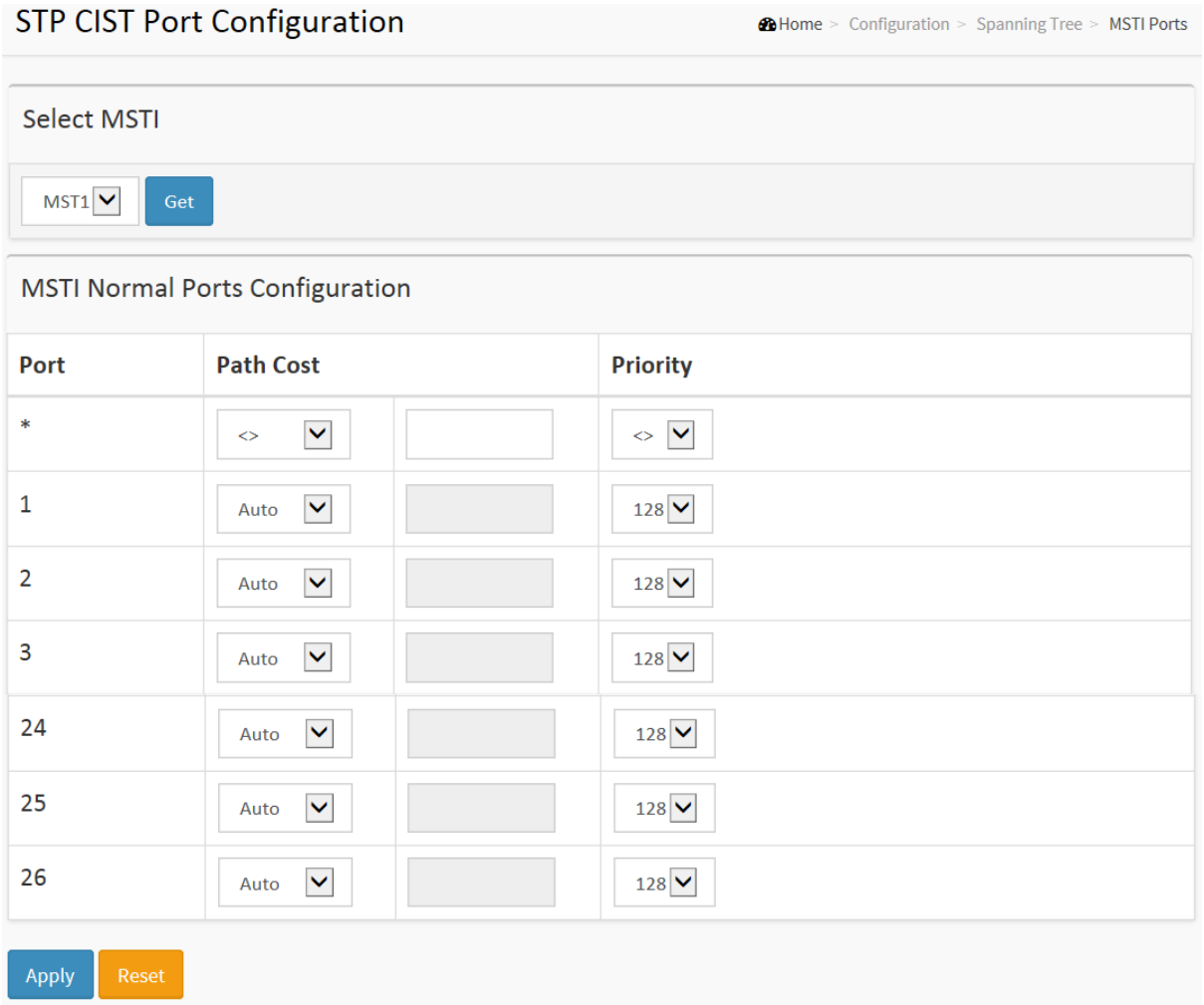


Fig: The MSTI Port Configuration

Parameter	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port.
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favors 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).
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

IPMC Profile

This page provides IPMC Profile related configurations.

Profile Table

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

Information

To configure the IPMC Profile parameters via the Web Interface:

1. Click **Configuration** > **IPMC Profile** > **Profile Table**
2. To enable Profile Mode, Select **Enabled** from the Global Profile Drop down menu
3. To add a new profile, click **Add New IMPC Profile** Option.
4. Click **Apply** to save the settings or **Reset** to revert any recently made changes.

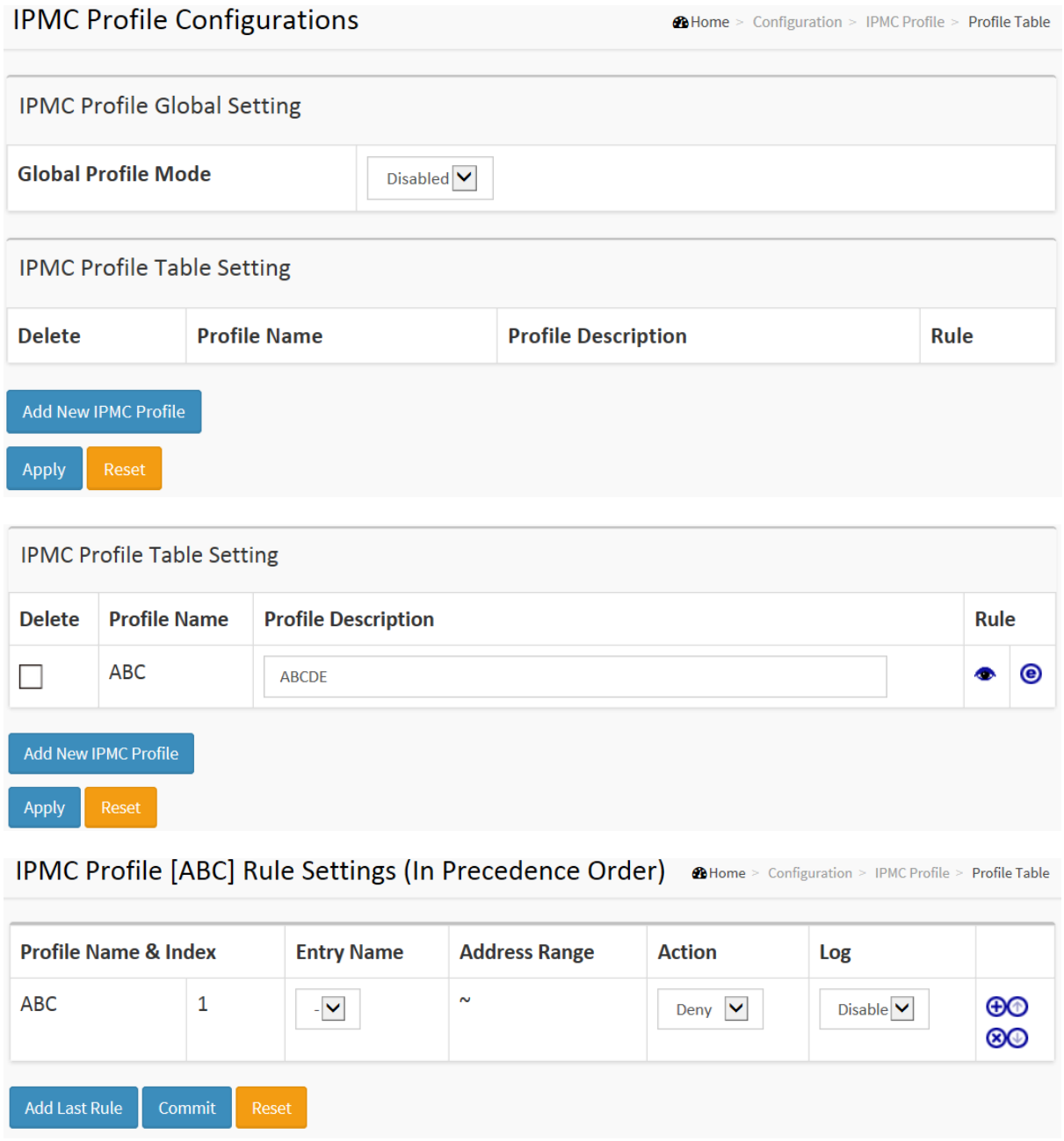


Fig: The IPMC Profile Configuration

Parameter	Description
Port	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
Global Profile Mode	Enable/Disable the Global IPMC Profile. System starts to do filtering based on profile settings only when the global

	profile mode is enabled.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has the unique name which is composed of at maximum 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.
Rule	When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons: List the rules associated with the designated profile. Adjust the rules associated with the designated profile.
Button	**Add New IPMC Profile** – Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save". **Apply** – Click to save changes. **Reset** – Click to undo any changes made locally and revert to previously saved values.

Address Entry

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

Information

To configure the IPMC Address Entry parameters via the Web Interface:

1. Click **Configuration** > **IPMC Profile** > **Address Entry**
2. To add a New Entry, Select **Add New Address (Range Entry)**
3. Select **Apply** to Save or **Reset** to revert any recently unsaved settings.

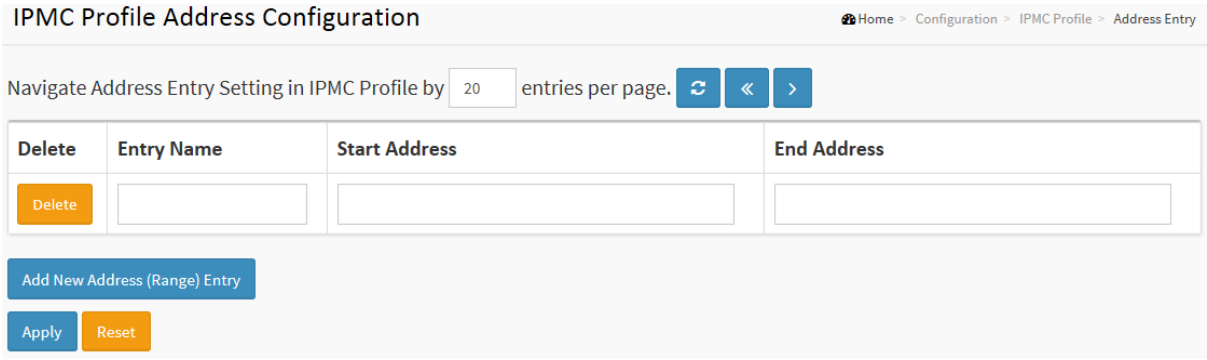


Fig: The IPMC Profile Address Configuration

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

Buttons	**Add New Address (Range) Entry** – Click to add new address range. Specify the name and configure the addresses. Click "Save" **Apply** – Click to save changes. **Reset** – Click to undo any changes made locally and revert to previously saved values.

MVR

Multicast VLAN registration (MVR) allows you to efficiently distribute IPTV multicast stream across an Ethernet ring-based Layer 2 network and reduce the amount of bandwidth consumed by this multicast traffic.

In a standard Layer 2 network, a multicast stream received on one VLAN is never distributed to interfaces outside that VLAN. If hosts in multiple VLANs request the same multicast stream, a separate copy of that multicast stream is distributed to the requesting VLANs.

MVR introduces the concept of a multicast source VLAN (MVLAN), which is created by MVR and becomes the only VLAN over which IPTV multicast traffic flows throughout the Layer 2 network. The Alloy AS Series Switches that are enabled for MVR selectively forward IPTV multicast traffic from interfaces on the MVLAN (source interfaces) to hosts that are connected to interfaces that are not part of the MVLAN. These interfaces are known as MVR receiver ports. The MVR receiver ports can receive traffic from a port on the MVLAN but cannot send traffic onto the MVLAN, and they remain in their own VLANs for bandwidth and security reasons.

Information

To configure the MVR parameters via the Web Interface:

1. Click **Configuration** > **MVR**
2. Select to enable or disable MVR.
3. Configure settings for each individual port.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

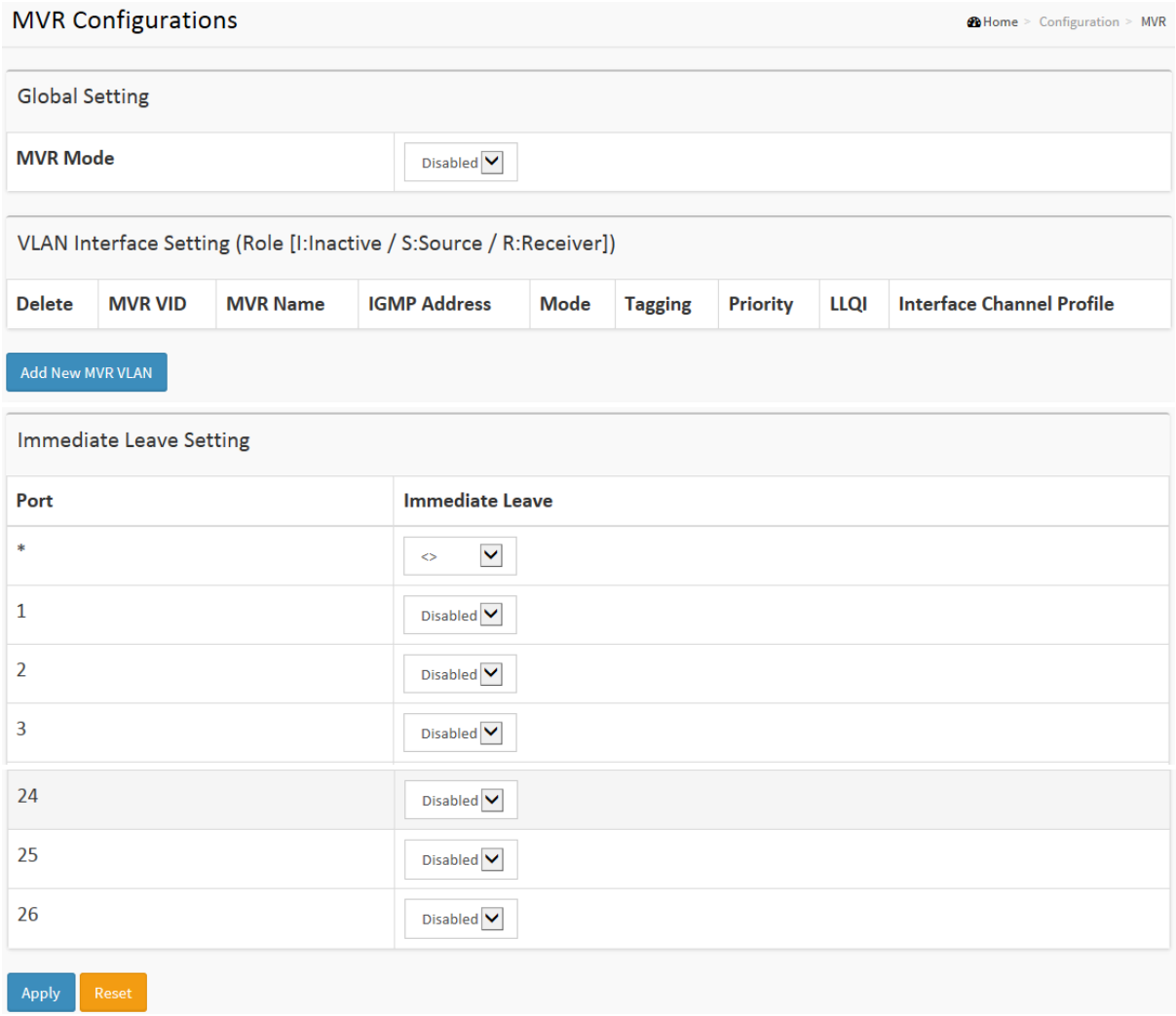


Fig: The MVR Configuration

Parameter	Description
MVR Mode	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping. It is suggested to enable Unregistered Flooding control when the MVR group table is full.
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
MVR VID	Specify the Multicast VLAN ID. **Caution**: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 32. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.
LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.
Interface Channel Setting	When the MVR VLAN is created, click the Edit symbol to expand the corresponding multicast channel settings for the specific MVR VLAN. Summary about the Interface Channel Setting (of the MVR VLAN) will be shown besides the Edit symbol.
Port	The logical port for the settings.
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles. **Inactive**: The designated port does not participate MVR operations.

	Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. **Receiver**: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. **Caution:** MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.
Immediate Leave	Enable the fast leave on the port.

IPMC

IGMP Snooping

IGMP Snooping is a way for Layer 2 switches to reduce the amount of multicast traffic on a LAN. Without IGMP Snooping, Layer 2 switches handle IP multicast traffic in the same manner as broadcast traffic and forward multicast frames received on one port to all other ports in the same VLAN. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic, by looking into IGMP packets to learn which attached hosts need to receive which multicast groups. This allows the switch to forward multicast traffic only out the appropriate ports. If it sees multiple reports sent for one group, it will forward only one of them.

Joining a multicast group (Membership report)

When a host wants to receive a stream, referred to as “joining a group”, it sends out an IGMP packet containing the address of the group it wants to join. This packet is called an IGMP Membership report, often referred to as a “join packet”. This packet is forwarded through the LAN to the local IGMP querier, which is typically a router. Once the querier has received an IGMP join message, it knows to forward the multicast stream to the host. If it is not already receiving the stream, it must tell the devices between itself and the multicast source, which may be some hops away from the querier, that it wishes to receive the stream. This might involve a process of using Layer 3 multicast protocols to signal across a WAN, or it might be as simple as receiving a stream from a locally connected multicast server.

Staying in the multicast group (Query message)

The Query message is used by a querier to determine whether hosts are still interested in an IGMP group. At certain time intervals (the default is 125 seconds), the querier sends an IGMP query message onto the local LAN. The destination address of the query message is a special “all multicast groups” address. The purpose of this query is to ask “Are there any hosts on the LAN that wish to remain members of multicast groups?” After receiving an IGMP query, any host that wants to remain in a multicast group must send a new join packet for that group. If a host is a member of more than one group, then it sends a join message for each group it wants to remain a member of. The querier looks at the responses it receives to its query, and compares these to the list of multicast stream that it is currently registered to forward. If there are any items in that list for which it has not received query responses, it will stop forwarding those stream. Additionally, if it is receiving those stream through a Layer 3 network, it will send a Layer 3 routing protocol message upstream, asking to no longer receive that stream.

Leaving the multicast group (Leave message)

How a host leaves a group depends on the IGMP version that it is using. Under IGMP version 1, when a host has finished with a data stream, the local querier continues to send the stream to the host until it sends out the next query message and receives no reply back from the host. IGMP version 2 introduced the Leave message. This allows a host to explicitly inform its querier that it wants to

leave a particular multicast group. When the querier receives the Leave message, it sends out a group specific query asking whether any hosts still want to remain members of that specific group. If no hosts respond with join messages for that group, then the querier knows that there are no hosts on its LAN that are still members of that group. This means that for that specific group, it can ask to be pruned from the multicast tree. IGMP version 3 removed the Leave message. Instead a host leaves a group by sending a join message with no source specified.

The AS Series supports IGMP Snooping V1, V2 and V3 and supports up to 1024 multicast groups, both IGMP Querier and IGMP Proxy are also supported.

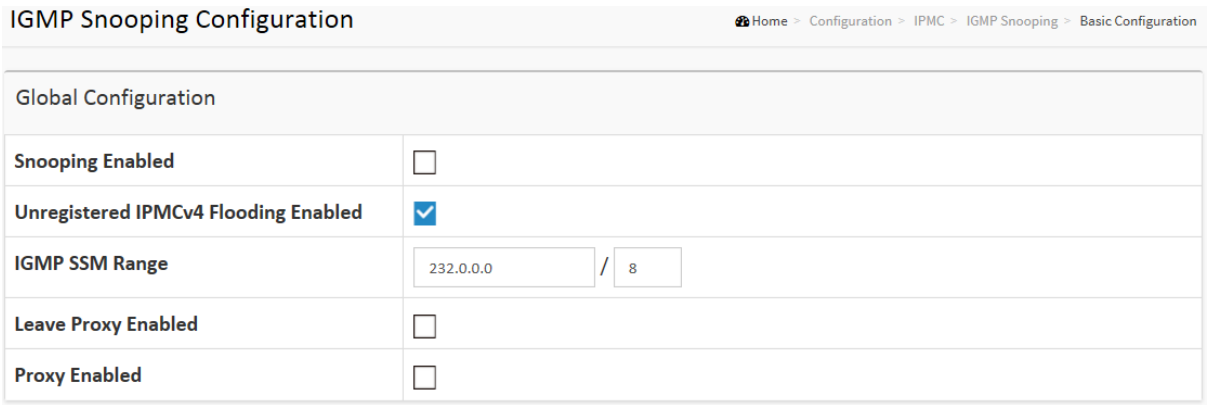
Basic Configuration

The section describes how to set the basic IGMP snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP

Information

To configure the IGMP Snooping parameters via the Web Interface:

1. Click **Configuration** > **IPMC** > **IGMP Snooping** > **Basic Configuration**
2. Select to Enable or Disable IGMP Snooping on the switch.
3. Configure ports to be Router Ports, Fast Leave Ports and select whether you would like to enable throttling.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.



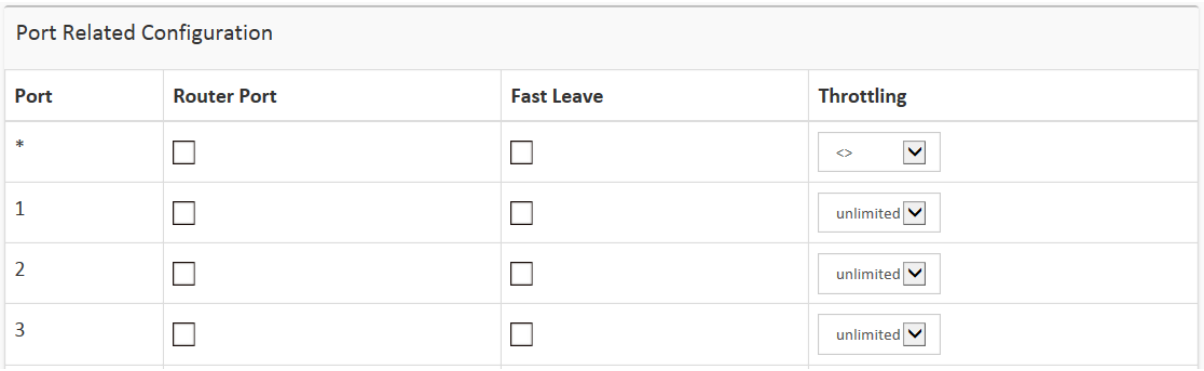


Fig: The IGMP Snooping Configuration.

Parameter	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding enabled	Enable unregistered IPMCv4 traffic flooding.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Format: (IP address/ sub mask)
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Port	It shows the physical Port index of switch.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Enable the fast leave on the port.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.

VLAN Configuration

This section is used to configure specific IGMP Settings for each of the configured VLAN groups. IGMP Snooping can be enable or disabled for every individual VLAN group. 20 VLAN groups will be displayed on the screen by default this can be increased to a maximum of 99. The VLAN with the lowest VID will be displayed at the top of the table. To browse to additional pages use the arrow keys at the top of the page.

Information

To configure the IGMP VLAN parameters via the Web Interface:

1. Click **Configuration** > **IPMC** > **IGMP Snooping** > **VLAN Configuration**
2. Select the appropriate IGMP parameters for the specific VLAN group.
3. Repeat for all VLAN groups configured on the switch. Use the arrow keys to move between pages. The Refresh button can be used to refresh the page for the latest information.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

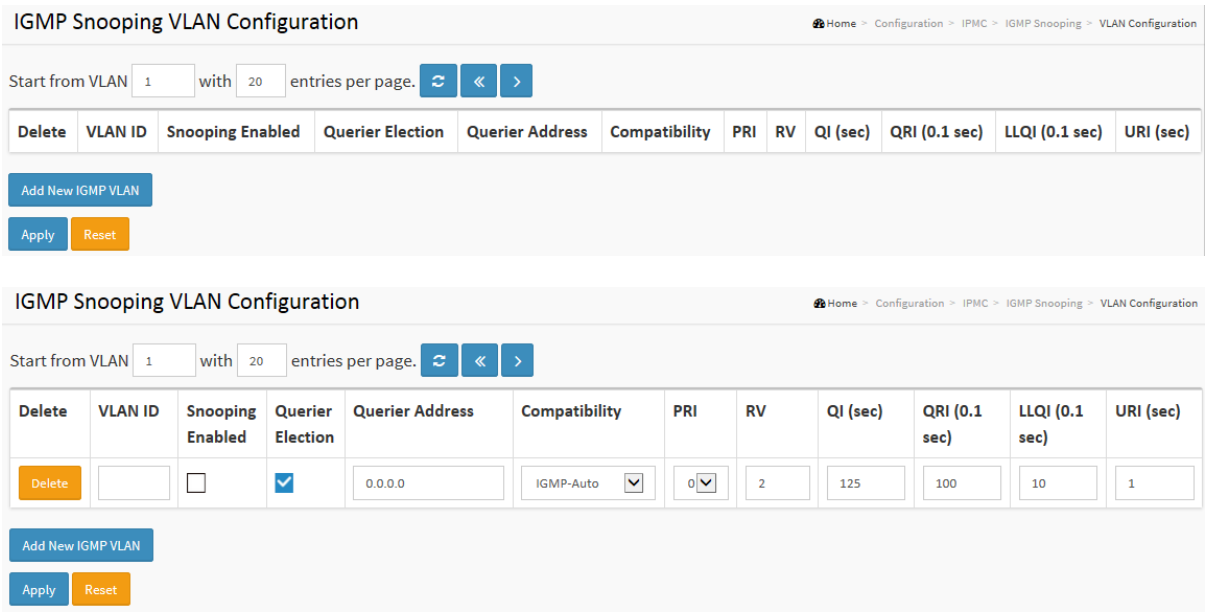


Fig: The IGMP Snooping VLAN Configuration.

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

IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
Rv	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.
QRI	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).
LLQI (LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds;

	default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. .
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Information

To configure the IGMP Port Group Filtering parameters via the Web Interface:

1. Click **Configuration** > **IGMP** > **IGMP Snooping** > **Port Filtering**
2. Click Add New Filtering Group.
3. Specify the Multicast IP Address and click Apply to save the settings.
4. If you wish to delete an entry check the delete tick box and click Apply.
5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

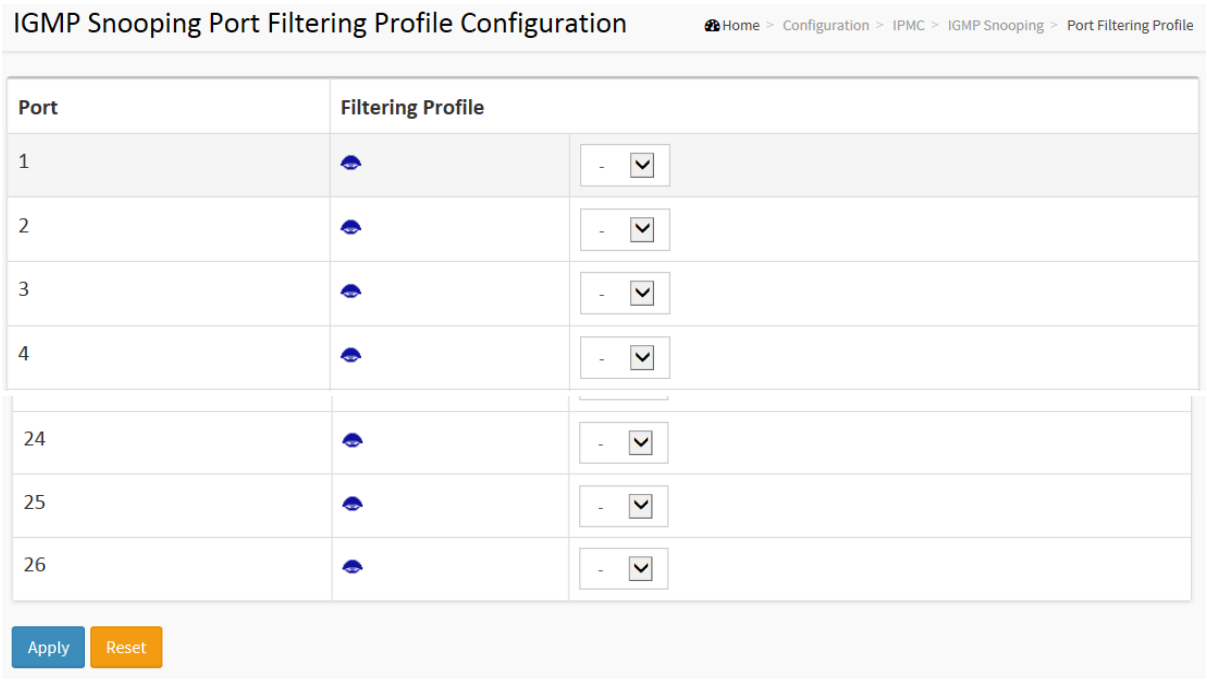


Fig: The IGMP Snooping Port Group Filtering Profile.

Port Filtering Profile

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and when applied to a port to deny access to that port on the configured multicast address. 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.
IGMP filtering controls only IGMP membership join reports and has no relationship to the function that directs the forwarding of IP multicast traffic.

Parameter	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button
Profile Management Button	You can inspect the rules of the designated profile by using the following button:  : List the rules associated with the designated profile.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

MLD Snooping

Multicast Listener Discovery (MLD) snooping constrains the flooding of IPv6 multicast traffic on VLANs on a switch. When MLD snooping is enabled on a VLAN, the AS Series Switches examine MLD messages between hosts and multicast routers and learn which hosts are interested in receiving traffic for a multicast group. Based on what it learns, the switch then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

By default, a switch floods Layer 2 multicast traffic on all interfaces on a switch, except for the interface that is the source of the multicast traffic. This behaviour can consume significant amounts of bandwidth.

You can enable MLD snooping to avoid this flooding. When you enable MLD snooping, the switch monitors MLD messages between receivers and multicast routers and uses the content of the messages to build an IPv6 multicast forwarding table—a database of IPv6 multicast groups and the interfaces that are connected to members of the groups. When the switch receives multicast traffic for a multicast group, it uses the forwarding table to forward the traffic only to interfaces that are connected to receivers that belong to the multicast group.

The AS Series switches support MLD v1 and v2.

Basic Configuration

This section is used to enable and configure MLD Snooping on the AS Series switches.

Information

To configure the MLD Snooping parameters via the Web Interface:

1. Click **Configuration** > **IPMC** > **MLD Snooping** > **Basic Configuration**
2. Select to enable or disable MLD Snooping on the switch.
3. Configure ports to be Router Ports, Fast Leave Ports and select whether you would like to enable throttling.
4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

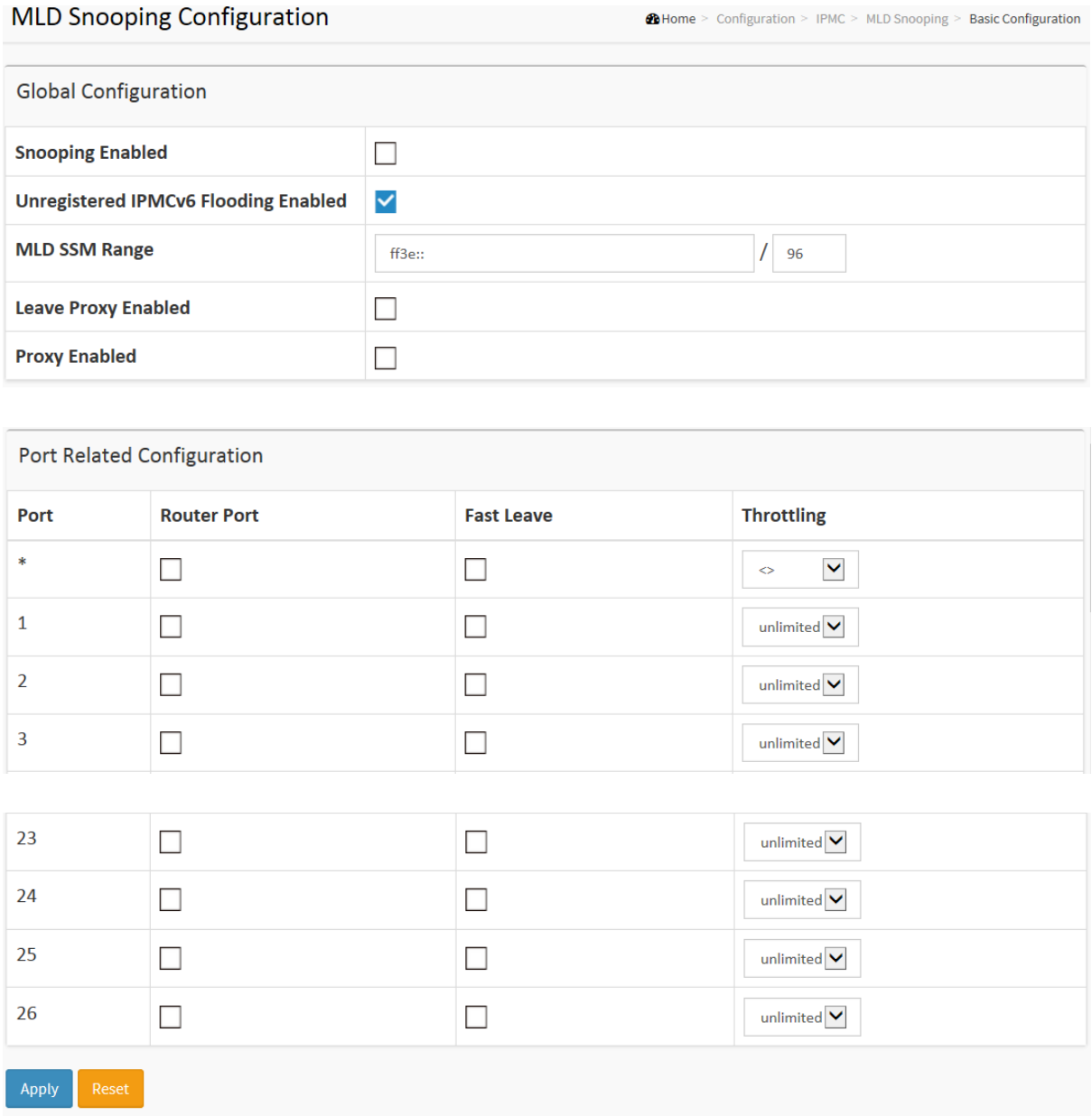


Fig: The MLD Snooping Basic Configuration.

Parameter	Description
Snooping Enabled	Enable the Global MLD Snooping.
Unregistered IPMCv6 Flooding enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address (Using IPv6 Address) range.
Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Fast leave	To evoke to enable the fast leave on the port.
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.
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

VLAN Configuration

This section is used to configure specific MLD Settings for each of the configured VLAN groups. MLD Snooping can be enabled or disabled for every individual VLAN group. 20 VLAN groups will be displayed on the screen by default this can be increased to a maximum of 99. The VLAN with the lowest VID will be displayed at the top of the table. To browse to additional pages use the arrow keys at the top of the page.

Information

To configure the MLD Snooping VLAN parameters via the Web Interface:

1. Click **Configuration** > **IPMC** > **MLD Snooping** > **VLAN Configuration**
2. Select the appropriate MLD parameters for the specific VLAN group.
3. Repeat for all VLAN groups configured on the switch. Use the arrow keys to move between pages. The Refresh button can be used to refresh the page for the latest information.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

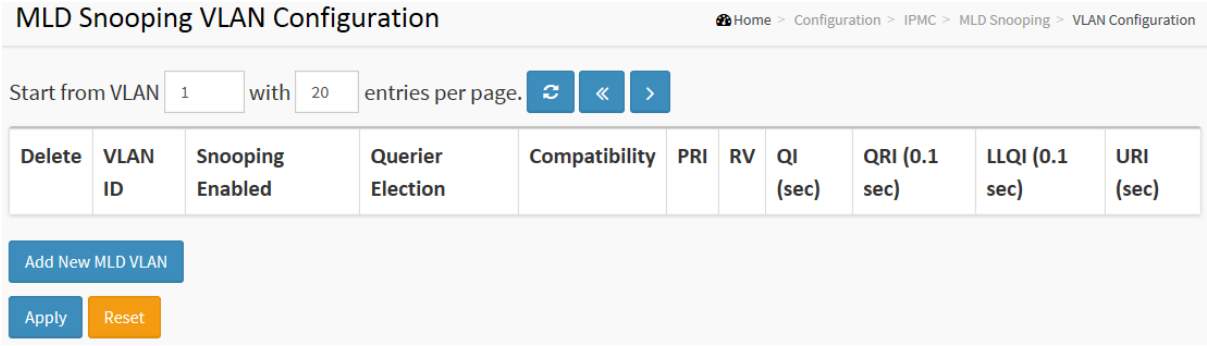


Fig: The MLD Snooping VLAN Configuration.

Parameter	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	It displays the VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected. .
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier

	election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.
Rv	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255; default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds; default query interval is 125 seconds.
QRI	Query Response Interval. The Max Response Time used to calculate the Max Resp Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds; default query response interval is 100 in tenths of seconds (10 seconds).
LLQI(LMQI for IGMP)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds; default last member query interval is 10 in tenths of seconds (1 second).
URI	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second. .

Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Port Group Filtering

With this feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and when applied to a port to deny access to that port on the configured multicast address. 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.

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

Information

To configure the MLD Snooping Port Group Filtering parameters via the Web Interface:

1. Click **Configuration** > **IPMC** > **MLD Snooping** > **Port Group Filtering**
2. Click Add New Filtering Group.
3. Specify the Multicast IP Address and click Apply to save the settings.
4. If you wish to delete an entry check the delete tick box and click Apply.
5. Click the Apply button to save your changes or the Reset button to revert to previous settings.

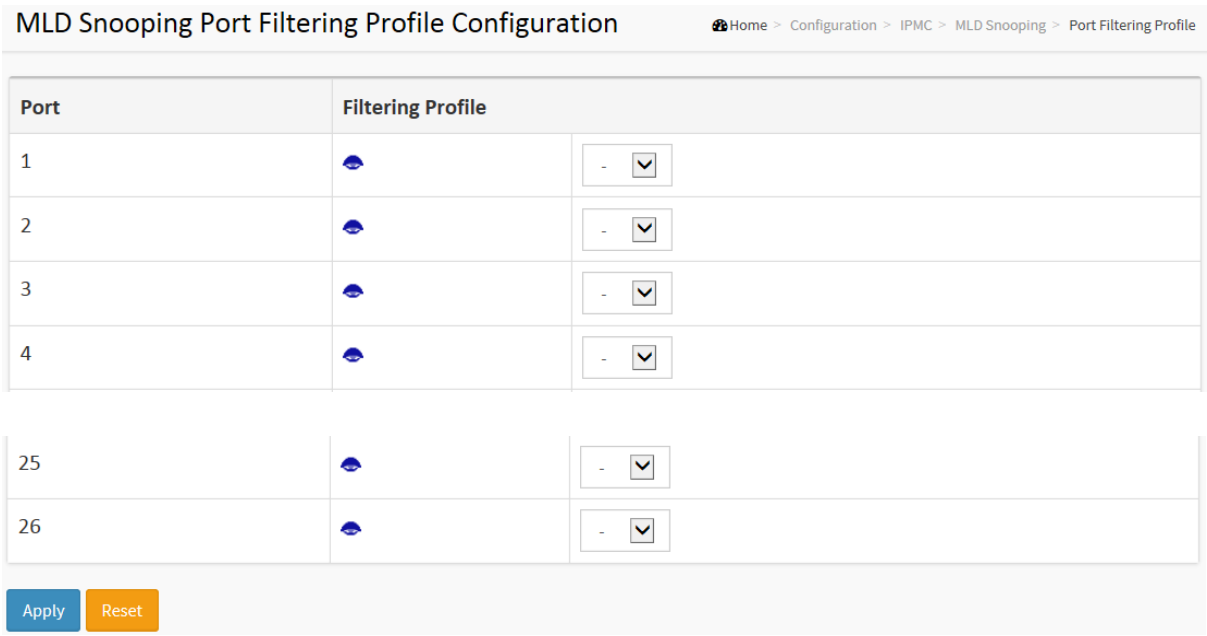


Fig: MLD Snooping Port Configuration

Parameter	Description
Port	The logical port for the settings.
Filtering Profile	Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.
Profile management Button	You can inspect the rules of the designated profile by using the following button:  : List the rules associated with the designated profile.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

LLDP

LLDP enables Ethernet network devices, such as switches and routers, to transmit and/or receive device-related information to or from directly connected devices on the network, and to store such information learned about other devices. The data sent and received by LLDP is useful for many reasons. The switch can discover neighbors—other devices directly connected to it. Devices can use LLDP to advertise some parts of their Layer 2 configuration to their neighbors, enabling some kinds of misconfiguration to be more easily detected and corrected.

LLDP is a link level ("one hop") protocol; LLDP information can only be sent to and received from devices that are directly connected to each other, or connected via a hub or repeater. Advertised information is not forwarded on to other devices on the network.

The information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgement.

LLDP operates over physical ports (Layer 2) only. For example, it can be configured on switch ports that belong to static or dynamic aggregated links (channel groups), but not on the aggregated links themselves; and on switch ports that belong to VLANs, but not on the VLANs themselves.

LLDP Configuration

This section is used to enable and configure LLDP on the AS Series switches.

Information

To configure the LLDP parameters via the Web Interface:

1. Click **Configuration** > **LLDP** > **LLDP**.
2. Modify any LLDP timing parameters if needed.
3. Disable, enable two way communication, Tx only or Rx only on a per port basis.
4. Specify the information to include in the TLV field of advertised messages.
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

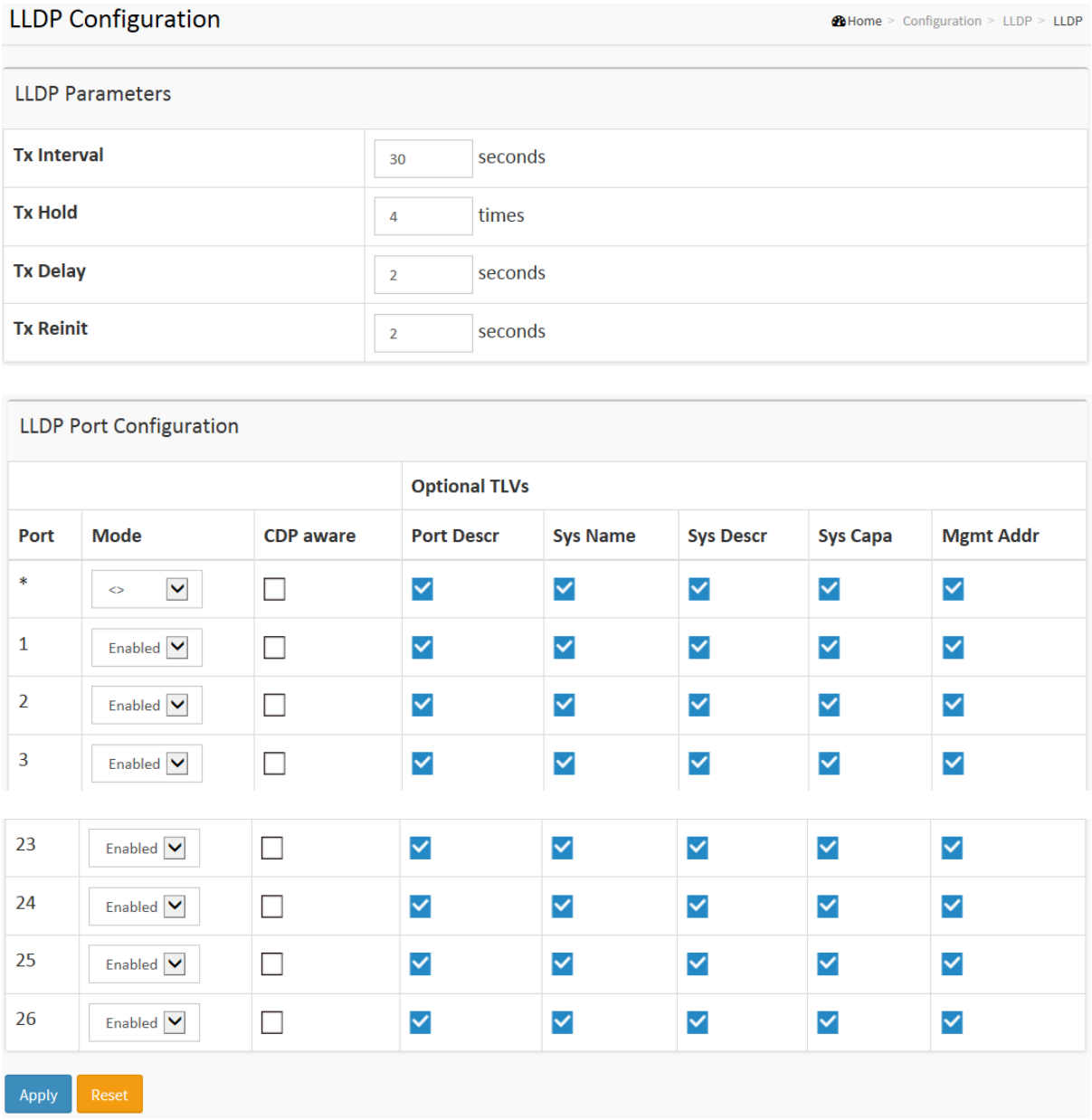


Fig: The LLDP Configuration

LLDP Parameters

Parameter	Description
Tx Interval	The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 -

	10 times.
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.
Tx Reinit	When a port is disabled, LLDP is disabled or the switch is rebooted, an LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP Port Configuration

Parameter	Description
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. **Rx only** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. **Tx only** The switch will drop LLDP information received from neighbors, but will send out LLDP information. **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbors. **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
CDP Aware	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the port is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The

	CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors' table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table. If all ports have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets when the hold time is exceeded.
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

LLDP-MED

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

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

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

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

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

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

Information

To configure the LLDP-MED parameters via the Web Interface:

1. Click **Configuration** > **LLDP** > **LLDP-MED**
2. Modify the fast repeat setting if required.
3. Fill in the required fields for the location parameters.
4. Add a new LLDP-MED policy and configured additional settings.
5. Assign **Policy** for required ports.
6. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

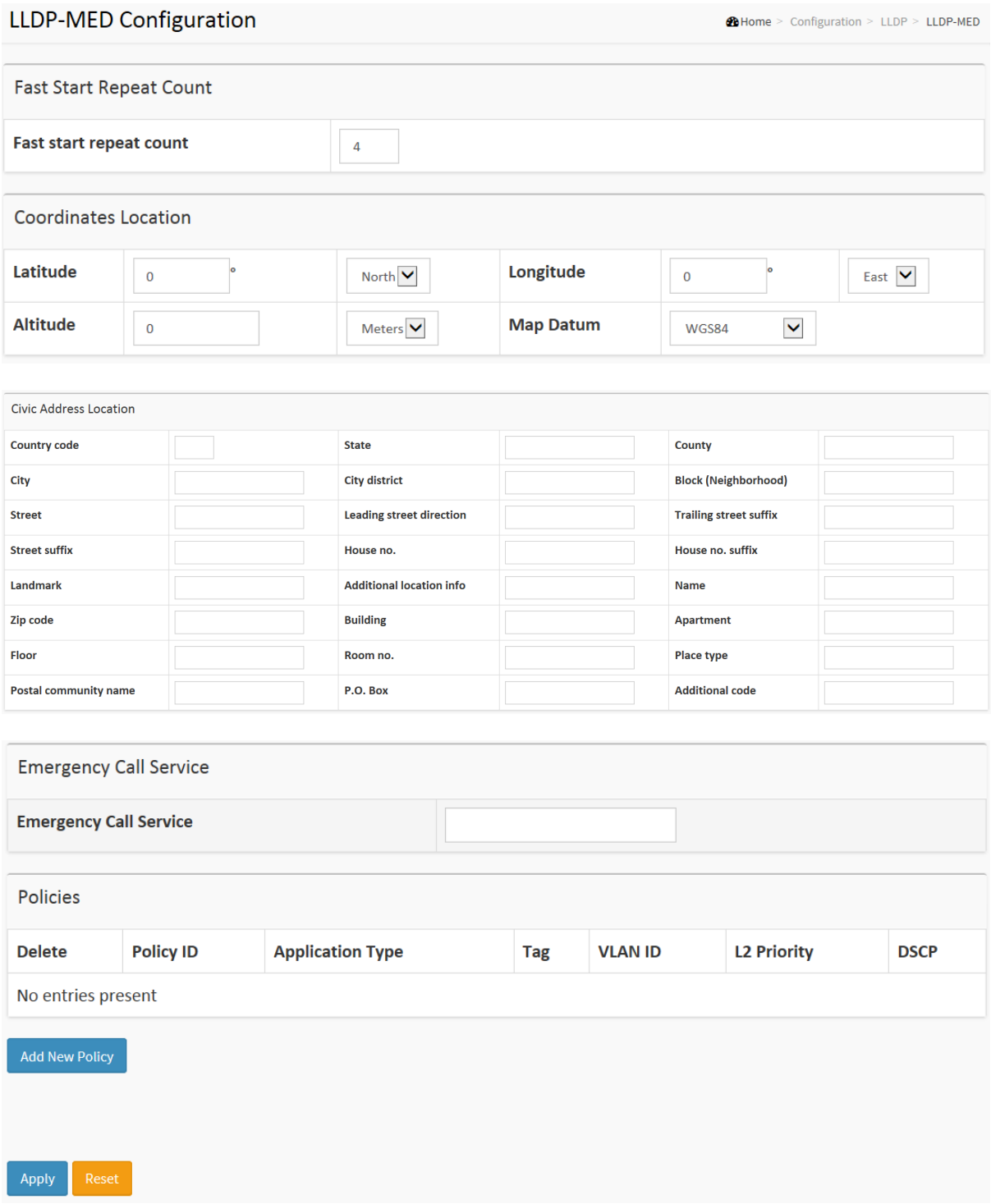


Fig: LLDP-MED Configuration

Fast start repeat count

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

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

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission will be repeated. The recommended value is 4 times,

given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

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

Coordinates Location

Parameter	Description
Latitude	Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.
Longitude	Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Attitude	Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). Meters: Representing meters of Altitude defined by the vertical datum specified. Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.
Map Datum	The Map Datum is used for the coordinates given in these options: WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich. NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW). NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.
Civic Address Location	IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).
Country Code	The two-letter ISO 3166 country code in capital ASCII letters - Example: AU, DE or US.
State	National subdivisions (state, canton, region, province, prefecture).
Country	County, parish, gun (Japan), district.
City	City, township, shi (Japan) - Example: Copenhagen.
City District	City division, borough, city district, ward, chou (Japan).
Block (Neighborhood)	Neighborhood, block.
Street	Street - Example: Poppelvej.

Leading Street direction	Leading street direction - Example: N.
Training Street suffix	Trailing street suffix - Example: SW.
Street suffix	Street suffix - Example: Ave, Platz.
House No	House number - Example: 21.
House No suffix	House number suffix - Example: A, 1/2.
Landmark	Landmark or vanity address - Example: Columbia University.
Additional Location info	Additional location info - Example: South Wing.
Name	Name (residence and office occupant) - Example: Flemming Jahn.
Zip Code	Postal/zip code - Example: 2791.
Building	Building (structure) - Example: Low Library.
Apartment	Unit (Apartment, suite) - Example: Apt 42.
Floor	Floor - Example: 4.
Room no	Room number - Example: 450F.
Place type	Place type - Example: Office.
Postal Community Name	Postal community name - Example: Leonia.
P.O Box	Post office box (P.O. BOX) - Example: 12345.
Additional Code	Additional code - Example: 1320300003.
Emergency Call Service	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

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

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

The network policy attributes advertised are:

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

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

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

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

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

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

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

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

Parameter	Description
Delete	Check to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific ports.
Application Type	Intended use of the application types: 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. Voice Signaling (conditional) - for use in network topologies that require a different policy for the voice signaling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy. 3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. Guest Voice Signaling (conditional) - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services. 7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. Video Signaling (conditional) - for use in network topologies that require a separate policy for the video signaling than for the video media. This

	application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.
Tag	Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance. Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003
VLAN ID	VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003.
L2 Priority	L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.
DSCP	DSCP value to be used to provide Diffserv node 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. Click "Save".
Port Policies Configuration	Every port may advertise a unique set of network policies or different attributes for the same network policies, based on the authenticated user identity or port configuration.
Port	The port number to which the configuration applies.
Policy ID	The set of policies that shall apply to a given port. The set of policies is selected by check marking the checkboxes that corresponds to the policies.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

PoE

PoE or Power over Ethernet is an IEEE standard used to pass electrical power along with data over standard Ethernet Cable. Utilising 2 of the 4 pairs of an Ethernet Cable PoE provides up to 15.4W (IEEE 802.3af) or 25.5W (IEEE 802.3at) of power. PoE is used to power devices such as IP Phones, Wireless Access Points and IP Cameras. Being able to use a single cable to run both data and power saves in cabling costs, helps unclutter messy cables on your desk and is perfect for those environments where a power point is not able to be installed where your Ethernet equipment is needed.

The AS Series switches are IEEE 802.3at compliant and can supply up to 25.5W per port.

Advanced features such as PoE Power scheduling, PoE priority and having the ability to allocate a particular amount of power per port are just some of the features that the AS series support.

Configuration

This section is used to enable/disable PoE on a per port basis, set the priority level and set the maximum power allowed per port on the AS Series switches.

Information

This section is used to configure PoE Settings on the AS Series switches.

1. Select **Configuration** > **PoE** > **Configuration**
2. Select the **Reserved Power** option (Class/Allocation or LLDP-MED)
3. Choose the **Power Management Mode** (Actual Consumption or Reserved power)
4. Select to **Enable** or **Disable** PoE on each port. By selecting the option from the PoE Mode drop down menu
5. Set the required priority level and set the maximum power allowed for the port. 30W is the Maximum Power Allowed as per the IEEE 802.3at Class 4 PDs standard
6. Tick the **Reset** button next to the required port to reset the device connected.
7. Click the **Apply** button to save your changes or the Reset button to revert to previous settings.

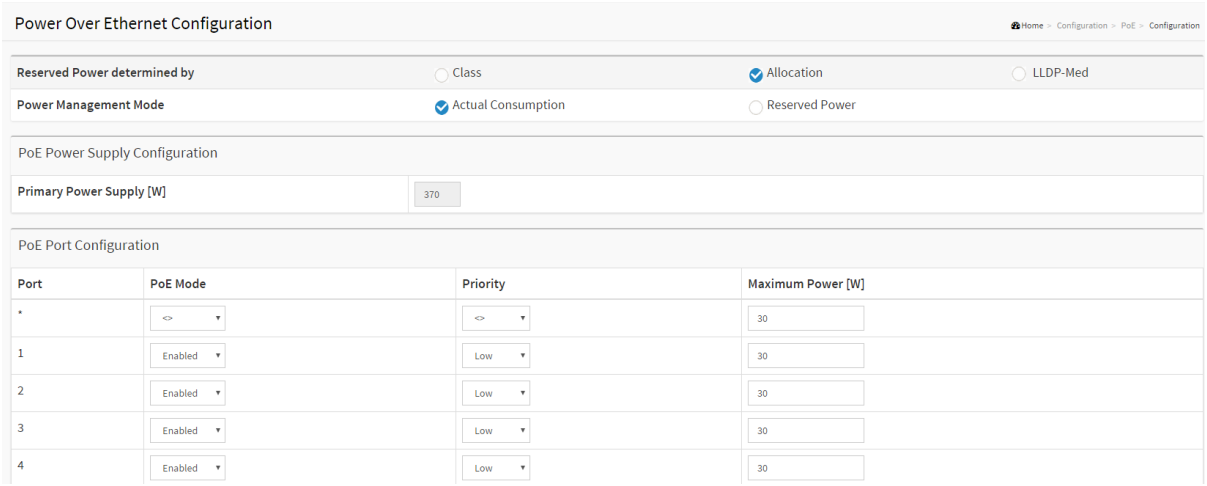


Fig: The PoE Configuration

Power Supply Configuration

Parameter	Description
Reserved Power determined by	There are three modes for configuring how the ports/PDs may reserve power. 1. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. 2. Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect. 3. LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class modeIn this mode the Maximum Power fields have no effect For all modes: If a port uses more power than the reserved power for the port, the port is shut down.
Power Management Mode	There are 2 modes for configuring when to shut down the ports: 1. Actual Consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

	2. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.
Port	This is the logical port number for this row. Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.
PoE Mode	**Enabled**: PoE enabled for the port. **Disabled**: PoE disabled for the port.
Priority	The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical. The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.
Maximum Power	The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device. The maximum allowed value is 30 W.-

Power Delay

This section is used to configure time periods in which particular ports will power on the connected PoE devices.

Information

This section is used to configure PoE Power Delay settings on the AS Series switches.

1. Select **Configuration > PoE > Power Delay**
2. **Enable** or **Disable** the Power Delay function for each port and set the delay period in seconds.
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

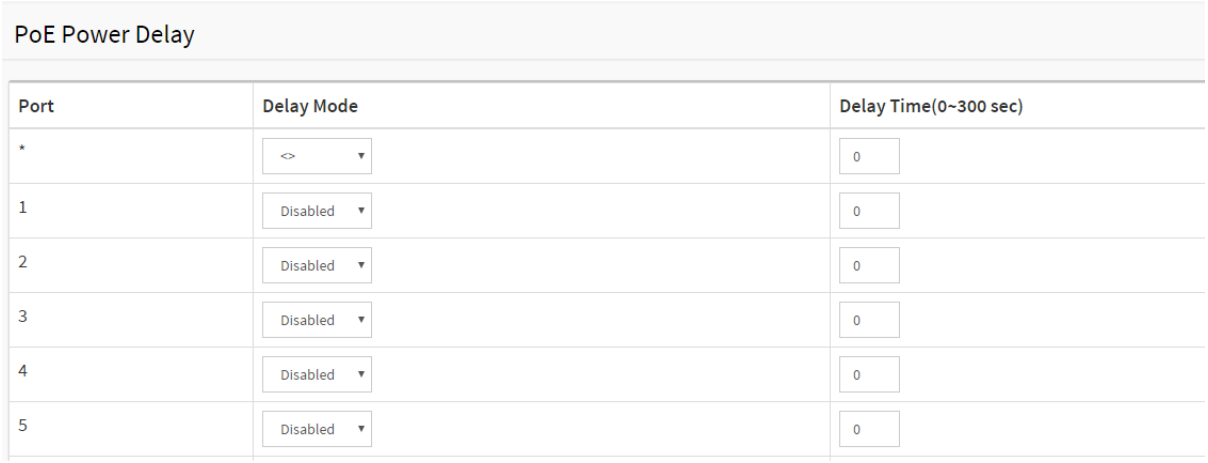


Fig: PoE Power Delay

Parameter	Description
Port	This is the logical port number for this row
Delay Mode	Turn on / off the power delay function. **Enabled**: Enable POE Power Delay. **Disabled**: Disable POE Power Delay.
Delay Time (0-300sec)	When rebooting, the PoE port will start to provide power to the PD when it out of delay time. default: 0, range: 0-300 sec.

Scheduling

The AS Series PoE switches support a PoE Scheduling feature that allows the administrator to power off devices when they are not in use. This can be used as a power saving feature to limit the amount of power draw of the switch.

Information

To configure the PoE Scheduling function via the Web Interface:

1. Click **Configuration** > **PoE** > **Scheduling**
2. Select the Port from the drop down box and select to enable or disable the scheduling feature.
3. Set the time required for the device to be powered on by ticking the check boxes next to the appropriate time and days.
4. Click the **Apply** button to save your changes or the Reset button to revert to previous settings.

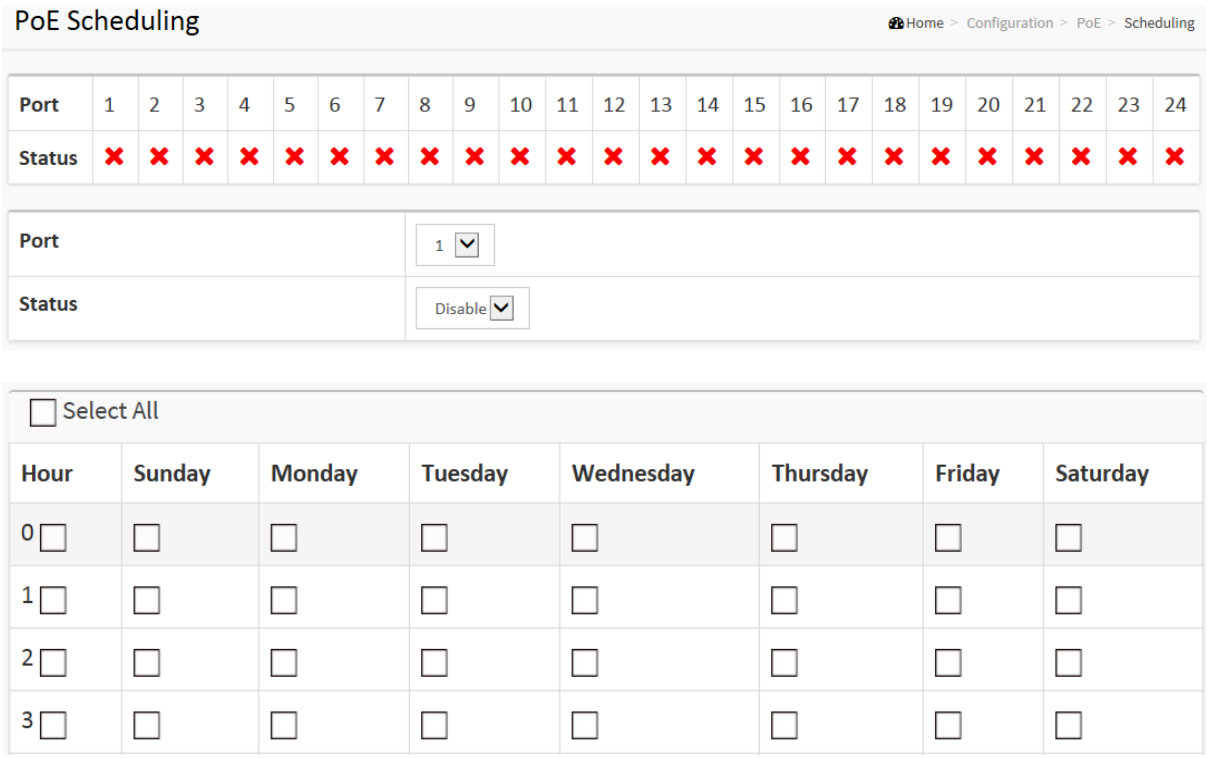


Fig: The PoE Scheduling Section

Parameter	Description
Port	This is the logical port number for this row
Status	PoE Scheduling Status. **Enabled:** Enable POE Scheduling. **Disabled:** Disable POE Scheduling.
Hour	The time of PoE port provide power of a day.

Auto Checking

The AS Series PoE switches have a feature that allows the administrator to constantly monitor the PD device connected to the switch. Periodically it will ping the device, if there is no response the switch can reboot the device.

Information

To configure the PoE Auto Checking function via the Web Interface:

1. Click **Configuration** > **PoE** > **Auto Checking**.
2. Enter the **IP Address** and time intervals into the sections provided.
3. Configure the appropriate Failure action and the reboot time for the device.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

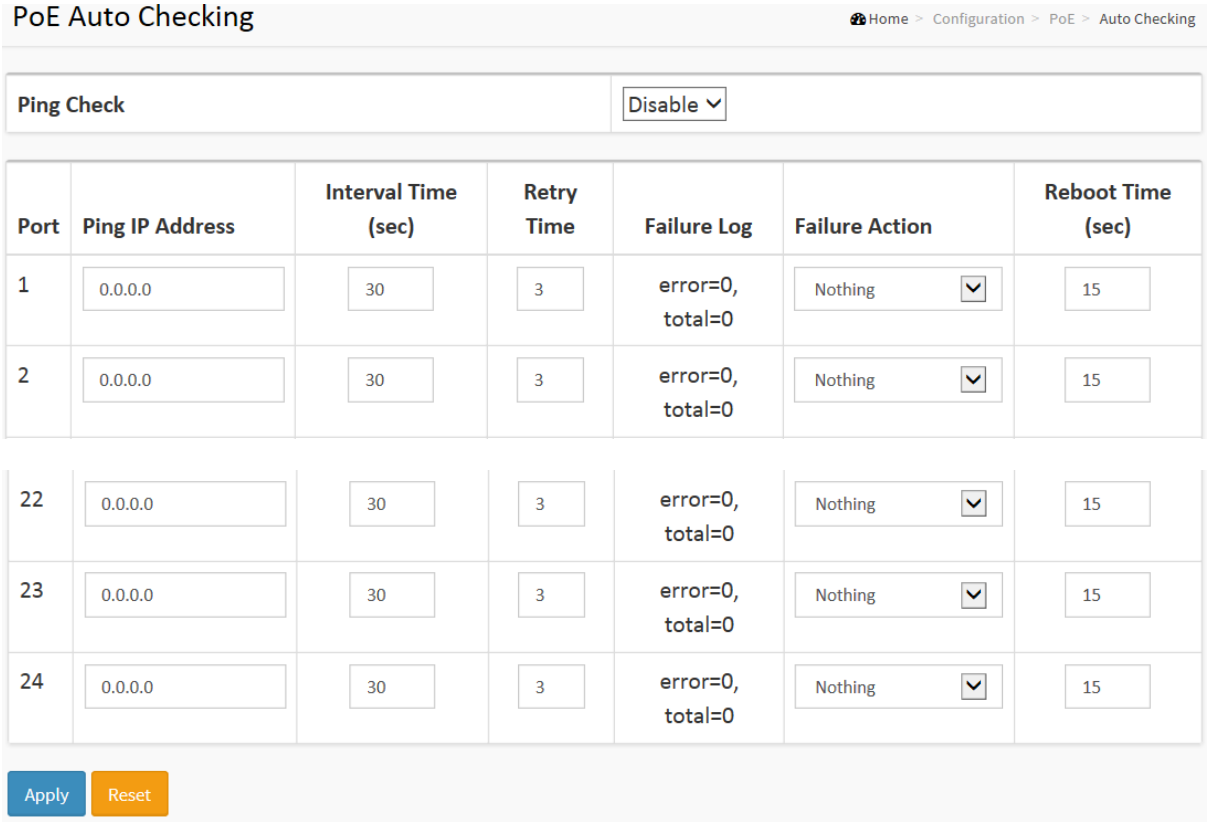


Fig: PoE Auto Checking

Power Supply Configuration

Parameter	Description
Ping Check	Enable Ping Check function can detects the connection between PoE port and power device. Disable will turn off the detection.
Port	Physical port of the switch.
Ping IP Address	The IP Address of the device connected to this port.
Interval Time (sec)	Enter the Interval time in seconds. This is the time between pinging the connected device. Default is 30 seconds.
Retry Time	How many times the switch will try and ping the device before the failure is logged and the Failure Action is implemented. Default is 3.
Failure Log	Displays the amount of errors and the amount of times the device has entered the failure state.
Failure Action	Select the appropriate action to be performed once the device cannot be detected. Options are Nothing and Reboot Remote.
Reboot time(sec)	The time for the device to reboot before the switch will start checking its state. Default is 15 seconds.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved

MAC Table

Switching of frames is based upon the Destination MAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the Destination MAC 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 Destination MAC address and switch ports. The frames also contain a Source 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 has been seen after a configurable age time.

Information

This section is used to configure MAC Address settings on the AS Series switches.

1. Select **Configuration > MAC Table.**
2. Specify the **Aging Configuration**, **MAC Learning Table** and **Static MAC Table Configuration**
3. Click **Apply** to save any of the changed sections, or **Reset** to revert changes.

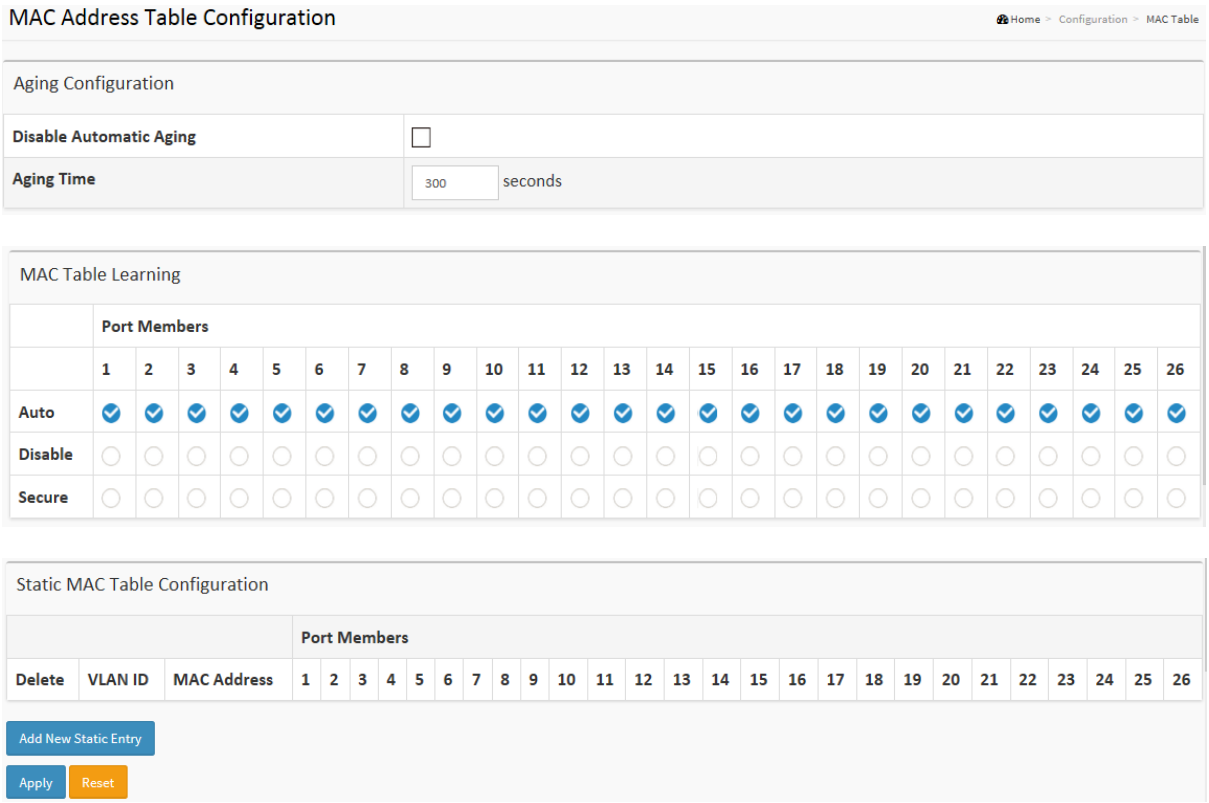


Fig: MAC Table Configuration

Aging Configuration

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

MAC Table Learning

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

Parameter	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack, and not per switch.

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

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
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.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved

	values.

VLAN's

The virtual LAN (VLAN) allows you to group physically separate users into the same broadcast domain. The use of VLANs improves security, segmentation, and flexibility. The use of VLANs also decreases the cost of arranging users, because no extra cabling is required.

VLANs allow an administrator to define user groups logically rather than by their physical locations. For example, you can arrange user groups such as accounting, engineering, and finance rather than grouping everyone on the first floor, everyone on the second floor, and so on.

- VLANs define broadcast domains that can span multiple LAN segments.
- VLAN segmentation is not bound by the physical location of users.
- Each switch port can be assigned to only one VLAN.
- Ports not assigned to the same VLAN do not share broadcasts, improving network performance.
- A VLAN can exist on one switch or on multiple switches.
- VLANs can connect across wide-area networks (WANs). The figure shows a VLAN design. VLANs are defined by user functions rather than locations.
- Each VLAN on a switch behaves as if it were a separate physical bridge. The switch forwards packets (including unicasts, multicasts, and broadcasts) only to ports assigned to the same VLAN from which it originated. This reduces on network traffic. VLANs require a trunk to span multiple switches. Each trunk can carry traffic for multiple VLANs

Information

This section of the switch allows for the configuration of VLANs on the switch. This page is divided into a global section at the top of the page and a per port configuration section.

1. Select **Configuration > VLANs.**
2. Enter the **Allowed Access VLANs** into this field. By default only VLAN 1 exists. However if you wish to create additional Access VLANs enter these here.
3. Enter the value for **Ethertype for Custom S-ports.** This field should only be changed if you are using Custom S-ports.
4. For **Port VLAN Configuration** this is where you configure each of the ports on the switch to the VLAN specifications you prefer. To configure specific options for individual ports either select from the drop down menu for options such as **Port VLAN**, **Port Type Ingress Acceptance** and **Egress Tagging.** For Port VLAN, Allowed VLAN's and Forbidden VLANs you need to enter in the number manually. For example for the **Allowed VLAN**, to specify a range you need to enter in in a dash such as 1-4095 This will allocate VLAN 1

through to 4095.
To enter in single VLANs you use a comma. Adding 1, 3, 8 will only allocate VLAN's 1, 3 and 8.
Note: If an option is greyed out it is not available to be modified in that configuration mode. For example if the Mode is set to access, you will not be able to allocate multiple VLAN's to the port, or change the Port Type as it is not applicable.

5. Select **Apply** to save the changes, to **Reset** to revert changes.

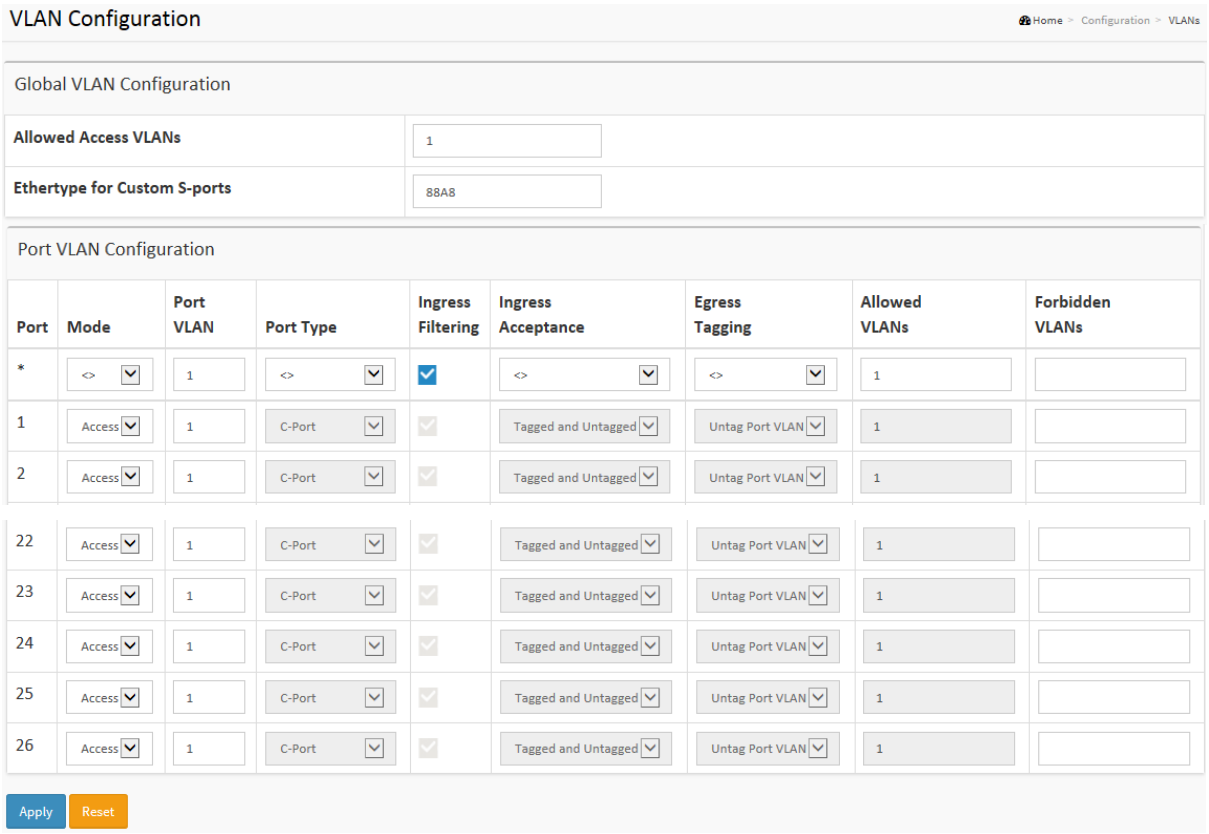


Fig. Global VLAN Configuration

Parameter	Description
Allowed Access VLAN's	This field shows the VLANs that are created on the switch. By default, only VLAN 1 exists. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

Parameter	Description
Port	This is the logical port number of this row.
Mode	The port mode (default is Access) determines the fundamental behaviour of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either greyed out or made changeable depending on the mode in question. Greyed out fields show the value that the port will get when the mode is applied. **Access:** Access ports are normally used to connect to end stations such as Computers and IP Handsets. Dynamic features like Voice VLANs may add the port to more VLANs behind the scenes. Access ports have the following characteristics: • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN). The default VLAN is 1. • accepts untagged frames and C-tagged frames. • discards all frames that are not classified to the Access VLAN. • on egress all frames are transmitted untagged. **Trunk:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches or routers. Trunk ports have the

	following characteristics: • By default, a trunk port is member of all existing VLANs. This may be limited by the use of Allowed VLANs. • unless VLAN Trunking is enabled on the port, frames classified to a VLAN that the port is not a member of will be discarded. • By default, all frames except frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress. • egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress. • VLAN trunking may be enabled. **Hybrid:** Hybrid ports resembles trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware. • ingress filtering can be controlled. • ingress acceptance of frames and configuration of egress tagging can be configured independently.
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
Port Type	Only ports in hybrid mode allow this value to be modified. A frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, if so which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

	C-Port: C-Ports is the more commonly used port type for VLAN for Tagged ports. We recommend using this Port type for Tagged VLANs unless you are a service provider or require QinQ stacked VLAN's. On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** S-Ports are used for provider bridging (also known as QinQ, stacked VLANs, or double tagging). QinQ is used when a customer has to transport VLAN tagged traffic across a service provider network. The service provider will have its own set of VLAN tags, such as a tag per customer. S-TAGs are correlated with the 0x88a8 TPID to signify the existence of the inner C-TAG which uses TPID 0x8100 (S-TAGs are inserted before C-TAGs). On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filtering	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
VLAN Trunking	Trunk and Hybrid ports allow for enabling VLAN trunking. When VLAN trunking is enabled, frames classified to unknown VLANs are accepted on the port whether ingress filtering is enabled or not. This is useful in scenarios where a cloud of intermediary switches must bridge

	VLANs that haven't been created. By configuring the ports that connect the cloud of switches as trunking ports, they can seamlessly carry those VLANs from one end to the other.
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. **Tagged Only** Only tagged frames are accepted on ingress. Untagged frames are discarded. **Untagged Only** Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access/Untagged VLAN. The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become member of all possible VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not be member of any of the existing VLANs, but if it is configured for VLAN Trunking it will still be able to carry all unknown VLANs.
Forbidden VLANs	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field. By default, the field is left blank, which means that the port may become a

	member of all possible VLANs.

Private VLAN's

The Private VLAN membership configurations for the switch can be monitored and modified under this section. Port members of each Private VLAN can be added and removed.

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

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

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

VLAN Membership

Information

This section is used to assign ports to private VLANs. Port members of each Private VLAN can be added or removed from this section.

1. Select **Configuration > VLANs. > Private VLANs > Membership**
2. To Assign ports to private vlans, tick the corresponding box under **Port Members**
3. To add a new Private VLAN, select the **Add New Private VLAN** option, then enter in the **PVLAN ID** you wish to assign to the port.
4. Select Apply to save any changes or Reset to revert any changes.
5. To delete a **PVLAN ID**, click on the tick box under the delete section, then select **Delete**

To revert any changes, select **Reset**.

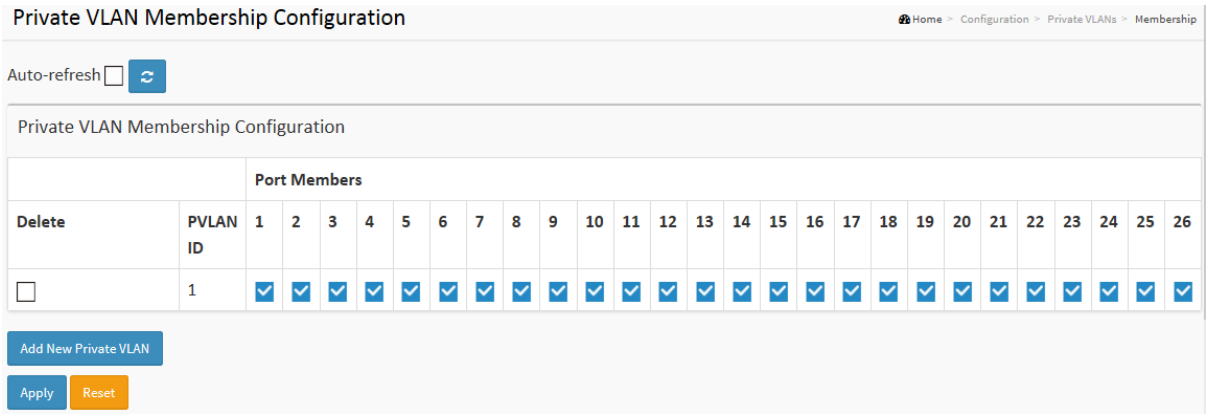


Fig: Private VLAN Membership Configuration

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 Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard the incorrect entry, or click "Cancel" to return to the editing and make a correction. The Private VLAN is enabled when you click "Save". The Delete button can be used to undo the addition of new Private VLANs.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Port Isolation

Port Isolation provides a method that isolates ports on layer 2 switches on the same VLAN to restrict traffic flow.
Port isolation is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given "uplink". The restricted ports are called "private ports". Each private VLAN typically contains many private ports, and a single uplink. The uplink will typically be a port (or link aggregation group) connected to a router, firewall, server,

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

Information

This page is used for enabling and disabling Port Isolation for specific ports on the switch.

1. Select **Configuration > VLANs. > Private VLANs > Port Isolation**
2. To Isolate Ports, tick the **Port Member** you wish to isolate and select Apply.

To revert any unsaved changes select **Reset**.

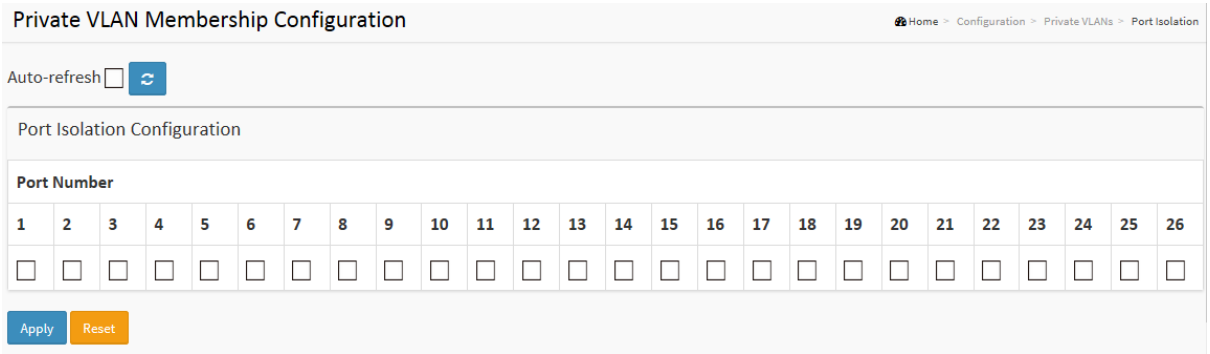


Fig: Private Port Isolation

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.
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

VCL

MAC Based VLAN

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

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

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

Information

MAC-based VLAN entries are configured on this page. You can add and delete MAC-based VLAN entries as well as assign entries to different ports from this section.

1. Select **Configuration > VCL. > MAC-based VLAN**
2. By default there will be no entries present, to configure select the **Add New Entry** Option
3. Add the **MAC Address** of the device you wish to configure, and assign the VLAN ID for the device.
4. Assign **the Port Members** by ticking the check box and select **Apply** to save.

To revert any changes select **Reset**

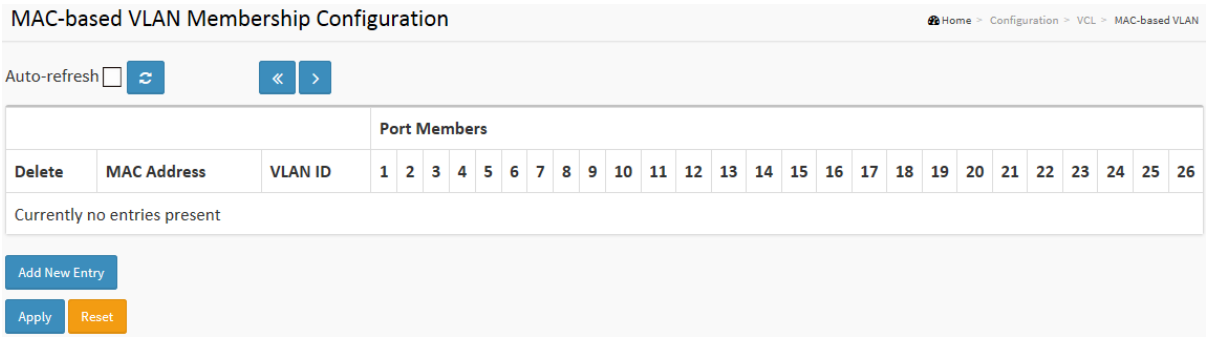


Fig: MAC-based VLAN Membership Configuration.

Parameter	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry will be deleted on the selected switch in the stack.
MAC Address	Indicates the MAC address
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port is displayed for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, check the box. To remove or exclude the port from the MAC-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New MAC-based VLAN	Click to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". A MAC-based VLAN without any port members on any stack unit will be deleted when you click "Save". The button can be used to undo the addition of new MAC-based VLANs.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Protocol Based VLAN

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

LLC

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

SNAP

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

Protocol to Group

Information

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

1. Select **Configuration > VCL > Protocol-based VLAN > Protocol to Group**
2. By Default there will be nothing in the protocol to **Group Mapping Table.** To create a mapping Select **Add New Entry**
3. Choose the **Frame Type** from the drop down menu and then assign the Etype **Value** by entering this into the text box.
4. Add the Group name then select **Apply**

To revert any settings select **Reset**

The Protocol to Group Mapping Table

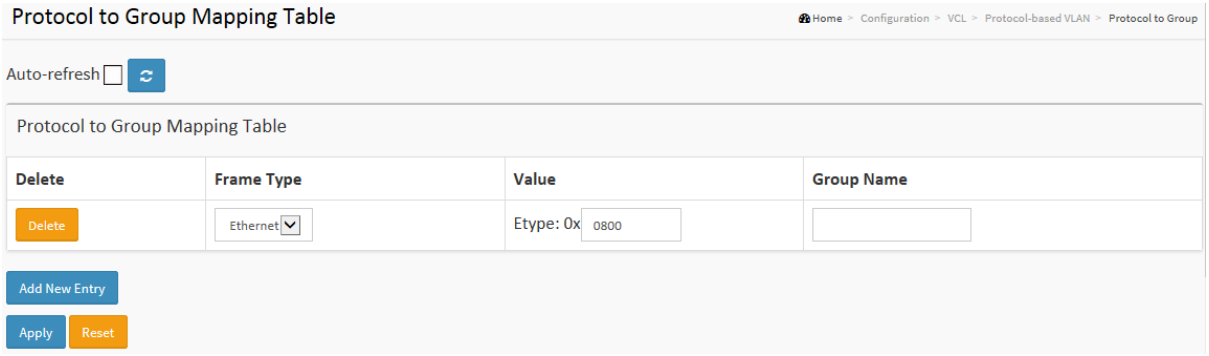


Fig: Protocol to Group Mapping Table

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 Save.
Frame Type	Frame Type can have one of the following values: 1. Ethernet 2. LLC 3. SNAP
Value	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below is the criteria for three different Frame Types: **1. For Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff **2. For LLC:** Valid value in this case is comprised of two different sub-values. a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) **3. For SNAP**: Valid value in this case also is comprised of two different sub-values. a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an

	OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
Group Name	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).
Adding a New Group to VLAN mapping entry	Click to add a new entry in mapping table. An empty row is added to the table; Frame Type, Value and the Group Name can be configured as needed. The button can be used to undo the addition of new entry.
Buttons	Apply – Click to save changes. Reset- Click to undo any changes made locally and revert to previously saved values.
Upper right icon (Refresh)	You can click them for refresh the Protocol Group Mapping information by manual.

Group to VLAN

Information

This page allows you to map an already configured Group Name to a VLAN Switch.

1. Select **Configuration > VCL > Protocol-based VLAN > Group to VLAN**
2. By Default there will be no Group Entries. To create an entry, select **Add New Entry**
3. Enter in the **Group Name**, and the **VLAN ID** you wish to assign.
4. Select **the Port Members** you wish to assign by ticking the corresponding check boxes
5. Select **Apply**

To revert any changes, select **Reset**.

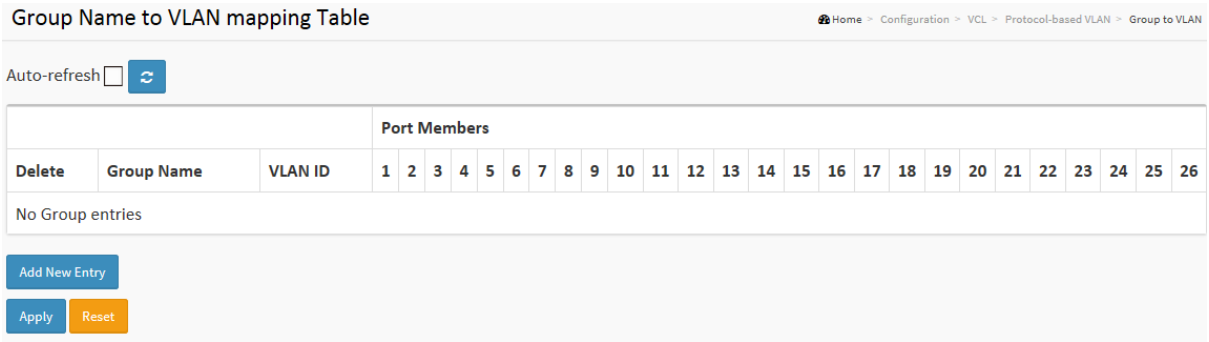


Fig: Group Name of VLAN Mapping Table

Parameter	Description
Delete	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
Group Name	A valid Group Name is a string of at most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers (0-9), no special character is allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
VLAN ID	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.

Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New Group to VLAN mapping entry	Click to add a new entry in mapping table. An empty row is added to the table, the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The button can be used to undo the addition of new entry.
Buttons:	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.
Auto-refresh	To evoke the auto-refresh icon then the device will refresh the information automatically.
Upper right icon (Refresh)	You can click them for refresh the Protocol Group Mapping information by manual.

IP Subnet-based VLAN

Information

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

1. Select **Configuration > VCL > Protocol-based VLAN > IP Subnet-based VLAN**
2. To add a New IP Subnet-based VLAN Membership Configuration, select **Add New Entry**.
3. Enter in the VCE ID from 0-128. The **IP address**, **Subnet Mask Length** and **VLAN ID** you wish to create
4. Add the **Port Members** by ticking the corresponding ports then select **Apply**

To revert any changes, select **Reset**.

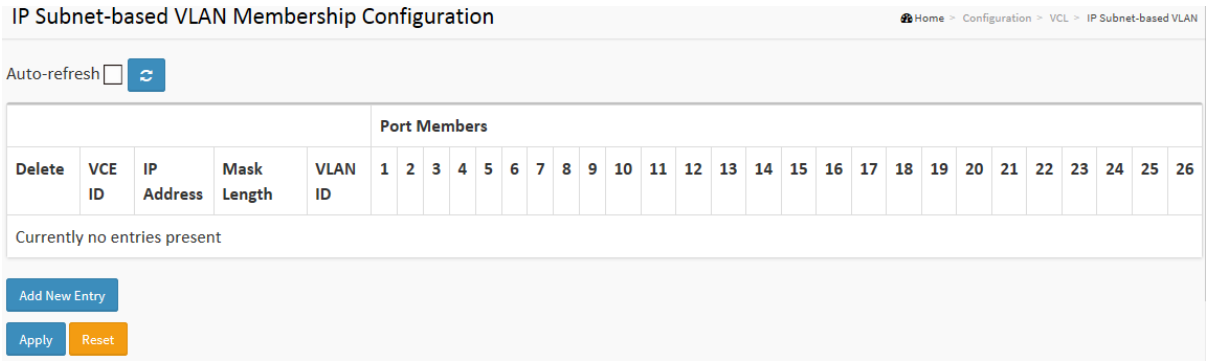


Fig: IP Subnet-based VLAN Membership Configuration

Parameter	Description
Delete	To delete a Group Name to VLAN map entry, check this box. The entry will be deleted on the switch during the next Save
VCE ID	Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.

Port Members	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding a New IP Subnet-based VLAN	Click “Add New Entry” to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095. The IP subnet-based VLAN entry is enabled on the selected stack switch unit when you click on "Save". The “Delete” button can be used to undo the addition of new IP subnet-based VLANs. The maximum possible IP subnet-based VLAN entries are limited to 128.

Voice VLAN

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

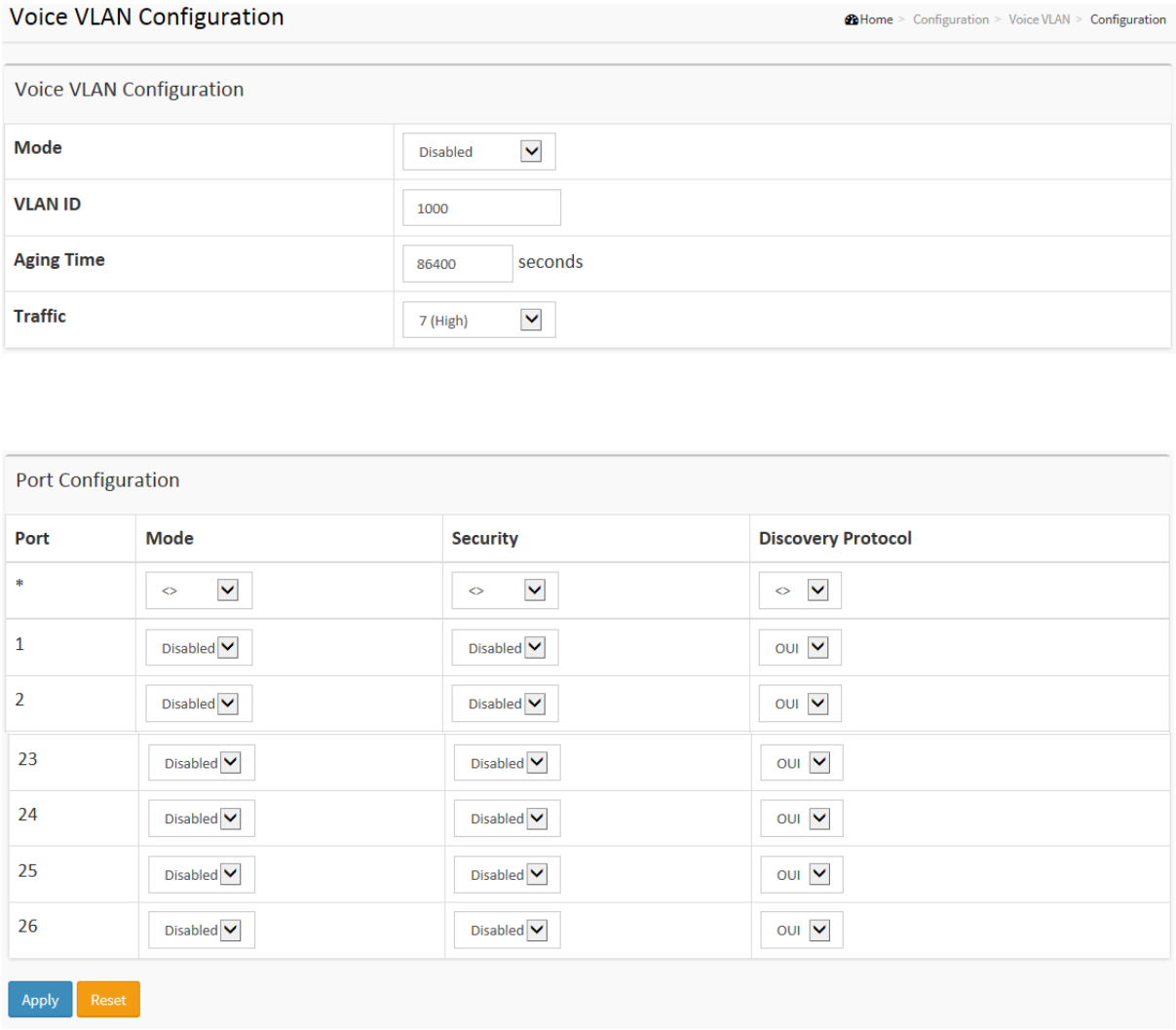
Information

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

1. Select **Configuration > Voice VLAN > Configuration**
2. Configure the Voice VLAN Configuration **Mode** either Enabled or Disabled.
3. Set the **VLAN ID** you wish to assign to the Voice VLAN. Acceptable range is from 1 to 4095
4. Enter in the **Aging time**. Default is 86400 sections
5. Enter in the **Traffic** Priority from 0-7. 7 being the highest.
6. Under Port Configuration, Enter in the **Mode**, either Disabled, Auto or Forced.
7. Select the **Security** Option either Enabled or Disabled
8. Select the Discovery Protocol you wish to use. OUI, LLDP or Both. Note changing the discovery protocol will restart the auto detect process.
9. Select Apply to save changes

To revert any changes, select **Reset**.

Fig: The IP Voice VLAN Configuration



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

	"OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: **OUI:** Detect telephony device by OUI address. **LLDP:** Detect telephony device by LLDP. **Both:** Both OUI and LLDP.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

OUI

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

Information

To configure the Voice VLAN OUI settings via the Web Interface:

1. Click **Configuration** > **Voice VLAN** > **OUI.**

2. Click Add New Entry to add additional OUI information.

3. Specify the OUI and Description.

4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

Fig: The Voice VLAN OUI Table

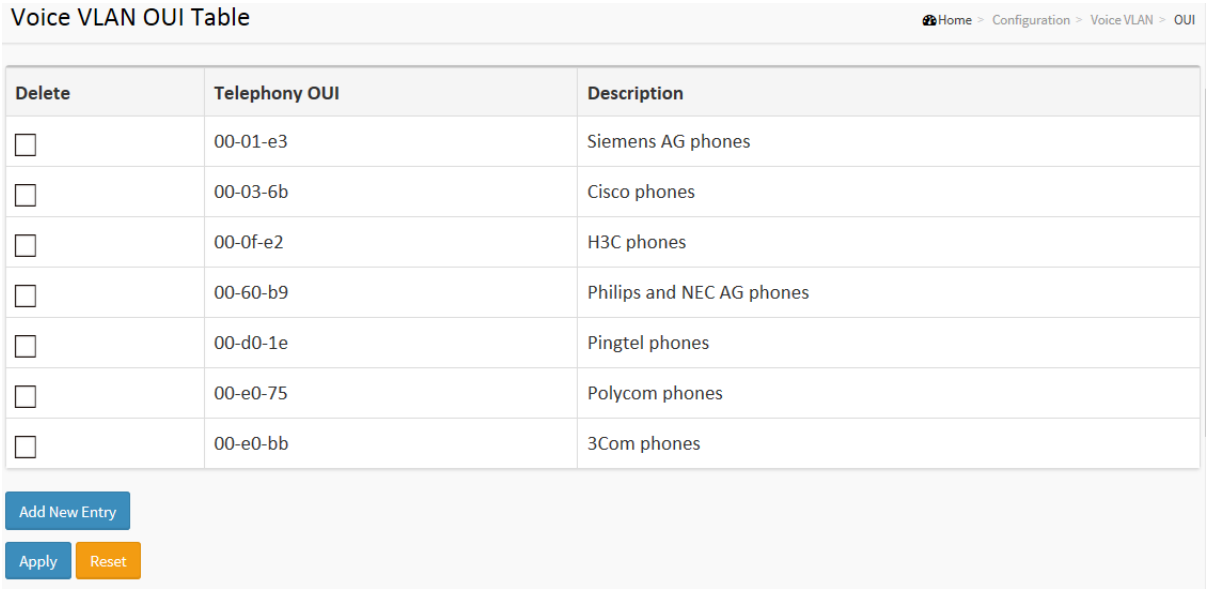


Fig: The Voice VLAN OUI Table

Parameter	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Telephony OUI	A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.
Add New Entry	Click to add a new entry to the Voice VLAN OUI table. An empty row is added to the table, please enter the Telephony OUI and Description.
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values.

QoS

The AS Series switches support 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.

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. This QoS classification mechanism is implemented in a QoS control list (QCL). The QoS class assigned to a frame is used throughout the device for providing queuing, scheduling, and congestion control guarantees priority to the frame according to what was configured for that specific QoS class.

The AS Series switches support advanced memory control mechanisms providing excellent performance of all QoS classes under any traffic scenario, including jumbo frames. A super priority queue with dedicated memory and strict highest priority in the arbitration. 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.

Port Classification

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

Information

To configure the QoS Port Classification settings via the Web Interface:

1. Click **Configuration** > **QoS** > **Port Classification**
2. Scroll to select QoS class, DP Level, PCP and DEI parameters
3. Click the save to save the setting
4. If you want to cancel the setting then you need to click the Reset button.
   It will revert to previously saved values

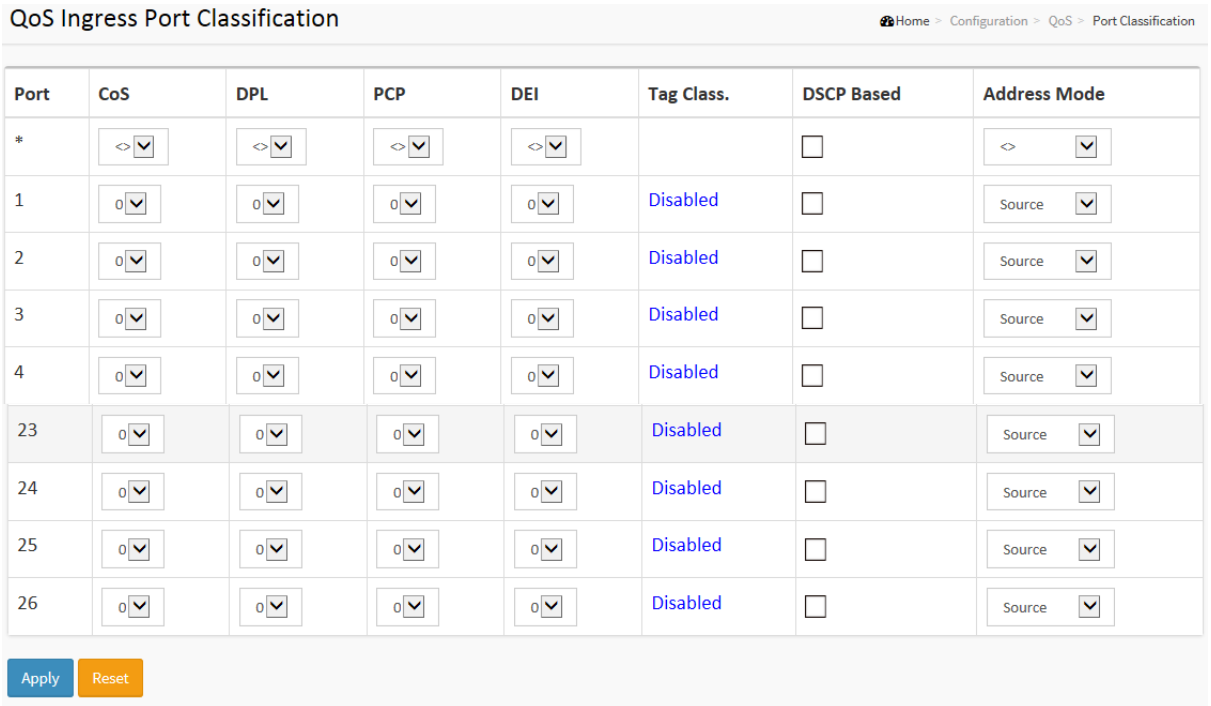


Fig: The QoS Configuration

Parameter	Description
Port	Physical port of the switch.
CoS	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.
DPL	Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. This setting controls the default DP level, i.e., the DP level for frames not classified in any other way.
PCP	Controls the default PCP for untagged frames. PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame.
DEI	Controls the default DEI for untagged frames. DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
Tag Class	Shows 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. **NOTE:** This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL
DSCP Based	Click to Enable DSCP Based QoS Ingress Port Classification.
Address mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: **Source**: Enable SMAC/SIP matching. **Destination**: Enable DMAC/DIP matching.
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values.

Port Policing

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

Information

To display the QoS Port Schedulers in the web interface:

1. Click **Configuration** > **QoS** > **Port Policing**
2. Evoke which port need to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll to select the Rate limit Unit with kbps, Mbps, fps and kfps.
4. Click Apply to save the configuration.

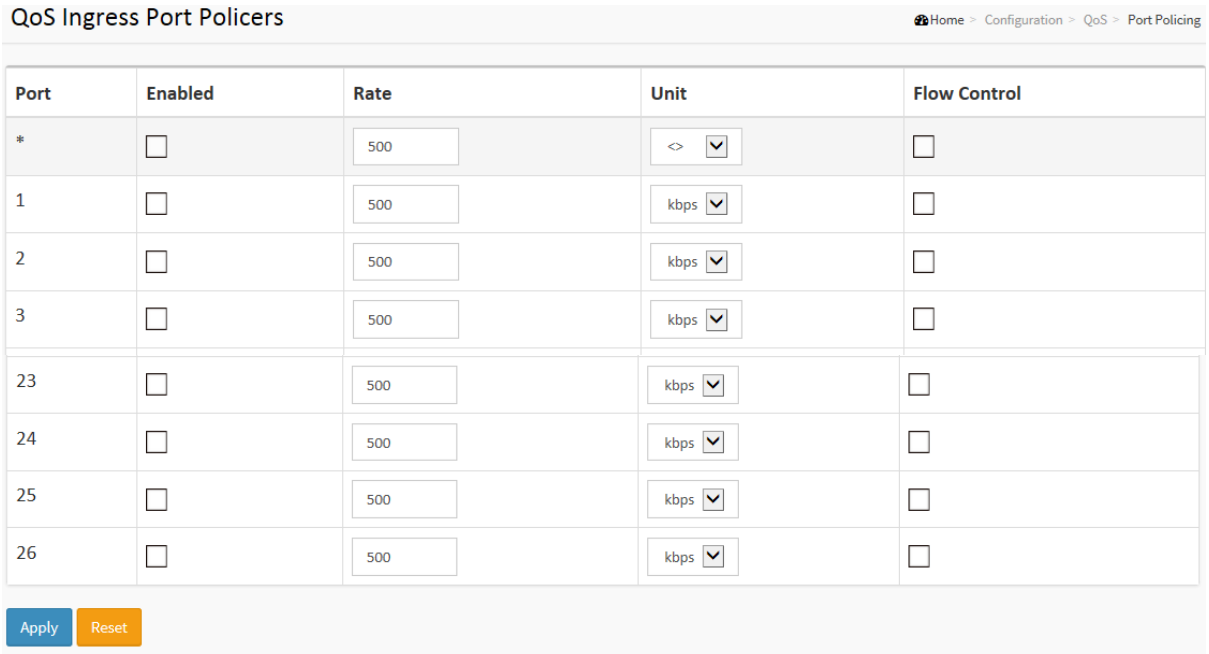


Fig: The QoS Ingress Port Policers Configuration

Parameter	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.
Enabled	To evoke which Port you need to enable the QoS Ingress Port Policers function.
Rate	To set the Rate limit value for this port, the default is 500.
Unit	To scroll to select what unit of rate includes kbps, Mbps, fps and kfps. The default is kbps.
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values.

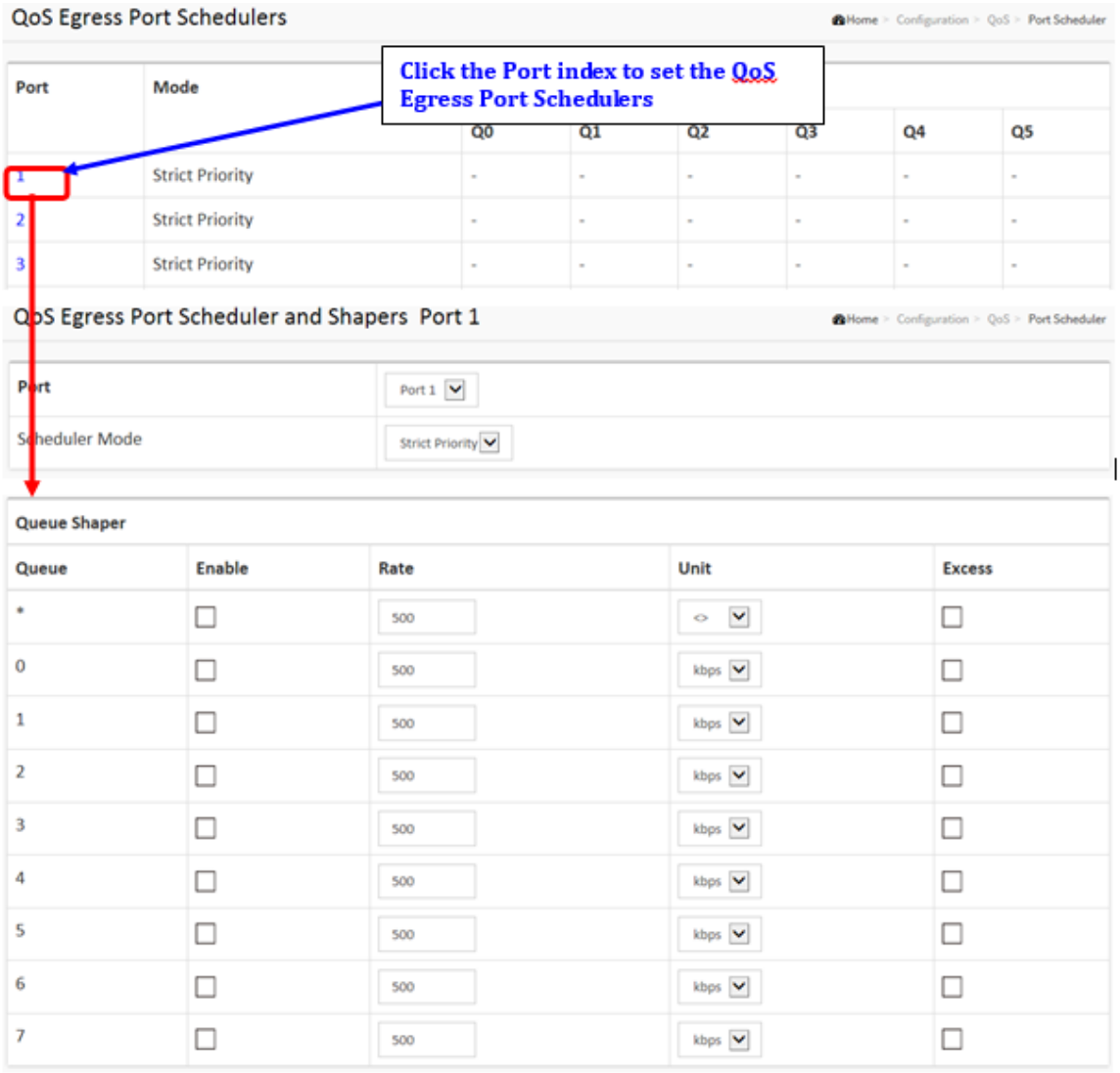
Port Schedulers

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

Information

To display the QoS Port Schedulers in the web interface:

1. Click **Configuration** > **QoS** > **Port Scheduler**.
2. Click on the required port to configure the scheduling options.
3. You will now be prompted with another screen, here you can select to use Strict Priority or Weighted.
4. Configure your Egress bandwidth parameters based on Queue Settings or force the port to a desired speed. If using Weighted a total percentage of a queue can also be set.
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.


QoS Egress Port Schedulers
Home > Configuration > QoS > Port Scheduler
Click the Port index to set the QoS Egress Port Schedulers
Port
Mode
Q0
Q1
Q2
Q3
Q4
Q5
1
Strict Priority
2
Strict Priority
3
Strict Priority
QoS Egress Port Scheduler and Shapers Port 1
Home > Configuration > QoS > Port Scheduler
Port
Port 1
Scheduler Mode
Strict Priority
Queue Shaper
Queue
Enable
Rate
Unit
Excess
*
500
<>
0
500
kbps
1
500
kbps
2
500
kbps
3
500
kbps
4
500
kbps
5
500
kbps
6
500
kbps
7
500
kbps


Port Shaper
Enable
Rate
Unit
500
kbps
Apply
Reset
Cancel

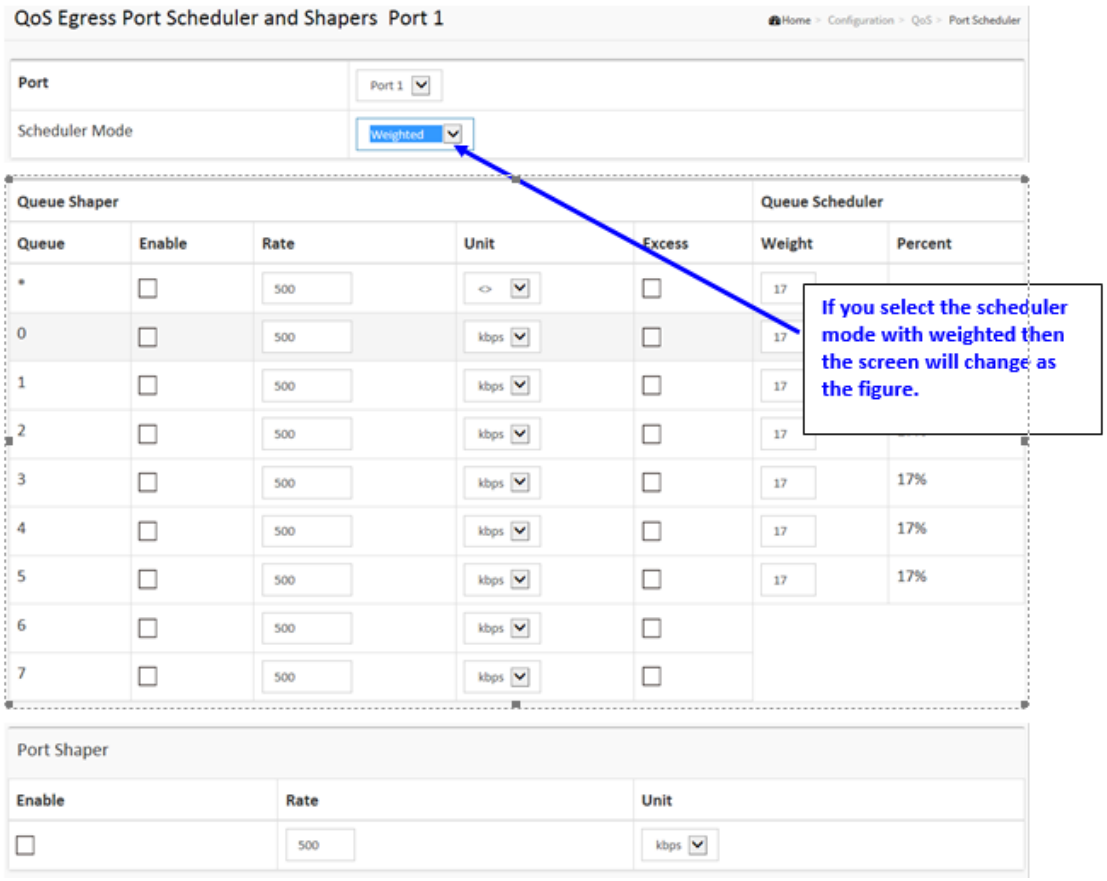


Fig: The QoS Egress Port Schedules

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	Shows the scheduling mode for this port.
Weight (Qn)	Shows 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 switch port.
Queue Shaper Rate	Controls the rate for the queue shaper. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 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	Controls whether the queue is allowed to use excess bandwidth.

Excess	
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 1000000 when the "Unit" is "kbps", and it is restricted to 1-13200 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".
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values.

Port Tag Remarking

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

Information

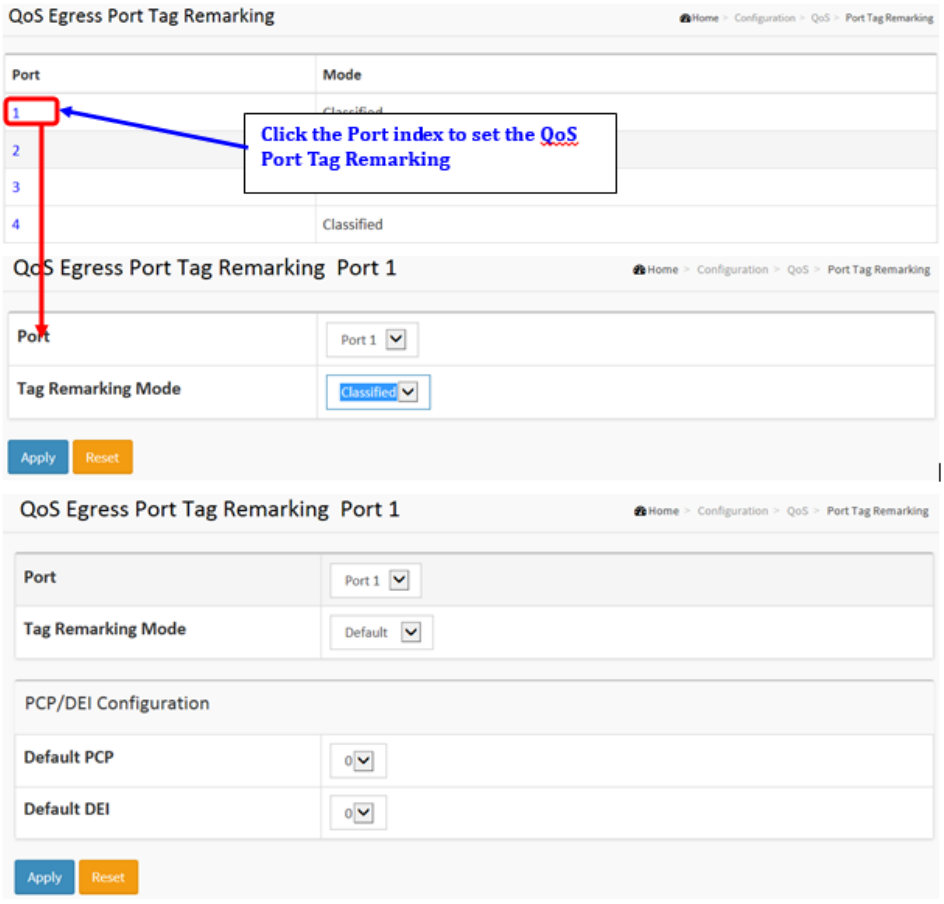
To configure the QoS Port Tag Remarking settings via the Web Interface:

1. Click **Configuration** > **QoS** > **Port Tag Remarking**.

2. Click on the port you want to configure.

3. Select the required Mode, Classified, Default or Mapped.

4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.



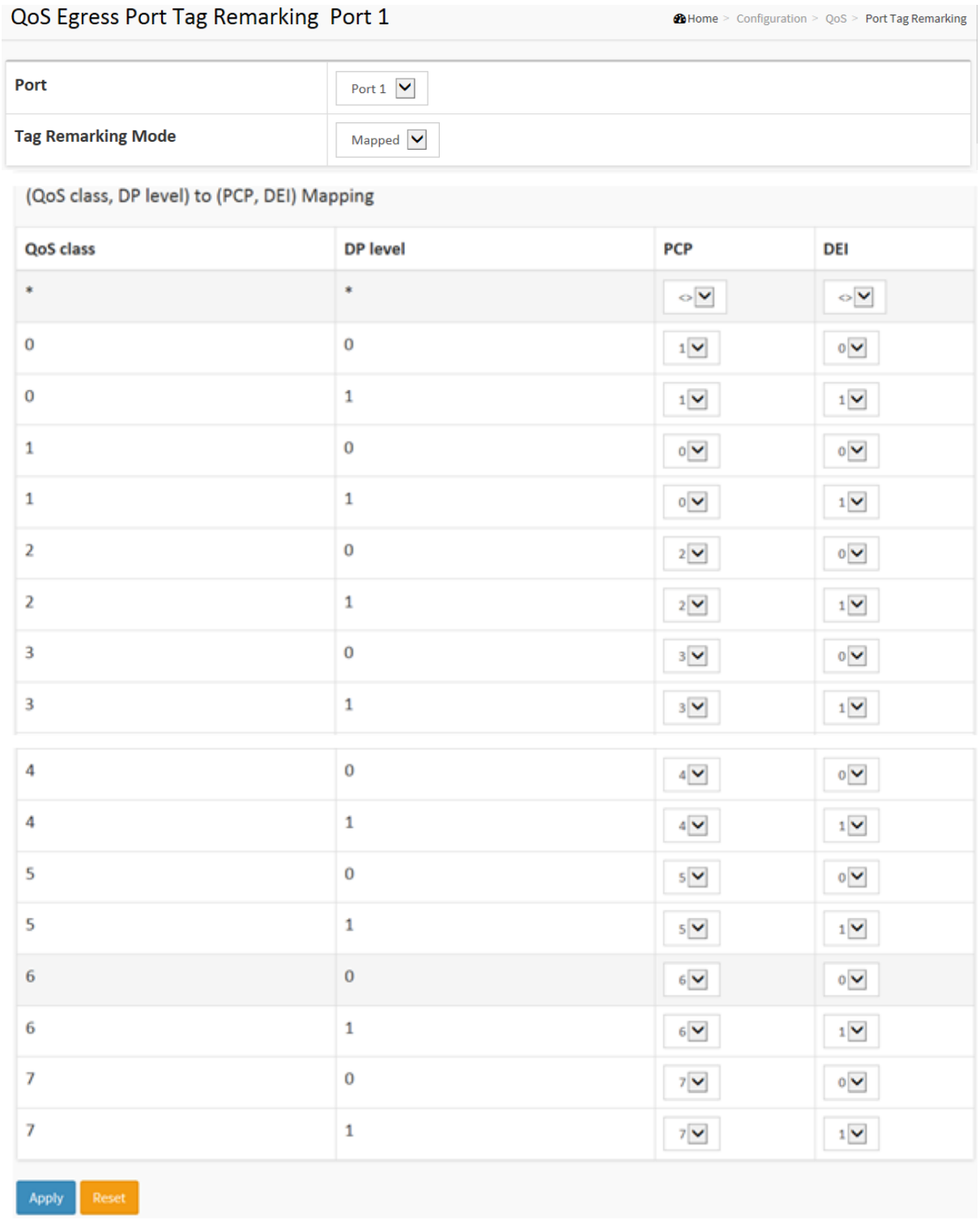


Fig: The Port Tag Remarking

Parameter	Description
Mode	Controls the tag remarking mode for this port. **Classified:** Use classified PCP/DEI values. **Default:** Use default PCP/DEI values. **Mapped:** Use mapped versions of QoS class and DP level.
PCP/DEI Configuration	Controls the default PCP and DEI values used when the mode is set to Default.
(Qos Class, DP level)to (PCP, DEI Mapping)	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped.
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values. **Cancel** – Click to cancel the changes.

Port DSCP

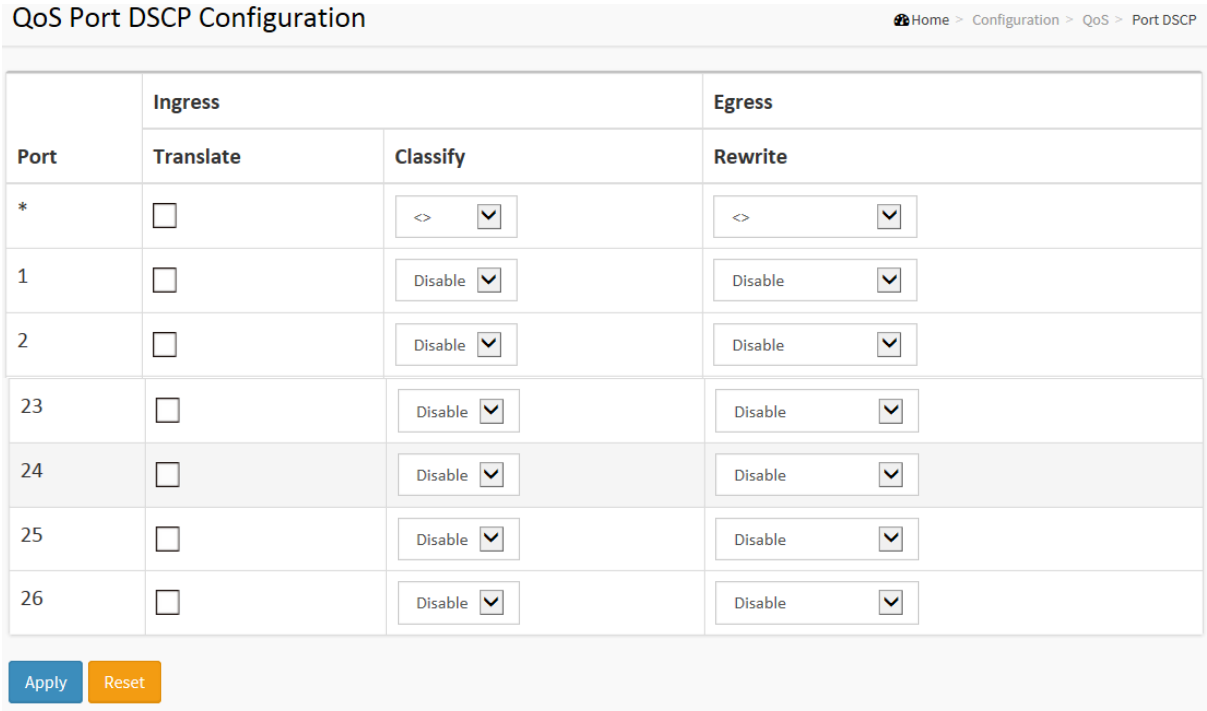
This section will teach user to set the QoS Port DSCP configuration that was allowed you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

Information

To configure the QoS Port DSCP settings via the Web Interface:

1. Click **Configuration** > **QoS** > **Port DSCP**.
2. Check the tick box next to each corresponding port to enable the DSCP feature.
3. Specify the Ingress Classify parameter and whether the Egress packets will be rewritten.
4. Click the Apply button to save your changes or the Reset button to revert to previous settings.

Fig: The QoS Port DSCP Configuration



Parameter	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings
Ingress	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. **Translate** : To Enable the Ingress Translation click the checkbox 2. **Classify**: Classification for a port have 4 different values • Disable: No Ingress DSCP Classification. • DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0. • Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. • All: Classify all DSCP.
Egress	Port Egress Rewriting can be one of below parameters • Disable: No Egress rewrite. • Enable: Rewrite enable without remapped. • Remap: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values.

DSCP-Based QoS

This section is used to configure DSCP-based QoS settings for all switch ports.

Information

To configure the DSCP-based QoS settings via the Web Interface:

1. Click **Configuration** > **QoS** > **DSCP-based QoS**.
2. Specify whether the DSCP value is trusted, and set the corresponding QoS value and DP level used for ingress processing.
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

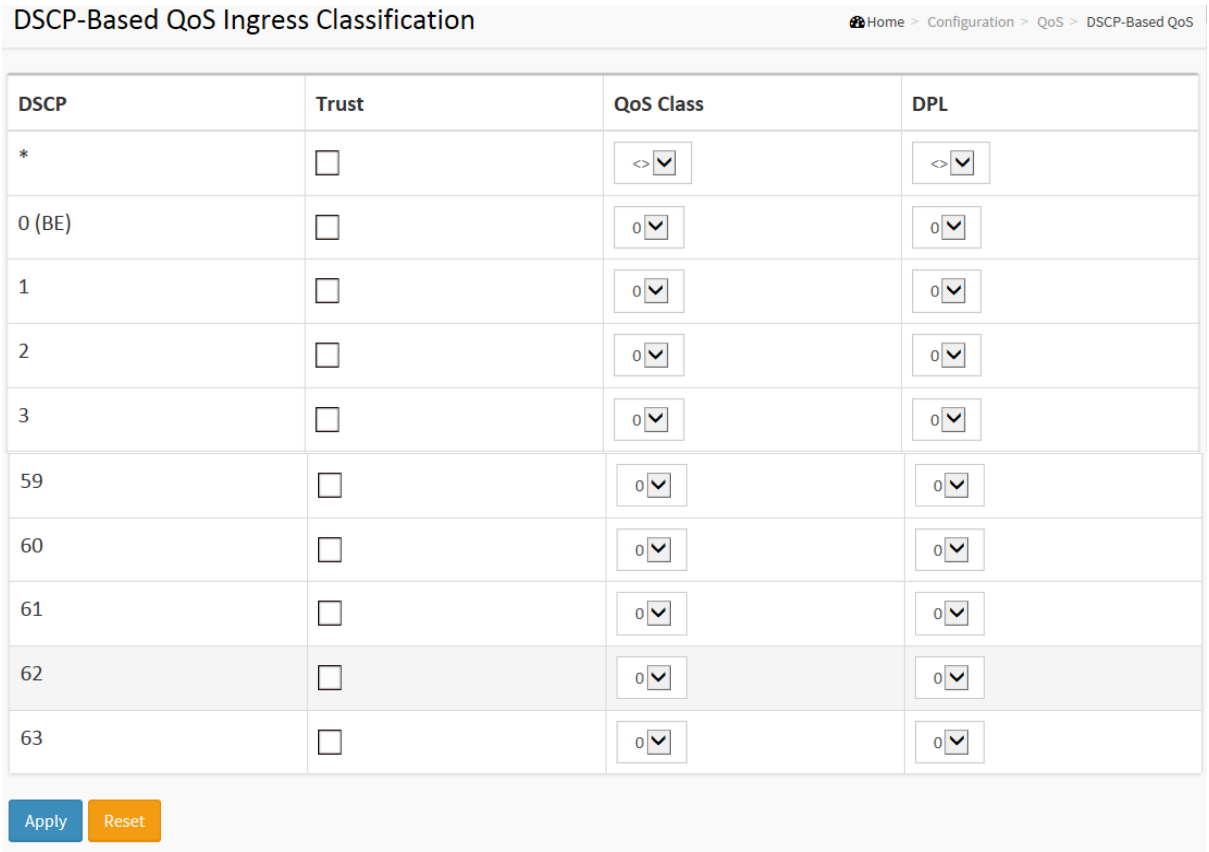


Fig: The DSCP-Based QoS Ingress Classification Configuration

Parameter	Description
DSCP	Maximum number of supported DSCP values are 64.
Trust	Click to check if the DSCP value is trusted.
QoS Class	QoS Class value can be any of (0-7)

DPL	Drop Precedence Level (0-3)
Buttons	**Apply** – Click to save changes. **Reset-** Click to undo any changes made locally and revert to previously saved values.

DSCP Translation

This section is used to configure DSCP translation for ingress traffic or DSCP re-mapping for egress traffic.

Information

To configure the DSCP-based QoS settings via the Web Interface:

1. Click **Configuration** > **QoS** > **DSCP Translation**
2. Scroll to set the **Ingress Translate** and **Egress Remap DP0** and **Remap DP1 Parameters**
3. **Evoke** to enable or disable Classify
4. Click the **save** to save the setting
5. If you want to cancel the setting then you need to click the **Reset** button. It will revert to previously saved values

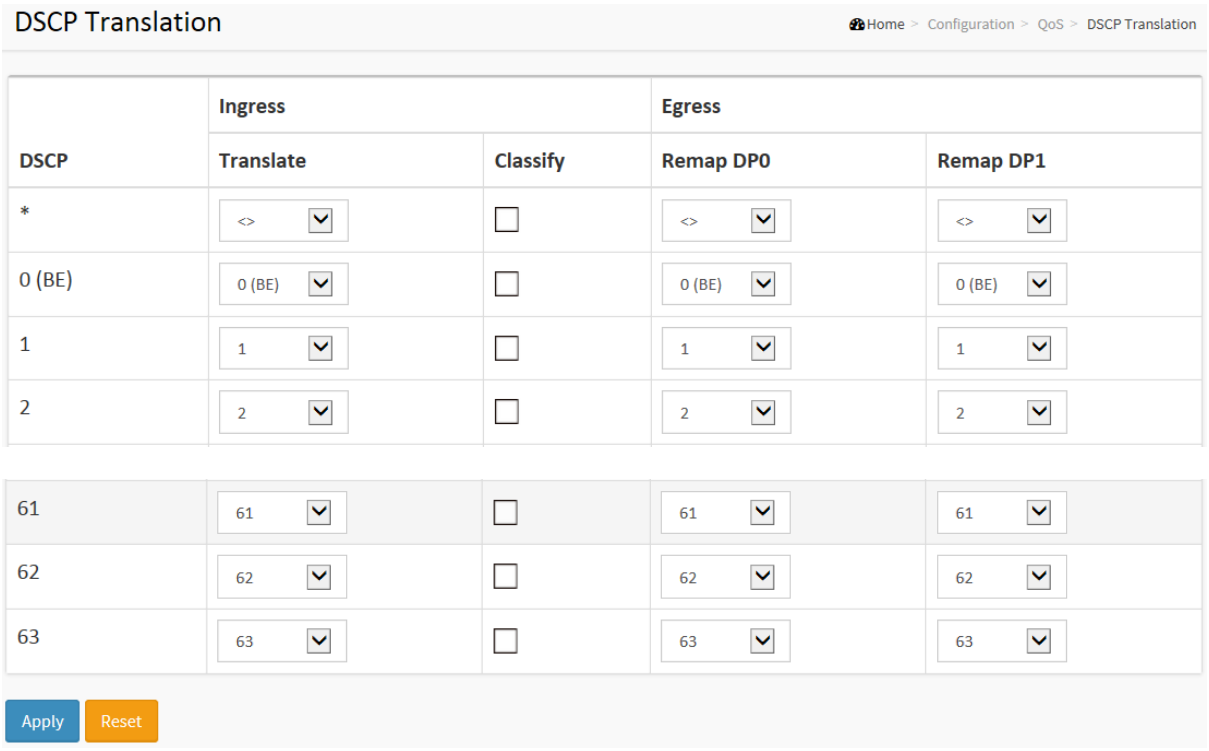


Fig: The DSCP Translation Configuration

Parameter	Description
DSCP	Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation – 1. **Translate**: DSCP at Ingress side can be translated to any of (0-63) DSCP values. 2. **Classify**: Click to enable Classification at Ingress side.
Egress	There are following configurable parameters for Egress side – 1. **Remap DP0**: Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63 2. **Remap DP1**: Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.
Buttons	**Apply** – Click to save changes. **Reset** – Click to undo any changes made locally and revert to previously saved values.

DSCP Classification

This section is used to map DSCP values to a QoS class and drop precedence level.

Information

To configure the DSCP-based QoS settings via the Web Interface:

1. Click **Configuration > QoS** > **DSCP Classification.**
2. Map the **DSCP** values to a corresponding **QoS class** and **drop precedence level.**
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

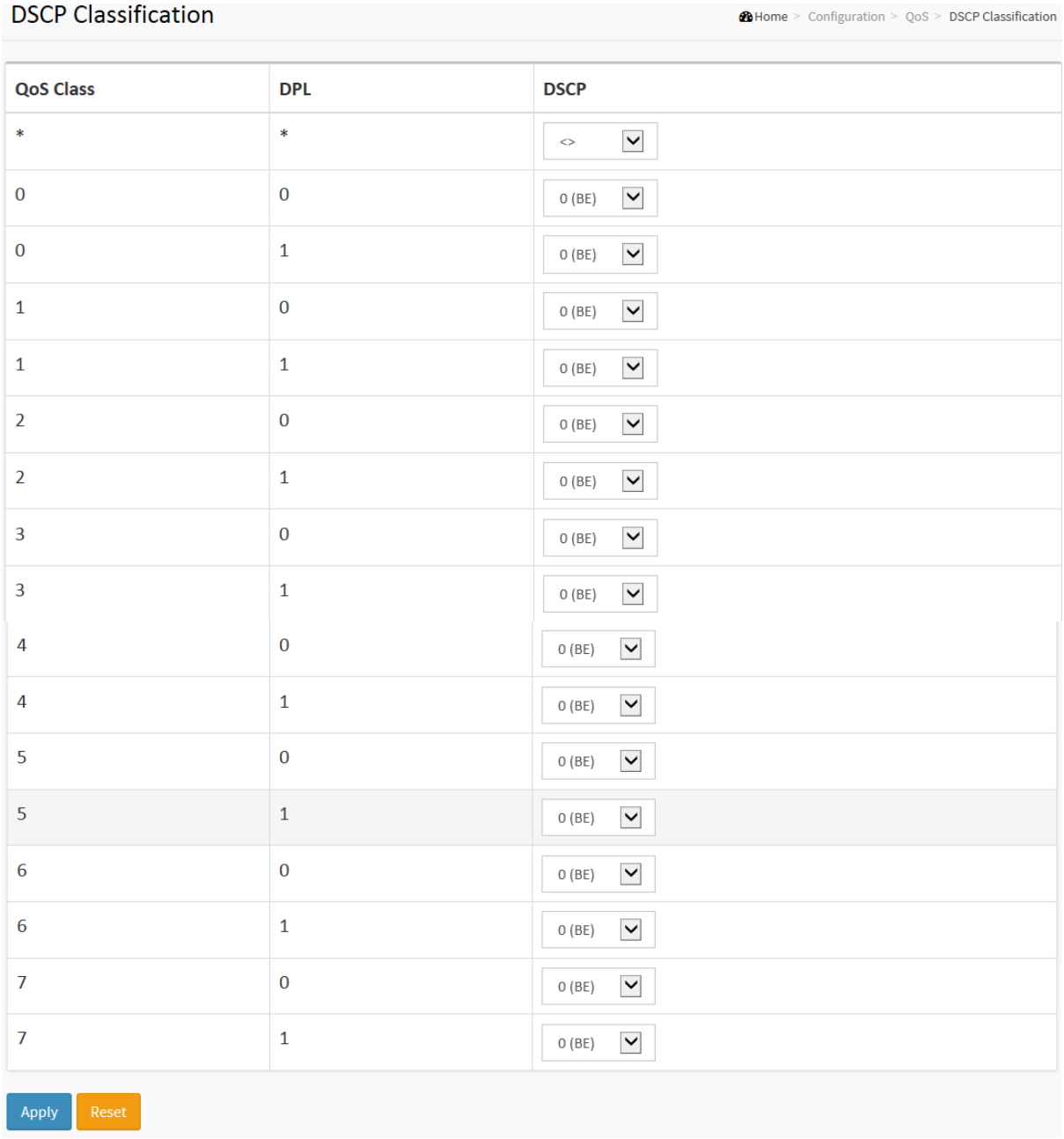


Fig: The DSCP Classification Configuration

Parameter	Description
QoS Class	Available QoS Class value ranges from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
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 DSCP to corresponding QoS Class and DPL value
Buttons	**Apply** – Click to save changes. **Reset** - Click to undo any changes made locally and revert to previously saved values.

QoS Control list Configuration

Use the QoS Control List Configuration page to configure Quality of Service policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag.

Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.

Information

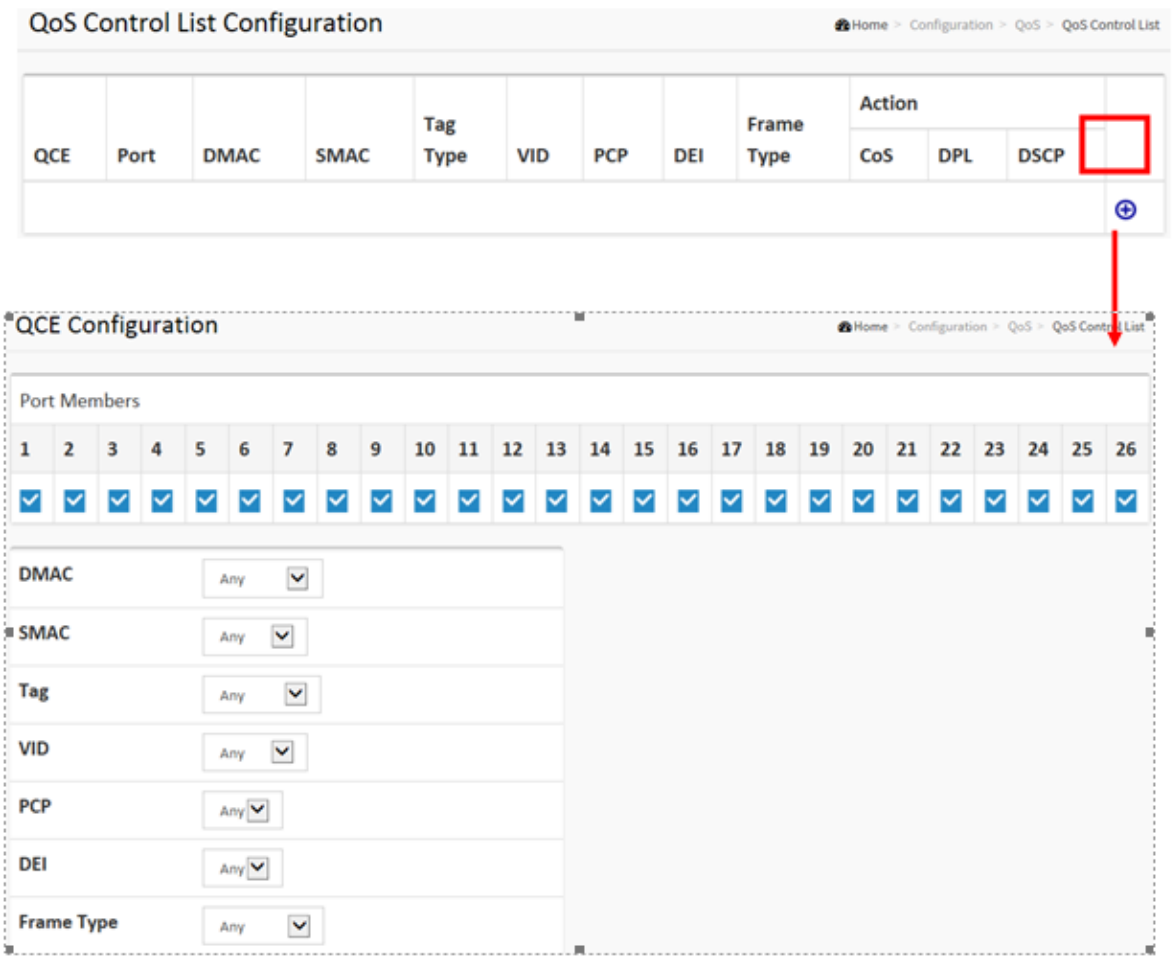
To configure the DSCP-based QoS settings via the Web Interface:

1. Click **Configuration** > **QoS** > **QoS Control List**.

2. Click the button to add a new **QCE**, or use the other QCE modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).

3. When editing an entry on the **QCE Configuration** page, specify the relevant criteria to be matched, and the response to a match.

4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.



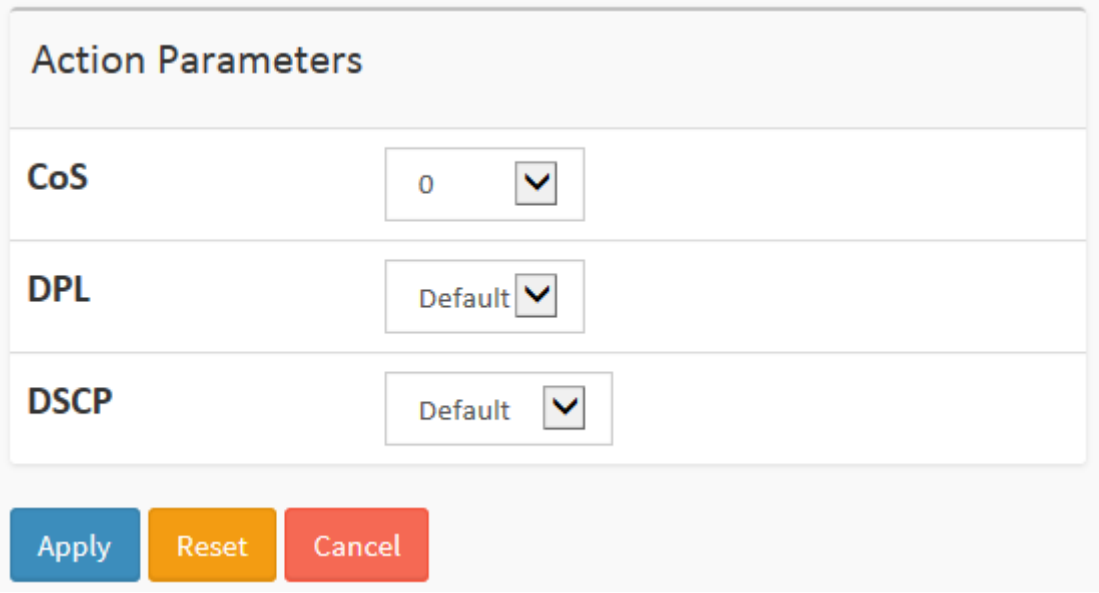


Fig: The QoS Control List Configuration

Parameter	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE
DMAC	Indicates the destination MAC address. Possible values are: Any: Match any DMAC. Unicast: Match unicast DMAC. Multicast: Match multicast DMAC. Broadcast: Match broadcast DMAC. <MAC>: Match specific DMAC. The default value is 'Any'.
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on DMAC/DIP, this field indicates the DMAC.
Tag Type	Indicates tag type. Possible values are: **Any:** Match tagged and untagged frames. **Untagged**: Match untagged frames. **Tagged**: Match tagged frames. **C-Tagged**: Match C-tagged frames. **S-Tagged**: Match S-tagged frames. The default value is 'Any'.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'
PCP	Priority Code Point: Valid values of PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.
Frame Type	Indicates the type of frame to look for incomming frames. Possible frame types are: **Any:** The QCE will match all frame type.

	Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC:** Only (LLC) frames are allowed. **SNAP:** Only (SNAP) frames are allowed **IPv4:** The QCE will match only IPV4 frames. **IPv6:** The QCE will match only IPV6 frames
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class, DPL and DSCP. **Class: Classified QoS Class;** if a frame matches the QCE it will be put in the queue. **DPL:** Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column. **DSCP:** If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
Modification Buttons	You can modify each QCE (QoS Control Entry) in the table using the following buttons:  : Inserts a new QCE before the current row.  : Edits the QCE.  : Moves the QCE up the list.  : Moves the QCE down the list.  : Deletes the QCE.  : The lowest plus sign adds a new entry at the bottom of the QCE listings.
Port Members	Check the checkbox button in case you what to make any port member of the QCL entry. By default all ports will be checked
Key Parameters	Key configuration are described as below: Tag Value of Tag field can be 'Any', 'Untag' or 'Tag' VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs PCP Priority Code Point: Valid value PCP are specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'

DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'

SMAC Source MAC address: 24 MS bits (OUI) or 'Any'

DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'

Frame Type Frame Type can have any of the following values

1. Any
2. Ethernet
3. LLC
4. NAP
5. IPv4
6. IPv6

NOTE: All frame types are explained below:

1. **Any**: Allow all types of frames.

2. **Ethernet**: Ethernet Type Valid Ethernet type can have value within 0x600-0xFFFF or 'Any', default value is 'Any'.

3. **LLC**: SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any' Control Address Valid Control Address can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'

4. SNAP : PID Valid PID(a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'

5. IPv4 : Protocol IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero 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
IP Fragment IPv4 frame fragmented option: **yes|no|any**
Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP

	6. IPv6 : Protocol IP protocol number: (0-255, TCP or UDP) or 'Any' Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits 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 Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP
Action Configuration	**Class QoS Class:** "class (0-7)", default- basic classification **DP Valid** DP Level can be (0-3)", default- basic classification **DSCP Valid** dscp value can be (0-63, BE, CS1-CS7, EF or AF11-AF43)
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Storm Control

Use the Storm Control Configuration page to set limits on broadcast, multicast and unknown unicast traffic to control traffic storms which may occur when a network device is malfunctioning, the network is not properly configured, or application programs are not well designed or properly configured. Traffic storms caused by any of these problems can severely degrade performance or bring your network to a complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast, or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped. Note that the limit specified on this page applies to each port.

Information

To configure the DSCP-based QoS settings via the Web Interface:

1. Click **Configuration > QoS** > **Storm Control**.

2. Enable storm control for unknown **unicast**, **broadcast**, or **multicast** traffic by marking the Status box next to the required frame type.

3. Select the **control rate** for the selected traffic type.

4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

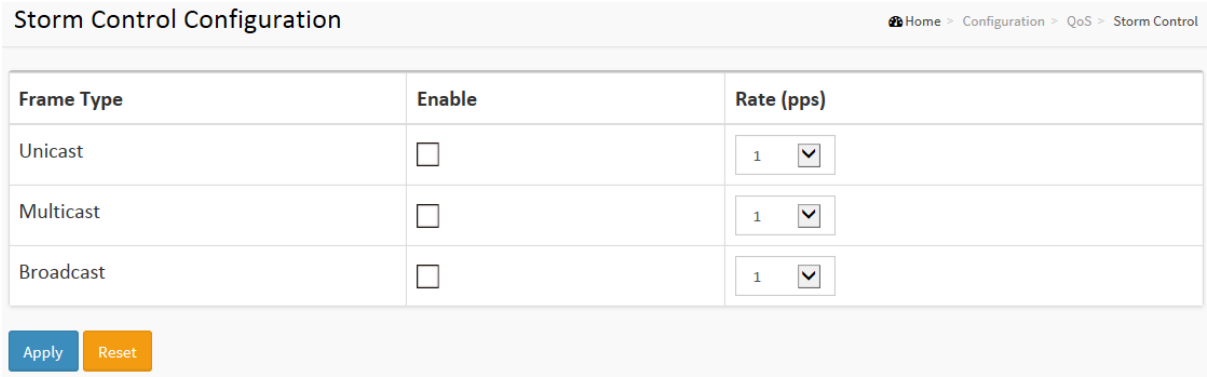


Fig: The Storm Control Configuration

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	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. The 1 kpps is actually 1002.1 pps.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Mirroring

The AS Series switches support traffic mirroring to capture and analyze real time traffic.

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

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Information

To configure the Port Mirroring settings via the Web Interface:

1. Click **Configuration** > **Mirroring**.

2. Select the **port** that you wish to mirror on. This port will be used to collect the data.

3. Select the **ports** and **mode** that you wish to monitor. All traffic from this port will be sent to the port selected above.

4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

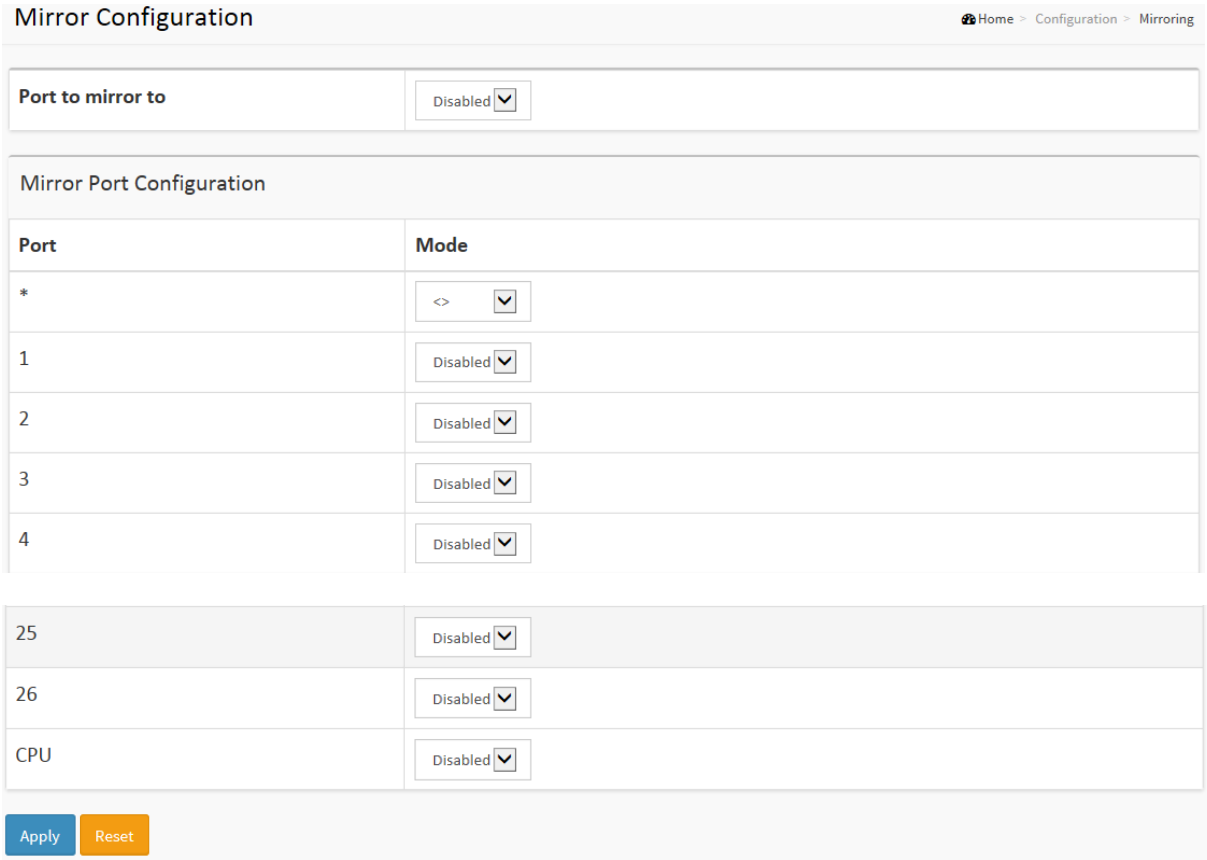


Fig: The Mirror Configuration

Parameter	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. **Rx only Frames** received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. **Tx only Frames** transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. **Disabled** Neither frames transmitted nor frames received are mirrored. **Enabled** Frames received and frames transmitted are mirrored on the mirror port. **NOTE:** For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

UPnP

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

Information

To configure the UPnP settings via the Web Interface:

1. Click **Configuration** > **UPnP**.
2. Select to **enable** or **disable** UPnP.
3. Configure the required parameters.
4. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

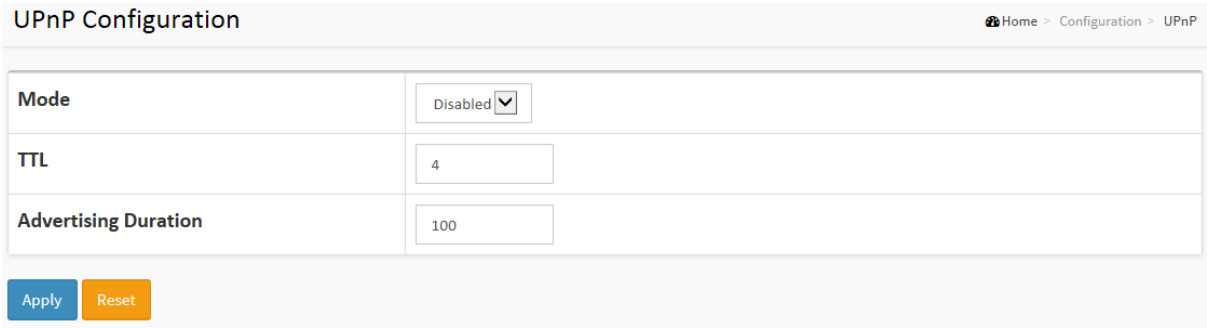


Fig: The UPnP Configuration

Parameter	Description
Mode	Indicates the UPnP operation mode. Possible modes are: **Enabled**: Enable UPnP mode operation. **Disabled**: Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.
TTL	The TTL value is used by UPnP to send SSDP advertisement messages. Valid values are in the range 1 to 255.
Advertising	The duration, carried in SSDP packets, is used to inform a control point or

Duration	control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.
Buttons:	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values

GVRP

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches. With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

Here are the guidelines for GVRP:

- GVRP is supported with STP or RSTP or without spanning tree.
- Both ports that constitute a network link between the switch and the other device must be running GVRP.
- You cannot modify or delete dynamic GVRP VLANs.
- You cannot remove dynamic GVRP ports from static or dynamic VLANs.
- To be detected by GVRP, a VLAN must have at least one active node or have at least one port with a valid link to an end node. GVRP cannot detect a VLAN that does not have any active nodes or valid port links.
- Resetting the switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The dynamic assignments are relearned by the switch as PDUs arrive on the ports from other switches.
- GVRP has three timers: join timer, leave timer, and leave all timer. The values for these timers must be identically configured on all switches running GVRP. Timers with different values on different switches can result in GVRP compatibility problems.
- You can convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments.

Global Config

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

There are three system files:

• **running-config**: A virtual file that represents the currently active configuration on the switch. This file is volatile.

• **startup-config**: The startup configuration for the switch, read at boot time.

•**default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

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

Information

This page allows you to configure the Global GVRP Configuration settings for all switch ports.

1. Click **Configuration** > **GVRP** > **Global Config**.
2. Specify the **GVRP Global Configuration** parameters for the required ports.
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

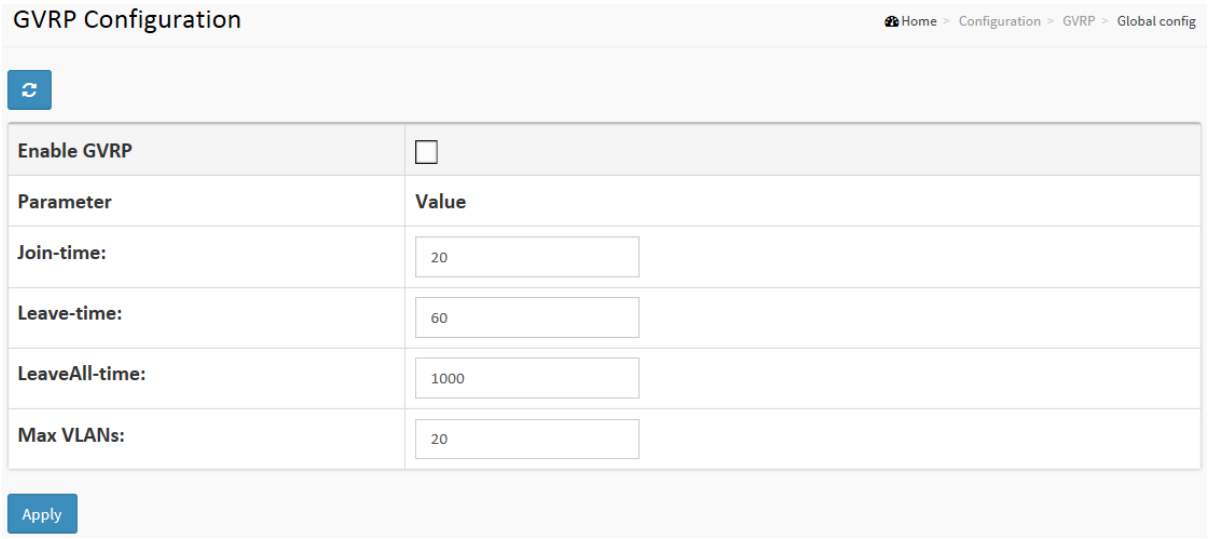


Fig: The GVRP Configuration

Parameter	Description
Enable GVRP Globally	The GVRP feature is enabled by setting the check mark in the checkbox named Enable GVRP.
GVRP protocol timers	**Join-time** is a value in the range 1-20 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 20. **Leave-time** is a value in the range 60-300 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 60.

	Leave All-time is a value in the range 1000-5000 in the units of centi seconds, i.e. in units of one hundredth of a second. The default is 1000.
Max number of VLAN's	When GVRP is enabled a maximum number of VLANs supported by GVRP is specified. By default this number is 20. This number can only be changed when GVRP is turned off.

Port Config

Information

This page allows you to configure the basic GVRP Configuration settings for all switch ports. The settings relate to the currently selected unit, as reflected by the page header.

1. Click **Configuration** > **GVRP** > **Port Config**.
2. Specify the **Port** and **Mode**
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

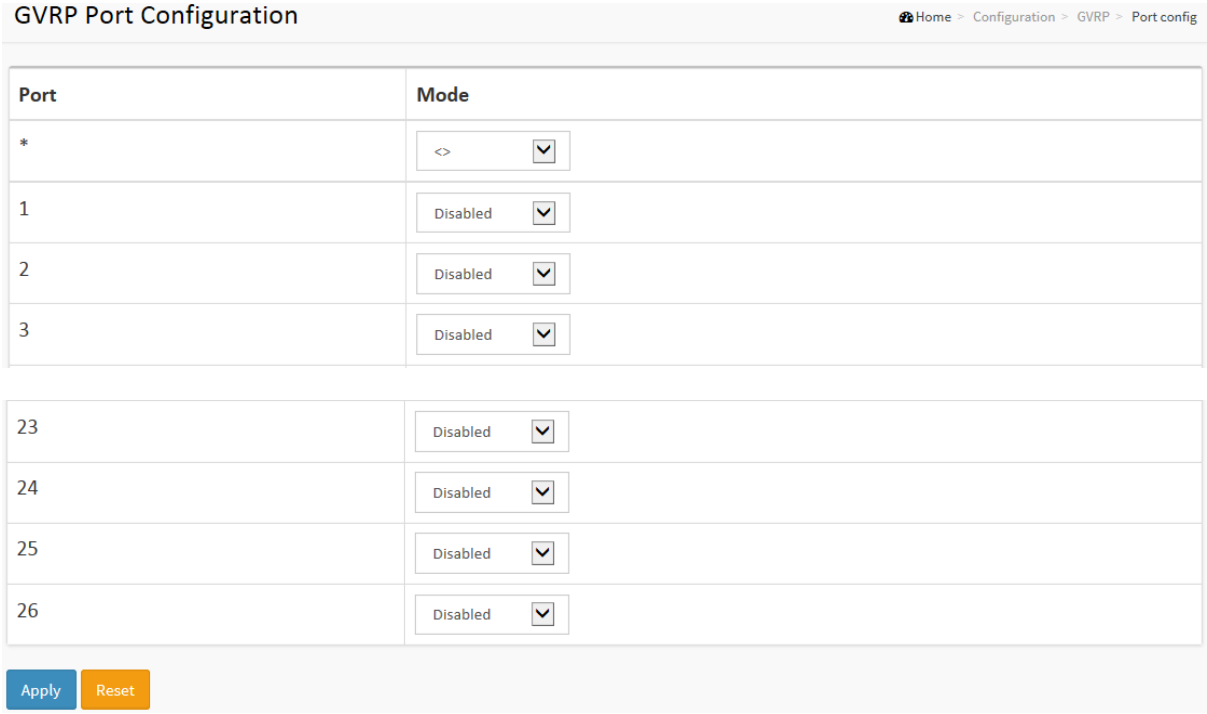


Fig: The GVRP Configuration

Parameter	Description
GVRP Mode	This configuration is to enable/disable GVRP Mode on particular port locally. **Disable**: Select to Disable GVRP mode on this port. **Enable**: Select to Enable GVRP mode on this port.

sFlow

The AS Series switches support s-Flow network monitoring. sFlow is a sampling technology that meets the key requirements for a network traffic monitoring solution:

- sFlow provides a network-wide view of usage and active routes. It is a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location.
- sFlow is scalable, enabling it to monitor links of speeds up to 10Gb/s and beyond without impacting the performance of core internet routers and switches, and without adding significant network load.
- sFlow is a low cost solution. It has been implemented on a wide range of devices, from simple L2 workgroup switches to high-end core routers, without requiring additional memory and CPU.
- sFlow is an industry standard with a growing number of vendors delivering products with sFlow support.

sFlow is a multi-vendor sampling technology embedded within switches and routers. It provides the ability to continuously monitor application level traffic flows at wire speed on all interfaces simultaneously.

The sFlow Agent is a software process that runs as part of the network management software within a device. It combines interface counters and flow samples into sFlow datagrams that are sent across the network to an sFlow Collector. Packet sampling is typically performed by the switching/routing ASICs, providing wire-speed performance. The state of the forwarding/routing table entries associated with each sampled packet is also recorded.

The sFlow Agent does very little processing. It simply packages data into sFlow Datagrams that are immediately sent on the network. Immediate forwarding of data minimizes memory and CPU requirements associated with the sFlow Agent.

Information

To configure the sFlow Agent in the web interface:

1. Click **Configuration** > **sFlow**
2. Configure the Appropriate sFlow **Agent Configuration**, **Receiver Configuration** and **Port Configuration** Parameters
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings.

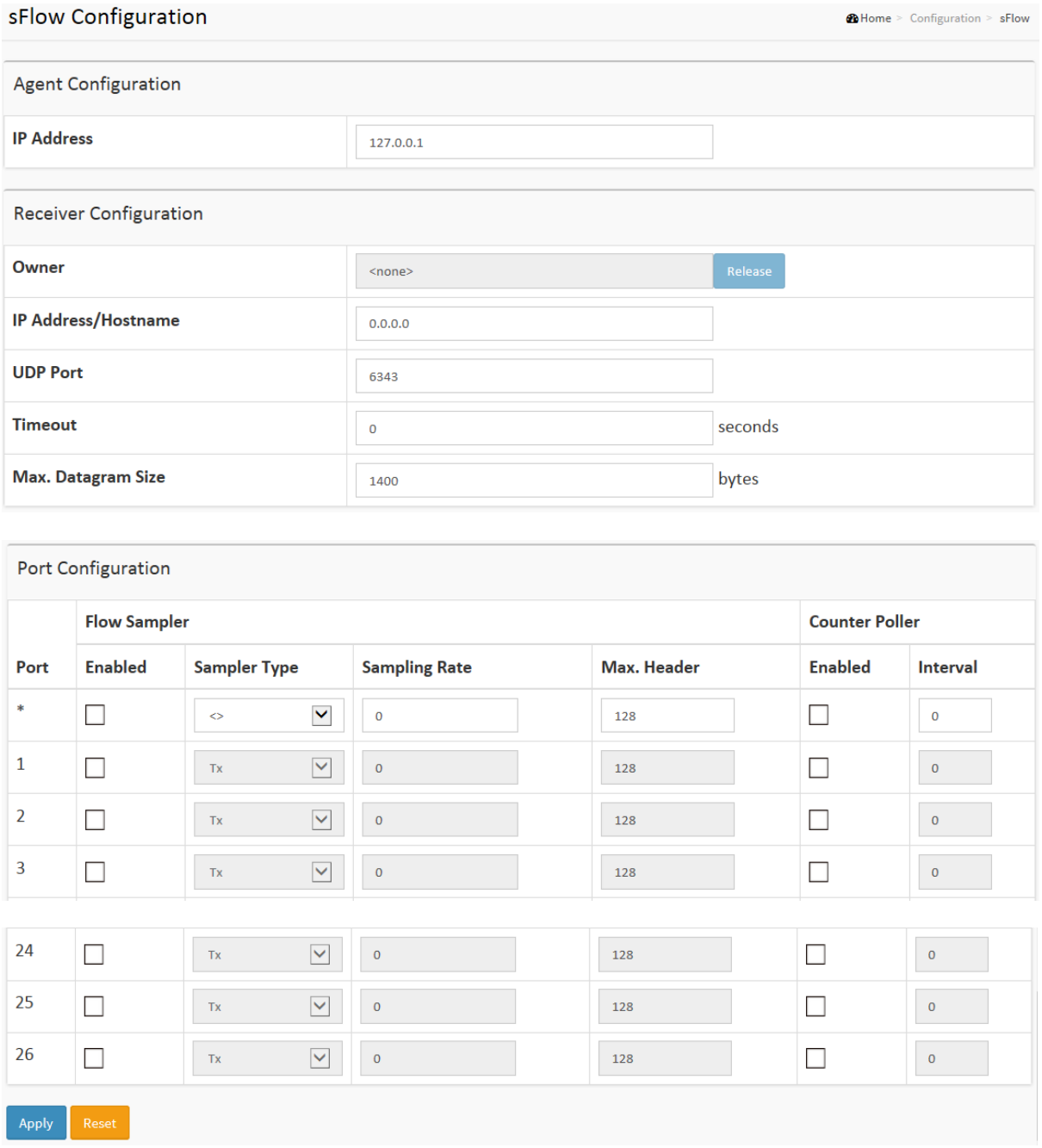


Fig: The sFlow Configuration

Agent Configuration

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

Receiver Configuration

Parameter	Description
Owner	sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows: • If sFlow is currently not configured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
IP Address/Hostname	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.
UDP Port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings.
Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

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

Enabled	
Flow Sampler Sampling Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field.
Flow Sampler Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.
Counter Poller Enabled	Enables/disables counter polling on this port.
Counter Poller Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Switch Alert

The Switch Alert Application makes configuration and troubleshooting your Alloy Managed Switches quick and easy. It offers features such as;

- Remotely manage and control Alloy managed switches via the mobile UI and Full web UI from any location at any time
- Remote troubleshooting to solve Networking issues quickly and effortlessly
- Receive real time critical network conditions and attack events from Alloy managed switches at any time
- Easily register your Alloy managed switches with the switch alert app via a one off 3 step process

Switch Alert Setting

Information

To configure the Switch Alert management via the web interface

1. Click **Configuration** > **Switch Alert** > **Switch Alert Setting**
2. To enable the Switch Alert functionality, change the **Switch Alert Mode** to enabled
3. Keep the default **Server Address** as ipush.cloudapp.net
4. Enter in the Router Settings such as **NAT**, **Ports** and **Protocol** Information and select Apply. If it is working the Server State will say “Successful connection to the server”
5. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings

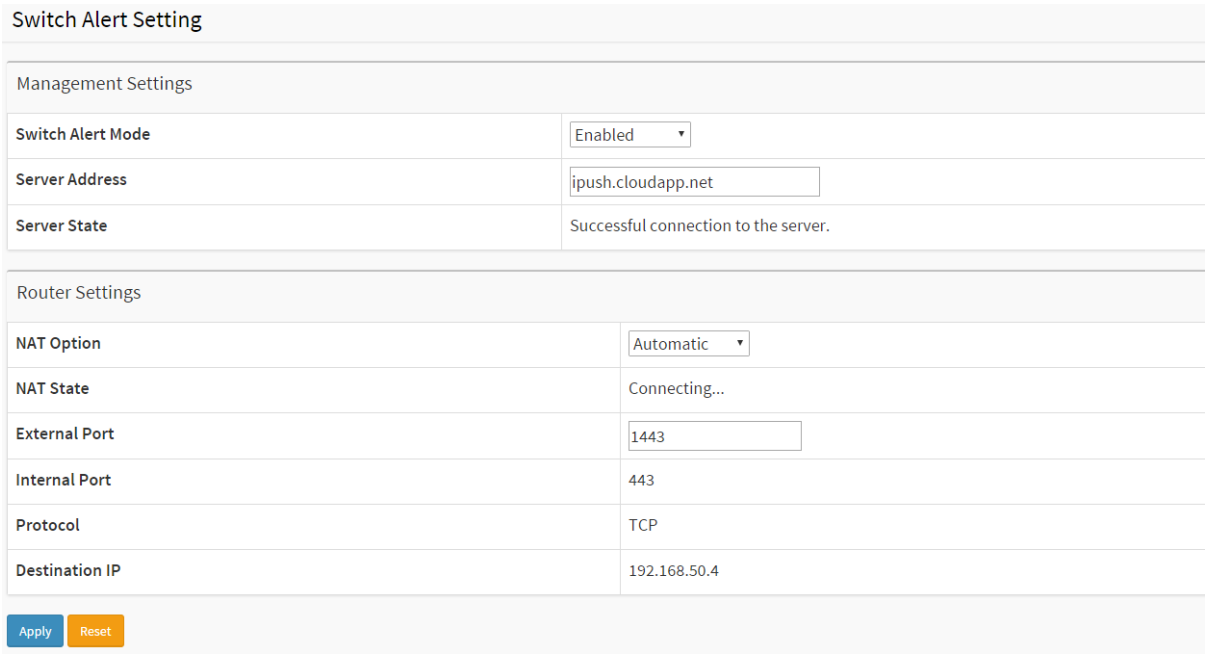


Fig: The Switch Alert Setting

Parameter	Description
Management Mode	Indicates the Management mode operation. When the mode operation is enabled, the message will send out to (or get from) the server. The protocol is based on TCP communication and received on TCP port 443 and the server will send acknowledgments/information back sender since TCP is a connection-oriented protocol. Possible modes are: **Enabled:** Enable Switch Alert Management mode operation. **Disabled:** Disable Switch Alert Management mode operation.
Server Address	Indicates the IPv4 host address of server. If the switch provide DNS feature, it also can be a host name.
Server State	Report network information between Switch and Server.
Link Option	Indicates the Link Option operation. When the Link Option in Automatic, enabling applications to access the services provided by an UPnP "Internet Gateway Device (IGN)" present on the network. When the Link Option in Manual, you should Setting External Port and Your IGN/NAT's Port Forward function by Manual. When Link function working success, Mobile(s) can access this NAT by Internet.

	Possible modes are: **Automatic:** Link Option in Automatic. **Manual:** Link Option in Manual.
Link State	Report network information between Switch and Internet Gateway Device (IGN).
External Port	When the Link Option in Manual, you should Setting External Port.
Internal Port	Information about Client's Internal Port.
Protocol	Information about Client's Protocol.
Destination IP	Information about Client's Destination IP.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Mobile Link Management

Configure the Mobile Link Management Settings on this page. This section is used to configure your mobile device to receive switch alerts from Switch Alert.

Information

To configure the Switch Alert management via the web interface

1. Click **Configuration** > **Switch Alert > Mobile Link Management**
2. Download the Switch Alert Application on your mobile device, either from the Apple store or Play Store. Alternately you can use the QR code from this page to direct you to the application.
3. Under Activity Code Settings select Get Activity Code.
4. On the mobile application, select the Blue + icon in the top left corner
5. Enter the 12 digit Activity Code that is displayed on the switch Web Interface into the phone and select Activate. If successful it should advise the device has been added.
6. The mobile device should now appear under the Mobile Link Management Section as Mobile 1.
7. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings

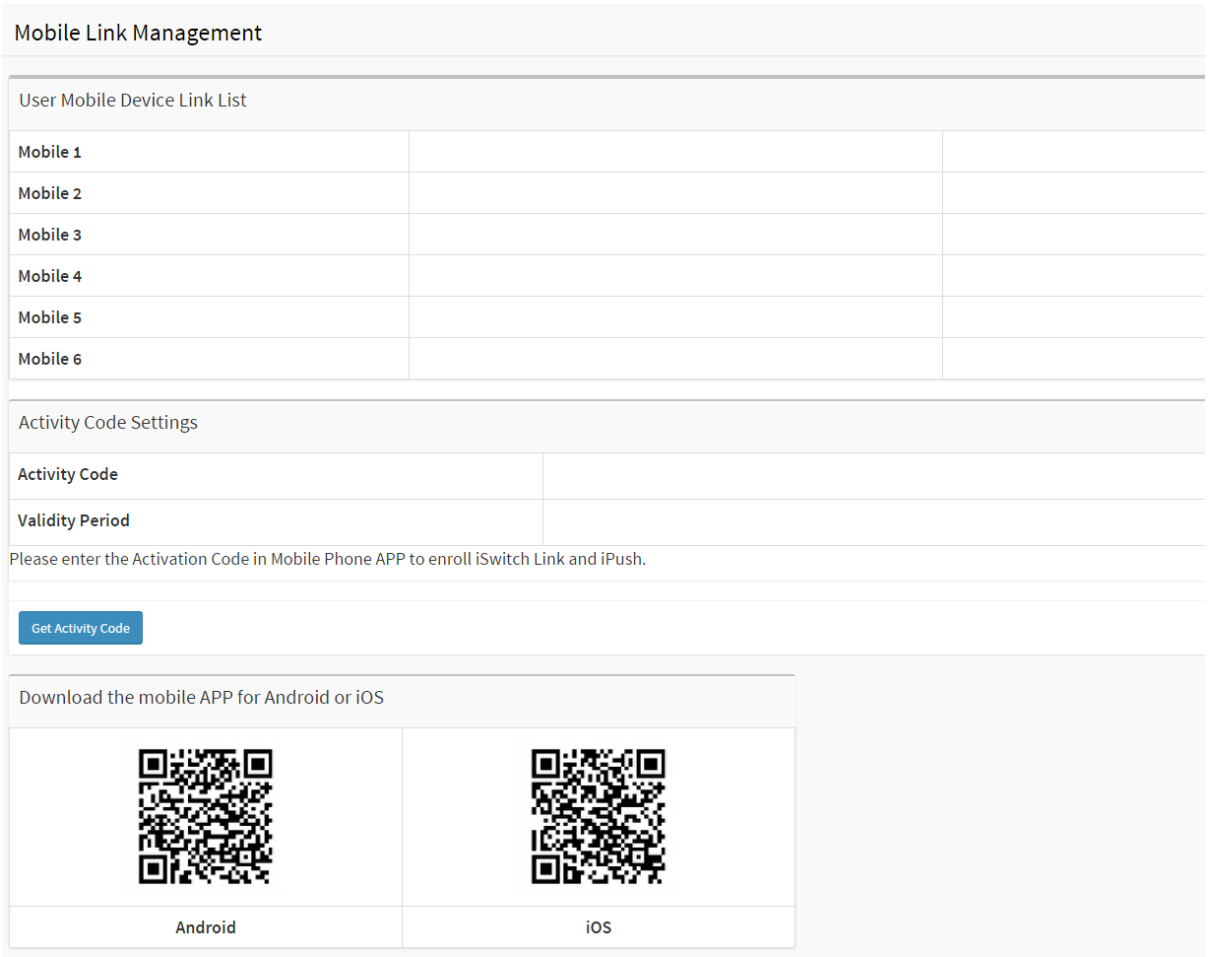


Fig: The Mobile Link Management

Parameter	Description
User Mobile Device Link List	Information about the mobile devices which can access this switch.
Activity Code	The Activity Code to register the mobile device to the Switch Alert Setting Server.
Validity Period	The expire time of the Activity Code
Get Activity Code	Click the Get Activity Code and enter the Activation Code in your mobile Phone App

iPush Options

iPush options are configured on this page. User can setup the events to trigger the iPush and the severity in iPush Event Severity Configuration. The name and role of each port also can be defined here.

Information

To configure the Switch Alert iPush Options via the web interface

1. Click **Configuration** > **Switch Alert > iPush Options**
2. Enter in the iPush Options such as the port name, and Role (Client/Server)
3. Click the **Apply** button to save your changes or the **Reset** button to revert to previous settings

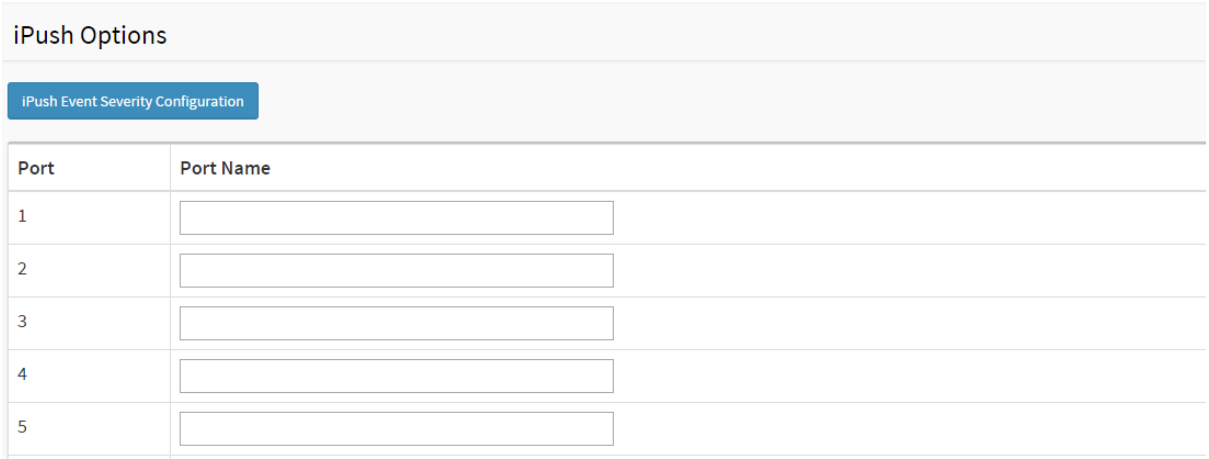


Fig: The Switch Alert iPush Options

Parameter	Description
Port	This is the logical port number for this row.
Port Name	Enter up to 47 characters to be descriptive name for identifies this port.
Role	Selects any available role for the given switch port. Possible role are: **Server** - Assign this as Server Port. **Client** - Assign this as Client Port.
Buttons	**Apply** – Click to save changes.

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

SMTP Configuration

The AS Series switches support trap events that can alert the administrator if a particular event occurs. This section is used to configure the mail server settings that will be used to send the emails. Email Addresses can also be configured here, these will be the addresses the events will be sent to.

Information

To configure the SMTP Configuration settings via the Web Interface:

1. Click **Configuration** >**SMTP.**

2. Enter the appropriate parameters as required.

3. Click the Apply button to save your changes or the Reset button to revert to previous settings.

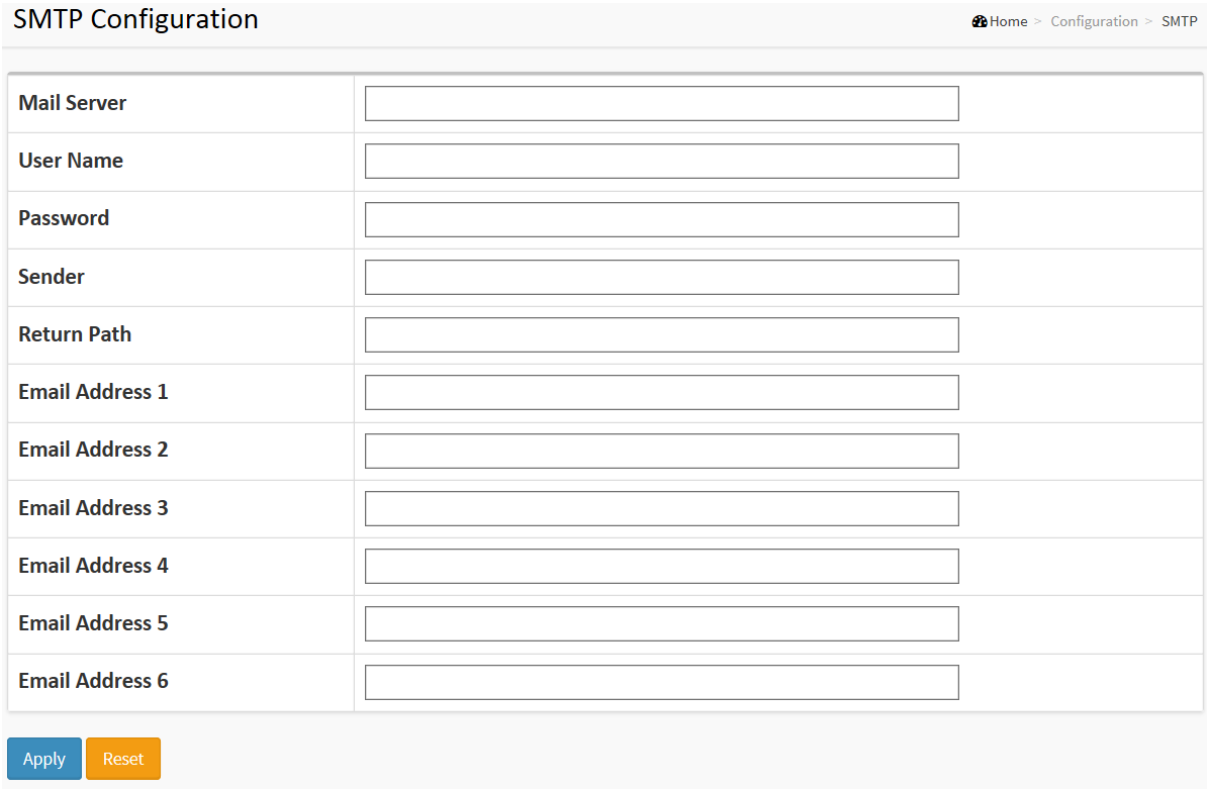


Fig: The SMTP Configuration

Parameter	Description
Mail Server	The IP address or hostname of the mail server. IP address is expressed in dotted decimal notation. This will be the device that sends out the mail for you
User name	Specify the username on the mail server.

Password	Specify the password on the mail server.
Sender	Specify the sender name of the alarm mail.
Return-Path	Specify the sender email address of the alarm mail. This address will be the "from" address on the email message.
Email Address 1-6	Email address that would like to receive the alarm message.
Buttons	**Apply** – Click to save changes. **Reset**- Click to undo any changes made locally and revert to previously saved values.

Monitor

This chapter describes all of the basic network statistics which includes the Ports, Layer 2 network protocol (e.g. NAS, ACL, DHCP, AAA and RMON etc.) and any setting of the Switch.

System

After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including “Model Name”, “System Description”, “Contact”, “Location”, “System Up Time”, “Firmware Version”, “Host Mac Address”, “Device Port”. With this information, you will know the software version used, MAC address, serial number, how many ports good and so on.

Information

The Switch system information is provided here.

To view the System Information settings via the Web Interface:

1. Click **Monitor** > **System > Information.**

System Information

Model Name	AS5152-P
System Description	52 Port Layer 2+ Managed PoE+ Switch with 48x 10/100/1000Mbps Ports + 4x 1Gb/10GbE SFP/SFP+ Ports
Location	
Contact	
System Name	AS5152-P
System Date	2016-03-08T09:59:30+10:00
System Uptime	5d 22:02:01
Bootloader Version	v1.15f
Firmware Version	v6.41.1662 2015-12-10
Hardware Version	v1.01
Mechanical Version	v1.01
Serial Number	15A412110006
MAC Address	00-00-8c-01-f3-77
Memory	Total=64085 KBytes, Free=24408 KBytes, Max=24243 KBytes
FLASH	0x40000000-0x41ffffff, 512 x 0x10000 blocks
Fan Speed	2262(rpm)
Powers	AC Power On 11.97 V ; DC Power On 0 V
Temperature 1	36(C) ; 96.8(F)
Temperature 2	44(C) ; 111.2(F)

Fig: System Information

Parameter	Description
Model Name	Displays the factory defined model name for identification purpose.
System Description	Displays the system description.
Location	The system location configured in Configuration | System | Information | System Location.
Contact	The system contact configured in Configuration | System | Information | System Contact.
System Name	Displays the user-defined system name that configured in System | System Information | Configuration | System Name.
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
System Uptime	The period of time the device has been operational.
Bootloader Version	Displays the current boot loader version number.
Firmware Version	The software version of this switch.
Mechanical Version	The hardware and mechanical version of this switch.
Series Number	The serial number of this switch.
MAC Address	The MAC Address of this switch.
Memory	Displays the memory size of the system.
FLASH	Displays the flash size of the system.
Fan Speed	The current Fan Speed
Powers	Shows the input power reading of the switch
Temperature 1	Temperature detector location near ventilation air outlet
Temperature 2	Temperature detector near CPU

IP Status

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

Information

To display the IP configuration Status via the Web Interface:

1. Click **Monitor** > **System > IP Status.**

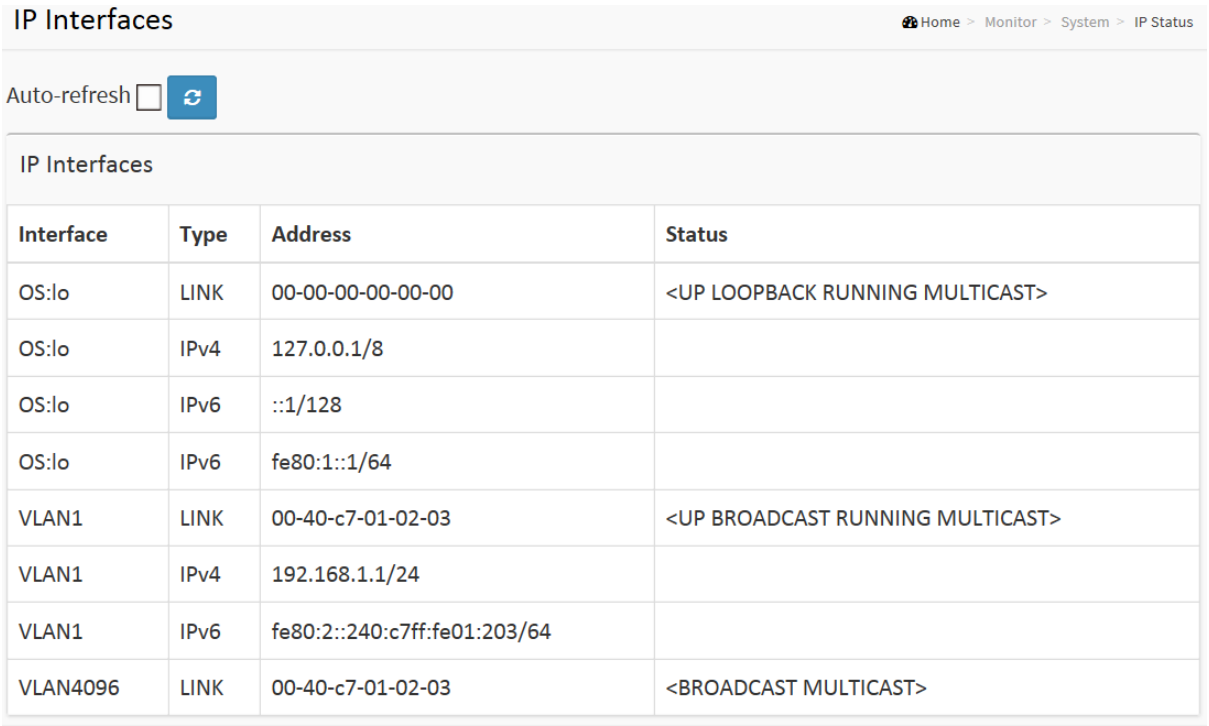


Fig: The IP Status

IP Routes

Network	Gateway	Status
0.0.0.0/0	192.168.1.254	<UP GATEWAY HW_RT>
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.1.0/24	VLAN1	<UP HW_RT>
::1/128	::1	<UP HOST>

Neighbour cache

IP Address	Link Address
192.168.1.100	VLAN1:3c-97-0e-16-eb-7e
fe80:2::240:c7ff:fe01:203	VLAN1:00-40-c7-01-02-03

IP Interfaces

Parameter	Description
Interface	Show the name of the interface.
Type	Show the address type of the entry. This may be LINK or IPv4.
Address	Show the current address of the interface (of the given type).
Status	Show the status flags of the interface (and/or address).

IP Routes

Parameter	Description
Network	Show the destination IP network or host address of this route.
Gateway	Show the gateway address of this route.
Status	Show the status flags of the route.

Neighbor Cache

Parameter	Description
IP Address	Show the IP address of the entry.
Link Address	Show the Link (MAC) address for which a binding to the IP address given exist.

Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page immediately.

Log

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

Information

To display the Log Information Status via the Web Interface:

1. Click **Monitor** > **System > Log**

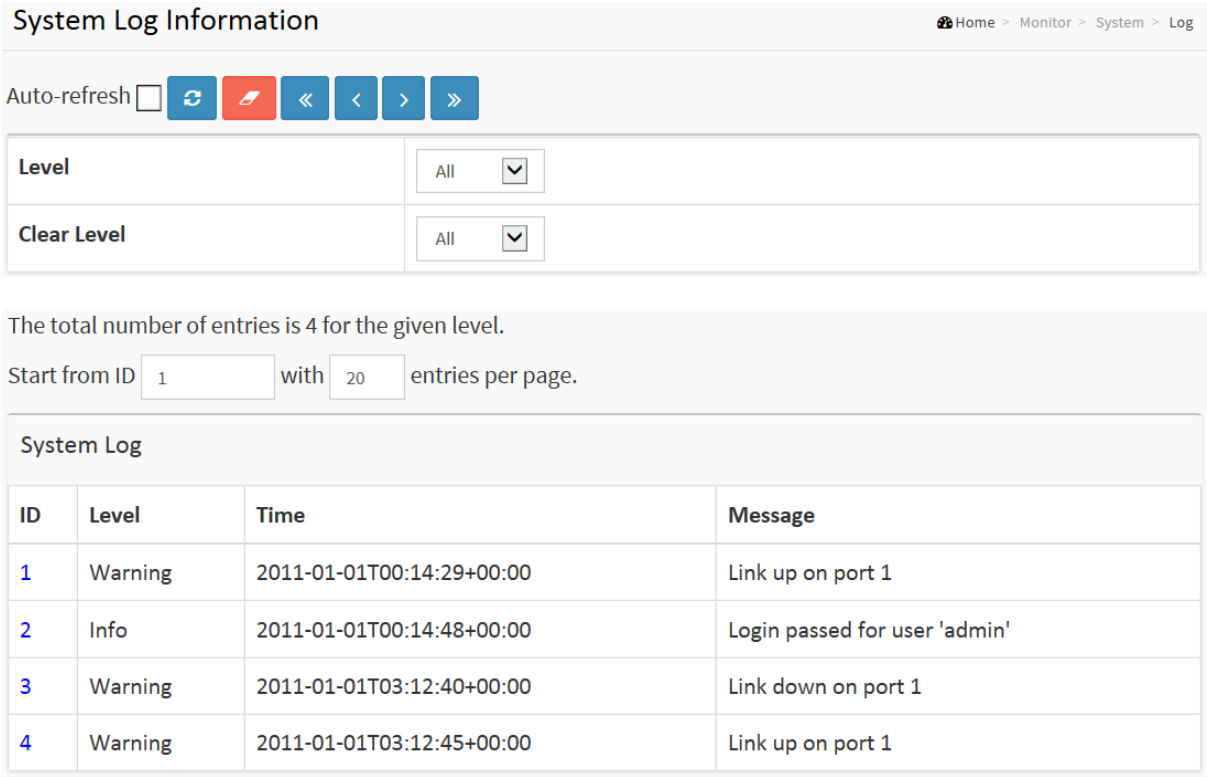


Fig: The System Log Information

Parameter	Description
Auto-refresh	To evoke the auto-refresh icon then the device will refresh the log automatically.
Level	Level of the system log entry. The following level types are supported: Information level of the system log. **Warning:** Warning level of the system log. **Error:** Error level of the system log. All: All levels.
ID	ID (>= 1) of the system log entry.
Time	It will display the log record by device time. The time of the system log entry.
Message	It will display the log detail message. The message of the system log entry.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Updates the system log entries, starting from the current entry ID. **Clear:** Flushes the selected log entries. **|<<:** Updates the system log entries, starting from the first available entry ID. **<< :** Updates the system log entries, ending at the last entry currently displayed. **>> :** Updates the system log entries, starting from the last entry currently displayed. **>>|:** Updates the system log entries, ending at the last available entry ID

Detailed Log

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

Information

To display the Detailed Log Information Status via the Web Interface:

1. Click **Monitor** > **System > Detailed Log**

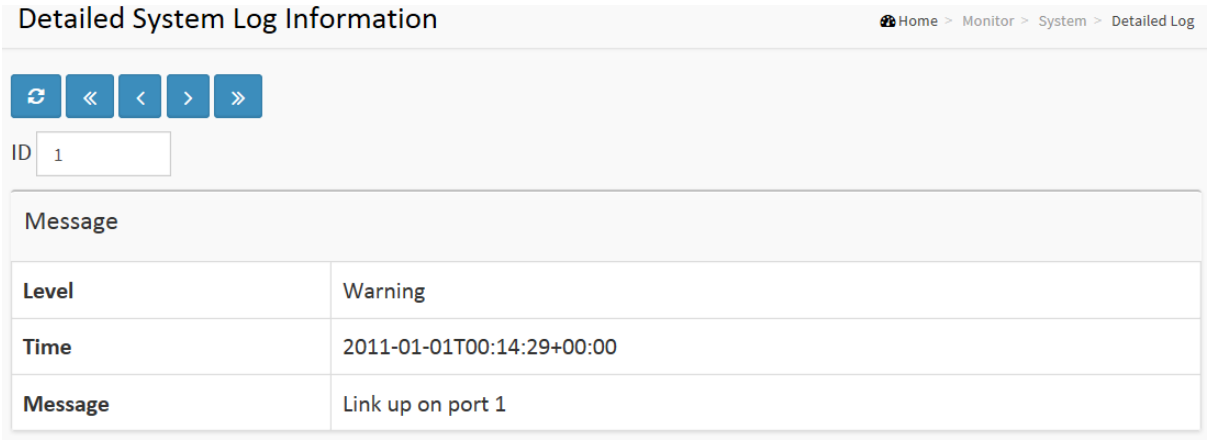


Fig: The Detailed System Log Information

Parameter	Description
ID	The ID (>= 1) of the system log entry.
Message	The detailed message of the system log entry.
Buttons	**Refresh:** Updates the system log entries, starting from the current entry ID. **|<<:** Updates the system log entries to the first available entry ID **<< :** Updates the system log entry to the previous available entry ID **>>** : Updates the system log entry to the next available entry ID **>>|:** Updates the system log entry to the last available entry ID.

Green Ethernet

Port Power Savings

This page provides the current status for Energy Efficient Ethernet (EEE)

Information

To display the Port Power Savings via the Web Interface:

1. Click **Monitor** > **Port Power Savings**

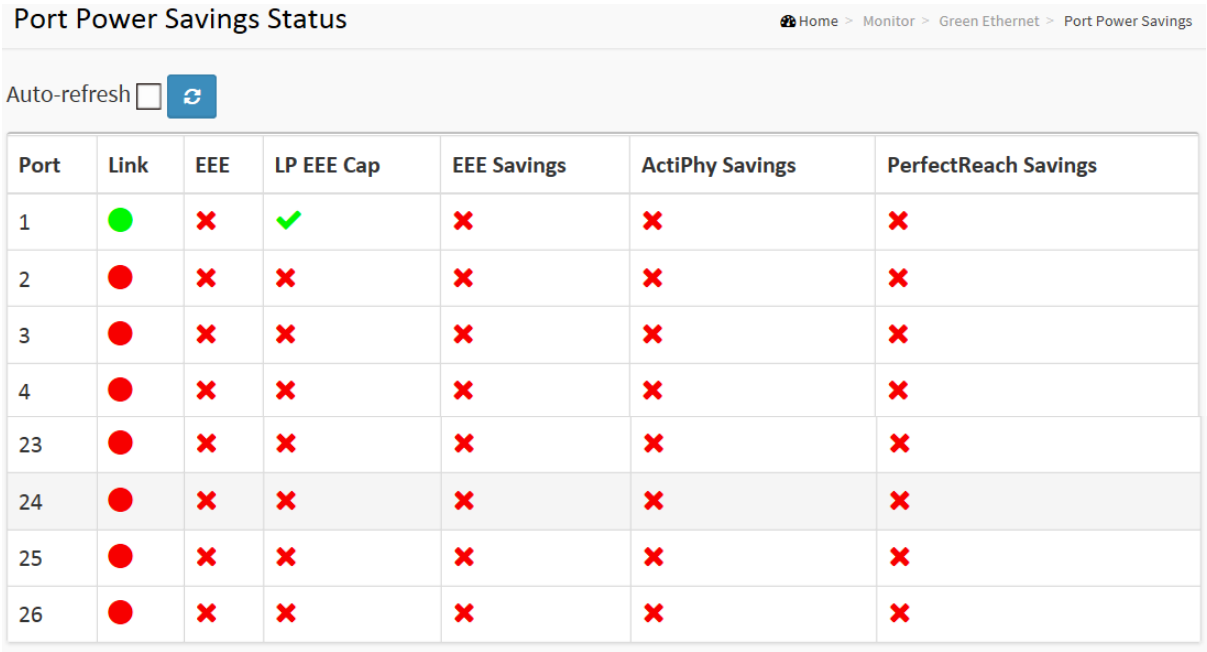


Fig: Green Ethernet Port Saving Settings

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

Actiphy Savings	Shows if the system is currently saving power due to ActiPhy.
PerfectReach Savings	Shows if the system is currently saving power due to PerfectReach.

Ports

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

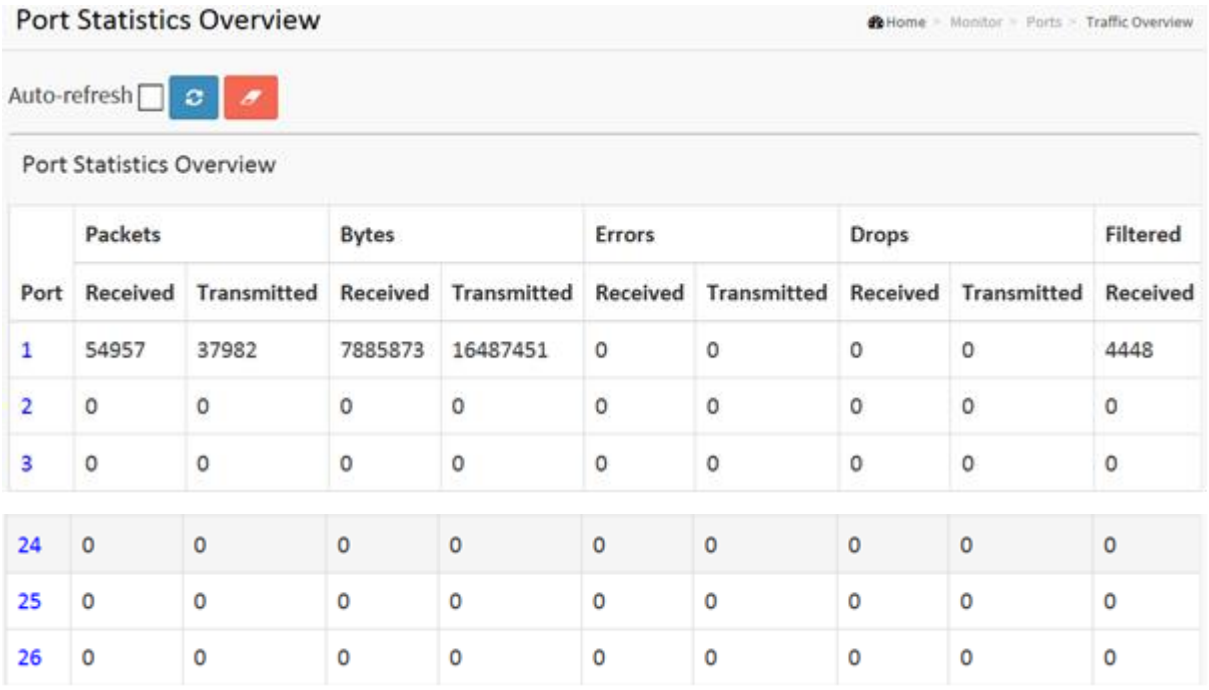
Traffic Overview

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

Information

To display the Traffic Overview details via the Web Interface:

1. Click **Monitor** > **Ports** > **Traffic Overview**
2. If you want to auto-refresh then you need to evoke the **Auto-refresh**.
3. Click " Refresh" to refresh the port statistics or clear all information when you click **Clear**



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	54957	37982	7885873	16487451	0	0	0	0	4448
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0

Fig: The Port Statistics Overview

Parameter	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **Clear:** Clears the counters for all ports.

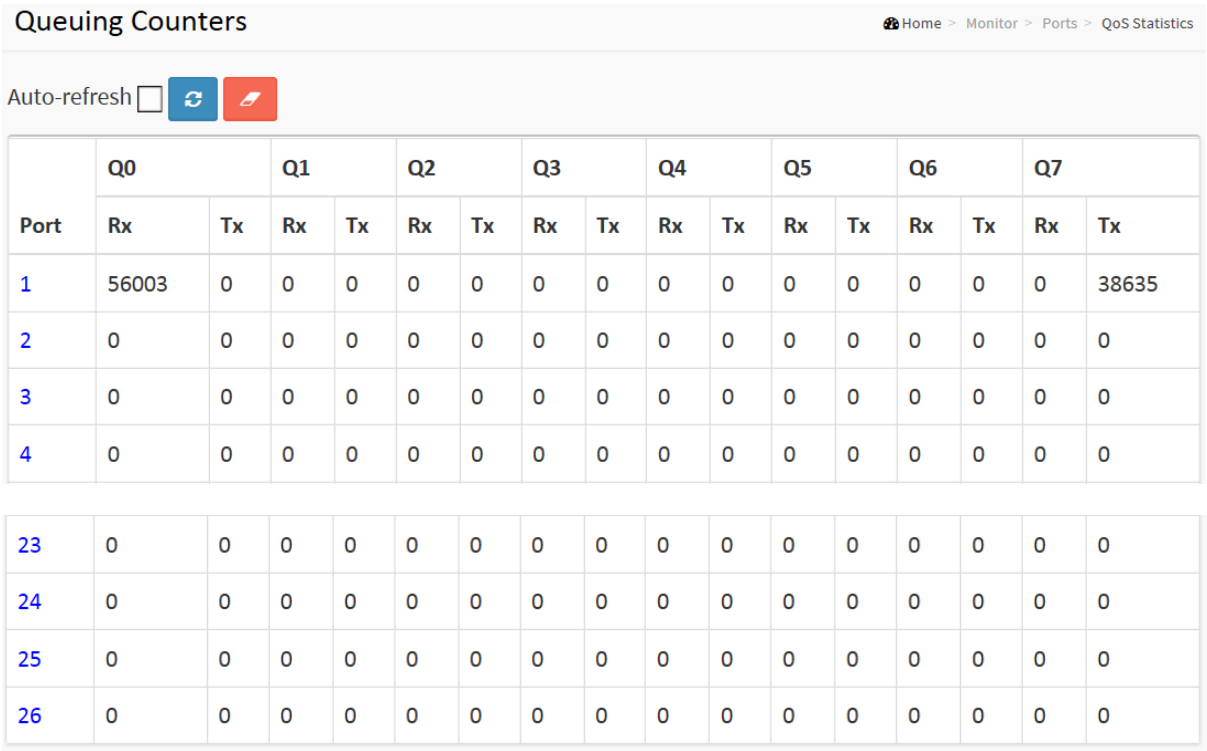
QoS Statistics

The section describes that switch could display the QoS detailed Queuing counters for a specific switch port. For the different queues for all switch ports.

Information

To Display the QoS Statistics in the web interface:

1. Click **Monitor** > **Ports** > **QoS Statistics**
2. If you want to auto-refresh the information then you need to evoke the **Auto-refresh**.
3. Click **Refresh** to refresh the Queuing Counters or clear all information when you click **Clear**.



	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
Port	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	56003	0	0	0	0	0	0	0	0	0	0	0	0	0	0	38635
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
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Fig: The Queuing Counters Overview

Parameter	Description
Port	The logical port for the settings contained in the same row.
Qn	Qn is the Queue number, There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic

	refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **Clear:** Clears the counters for all ports.

QCL Status

The section will let you know how to configure and shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Information

To Display the QCL Status in the web interface:

1. Click **Monitor** > **Ports** > **QCL Status**
2. If you want to auto-refresh the information then you need to evoke the **Auto-refresh**.
3. Scroll to select the combined, static, Voice VLAN and conflict.
4. To Click the **Refresh** to refresh an entry of the Statistics Information.

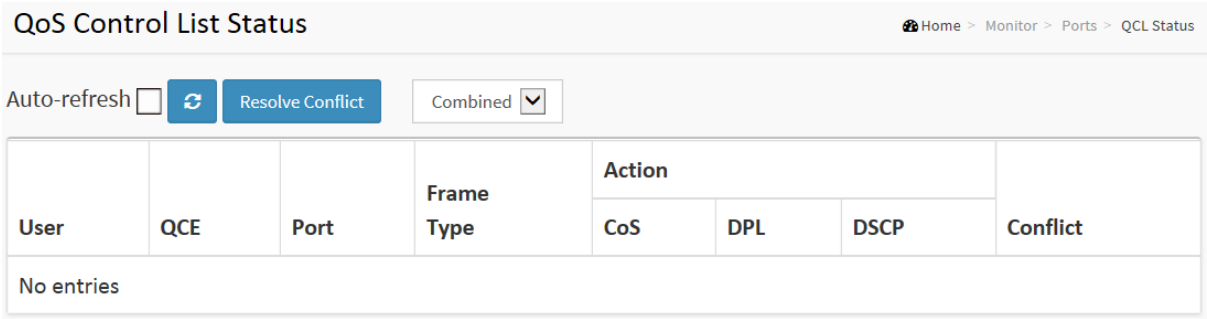


Fig: The QoS Control List Status

Parameter	Description
User	Indicates the QCL user.
QCE	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incomming frames. Possible frame types are: **Any:** The QCE will match all frame type. **Ethernet:** Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC: Only (LLC)** frames are allowed **LLC: Only (SNAP)** frames are allowed.

	IPv4: The QCE will match only IPV4 frames. **IPv6:** The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
Conflict	Displays Conflict status of QCL entries. It may happen that resources required to add a QCE may not available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Resolve Conflict:** Click to release the resources required to add QCL entry, incase conflict status for any QCL entry is 'yes'. **Refresh:** Click to refresh the page.

Detailed Statistics

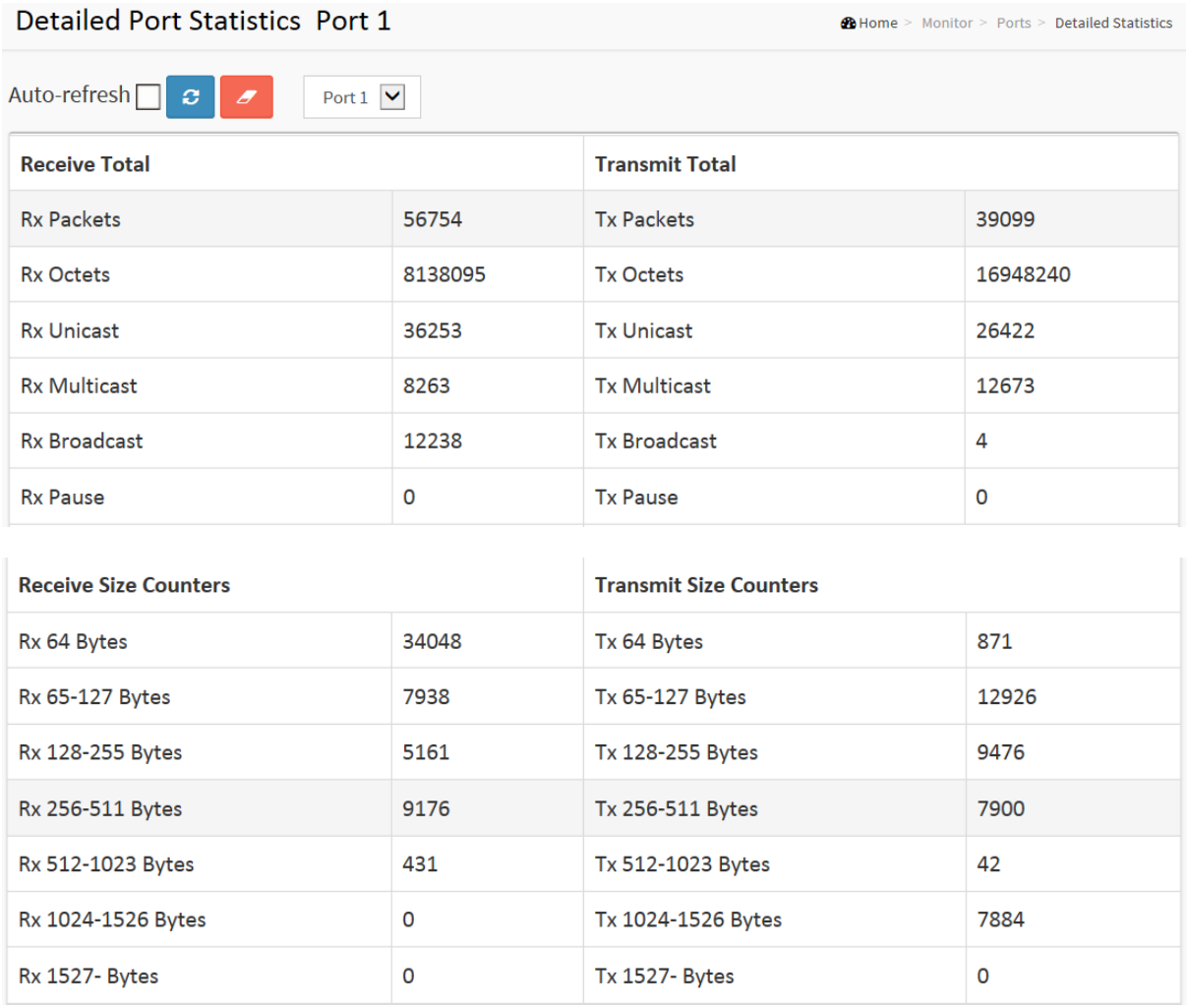
The section describes how to provide detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

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

Information

To Display the Detailed Statistics in the web interface:

1. Click **Monitor** > **Ports** > **Detailed Port Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the detailed statistics or clear all information when you click **Clear**.



Receive Total		Transmit Total	
Rx Packets	56754	Tx Packets	39099
Rx Octets	8138095	Tx Octets	16948240
Rx Unicast	36253	Tx Unicast	26422
Rx Multicast	8263	Tx Multicast	12673
Rx Broadcast	12238	Tx Broadcast	4
Rx Pause	0	Tx Pause	0

Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	34048	Tx 64 Bytes	871
Rx 65-127 Bytes	7938	Tx 65-127 Bytes	12926
Rx 128-255 Bytes	5161	Tx 128-255 Bytes	9476
Rx 256-511 Bytes	9176	Tx 256-511 Bytes	7900
Rx 512-1023 Bytes	431	Tx 512-1023 Bytes	42
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	7884
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Receive Queue Counters		Transmit Queue Counters	
Rx Q0	56754	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	39099

Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	4614		

Fig: The Detailed Port Statistics

Receive Total and Transmit Total

Parameter	Description
Auto-refresh	To evoke the auto-refresh to refresh the Port Statistics information automatically.
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	The number of received and transmitted (good and bad) broadcast packets.

Broadcast	
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation

Receive and Transmit Size Counters

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

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Parameter	Description
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.
Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process. Short frames are frames that are smaller than 64 bytes. Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters

Parameter	Description
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.
Auto-refresh	To evoke the auto-refresh to refresh the Queuing Counters automatically.

Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear**: Clears the counters for the selected port. **Refresh**: Click to refresh the page.

SFP Information

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

Information

To Display the SFP Information in the web interface:

1. Click **Monitor** > **Ports** > **SFP Information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the SFP Information statistics or clear all information when you click **Clear**.

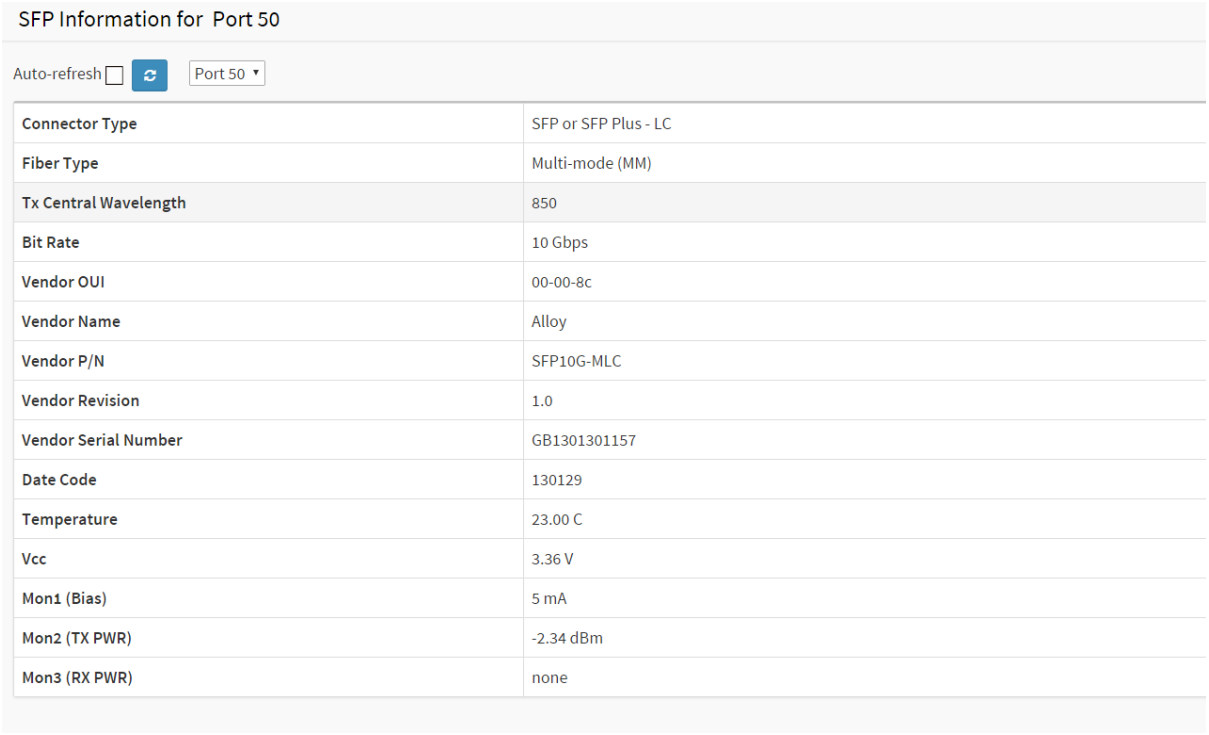


Fig: The SFP Information Overview

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 of the naming by module manufacturer.
Vendor Revision	Display the module revision.
Vendor Serial Number	Show the serial number assigned by the manufacturer.
Date Code	Show the date this SFP module was made.
Temperature	Show the current temperature of SFP module.
VCC	Show the working DC voltage of SFP module.
Mon1(Bias) mA	Show the Bias current of SFP module.
Mon2(TX PWR)	Show the transmit power of SFP module.
Mon3(RX PWR)	Show the receiver power of SFP module.

DHCP

Server

DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

Information

Display the DHCP server Statistics Overview in the web interface:

1. Click **Monitor** > **DHCP** > **Server > Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the DHCP statistics or clear all information when you click **Clear**.

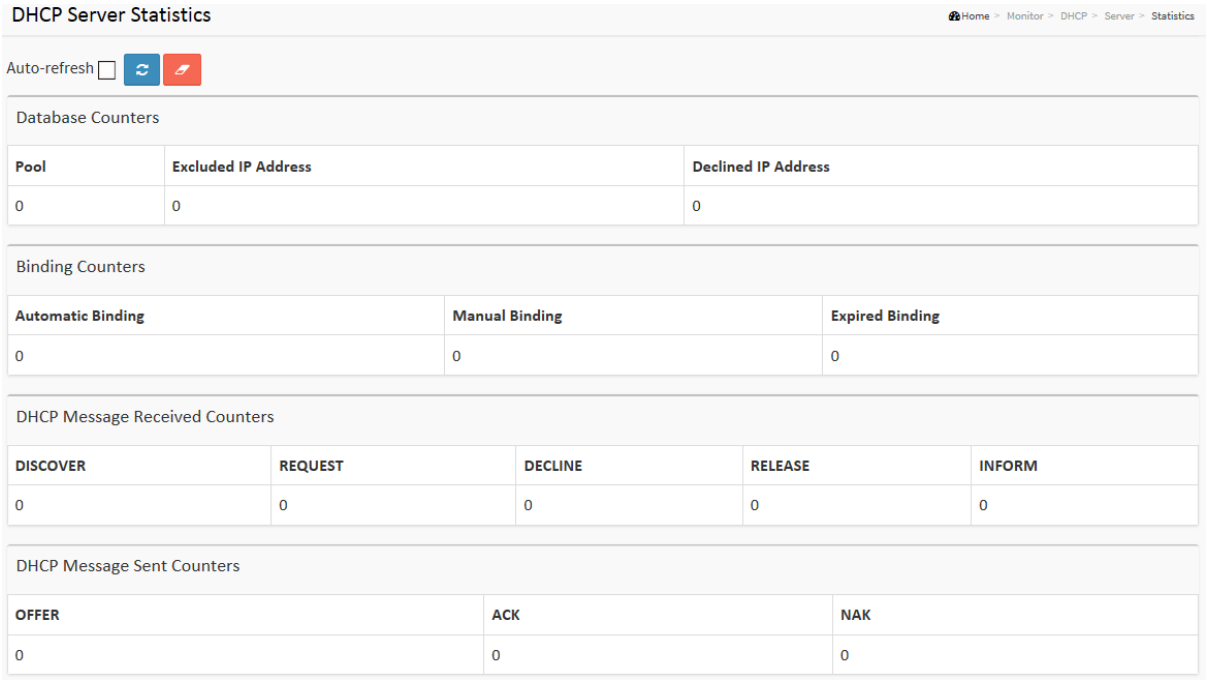


Fig: The Protocol to Group Mapping Table

Database Counters

Parameter	Description

Pool	Number of pools.
Excluded IP Address	Number of excluded IP address ranges.
Declined IP Address	Number of sec lined IP addresses.

Binding Counters

Parameter	Description
Automatic Binding	Number of bindings with network-type pools.
Manual Binding	Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.
Expired Binding	Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

Parameter	Description
DISCOVER	Number of DHCP DISCOVER messages received.
REQUEST	Number of DHCP REQUEST messages received.
DECLINE	Number of DHCP DECLINE messages received.
RELEASE	Number of DHCP RELEASE messages received.
INFORM	Number of DHCP INFORM messages received.

DHCP Message Sent Counters

Parameter	Description
OFFER	Number of DHCP OFFER messages sent.
ACK	Number of DHCP ACK messages sent.
NAK	Number of DHCP NAK messages sent.

Binding

This page displays bindings generated for DHCP clients.

Information

To Display DHCP Server Binding IP in the web interface:

1. Click **Monitor** > **DHCP** > **Server > Binding**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Binding statistics or clear all information when you click **Clear**.

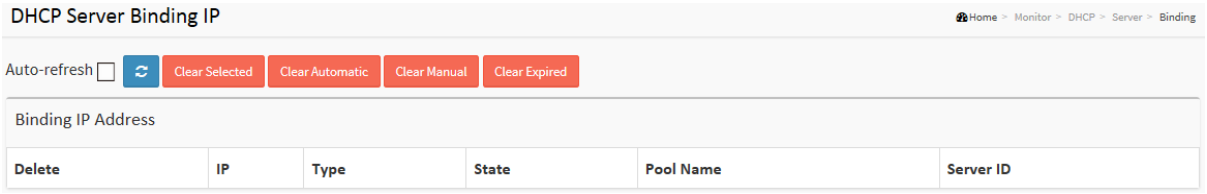


Fig: The Group Name of VLAN Mapping Table

Parameter	Description
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, and Expired.
State	State of binding. Possible states are Committed, Allocated, and Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

Declined IP

This page displays declined IP addresses.

Information

To Display Declined IPs in the web interface:

1. Click **Monitor** > **DHCP** > **Server > Declined IP**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Declined IP statistics or clear all information when you click **Clear**.

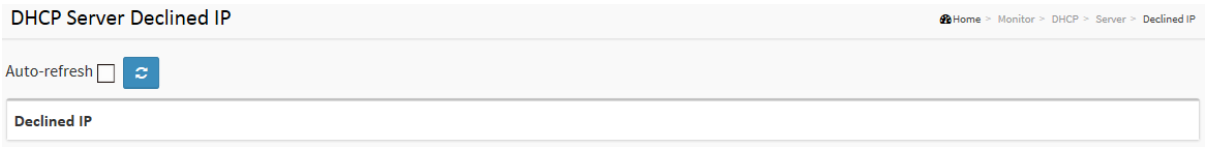


Fig: The Declined IP

Parameter	Description
IP	IP address allocated to DHCP client.
Type	Type of binding. Possible types are Automatic, Manual, and Expired.
State	State of binding. Possible states are Committed, Allocated, and Expired.
Pool Name	The pool that generates the binding.
Server ID	Server IP address to service the binding.

Snooping Table

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Information

To Display the Snooping Table Information in the web interface:

1. Click **Monitor** > **DHCP** > **Snooping Table**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Snooping Table statistics or clear all information when you click **Clear**.

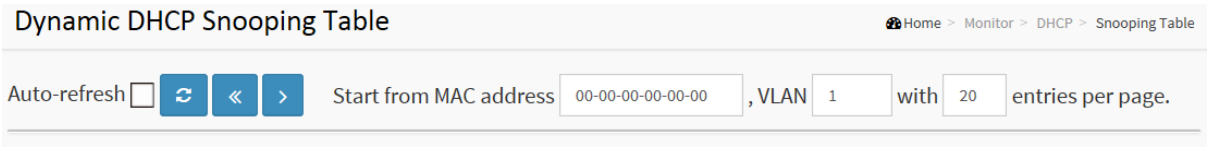


Fig: The DHCP snooping table

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

Relay Statistics

This page provides statistics for DHCP relay.

Information

To Display the Relay Statistics Information in the web interface:

1. Click **Monitor** > **DHCP** > **Relay Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Replay statistics or clear all information when you click **Clear**.

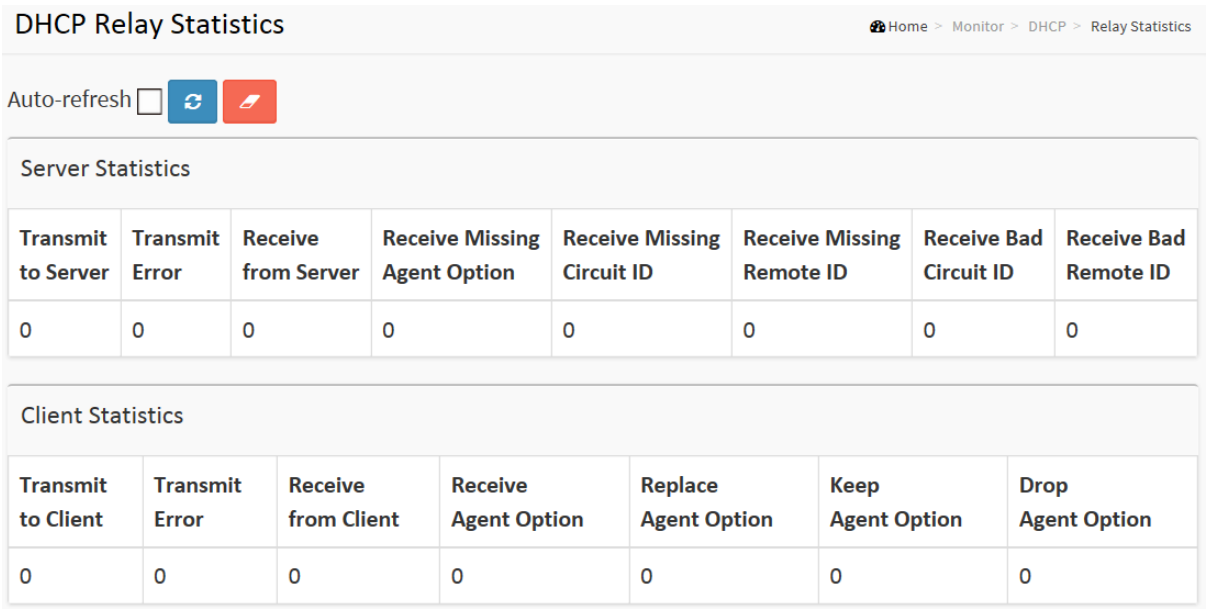


Fig: The DHCP relay statistics

Server Statistics

Parameter	Description
Transmit to Server	The number of packets that are relayed from client to server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from server.
Receive Missing Agent Options	The number of packets received without agent information options.
Receive Missing	The number of packets received with the Circuit ID option missing.

Circuit ID	
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Parameter	Description
Transmit to Client	The number of relayed packets from server to client.
Transmit Error	The number of packets that resulted in error while being sent to servers.
Receive from Client	The number of received packets from server.
Receive Agent Option	The number of received packets with relay agent information option.
Replace Agent Option	The number of packets which were replaced with relay agent information option.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	The number of packets that were dropped which were received with relay agent information.

Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Information

To Display the Detailed Statistics Information in the web interface:

1. Click **Monitor** > **DHCP** > **Detailed Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the detailed statistics or clear all information when you click **Clear**.

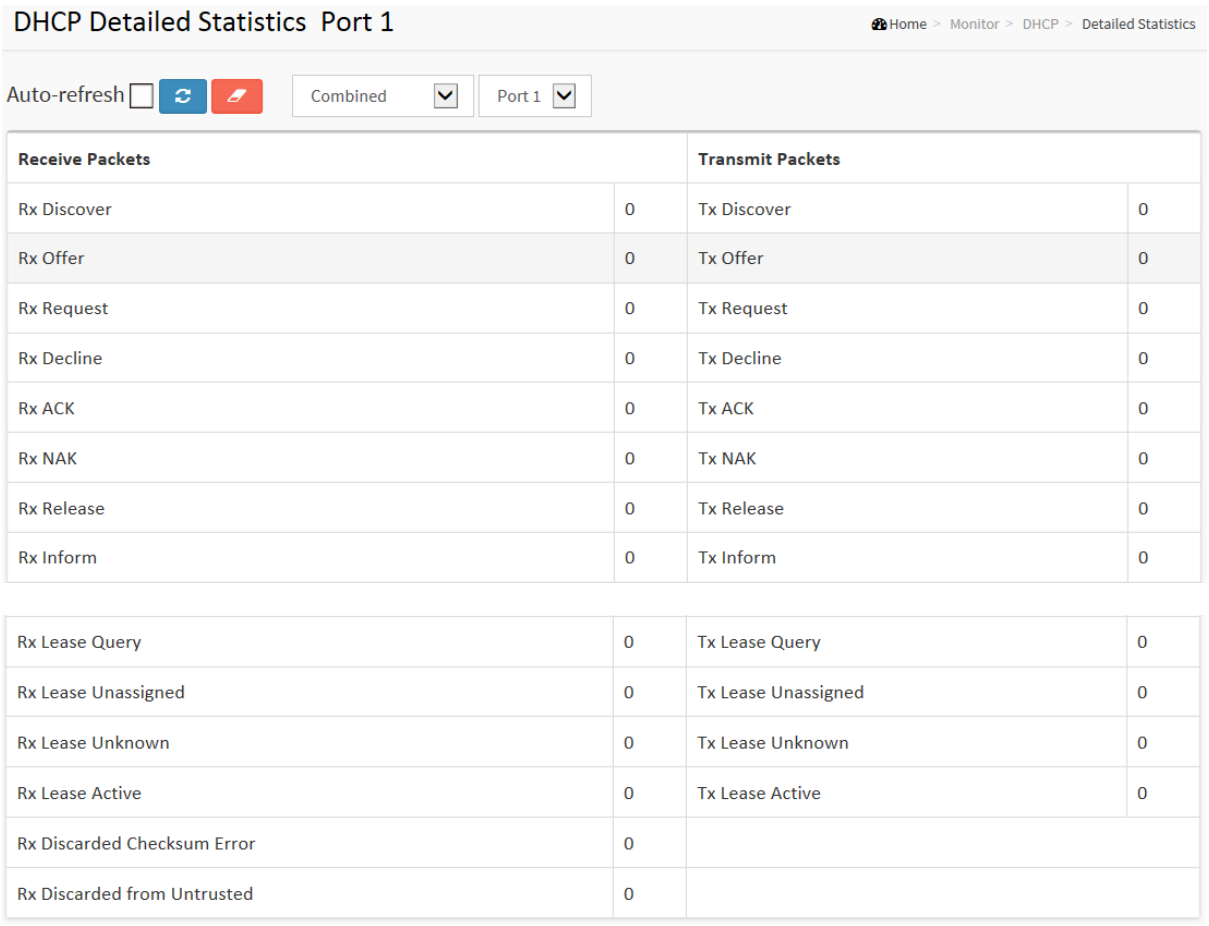


Fig: The DHCP Detailed Statistics

Parameter	Description
Rx and Tx Discover	The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer	The number of offer (option 53 with value 2) packets received and transmitted.
Rx and TX Request	The number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	The number of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted.
Rx and TX NAK	The number of NAK (option 53 with value 6) packets received and transmitted.
Rx and TX Release	The number of release (option 53 with value 7) packets received and transmitted.
Rx and Tx Inform	The number of inform (option 53 with value 8) packets received and transmitted.
Rx and Tx Lease Query	The number of lease query (option 53 with value 10) packets received and transmitted.
Rx and Tx Lease Unassigned	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Lease Unknown	The number of lease unknown (option 53 with value 12) packets received and transmitted. Rx and Tx Lease Active
Rx and Tx Lease Active	The number of lease active (option 53 with value 13) packets received and transmitted.
Rx Discarded checksum error	The number of discard packet that IP/UDP checksum is error.
Rx Discarded from Untrusted	The number of discarded packet that are coming from untrusted port.

Security

Access Management Statistics

This section shows you a detailed statistics of the Access Management including HTTP, HTTPS, SSH. TELNET.

Information

To Display the Access Management Statistics Information in the web interface:

1. Click **Monitor** > **Security** > **Access Management Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Access Management statistics or clear all information when you click **Clear**.

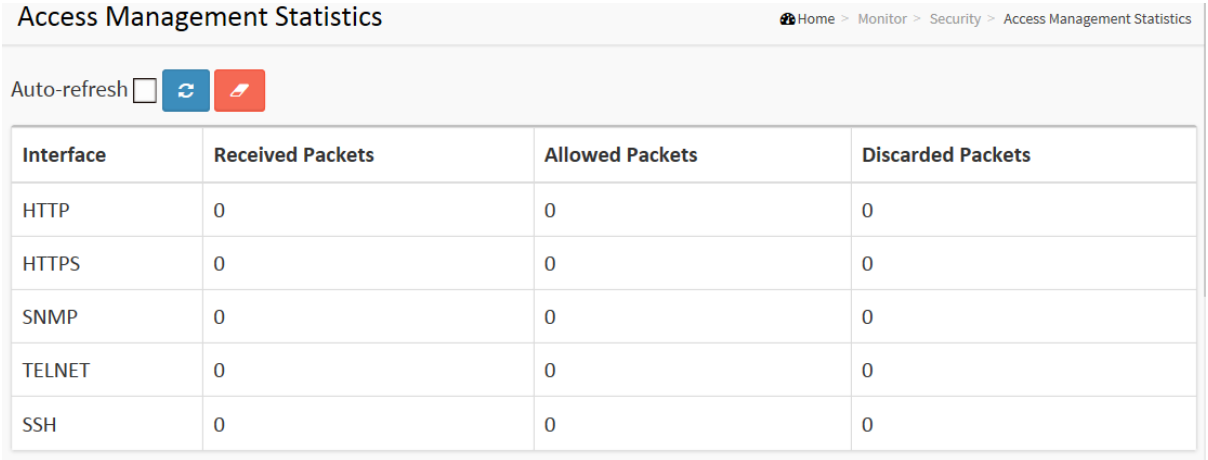


Fig: The Access Management Statistics

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.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page.

Network

Port Security

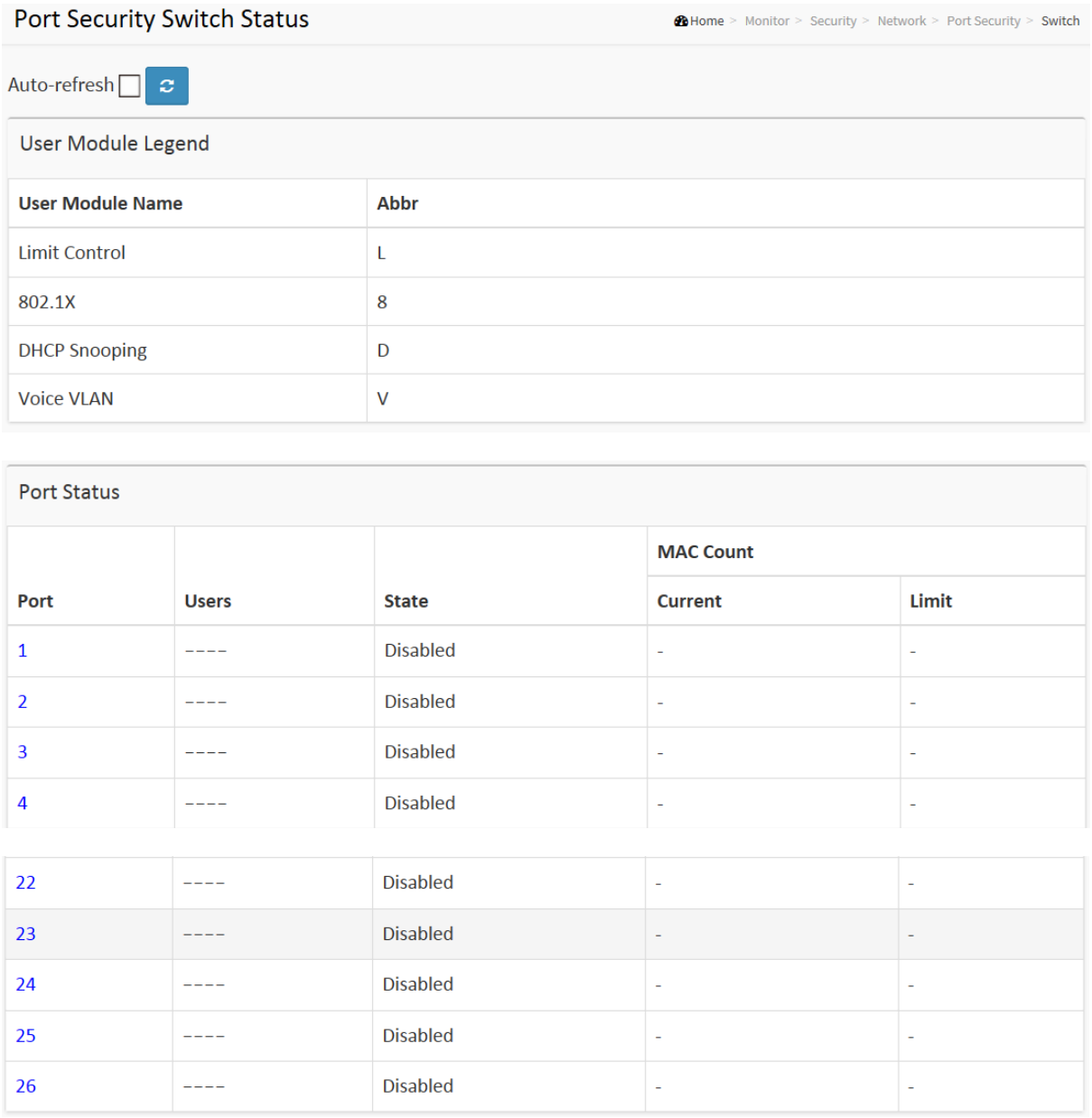
Switch

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

Information

To Display the Network port Security Statistics Information in the web interface:

1. Click **Monitor** > **Security** > **Network** > **Port Security** > **Switch**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Port Security statistics or clear all information when you click **Clear**.



Port Security Switch Status

Home > Monitor > Security > Network > Port Security > Switch

Auto-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	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	Disabled	-	-
25	----	Disabled	-	-
26	----	Disabled	-	-

Fig: The Port Security Switch Status

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.
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
Port Status	The table has one row for each port on the selected switch and a number of

	columns, which are:
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 (-). Indicates the number of currently learned MAC addresses (forwarding as well as blocked) on the port. If no user modules are enabled on the port, a dash (-) will be shown.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port

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 chooses to block it, it will be blocked until that user module decides otherwise.

Information

To Display the Port Statistics Information in the web interface:

1. Click **Monitor** > **Security** > **Network** > **Port Security** > **Port**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Port statistics or clear all information when you click **Clear**.

Fig: The 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 will not be allowed to transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC

	address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

NAS

Switch

The section describes to show the each port NAS status information of the switch. The status includes Admin State Port State, Last Source, Last ID, QoS Class, and Port VLAN ID.

Information

To Display the NAS Statistics Information in the web interface:

1. Click **Monitor** > **Security** > **Network** > **NAS** > **Switch**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the NAS statistics or clear all information when you click **Clear**.

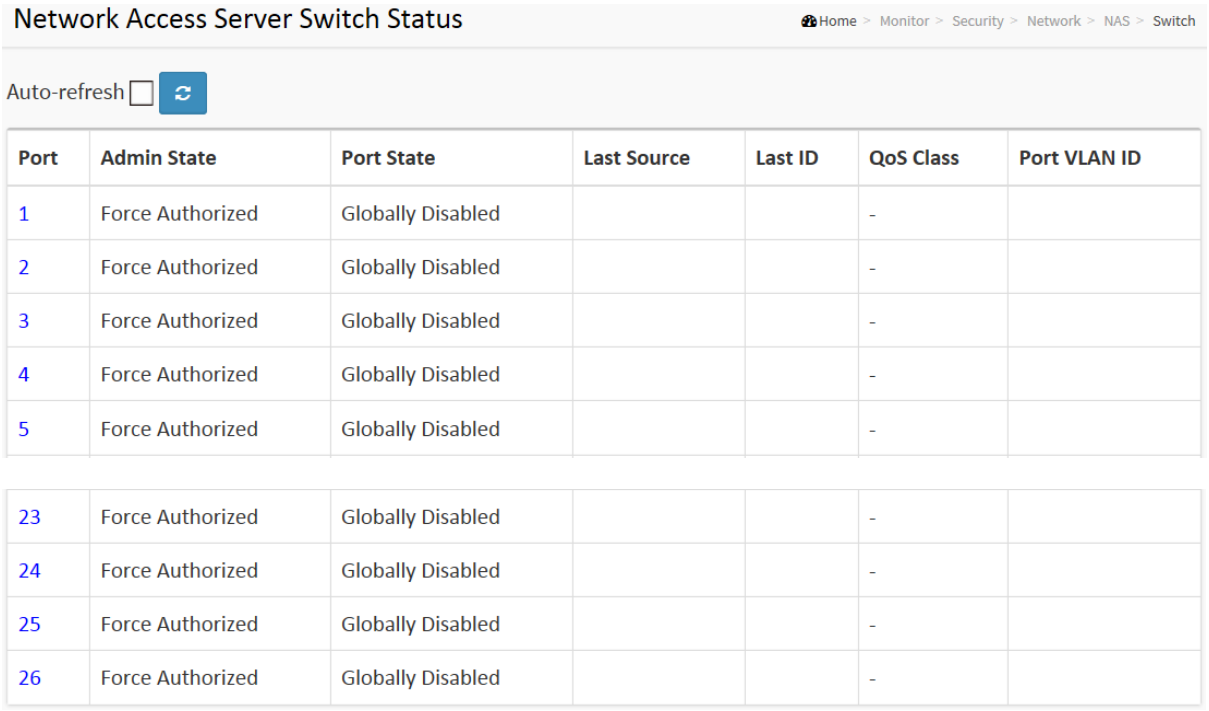


Fig: The Network Access Server Switch Status

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	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port

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

Information

To Display the NAS port Statistics Information in the web interface:

1. Click **Monitor** > **Security** > **Network** > **NAS** > **Port**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the port statistics or clear all information when you click **Clear**.

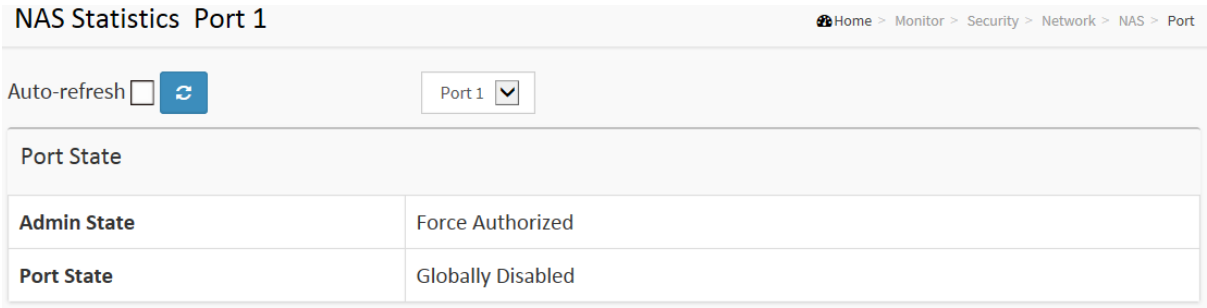


Fig: The NAS Statistics

Port State

Parameter	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

	Read more about Guest VLANs here.

Port Counters

Parameter	Description
EAPOL Counters	These supplicant frame counters are available for the following administrative states: • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X • Multi 802.1X
Backend Server Counters	These backend (RADIUS) frame counters are available for the following administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Last Supplicant/Client Info	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.

Selected Counters

Parameter	Description
Selected Counters	The Selected Counters table is visible when the port is in one of the following administrative states:

	• Multi 802.1X • MAC-based Auth. 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.

Attached MAC Addresses

Parameter	Description
Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. 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. This column is not available for MAC-based Auth.
MAC Address	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. 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.
VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't 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).
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

	Clear: This button is available in the following modes: • Force Authorized • Force Unauthorized • Port-based 802.1X • Single 802.1X **Clear All:** Click to clear the counters for the selected port. This button is available in the following modes: • Multi 802.1X • MAC-based Auth.X **Clear This:** Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however. This button is available in the following modes: • Multi 802.1X • MAC-based Auth.X Click to clear only the currently selected client's counters.

ARP Inspection

The section describes to configure the Dynamic ARP Inspection Table parameters of the switch. 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.

Information

To Display the ARP Inspection Information in the web interface:

1. Click **Monitor** > **Security** > **Network** > **ARP Inspection**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the ARP Inspection statistics or clear all information when you click **Clear**.

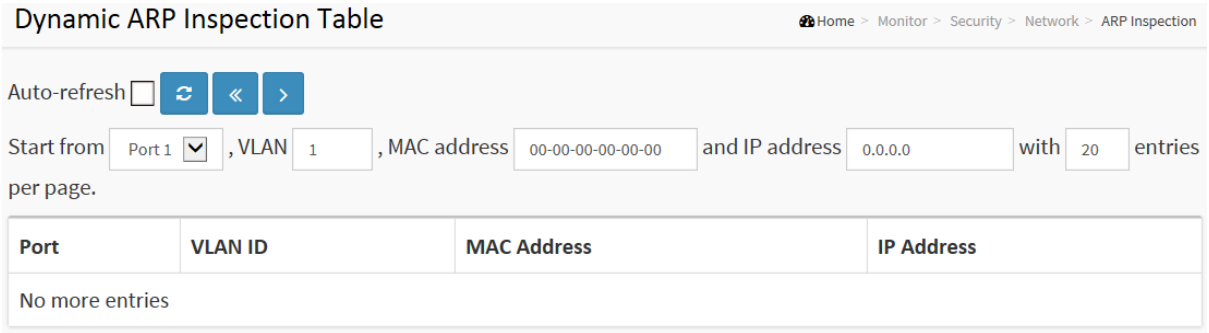


Fig: The Dynamic ARP Inspection Table

Navigating the ARP Inspection Table.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

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.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID. **>> :** Updates the system log entry to the next available entry ID.

IP Source Guard

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

Information

To Display the IP Source Guard in the web interface:

1. Click **Monitor** > **Security** > **Network** > **IP Source Guard**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the IP Source Guard statistics or clear all information when you click **Clear**.

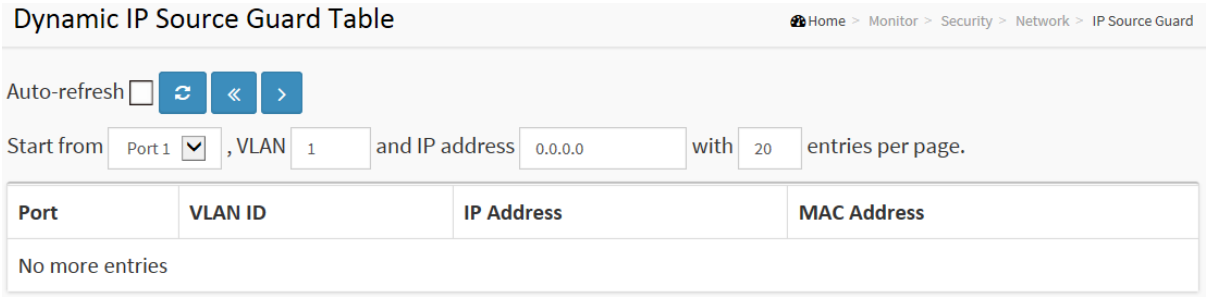


Fig: The IP Source Guard Table

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.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID. **>> :** Updates the system log entry to the next available entry ID.

AAA

Radius Overview

This section shows you an overview of the RADIUS Authentication and Accounting servers status to ensure the function is workable.

Information

To Display the Radius Overview Information in the web interface:

1. Click **Monitor** > **Security** > **AAA** > **RADIUS Overview**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Radius Overview statistics or clear all information when you click **Clear**.

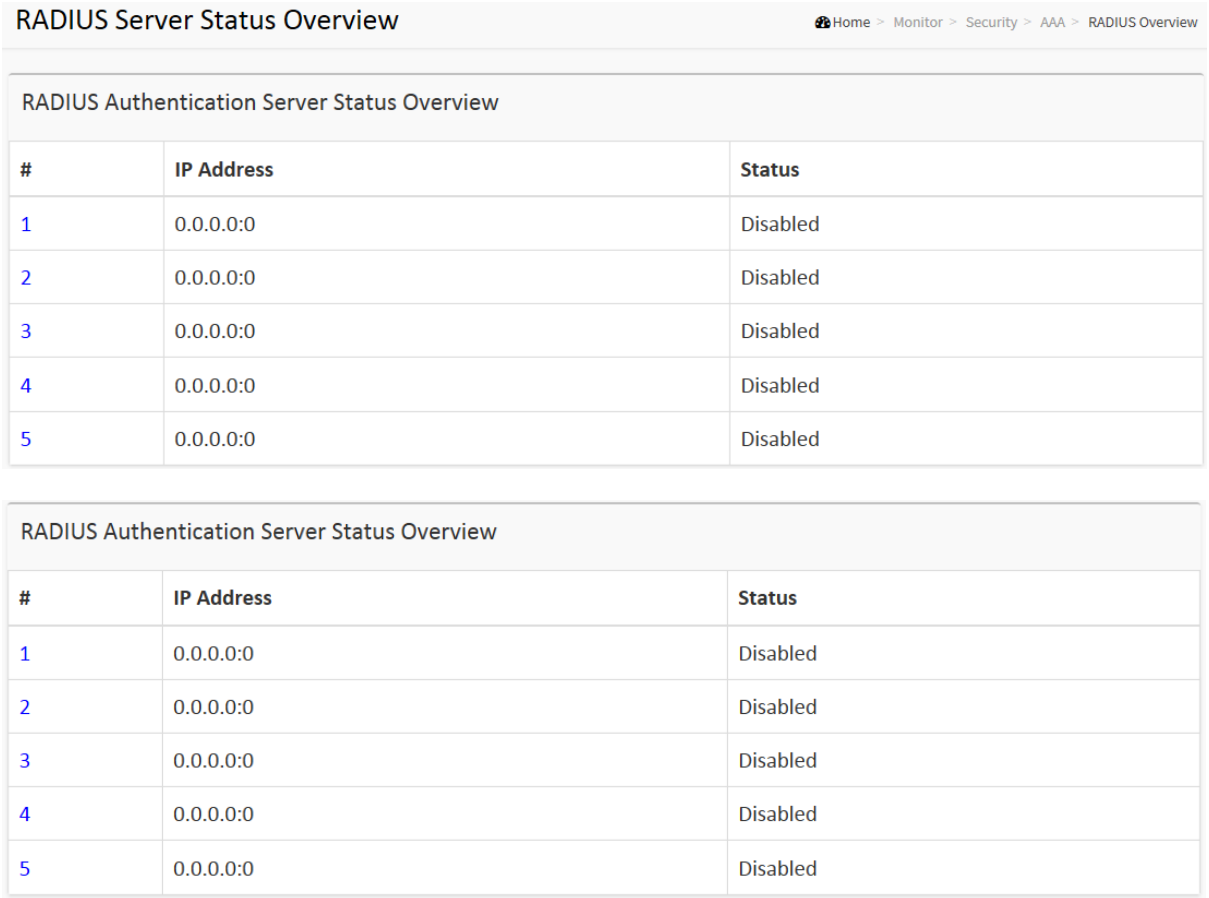


Fig: The RADIUS Authentication Server Status Overview

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	The current state of the server. This field takes one of the following values: **Disabled:** The server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left):** Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

RADIUS Accounting Servers

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	The current state of the server. This field takes one of the following values: **Disabled:** The server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. **Dead (X seconds left):** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of

	seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

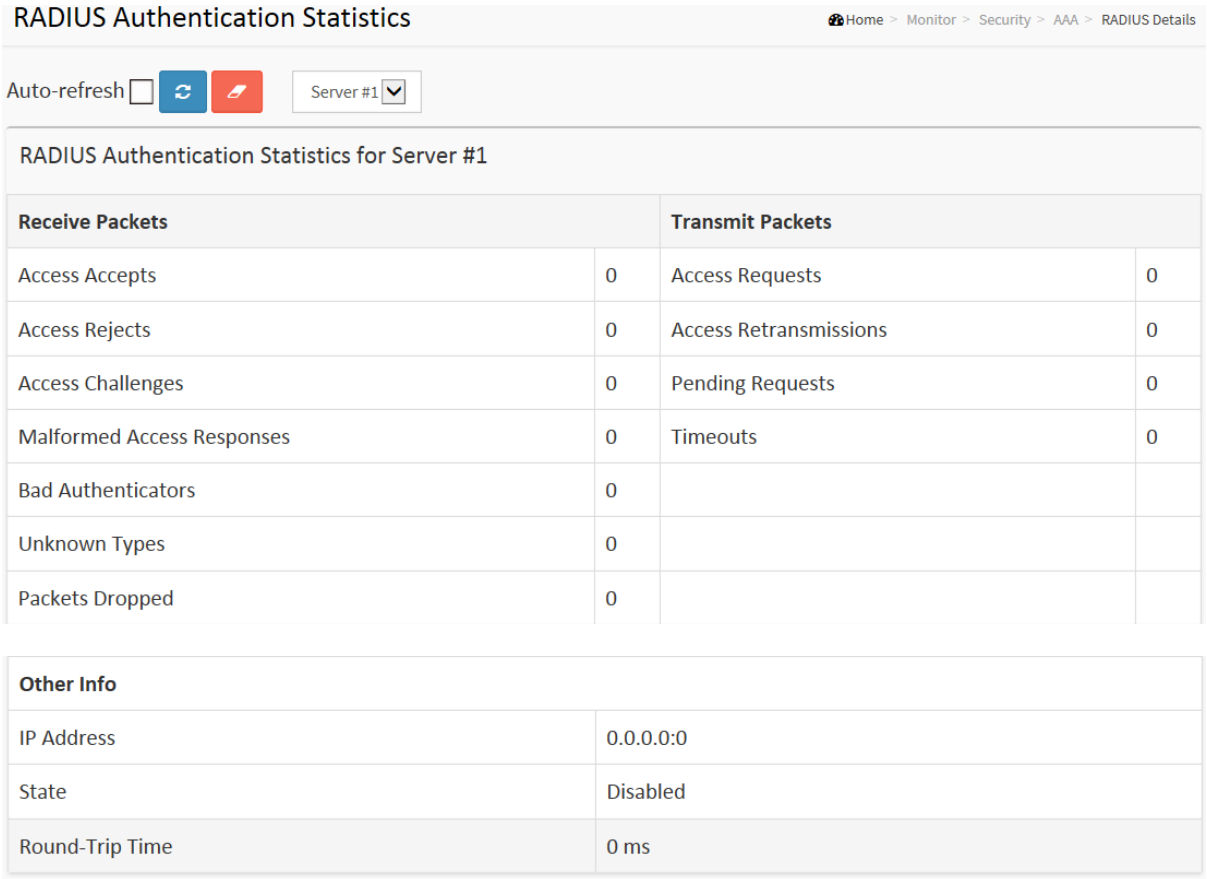
RADIUS Details

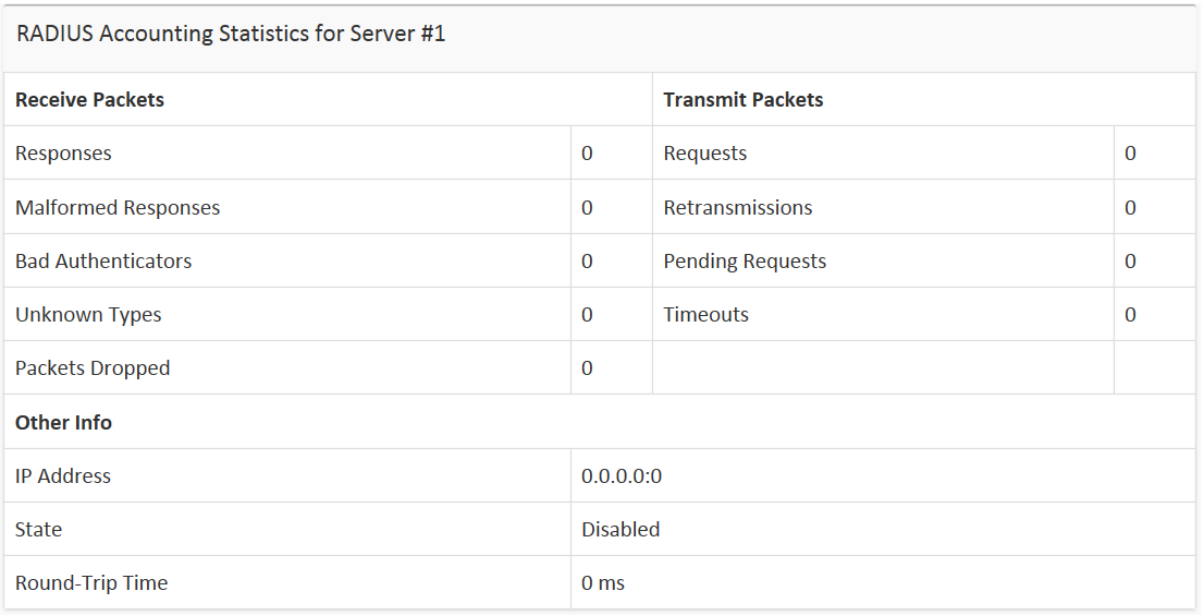
This section shows you the detailed statistics for a particular RADIUS server.

Information

To Display the Radius Details Information in the web interface:

1. Click **Monitor** > **Security** > **AAA** > **RADIUS Details**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the port detailed statistics or clear all information when you click **Clear**.





RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:0		
State	Disabled		
Round-Trip Time	0 ms		

Fig: The RADIUS Authentication Statistics Server

RADIUS Authentication Statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access	radiusAuthClientExtMalfo	The number of malformed RADIUS Access-Response

	Responses	rmedAccessResponses	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	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	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	radiusAuthClientExtTimeouts	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

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled:** The selected server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

		Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	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 Authentication Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	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	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	Pending Requests	radiusAccClientExtPendingRequests	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	radiusAccClientExtTimeouts	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

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled:** The selected server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. **Dead (X seconds left):** Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time	radiusAccClientExtRoundTripTime	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.

Parameter	Description
Buttons	**Auto-refresh** –Check this box to enable an automatic refresh of the page at regular intervals. **Refresh** - Click to refresh the page immediately. **Clear** - Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Switch

RMON

Statistics

From the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

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

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

Information

To Display the RMON Statistics Information in the web interface:

1. Click **Monitor** > **Security** > **RMON** > **Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the RMON Switch statistics or clear all information when you click **Clear**.

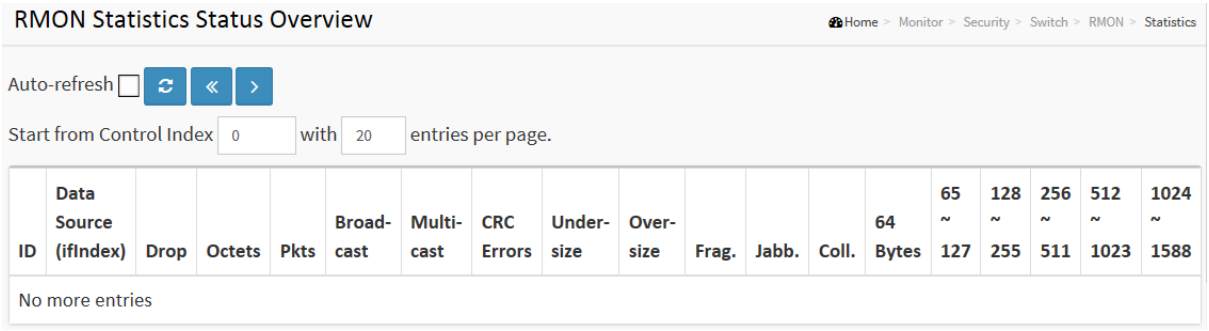


Fig: The RMON Statistics Status Overview

Parameter	Description
ID	Indicates the index of Statistics entry.

Data Source (ifindex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-Cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 1518 octets.
Frag	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll	The best estimate of the total number of collisions on this Ethernet segment.
64	The total number of packets (including bad packets) received that were 64 octets in length.
65-127	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
128-255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256-511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512-1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024-1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page immediately. **|<< :** Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID. **>> :** Updates the table, starting with the entry after the last entry currently displayed.

History

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

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table.

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

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

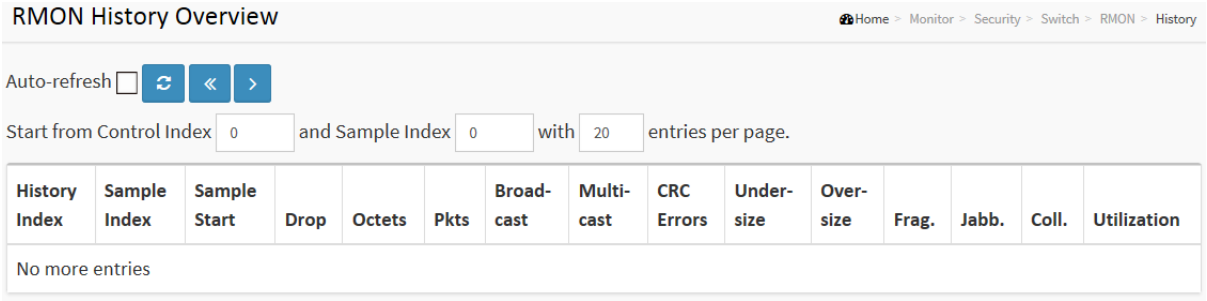


Fig: RMON History Overview

Information

To Display the RMON History Information in the web interface:

1. Click **Monitor** > **Security** > **RMON** > **History**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the History statistics or clear all information when you click **Clear**.

Parameter	Description
History Index	Indicates the index of Statistics entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.
CRCErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag	The number of frames which size is less than 64 octets received with invalid CRC.

Jabb	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page immediately. **|<< :** Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index **>> :** Updates the table, starting with the entry after the last entry currently displayed

Alarm

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

The "Start from Control Index" allows the user to select the starting point in the Alarm table.

Clicking the button will update the displayed table starting from that or the next closest Alarm table match.

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

Information

To Display the RMON History Information in the web interface:

1. Click **Monitor** > **Security** > **RMON** > **Alarm**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Alarm statistics or clear all information when you click **Clear**.

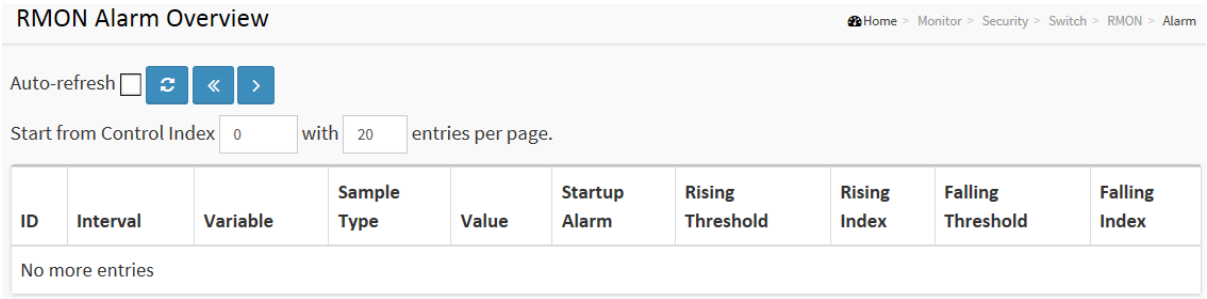


Fig: RMON Alarm Overview

Parameter	Description
ID	Indicates the index of Alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled

Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Value	The value of the statistic during the last sampling period.
Startup Alarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	Rising threshold value.
Rising index	Rising event index.
Falling Threshold	Falling threshold value.
Falling index	Falling event index.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page immediately. **|<<:** Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID. **>> :** Updates the table, starting with the entry after the last entry currently displayed.

Event

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

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

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

Information

To Display the RMON Alarm Information in the web interface:

1. Click **Monitor** > **Security** > **RMON** > **Event**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Event statistics or clear all information when you click **Clear**.

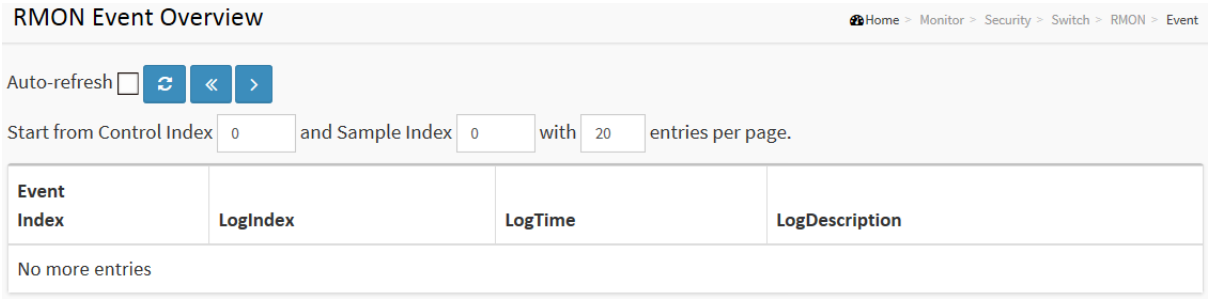


Fig: RMON Event Overview

Parameter	Description
Event Index	Indicates the index of the event entry.
Log index	Indicates the index of the log entry.
LogTime	Indicates Event log time
LogDescription	Indicates the Event description.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

	Refresh: Click to refresh the page immediately. **|<< :** Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index. **>>:** Updates the table, starting with the entry after the last entry currently displayed

LACP

System Status

This section describes that when you complete to set LACP function on the switch then it provides a status overview for all LACP instances.

Information

To Display the LACP Information in the web interface:

1. Click **Monitor** > **LACP** > **System Status**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the LACP statistics or clear all information when you click **Clear**.

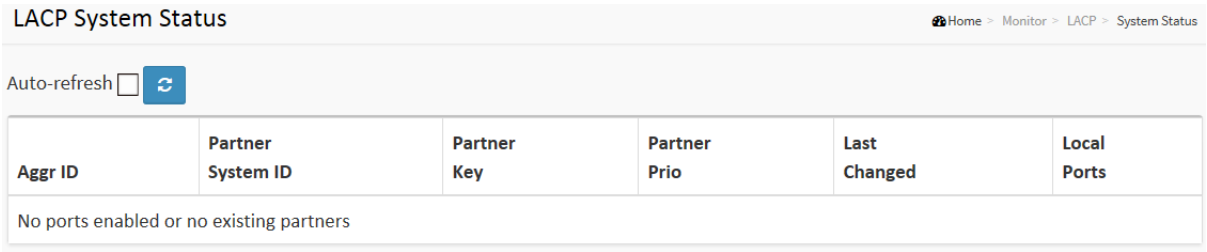


Fig: The LACP System Status

Parameter	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown 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	Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port Status

This section describes that when you complete to set LACP function on the switch then it provides a Port Status overview for all LACP instances

Information

To Display the LACP Port Status Information in the web interface:

1. Click **Monitor** > **LACP** > **Port Status**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Port Status statistics or clear all information when you click **Clear**.

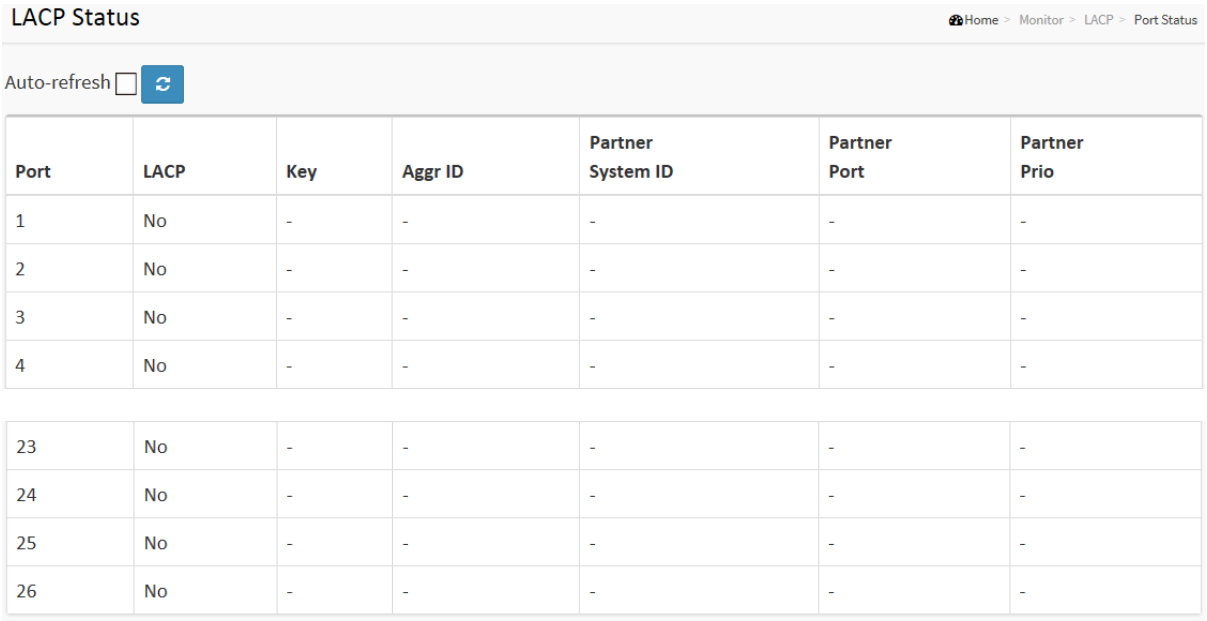


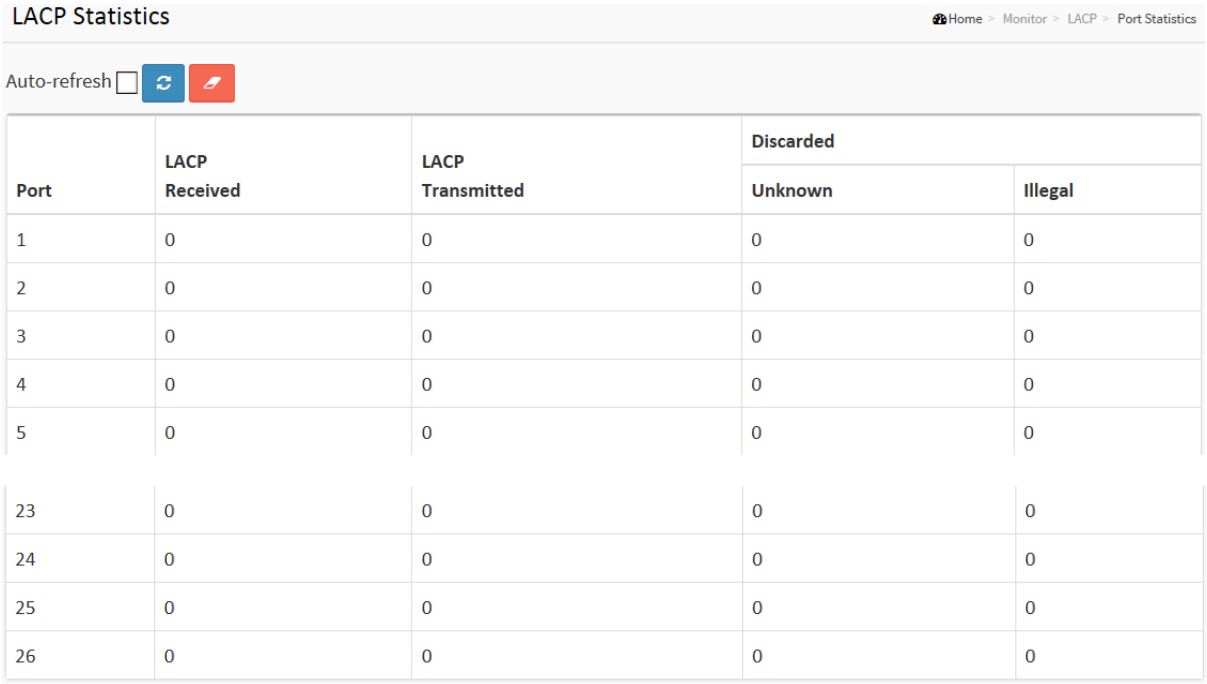
Fig: The LACP Status

Parameter	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID	The Aggregation ID assigned to this aggregation group. IDs 1 and 2 are GLAGs while IDs 3-14 are LLAGs.
Partner System ID	The partner's System ID (MAC address).
Partner Port	The partner's port number connected to this port.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port Statistics

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



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
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

Fig: The LACP Statistics

Parameter	Description
Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page.

Loop Protection

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

Information

To Display the Loop Protection Information in the web interface:

1. Click **Monitor** > **LACP** > **Port Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Loop Protection statistics or clear all information when you click **Clear**.

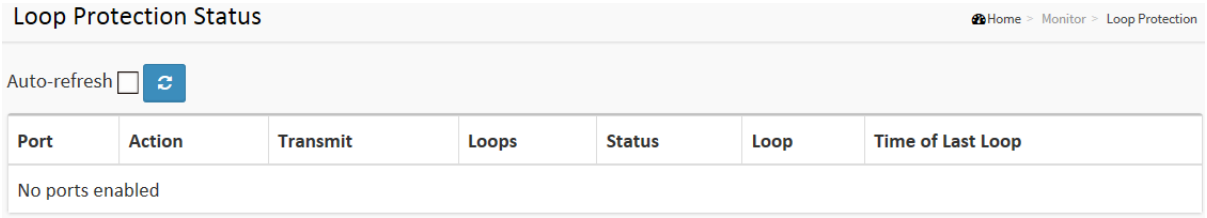


Fig: Loop Protection Status

Parameter	Description
Port	The switch port number of the logical port.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.
Buttons	**Refresh:** Click to refresh the page immediately. **Auto-refresh:** Check this box to enable an automatic refresh of the page at regular intervals.

Spanning Tree

Bridge Status

The Section provides a status overview of all STP bridge instances. The displayed tables on this page contain information on STP information such as Bridge ID, Root ID MSTI etc.

Information

To Display the Spanning Tree Information in the web interface:

1. Click **Monitor** > **Spanning Tree** > **STP Bridges**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the STP Bridge statistics or clear all information when you click **Clear**.

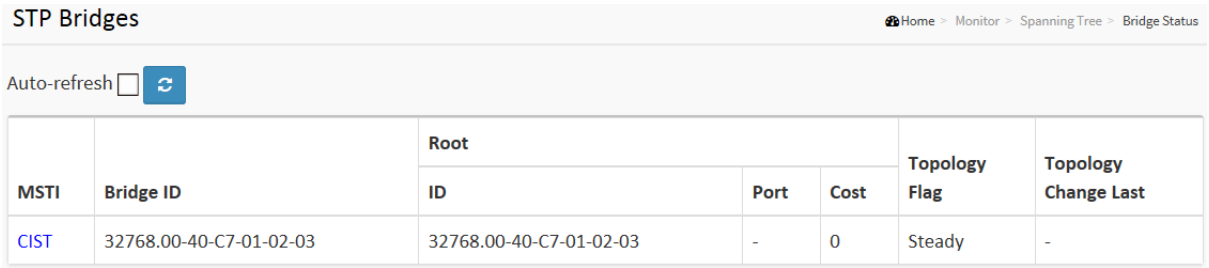


Fig: The STP Bridges status

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 Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic

	refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port Status

The Section provides you to ask switch to display the STP CIST port status for physical ports of the currently selected switch.

Information

To Display the STP Port Status Information in the web interface:

1. Click **Monitor** > **Spanning Tree** > **STP Port Status**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the STP Port statistics or clear all information when you click **Clear**.

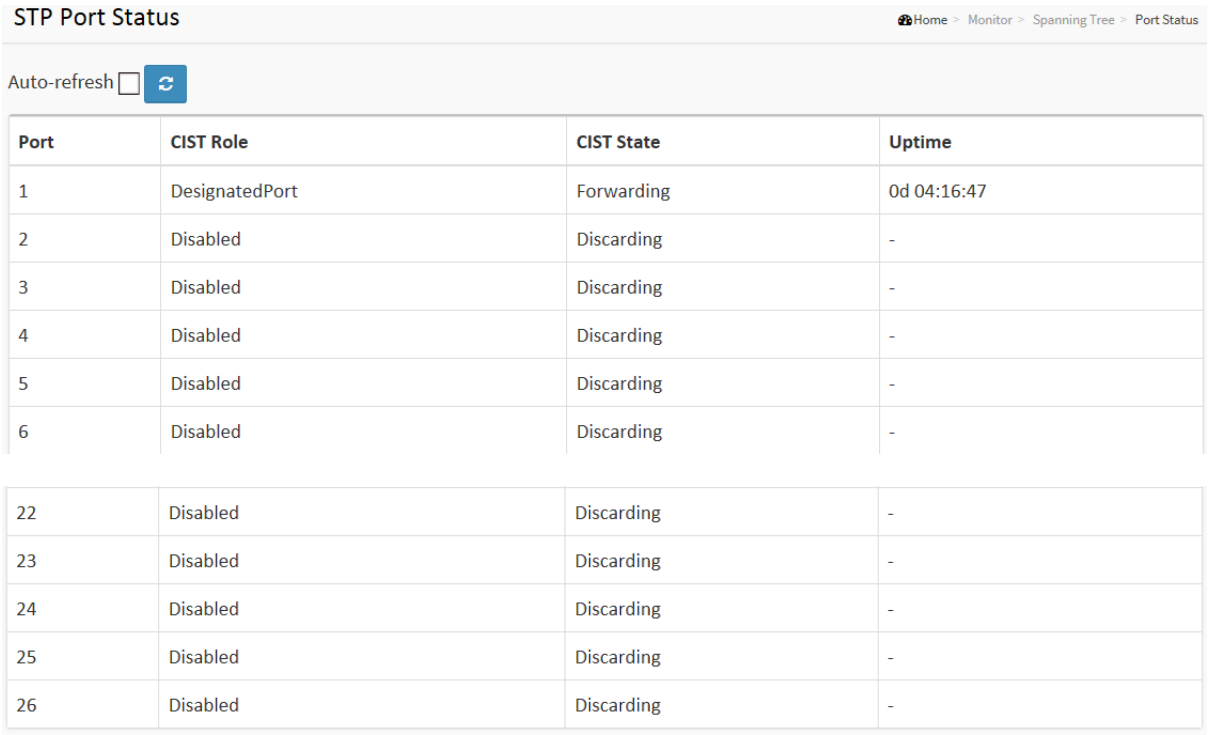


Fig: The STP Port status

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, Backup Port, RootPort, DesignatedPort Disabled.
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.

Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port Statistics

The Section provides you to ask switch to display the STP Statistics detail counters of bridge ports in the switch.

Information

To Display the STP Port Statistic information in the web interface:

1. Click **Monitor** > **Spanning Tree** > **STP Port Status**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the STP Port statistics or clear all information when you click **Clear**.

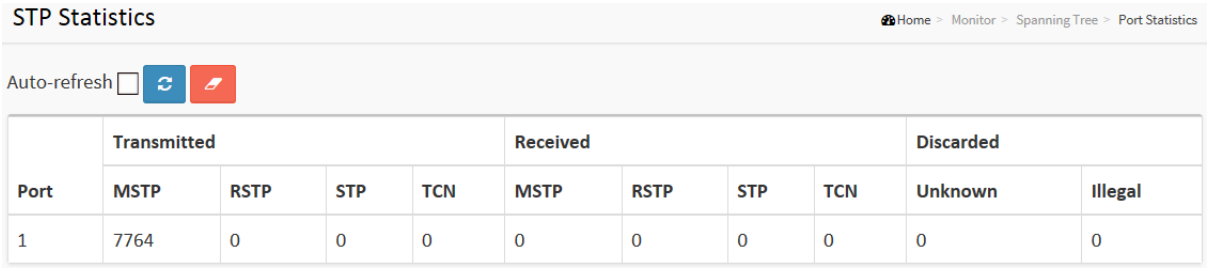


Fig: The STP Statistics

Parameter	Description
Port	The switch port number of the logical STP port.
MSTP	The number of MSTP Configuration BPDU's received/transmitted on the port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

	Clear: Clears the counters for the selected port. **Refresh:** Click to refresh the page.

MVR

Statistics

The section describes the switch will display the MVR detail Statistics after you had configured MVR on the switch. It provides the detail MVR Statistics Information

Information

To Display the MVR Information in the web interface:

1. Click **Monitor** > **MVR** > **Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.

Click **Refresh** to refresh the MVR VLAN statistics or clear all information when you click **Clear**

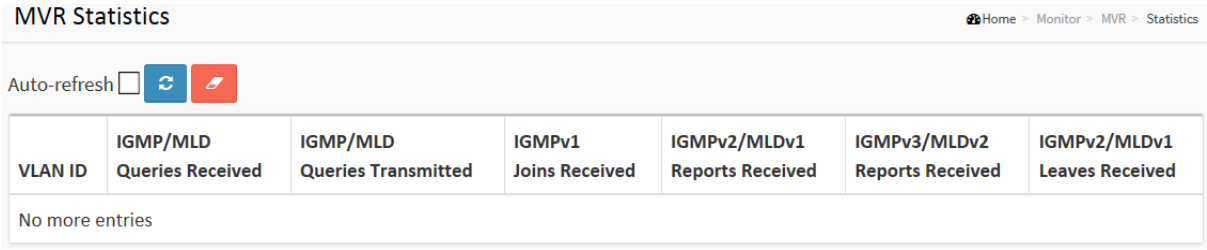


Fig: The MVR Statistics Information

Parameter	Description
VLAN ID	The Multicast VLAN ID.
IGMP/MLD Queries Received	The number of Received Queries for IGMP and MLD, respectively.
IGMP/MLD Queries Transmitted	The number of Transmitted Queries for IGMP and MLD, respectively.
IGMPv1 Joins Received	The number of Received IGMPv1 Join's.
IGMPv2/MLDv1 Reports Received	The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.
I IGMPv3/MLDv1 Reports Received	The number of Received IGMPv1 Join's and MLDv2 Report's, respectively.
IGMPv2/MLDv1	The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

Leave's Received	
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page.

MVR Channels Group

The section displays the MVR Groups detail information on the switch. Entries in the MVR Group Table are shown on this page. The MVR Group Table is sorted first by VLAN ID, and then by group.

Information

To Display the MVR Groups Information in the web interface:

1. Click **Monitor** > **MVR** > **Groups Information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the MVR Groups statistics or clear all information when you click **Clear**

Fig: The MVR Groups Information

Navigating the MVR Channels (Groups) Information Table

Each page shows up to 99 entries from the MVR Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the button will update the displayed table starting from that or the closest next MVR Channels (Groups) 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.

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

Parameter	Description

VLAN ID	VLAN ID of the group.
Groups	Group ID of the group displayed.
Port Members	Ports under this group.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>> :** Updates the system log entry to the next available entry ID

MVR SFM Information

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

Information

To Display the MVR SFM Information in the web interface:

1. Click **Monitor** > **MVR** > **MVR SFM Information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the MVR Groups statistics or clear all information when you click **Clear**
4. Click **<<** or **>>** to move to previous or next entry.

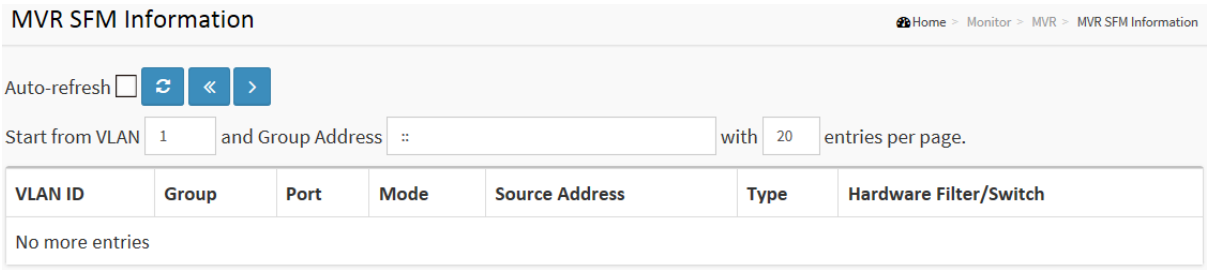


Fig: The MVR SFM Information

Navigating the MVR SFM Information Table

Each page shows up to 99 entries from the MVR SFM Information Table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MVR SFM 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.

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

Parameter	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128. When there is no any source filtering address, the text "None" is shown in the Source Address field.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>> :** Updates the system log entry to the next available entry ID

IPMC

IGMP Snooping

Status

The Section displays the IGMP Snooping detail status.

Information

To Display the IGMP Snooping Information in the web interface:

1. Click **Monitor** > **IPMC** > **IGMP Snooping** > **Status**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the IGMP Snooping statistics or clear all information when you click **Clear**

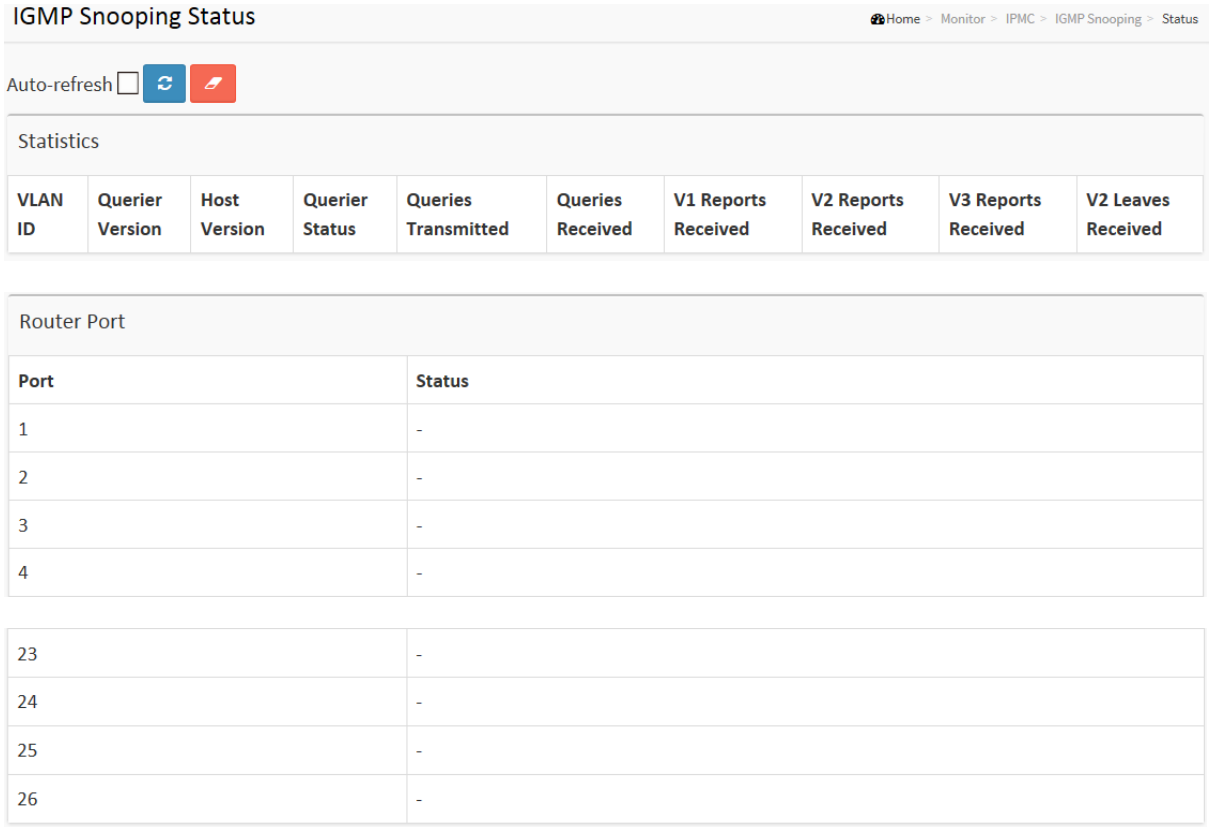


Fig: The IGMP Snooping Status.

Parameter	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is ACTIVE or IDLE. DISABLE denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page.

Group Information

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

Information

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

1. Click **Monitor** > **IPMC > IGMP Snooping** > **Group Information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the IGMP Snooping Group statistics or clear all information when you click **Clear**

Fig: The IGMP Snooping Groups Information.

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the button will update the displayed table starting from that or the closest next IGMP Group 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.

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

Parameter	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port members	Ports under this group.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>> :** Updates the system log entry to the next available entry ID

IPv4 SFM information

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

Information

To Display the IPv4 SFM IGMP Information in the web interface:

1. Click **Monitor** > **IPMC > IGMP Snooping** > **IPv4 SSM Information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the IPv4 SSM Information statistics or clear all information when you click **Clear**

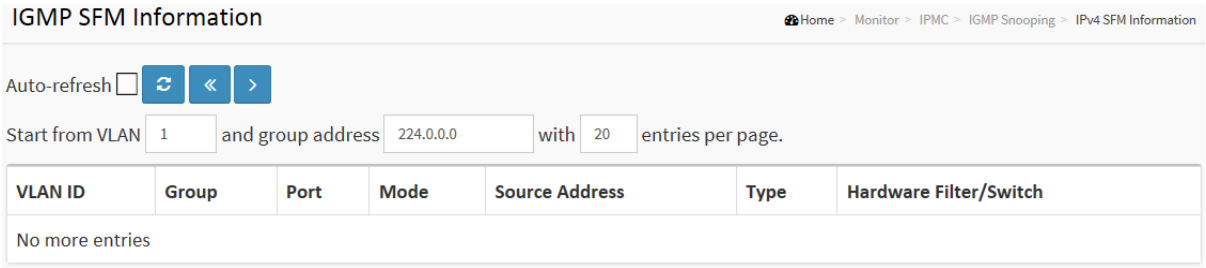


Fig: The IPv4 SFM Information.

Navigating the IGMP SFM Information Table

Each page shows up to 99 entries from the IGMP SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next IGMP SFM 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.

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

IGMP SFM Information Table Columns

Parameter	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>>:** Updates the system log entry to the next available entry ID

MLD Snooping

Status

The section displays the MLD Snooping Status and detail information. It will help you to find out the detail information of MLD Snooping status.

Information

To Display the IPv4 SFM IGMP Information in the web interface:

1. Click **Monitor** > **IPMC > MLD Snooping** > **Status**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the MLD Snooping Information statistics or clear all information when you click **Clear**

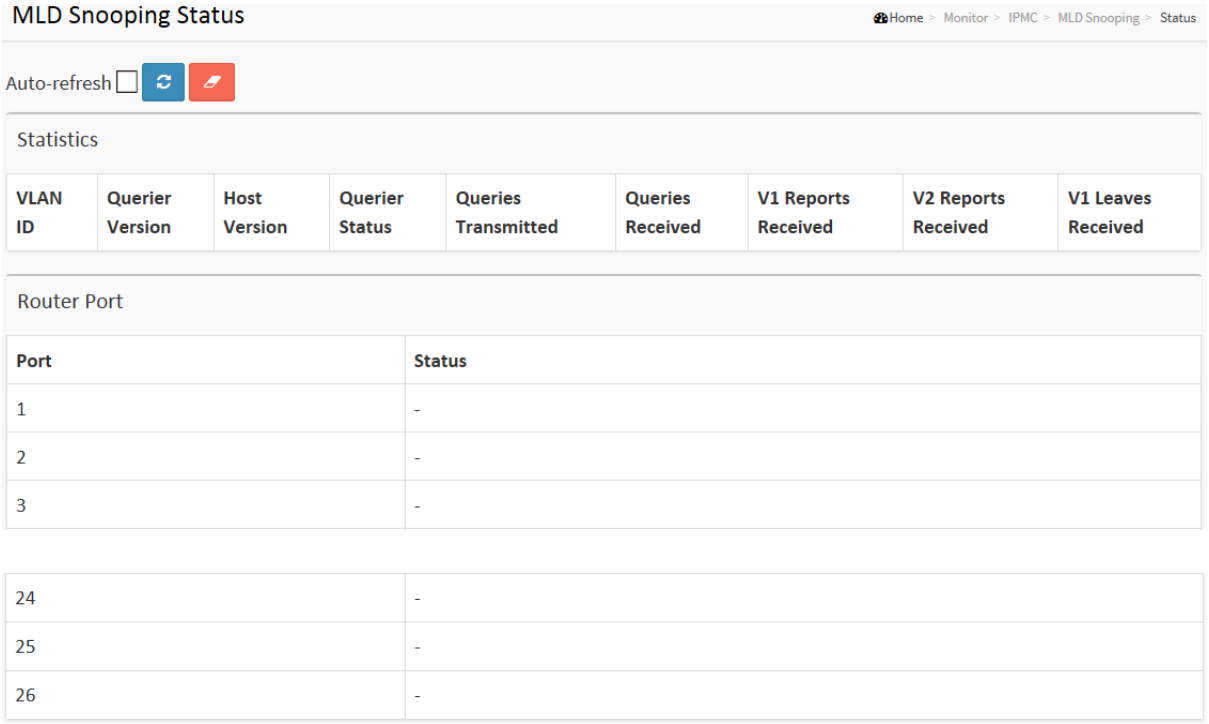


Fig: The MLD Snooping Status

Parameter	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Show the Querier status is ACTIVE or IDLE. DISABLE denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V1 leaves Received	The number of Received V1 Leaves.
Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page.

Group Information

The section the MLD Snooping Groups Information. The Start from VLAN, and group input fields allow the user to select the starting point in the MLD Group Table

Information

To Display the MLD Group Snooping Information in the web interface:

1. Click **Monitor** > **IPMC > MLD Snooping** > **Group information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the MLD Groups Snooping Information statistics or clear all information when you click **Clear**

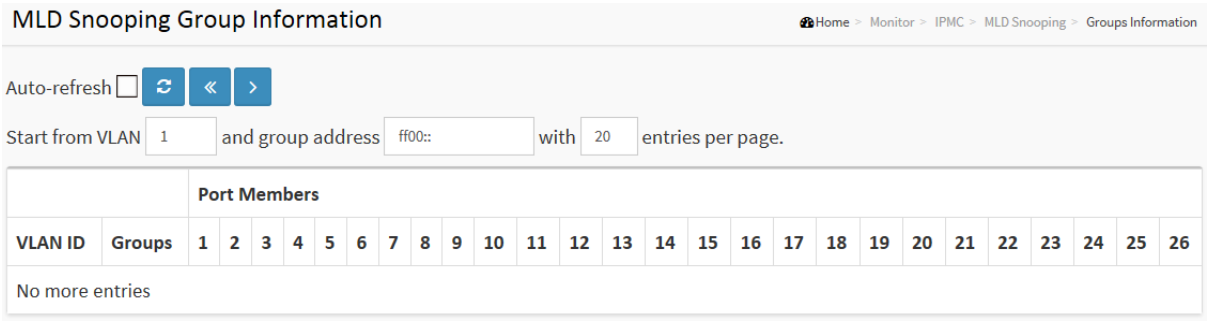


Fig: The MLD Snooping Group Information

Navigating the MLD Group Table

Each page shows 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 will show the first 20 entries from the beginning of the MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the button will update the displayed table starting from that or the closest next MLD Group 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.

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

Parameter	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>> :** Updates the system log entry to the next available entry ID

IPv6 SFM Information

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

Information

To Display the IPv6 SFM information in the web interface:

1. Click **Monitor** > **IPMC > MLD Snooping** > **IPv6 SFM Information**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the IPv6 SFM Information statistics or clear all information when you click **Clear**
4. Click **<<** or **>>** to move to previous or next entry.

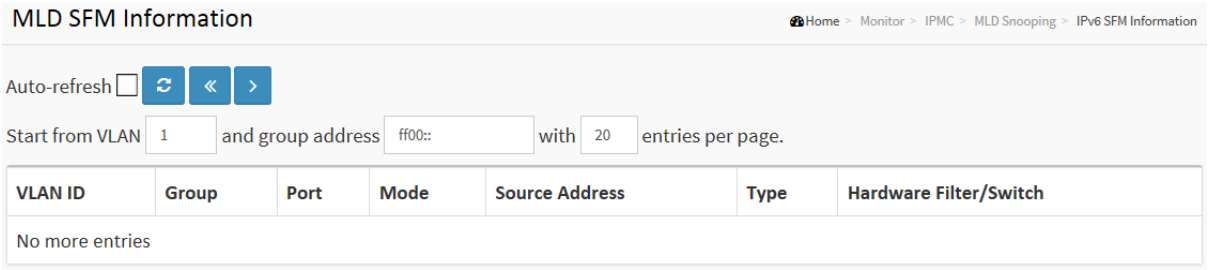


Fig: The IPv6 SFM Information

Navigating the MLD SFM Information Table

Each page shows up to 99 entries from the MLD SFM Information table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the button will update the displayed table starting from that or the closest next MLD SFM 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.

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

Parameter	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, system limits the total number of IP source addresses for filtering to be 128.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>> :** Updates the system log entry to the next available entry ID

LLDP

Neighbors

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

Information

To Display the LLDP information in the web interface:

1. Click **Monitor** > **LLDP > Neighbors**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the LLDP Neighbor Information statistics or clear all information when you click **Clear**

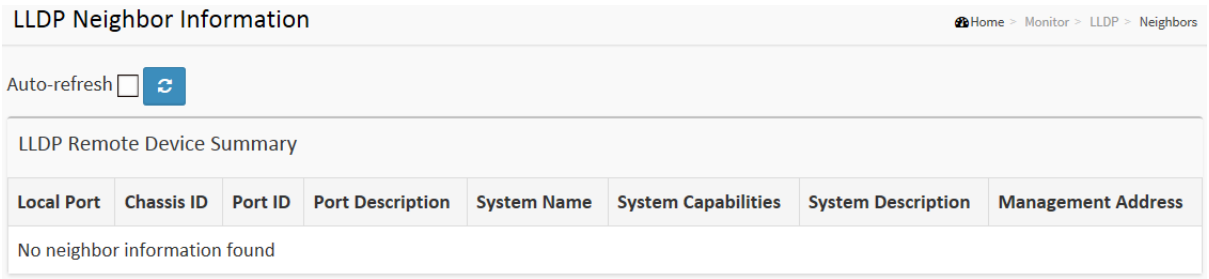


Fig: The LLDP Neighbors information

NOTE: If your network does not have any LLDP supported devices then the table will show 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.
Port ID	The Remote Port ID is the identification of the neighbor port.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater

	3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
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.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

LLDP-MED Neighbor

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

Information

To Display the LLDP-MED Neighbor information in the web interface:

1. Click **Monitor** > **LLDP > LLDP-MED Neighbor**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the LLDP-MED Neighbor Information statistics or clear all information when you click **Clear**

Fig: The LLDP-MED Neighbors information

NOTE: If your network does not have any LLDP-MED Neighbor supported devices then the table will show No LLDP-MED neighbor information found.

Parameter	Description
Port	The port on which the LLDP frame was received.
Device Type	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. **LLDP-MED Network Connectivity Device Definition** LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point

	5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. **LLDP-MED Endpoint Device Definition :** LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I). **LLDP-MED Generic Endpoint (Class I) :** The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management. **LLDP-MED Media Endpoint (Class II) :** The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery. **LLDP-MED Communication Endpoint (Class III) :** The LLDP-MED Communication Endpoint (Class III) definition is applicable to all

	endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support and inventory management.
LLDP-MED Capabilities	LLDP-MED Capabilities describes the neighborhood unit's LLDP-MED capabilities. The possible capabilities are: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI – PSE 5. Extended Power via MDI – PD 6. Inventory 7. Reserved
Application Type	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below. 1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications. 2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media. 3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services. 4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. 5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. 6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio

	services. 7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type. 8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.
Policy	Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown Unknown: The network policy for the specified application type is currently unknown. Defined: The network policy is defined.
TAG	TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged. Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. Tagged: The device is using the IEEE 802.1Q tagged frame format.
VLAN ID	VLAN ID is the VLAN identifier (VID) for the port as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress port is used instead.
Priority	Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).
DSCP	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Auto Negotiation	Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
Auto-Negotiation Status	Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.
Auto-Negotiation	Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Capabilities	
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

PoE

This page allows the user to inspect the current status for all PoE ports. The section show all port Power Over Ethernet Status.

Information

To Display the PoE LLDP information in the web interface:

1. Click **Monitor** > **LLDP > PoE**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the LLDP-PoE Information statistics or clear all information when you click **Clear**

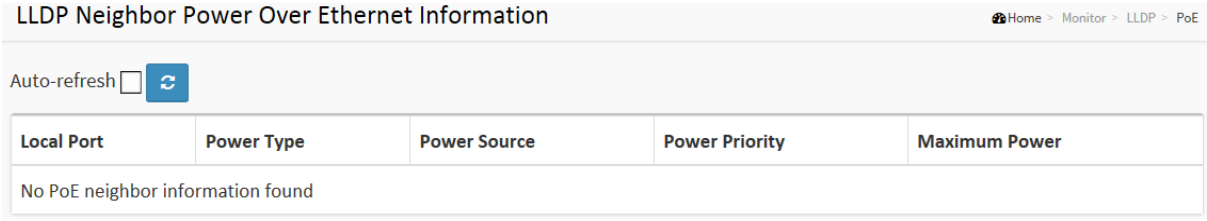


Fig: The LLDP PoE Neighbors EEE information

Parameter	Description
Local Port	The port for this switch on which the LLDP frame was received.
Power Type	The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as "Reserved".
Power Source	The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as "Unknown" If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as "Unknown"

Power Priority	Power Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's port that is sourcing the power. There are three levels of power priority. The three levels are: Critical, High and Low. If the power priority is unknown it is indicated as Unknown
Maximum Power	The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

EEE

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

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

Information

To Display the EEE information in the web interface:

1. Click **Monitor** > **LLDP > EEE**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the LLDP-EEE Information statistics or clear all information when you click **Clear**

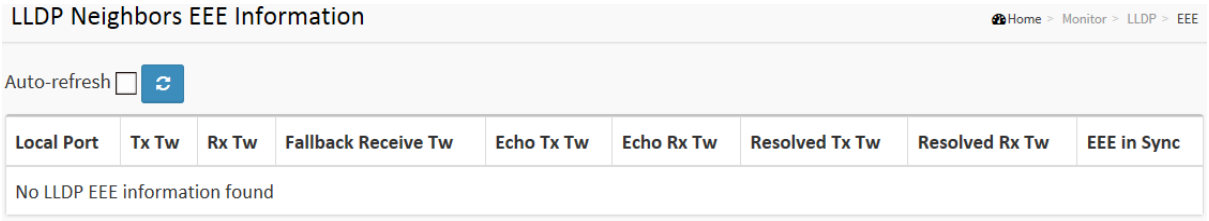


Fig: The LLDP Neighbors EEE information

NOTE: If your network does not have any LLDP-EEE supported devices then the table will show No LLDP-EEE information found.

Parameter	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Tw	The link partner's maximum time that transmit path can hold off sending data after reassertion of LPI.
Rx Tw	The link partner's time that receiver would like the transmitter to hold off to allow time for the receiver to wake from sleep.
Fallback Receive Tw	The link partner's fall back receive Tw. 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.
Echo Tx Tw	The link partner's Echo Tx Tw value. The respective echo values shall be defined as the local link partner's 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 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 partner 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 partner The resolved value that is the actual "tx wakeup time" used for this link (based on EEE information exchanged via LLDP).
EEE in Sync	Shows whether the switch and the link partner have agreed on wake times. Red - Switch and link partner have not agreed on wakeup times. Green - Switch and link partner have agreed on wakeup times.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Port Statistics

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

Information

To Display the LDAP Port information in the web interface:

1. Click **Monitor** > **LLDP > Port Statistics**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the LLDP Port Information statistics or clear all information when you click **Clear**

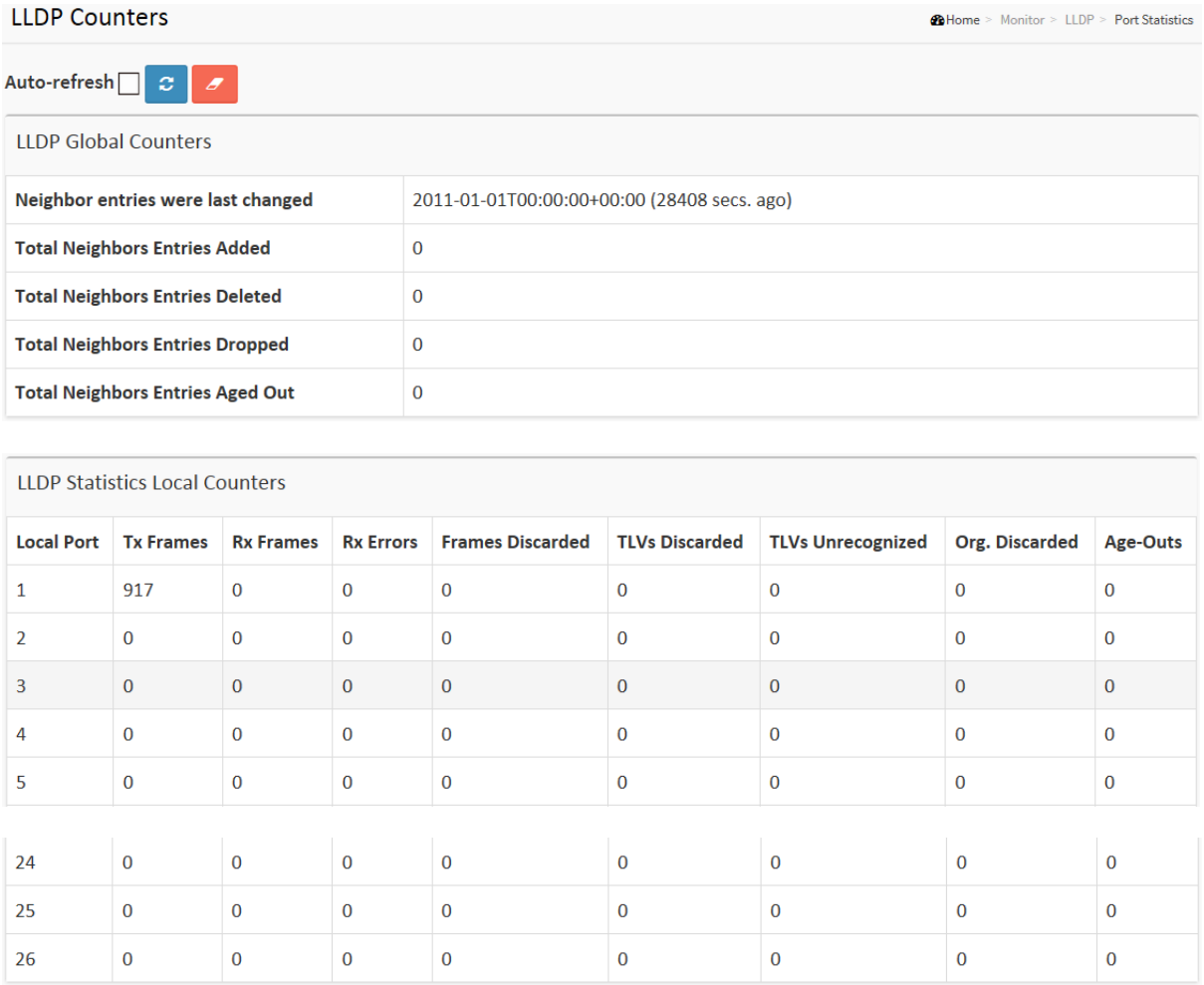


Fig: The LLDP Port Statistics information

Global Counters

Parameter	Description
Neighbor entries were last changed at	It also shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to the entry table being full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

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

Parameter	Description
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.

Org Discarded	The number of organizationally received TLVs.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page.

PoE Statistics

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

Information

To Display the PoE Statistics information in the web interface:

1. Click **Monitor** > **PoE**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the PoE statistics or clear all information when you click **Clear**

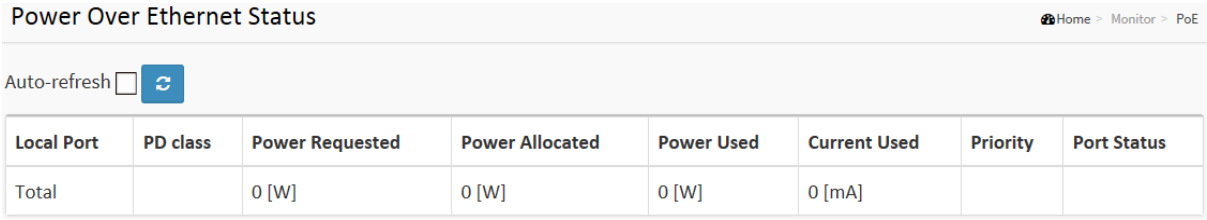


Fig: The PoE Statistics

Parameter	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five Classes are defined: Class 0: Max. power 15.4 W Class 1: Max. power 4.0 W Class 2: Max. power 7.0 W Class 3: Max. power 15.4 W Class 4: Max. power 30.0 W
Power Requested	The Power Requested shows the requested amount of power the PD wants to be reserved.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using.

Priority	The Priority shows the port's priority configured by the user.
Port Status	The Port Status shows the port's status. The status can be one of the following values: PoE not available - No PoE chip found - PoE not supported for the port. PoE turned OFF - PoE disabled: PoE is disabled by user. PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down. No PD detected - No PD detected for the port. PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down. PoE turned OFF - PD is off. Invalid PD - PD detected, but is not working correctly.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Information

To Display the MAC Table information in the web interface:

1. Click **Monitor** > **MAC Table**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the PoE statistics or clear all information when you click **Clear**

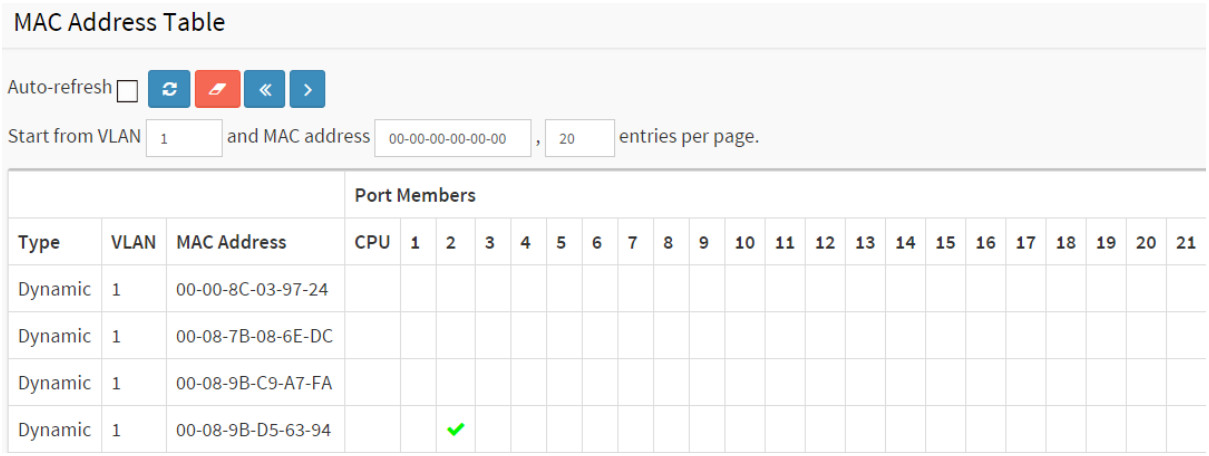


Fig: The MAC Address Table

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

MAC Table Columns

Parameter	Description
Type	Indicates whether the entry is a static or a dynamic entry.
VLAN	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	The ports that are members of the entry.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Clear:** Clears the counters for the selected port. **Refresh:** Click to refresh the page. **|<<:** Updates the system log entries to the first available entry ID **>> :** Updates the system log entry to the next available entry ID

VLANs

VLAN Membership

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

Information

To Display the VLAN information in the web interface:

1. Click **Monitor** > **VLANs > Membership**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the VLAN Membership statistics or clear all information when you click **Clear**

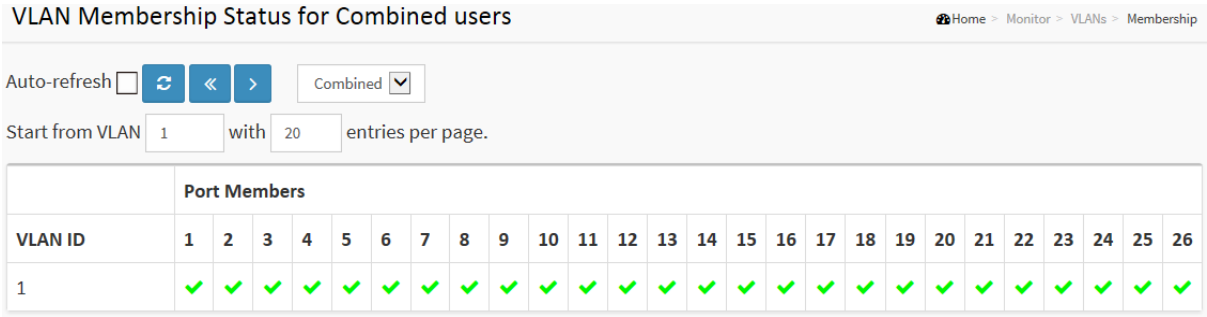


Fig: VLAN Membership Status

Navigating the VLAN Monitor page

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next VLAN Table match. The >> will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<<button to start over

Parameter	Description
VLAN User	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: **Admin**: These are referred to as static. **NAS :** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. **GVRP :** GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically **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.
VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, an image ✓ will be displayed. If a port is included in a Forbidden port list, an image ✗ will be displayed. If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then conflict port will be displayed as ✗.
VLAN Membership	The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User. When all VLAN Users are selected, it shall show this information for all the VLAN Users, and this is by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

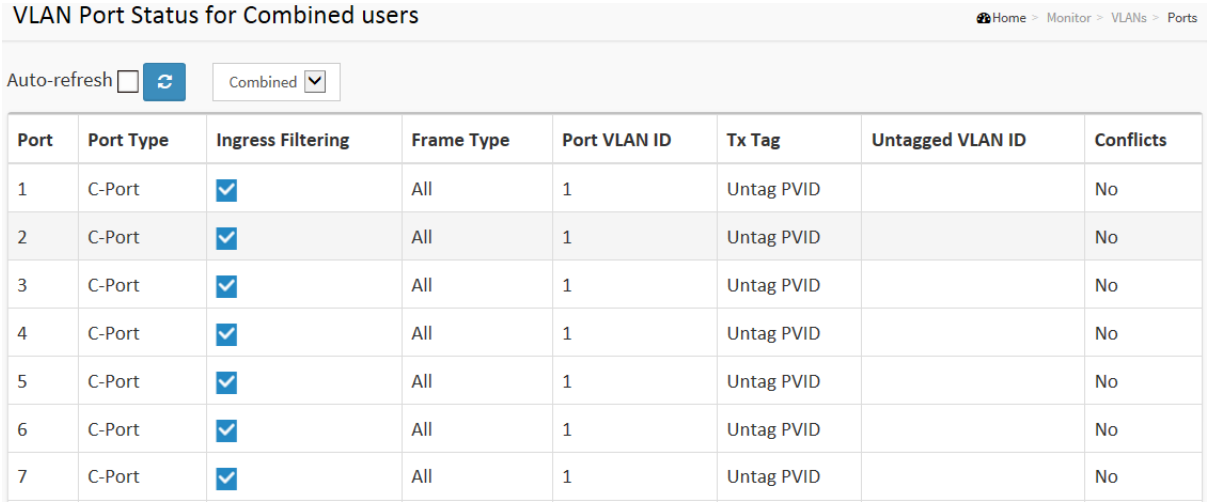
VLAN Ports

This section provides the VLAN Port Status Information

Information

To Display the VLAN information in the web interface:

1. Click **Monitor** > **VLANs > Ports**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the VLAN Port statistics or clear all information when you click **Clear**



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag PVID		No
2	C-Port	☑	All	1	Untag PVID		No
3	C-Port	☑	All	1	Untag PVID		No
4	C-Port	☑	All	1	Untag PVID		No
5	C-Port	☑	All	1	Untag PVID		No
6	C-Port	☑	All	1	Untag PVID		No
7	C-Port	☑	All	1	Untag PVID		No

Fig: The VLAN Port Status for Static user

Parameter	Description
VLAN User	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: **Admin**: These are referred to as static. **NAS:** NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. **GVRP :** GVRP, a single switch is manually configured with all the desired VLANs for the network, and all other switches on the network learn those VLANs dynamically **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.
Port	The logical port for the settings contained in the same row.
Port Type	Shows the Port Type. Port type can be any of Unaware, C-port, S-port, Custom S-port. If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed. C-port is Customer Port. S-port is Service port. Custom S-port is S-port with Custom TPID.
Ingres Filtering	Shows the ingress filtering on a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN, the frame is discarded.
Frame Type	Shows whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Port VLAN ID	Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
Tx Tag	Shows egress filtering frame status whether tagged or untagged.
UVID	Shows UVID (untagged VLAN ID). Port's UVID determines the packet's behavior at the egress side.
Conflicts	Shows status of Conflicts whether exists or not. When a Volatile VLAN User requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: Functional Conflicts between features. Conflicts due to hardware limitation. Direct conflict between user modules
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

VCL

MAC-based VLAN

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

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

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

Information

To Display the VLAN information in the web interface:

1. Click **Monitor** > **VCL > MAC-based VLAN**
2. Specify from the Dropdown list either Static, NAS, DMS or Combined
3. If you want to auto-refresh the information tick the **Auto-refresh option**.
4. Click **Refresh** to refresh the VLAN MAC-based statistics or clear all information when you click **Clear**

Parameter	Description
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	Port members of the MAC-based VLAN entry.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Protocol-based VLAN

Protocol to Group

This page shows you the protocols to Group Name (unique for each Group) mapping entries for the switch.

Information

To Display the Protocol-based VLAN information in the web interface:

1. Click **Monitor** > **VCL > Protocol-based VLAN > Protocol to Group**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the VLAN Protocol-based statistics or clear all information when you click **Clear**

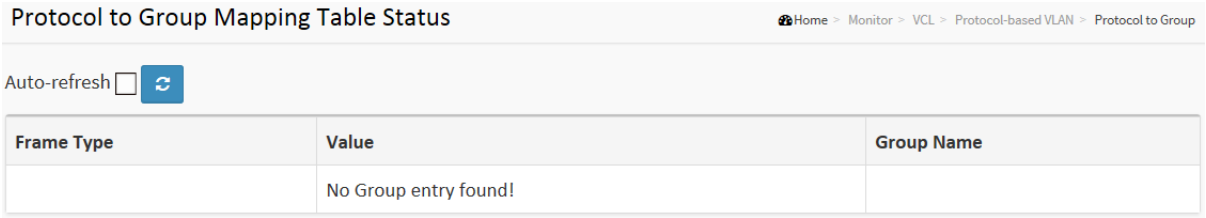


Fig: The MAC-based VLAN Membership Status

Parameter	Description
Frame Type	Frame Type can have one of the following values: 1. Ethernet 2. LLC 3. SNAP **NOTE:** On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.
Value	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below is the criteria for three different Frame Types: **1. For Ethernet:** Values in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype ranges from 0x0600-0xffff **2. For LLC:** Valid value in this case is comprised of two different sub-values.

	a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) **3. For SNAP:** Valid value in this case also is comprised of two different sub-values. a. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. b. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then valid value of PID will be any value from 0x0000 to 0xffff.
Group Name	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers(0-9). **NOTE:** Special characters and underscores(_) are not allowed.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

Group to VLAN

This page shows you the configured Group Name to a VLAN for the switch.

Information

To Display the Group to VLAN information in the web interface:

1. Click **Monitor** > **VCL > Protocol-based VLAN > Group to VLAN**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the Group to VLAN statistics

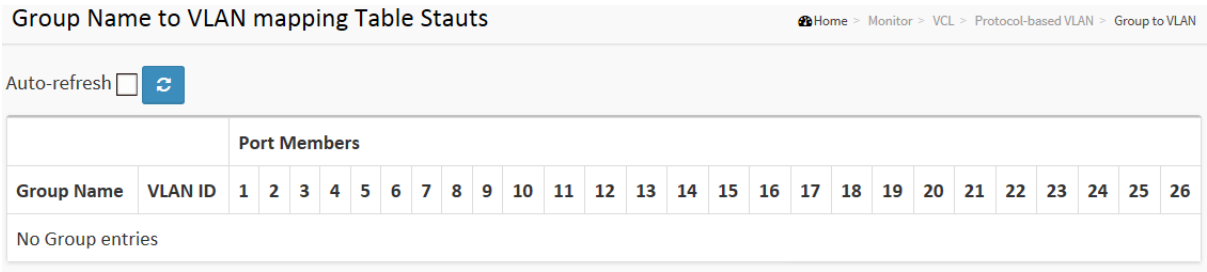


Fig: The MAC-based VLAN mapping Status

Parameter	Description
Group Name	A valid Group Name is a string at the most 16 characters which consists of a combination of alphabets (a-z or A-Z) and integers(0-9), no special characters are allowed. Whichever Group name you try map to a VLAN must be present in Protocol to Group mapping table and must not be pre-used by any other existing mapping entry on this page.
VLAN ID	Indicates the ID to which Group Name will be mapped. A valid VLAN ID ranges from 1-4095.
Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in a mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

IP Subnet-based VLAN

The page shows IP subnet-based VLAN entries. This page shows only static entries.

Information

To Display the IP Subnet-based VLAN information in the web interface:

1. Click **Monitor** > **VCL > IP Subnet-based VLAN**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the IP Subnet-based VLAN statistics

Fig: The MAC-based VLAN Membership Status

Parameter	Description
VCE ID	Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCE ID is 0, application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
Port Members	A row of check boxes for each port is displayed for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, check the box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page.

sFlow

This session shows receiver and per-port sFlow statistics

Information

To Display the IP Subnet-based VLAN information in the web interface:

1. Click **Monitor** > **sFLow**
2. If you want to auto-refresh the information tick the **Auto-refresh option**.
3. Click **Refresh** to refresh the sFlow statistics

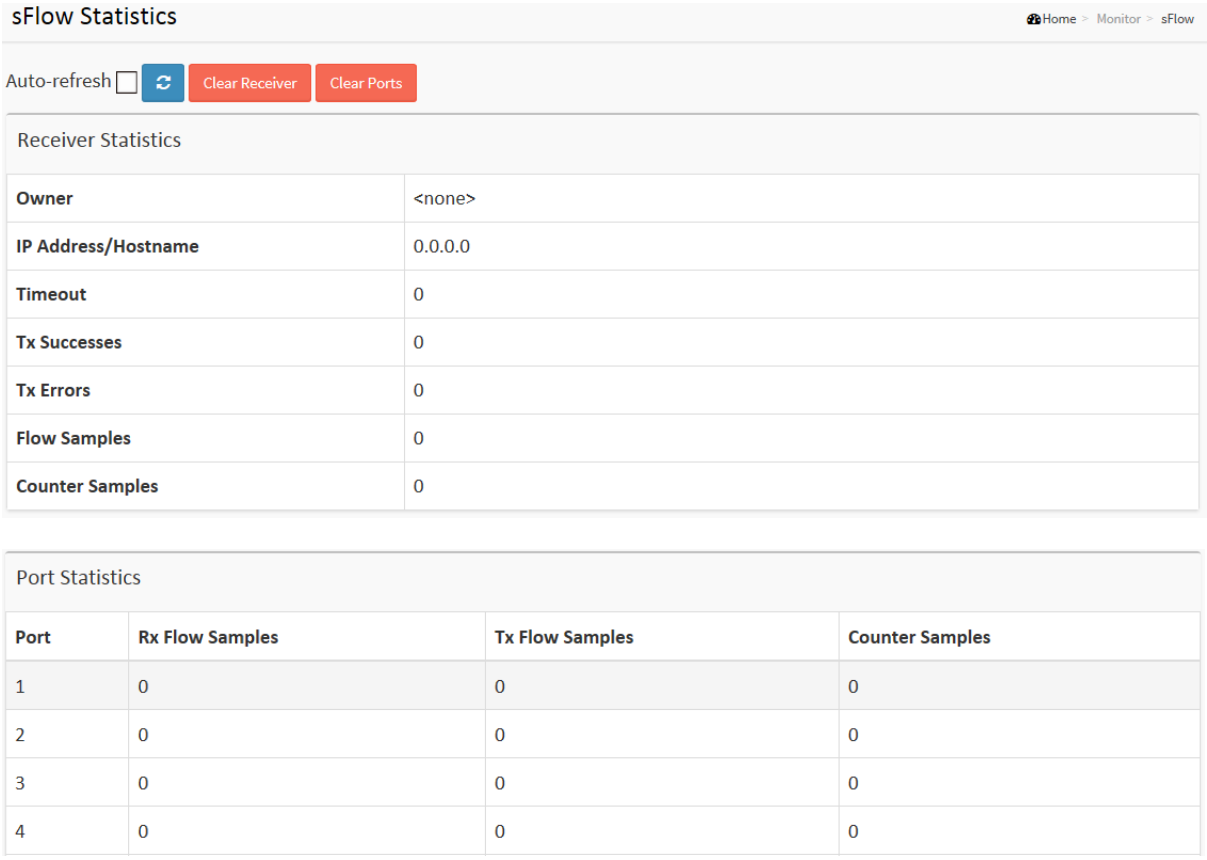


Fig: The sFlow Statistics

Parameter	Description
Owner	This field shows the current owner of the sFlow configuration. It assumes one of three values as follows: • If sFlow is currently unconfigured/unclaimed, Owner contains <none>. • If sFlow is currently configured through Web or CLI, Owner contains

	<Configured through local management>. • If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
IP Address/Hostname	The IP address or hostname of the sFlow receiver.
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released.
Tx Successes	The number of UDP datagrams successfully sent to the sFlow receiver.
Tx Errors	The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping/Ping6).
Flow Samples	The total number of flow samples sent to the sFlow receiver.
Counter Samples	The total number of counter samples sent to the sFlow receiver.

Port Statistics

Parameter	Description
Port	The port number for which the following statistics applies.
Rx and Tx Flow Samples	The number of flow samples sent to the sFlow receiver originating from this port. Here, flow samples are divided into Rx and Tx flow samples, where Rx flow samples contains the number of packets that were sampled upon reception (ingress) on the port and Tx flow samples contains the number of packets that were sampled upon transmission (egress) on the port.
Counter Samples	The total number of counter samples sent to the sFlow receiver originating from this port.
Buttons	**Auto-refresh:** Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. **Refresh:** Click to refresh the page. **Clear Receiver:** Clears the sFlow receiver counters. **Clear Ports:** Clears the per-port counters.

Diagnostics

This section provides a set of basic system diagnosis. It lets users know whether the system is healthy or needs to be fixed. Users can also check network connectivity issues with the Ping command. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

Ping

This section is used to test network connectivity issues using the Ping command.

Information

To test network connectivity issues using the Ping command.

1. Click **Diagnostics > Ping**.
2. Enter the **IP Address** of the device you are trying to communicate with.
3. Set the ping **Data Length**, **Ping Count** and **Ping Interval**.
4. Click the **Start** button to commence the test.

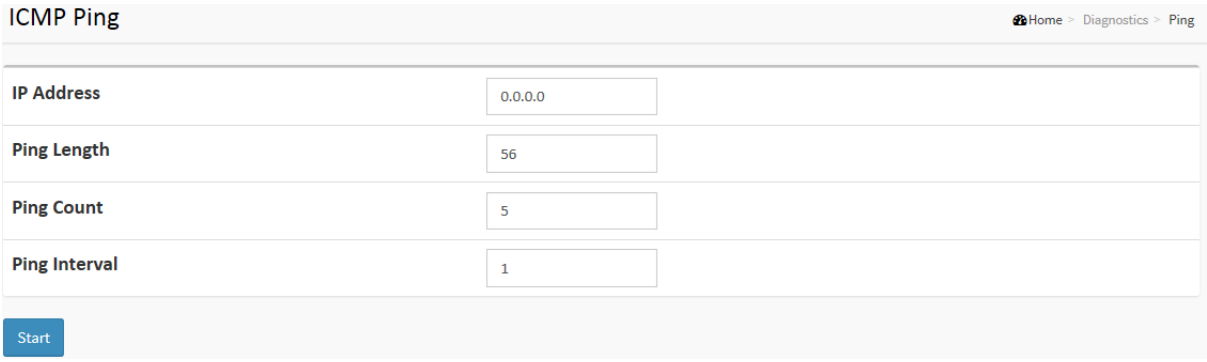


Fig: The ICMP Ping Statistics

Parameter	Description
IP Address	To set the IP Address of device what you want to ping it.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet

(Only for IPv6)	goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.
Start	Click the “Start” button then the switch will start to ping the device using ICMP packet size what set on the switch. After you press , 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs. PING6 server ::10.10.132.20 64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms 64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms Sent 5 packets, received 5 OK, 0 bad

Ping6

This section is used to test network connectivity issues using the Ping IPv6 command.

Information

To test network connectivity issues using the Ping command for IPv6.

1. Click **Diagnostics > Ping6**.
2. Enter the **IP Address** of the device you are trying to communicate with.
3. Set the ping **Data Length**, **Ping Count** and **Ping Interval** and **Egress Interface**.
4. Click the **Start** button to commence the test.

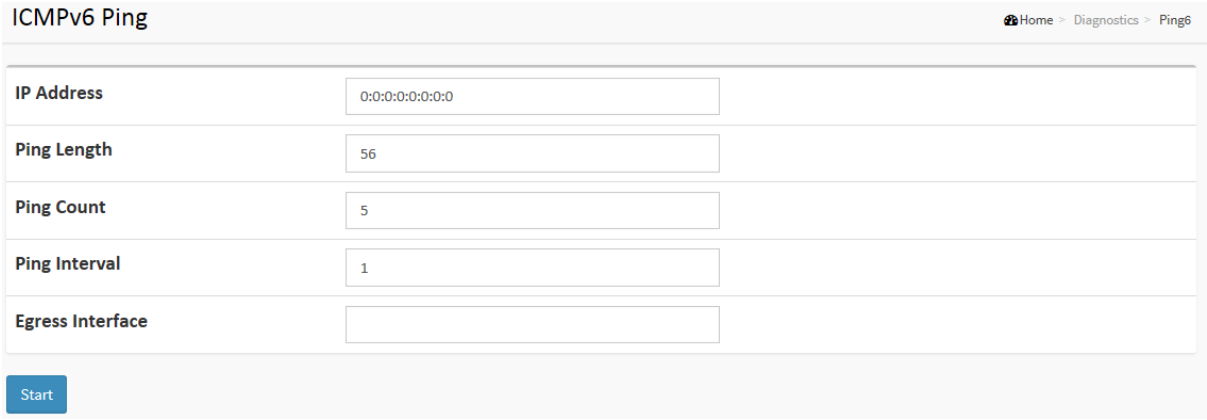


Fig: The ICMPv6 Ping Statistics

Parameter	Description
IP Address	To set the IP Address of device what you want to ping with IPv6
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.
Egress Interface (only for IPv6)	The VLAN ID (VID) of the specific egress IPv6 interface which ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid.

	When the egress interface is not given, PING6 finds the best match interface for destination. Do not specify egress interface for loopback address. Do specify egress interface for link-local or multicast address.
Start	Click the “Start” button then the switch will start to ping the device using ICMPv6 packet size what set on the switch. After you press , 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

VeriPhy

This section is used for running the VeriPHY Cable Diagnostics. Press to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY is only accurate for cables of length 7 -140 meters.10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

Information

To perform a VeriPHY Cable Diagnostic test via the Web Interface:

1. Click **Diagnostics > VeriPHY**.
2. Specify the port in which you wish to perform a test.
3. Click Start to perform the test.

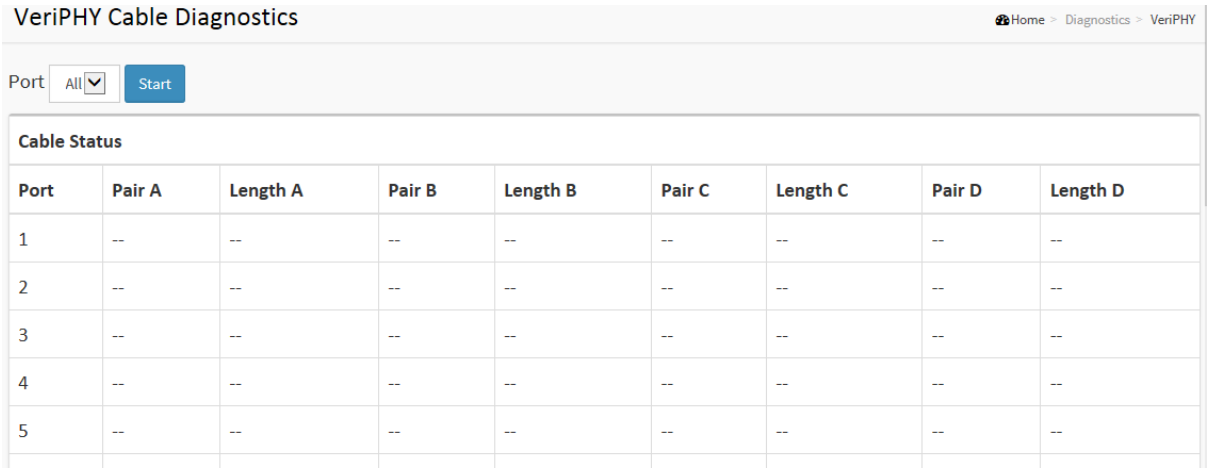


Fig: The VeriPHY Statistics

Parameter	Description
Port	The Port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	**Port**: Port number. **Pair**: The status of the cable pair. **Length**: The length (in meters) of the cable pair.

Traceroute

This page allows you to issue ICMP, TCP, or UDP packets to diagnose network connectivity issues.

Information

To test network pathing via the traceroute command in the web interface

1. Click **Diagnostics > Traceroute**
2. Specify the **Protocol** to use for the Traceroute
3. Specify Traceroute **IP Address**.
4. Specify **Wait time**, **Max TTL** and **Probe Count**.
5. Click **Start**.

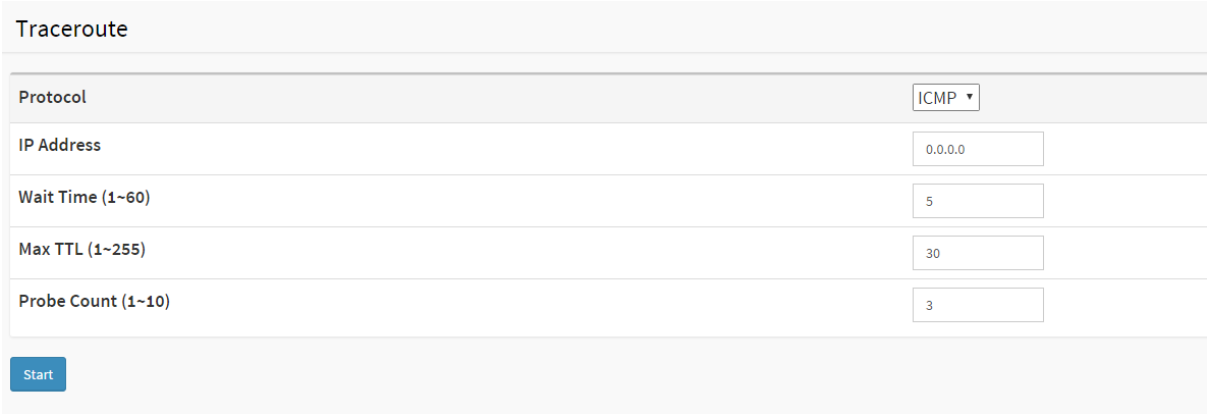


Fig: The Traceroute Command Parameters

Parameter	Description
Protocol	The protocol(ICMP, UDP, TCP) packets to send.
IP Address	The destination IP Address.
Wait Time	Set the time (in seconds) to wait for a response to a probe (default 5.0 sec). Values range from 1 to 60. The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Max TTL	Specifies the maximum number of hops (max time-to-live value) traceroute will probe. Values range from 1 to 255. The default is 30.
Probe Count	Sets the number of probe packets per hop. Values range from 1 to 10. The

	default is 3.

Maintenance

This chapter describes all of the switch Maintenance configuration tasks to enhance the performance of the switch, including Restart Device, Firmware upgrade, Save/Restore, Import/Export, and Diagnostics.

Restart Device

This section explains how to restart the device.

Information

To restart the switch via the Web Interface

1. Click **Maintenance > Restart Device**
2. Click **Restart Device.**
3. Select **Yes** to Restart

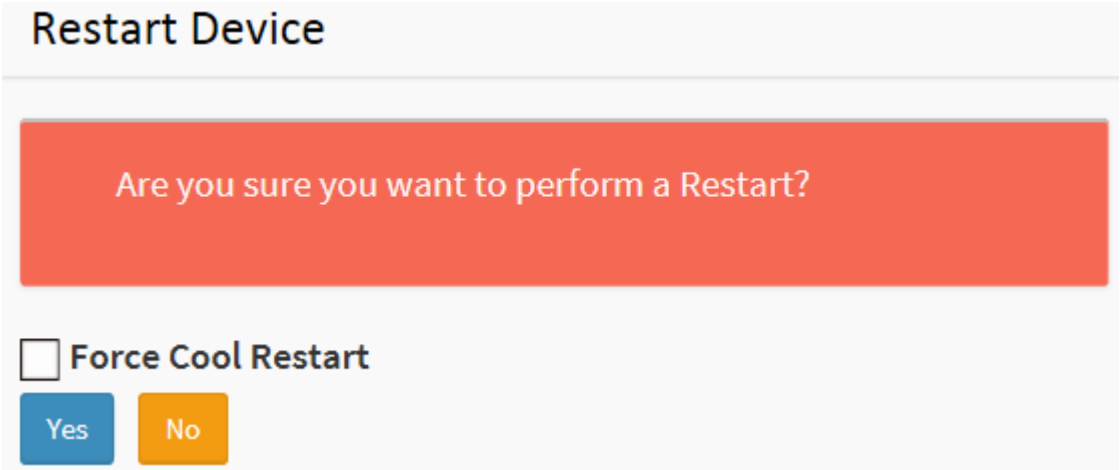


Fig: Restart Device Screen

Parameter	Description
Restart Device	You can restart the switch on this page. After restart, the switch will boot normally.
Buttons	**Yes** – Click to "Yes" then the device will restart.

	No- Click to undo any restart action.

Factory Defaults

This section is used to reset the switch back to its factory default settings.

Information

To perform a Factory Default of the Configuration in the web interface:

1. Click **Maintenance > Factory Defaults**
2. Click **Factory Defaults**
3. Select **Yes** to Factory Default the switch configuration

Parameter	Description
Buttons	**Yes** – Click to "Yes" button to reset the configuration to Factory Defaults. **No** - Click to return to the Port State page without resetting the configuration.

Firmware

This section describes how to upgrade Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

Firmware Upgrade

This page is where you upload the firmware for the AS Series Switch.

Information

To perform a Factory Default of the Configuration in the web interface:

1. Click **Maintenance > Firmware > Firmware Upgrade**
2. Click **Choose File** then navigate to the firmware location on your computer
3. Select **Upload**

Fig: The Firmware Upload Section

Parameter	Description
Choose File	Click the Choose File button to select the firmware file to upload. **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.
Upload	Uploads the firmware file you have selected.

Firmware Selection

This section is used to switch between the latest uploaded firmware image and the previously uploaded firmware image. This page displays both firmware file details including the version number.

Information

To perform a Factory Default of the Configuration in the web interface:

1. Click **Maintenance > Firmware > Firmware Selection**
2. Click on the **Activate Alternate Image** button to switch to the old firmware version.

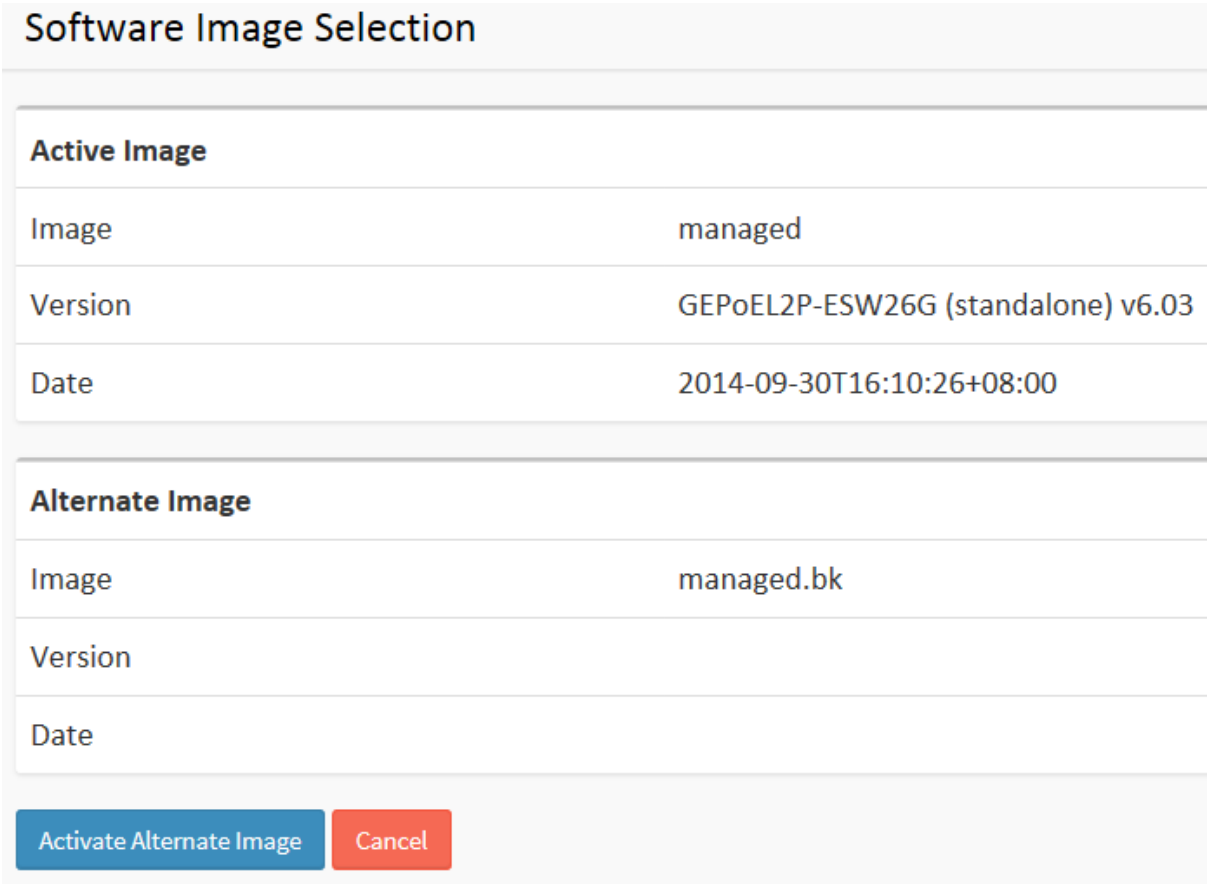


Fig: The Firmware selection

Parameter	Description
Image	The name of the firmware image. The name of primary (preferred) managed, the alternate image is named managed.bk.

Version	The version of the firmware image.
Date	The date where the firmware was produced.
Buttons	**Activate Alternate Image:** Click to use the “Activate Alternate Image”. This button may be disabled depending on system state. **Cancel:** Cancel activating the backup image. Navigates away from this page.

Configuration

This section is used to backup, restore and save the configuration files of the AS Series Switch.

Save startup-config

This section describes how to save the Switch Start configuration. Any current configuration files will be saved to start. This must be performed after configuration of the switch if you wish to retain any changed settings you have made upon a reboot. If the Start configuration is not saved after the switch has been powered off it will revert back to previous settings.

Information

To save the current configuration to startup in the web interface:

1. Click **Maintenance > Configuration > Save startup-config**
2. Select **Save Configuration**

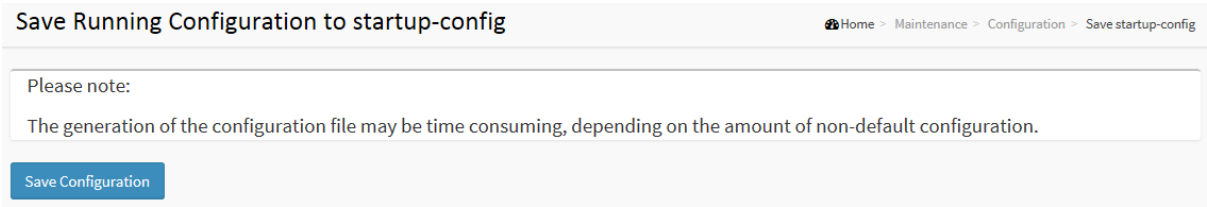


Fig: The Save Startup Configuration Screen

Parameter	Description
Buttons	**Save Configuration:** Click to save configuration, the running configuration will be written to flash memory for system boot up to load this startup configuration file.

Download

This section describes to export the Switch Configuration. Any current configuration files will be exported as text format.

Information

To download a copy of the configuration files for the switch in the web interface:

1. Click **Maintenance > Configuration > Download**
2. Select the Configuration you wish to download (**running-config/default-config/startup-config**)
3. Select **Download Configuration**

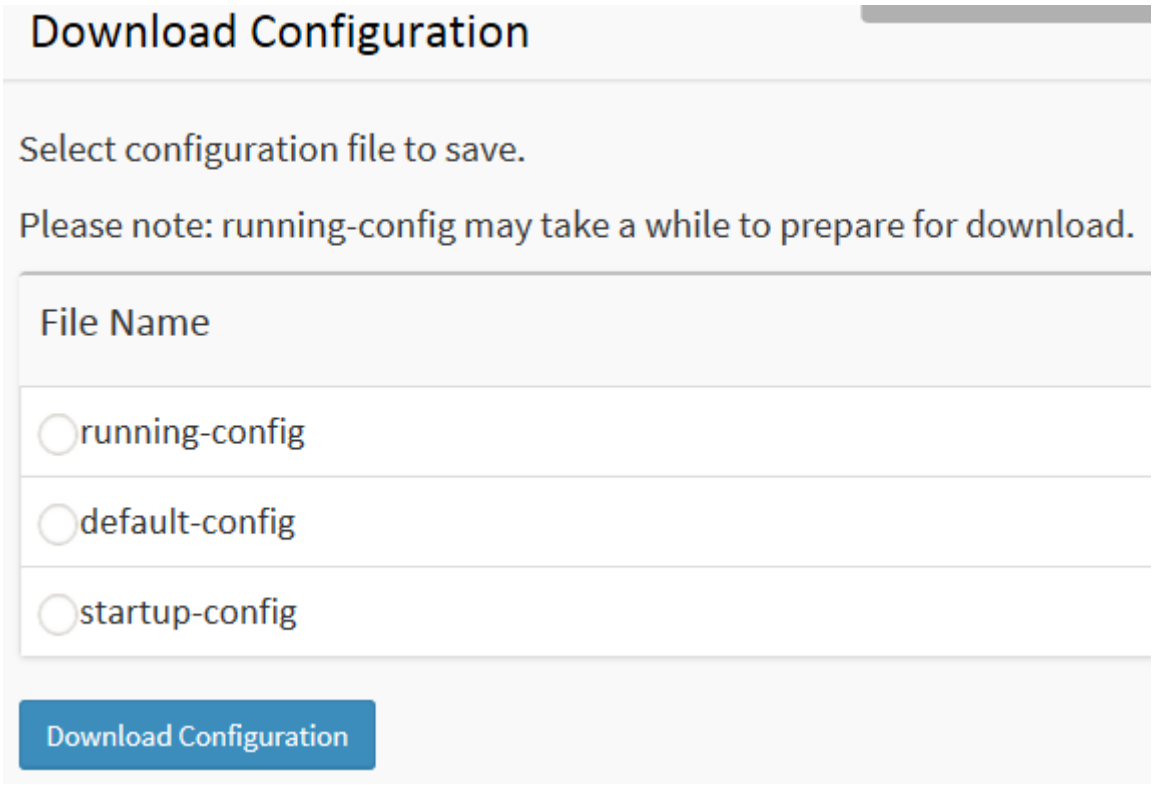


Fig: Configuration Download section

There are three system files:

running-config: A virtual file that represents the currently active configuration on the switch. This file is volatile.

startup-config: The startup configuration for the switch, read at boot time.

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

Parameter	Description
Buttons	**Download Configuration:** Click to save configuration, the running configuration will be written to flash memory for system boot up to load this startup configuration file.

Upload

This section is used to Import a saved configuration file into the switch.

Information

To Import a configuration file into the switch via the Web Interface:

1. Click **Maintenance** > **Configuration** > **Upload**.
2. Click Choose File to browse for the previously saved configuration file.
3. Select the Destination File you wish to over write, either **running-config**, **startup-config** or to **Create new file**.
4. Select If you wish to **Replace** or **Merge** the running-configuration
5. Select **Upload Configuration** to import the configuration.

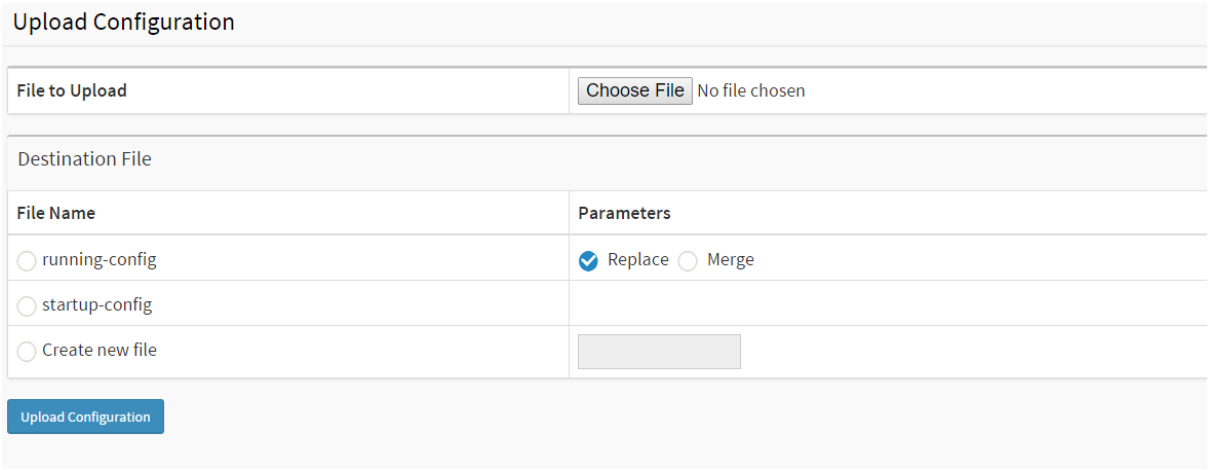


Fig: Configuration Upload Screen

Parameter	Description
File to Upload	Click the **Choose File** button to search the configuration text file and filename.
Upload Configuration	Click **Upload Configuration** to upload the file onto the switch

Activate

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

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

Information

To activate configuration in the web interface:

1. Click **Maintenance** > **Configuration** > **Activate**.
2. Select the file name you wish to activate to running-config.
3. Click **Activate Configuration**

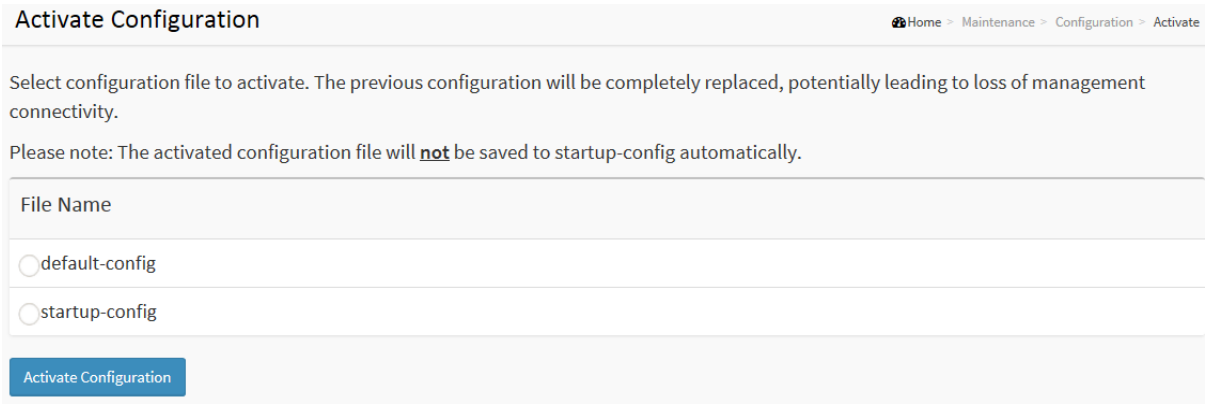


Fig: Activate Configuration Screen

There are two system files:

default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

startup-config: The startup configuration for the switch, read at boot time.

Parameter	Description
Buttons	**Activate Configuration:** Click Activate then the default-config or startup-config file will be activated and to be this switch's running configuration.

Delete

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

Information

To delete the configuration in the web interface:

1. Click **Maintenance** > **Configuration** > **Delete**.
2. Select the file you wish to delete
3. Select **Delete Configuration File**

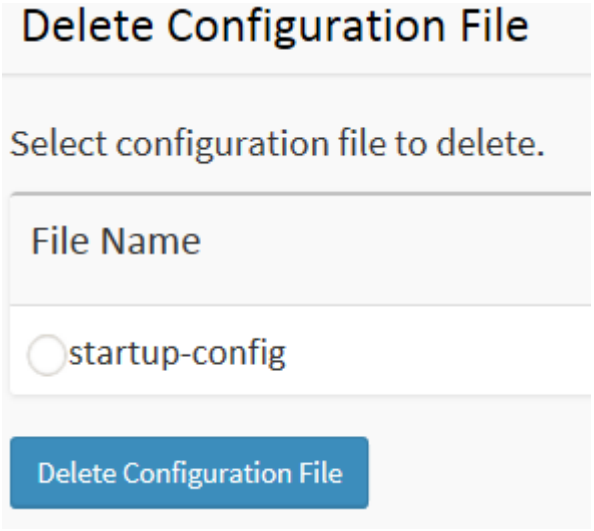


Fig: Delete Configuration screen

There is one system file:

startup-config: The startup configuration for the switch, read at boot time.

Parameter	Description
Buttons	**Delete Configuration**: Click the “Delete” button then the startup-config file will be deleted, this effectively resets the switch to default configuration.

DMS Management

Information

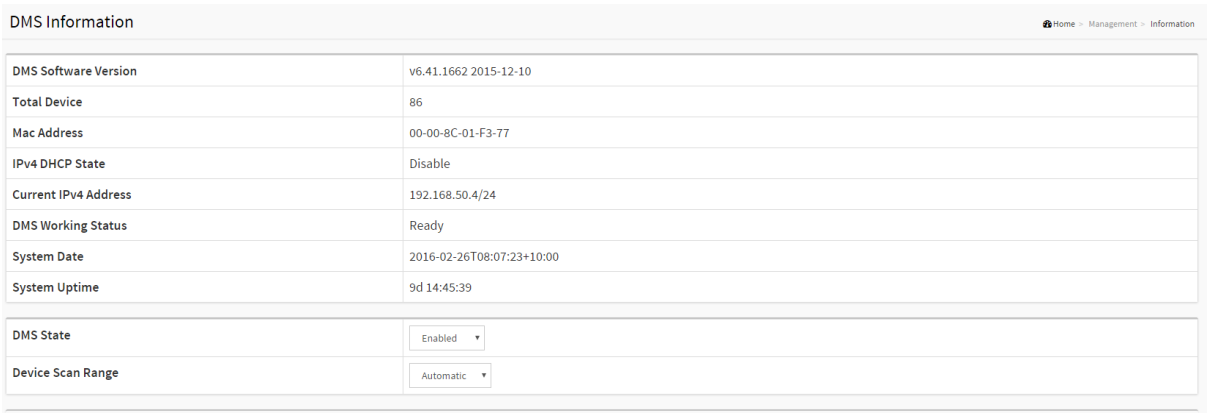
Device Management System

The Information page shows general system information for the Switch including its DMS software version, the maximum number of device can manage, MAC Address and IP Address for the Switch.

Information

To Configure DMS Information via the Web Interface

1. Click **DMS Tab** > **Management > Information**
2. To enable, Selected either **Enabled** or **Disabled** from the DMS State Dropdown menu
3. For the scanning options, select either **Automatic** or **Manual**
4. Specify the IP settings for VLAN1 If not already setup via the Configuration menu)
5. Select Enable or Disabled for the DHCP Server (If not configured already via the DHCP Configuration menu



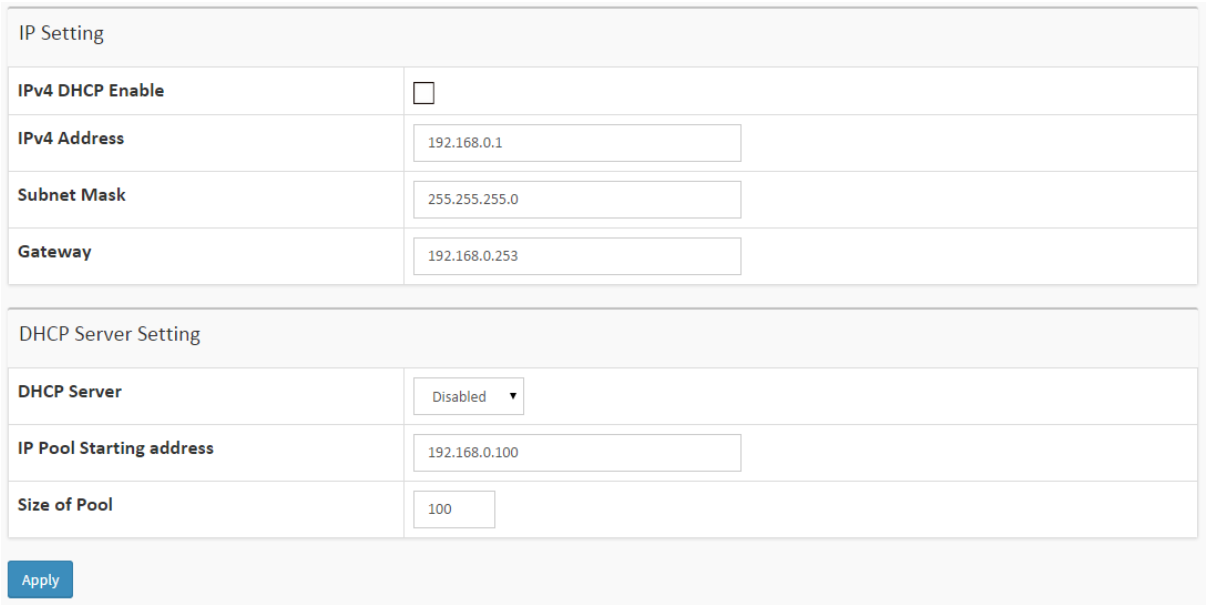


Fig: DMS Information Screen

Parameter	Description
DMS Software Version	Displays the current DMS firmware version number.
Total Device	Displays the number of devices in topology.
MAC Address	The MAC Address of this switch.
Current IP Address	The current address (IPv4). DMS use switch interface VLAN1.
DMS Working Status	Displays the Working Status of DMS
System Date	Displays the System Date and time
System Uptime	Displays the System Uptime of the switch
DMS State	Enabled or Disabled DMS.
Device Scan Range	Sets the Device Scan range, either Automatic or Manual.
IP Address	The IPv4 address of the interface VLAN1.
System Name	The IPv4 network mask of the interface VLAN1.

Device List

The DMS Device list shows all devices that have been found though DMS either via automatic or Manual Methods. It will show you details such as if the unit is online or not, the device, Model name (If applicable) as well as the Device Name, MAC Address and IP address.

Information

To Configure DMS Device List Information via the Web Interface

1. Click **DMS Tab** > **Management > Device List**
2. Click the **Edit** option to change the listed **HTTP port** of the Device
3. Click the Online/Offline Button to open the Device in the Diagnostic screen
4. Click the **Refresh** button to refresh devices in the list or **Auto-refresh** to set this automatically.

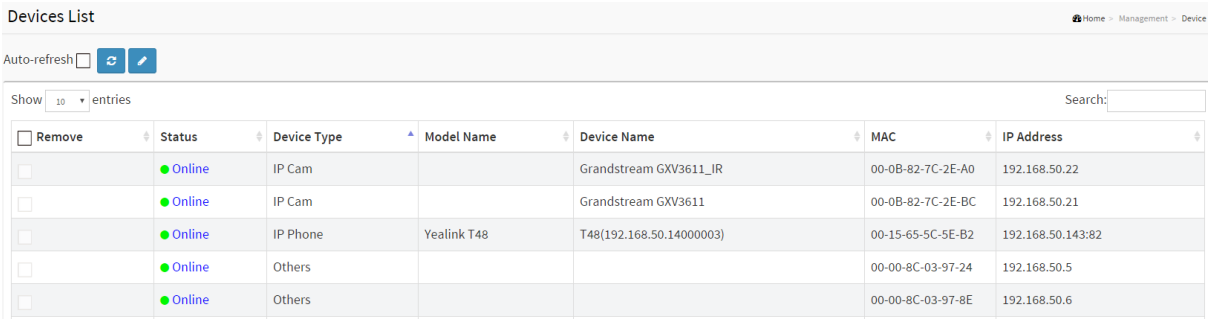


Fig: DMS Device List

Parameter	Description
Remove	Removes selected devices from DMS
Status	Device link state Online or Offline
Model Name	The device model name – EG Yealink T48
Device Name	Device name if applicable
Edit Device Name	Edit the device name
MAC	Device MAC Address.
IP Address	Device IP address, hyper-link re-direct to device website

Version	Device firmware version.

DMS Graphical Monitoring

Topology View

In this page, you can see a visual view of the topology in a cluster of networks.

Information

To Configure DMS Graphical Monitoring Information via the Web Interface

1. Click **DMS Tab** > **Graphical Monitoring > Topology View**
2. This will show a graphical view of your Network from the AS Series Switch.
3. Click on the details button  to list each device. To centre the view on any device simply left click on the device.
4. To log into the device via HTTP (if applicable) click on the icon then select the Login button.
5. To view diagnostics select the Diagnostics button, or for any notifications select the Notifications button.
6. To sort devices by type, select the drop down list in the right corner and select the category you wish to view. EG IP Phone, IP Camera, Switch.

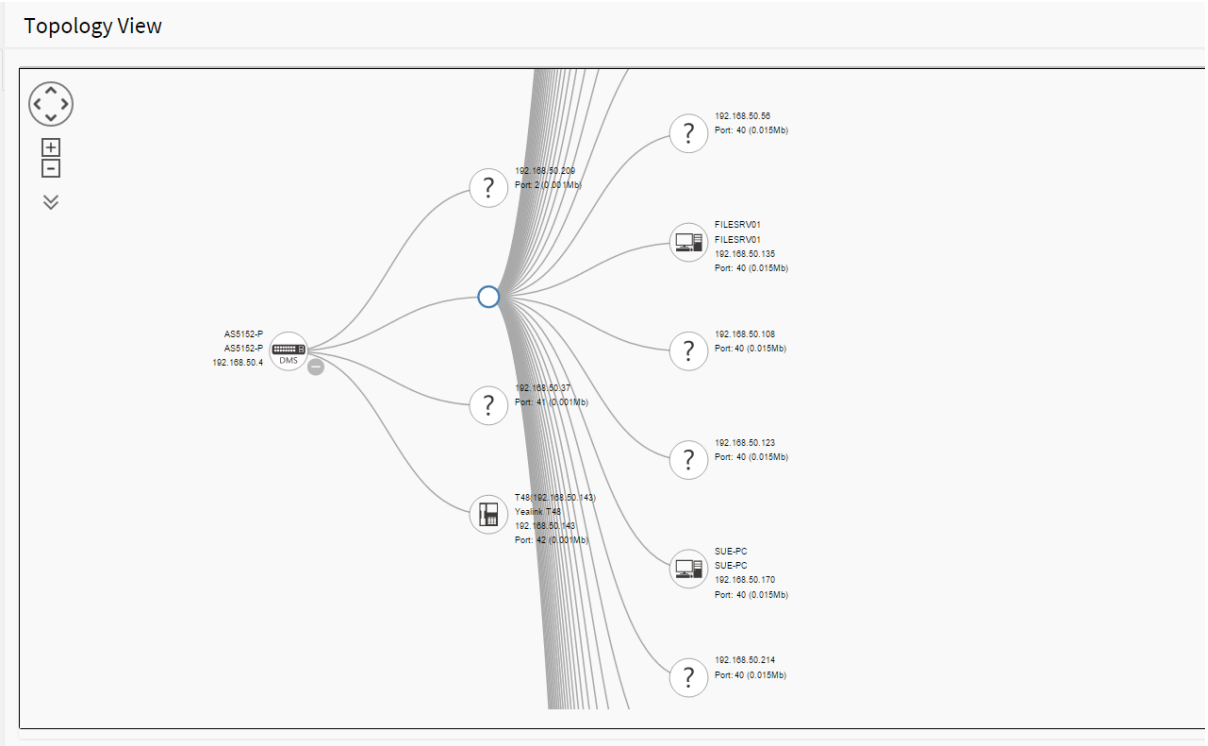


Fig DMS Topology View

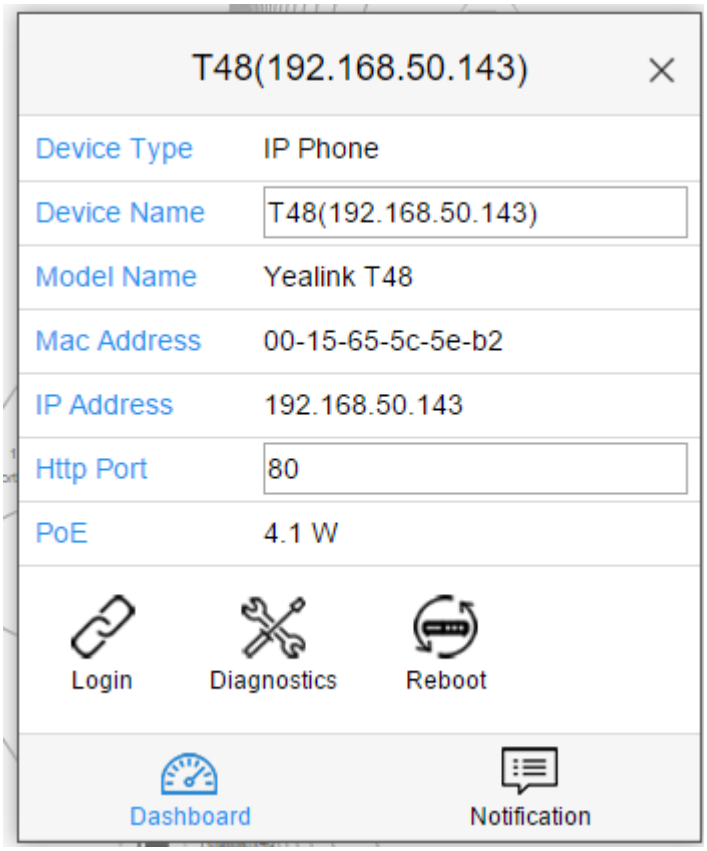


Fig DMS Topology Device View

Parameter	Description
Login	Removes selected devices from DMS
Reboot Device	Reboots the End Point Device If applicable
Device Type	Select Device Type to PC, IP phone, IP cam, AP or other device.
Diagnostics	Launches into the Maintenance Diagnostics section.
Notification	Shows Notifications for the device
Parent Node	Switches the graphical representation end point for that switch port.
Dashboard	Returns to the Dashboard view for the device
Search	Search for device by typing IP/MAC address or Model/Device name.

Buttons	Description
	Use the directional pad to scroll up, down, left, or right.
	Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.
	Saves a picture of the Topology in either SVG, PNG or PDF Format.
	Select the device category.
	Search for device by typing IP/MAC address or Model/Device name.

Floor View

In this page, the administrator can place a device per time onto the custom image, which you have already uploaded, by dragging-and-dropping markers in the device list.

Information

To Configure DMS Information via the Web Interface

1. Click **DMS Tab** > **Graphical Monitoring > Floor View**

2. This will show a floor plan view of your Network.

3. To upload a floor plan image, select the **DMS Tab** > **Maintenance** > **Floor Image**. Then select **Add Floor Image**.

4. 4. To add devices onto the Floor Image, select the  icon to the right, then left click the device you want to add to the Floor Plan. After you click the item, you can then drag and drop it to the location you wish

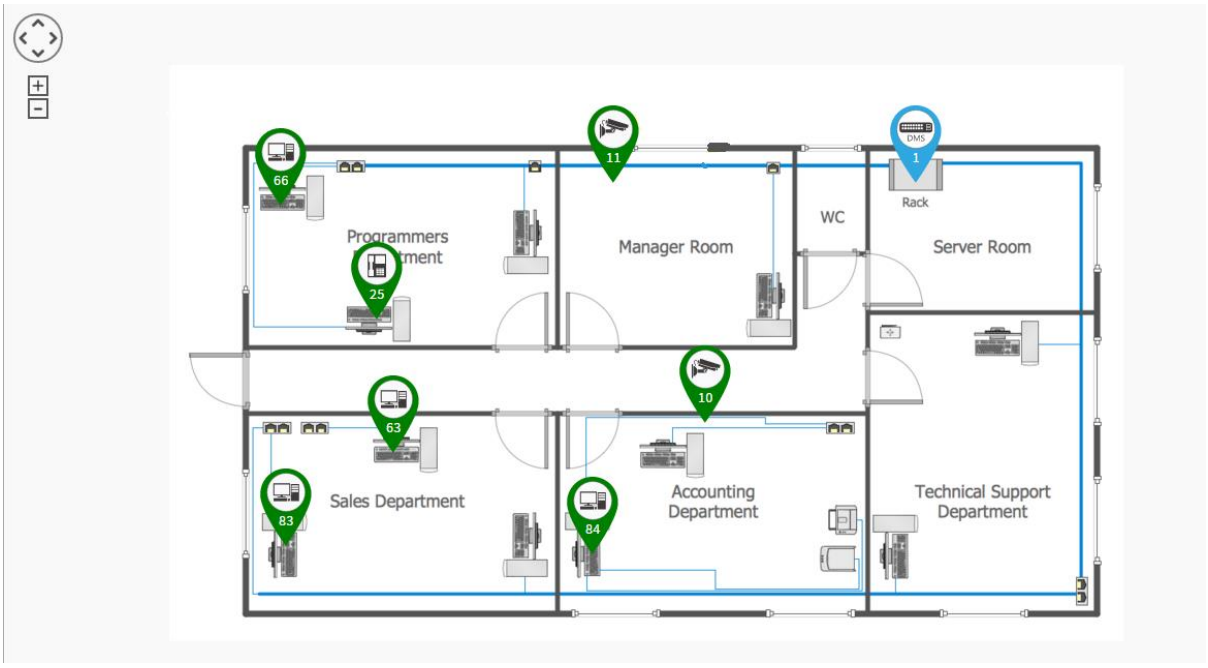


Fig: DMS Floor Plan

Buttons	Description
	Use the directional pad to scroll up, down, left, or right.
	Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.
	Saves a picture of the Topology in either SVG, PNG or PDF Format.
	Select the device category.
	Search for device by typing IP/MAC address or Model/Device name.

Map View

In this page, you can view a representation of where devices are located geographically in the network. To find one of devices within the network, enter the device name in the search bar. Click Device List to hide the Device List on the page or show a list of devices.

Information

To Configure DMS Map View Information via the Web Interface

1. Click **DMS Tab** > **Graphical Monitoring > Map View**
2. This will show a Geographical map view of your Network from the AS Series Switch.
3. To add devices onto the Map View, select the  icon to the right, then left click the device you want to add to the Map. After you click the item, you can then drag and drop it to the location you wish
4. To log into the device via HTTP (if applicable) click on the icon then select the Login button.
5. To view diagnostics select the Diagnostics button, or for any notifications select the Notifications button.
6. To sort devices by type, select the drop down list in the right corner and select the category you wish to view. EG IP Phone, IP Camera, Switch.

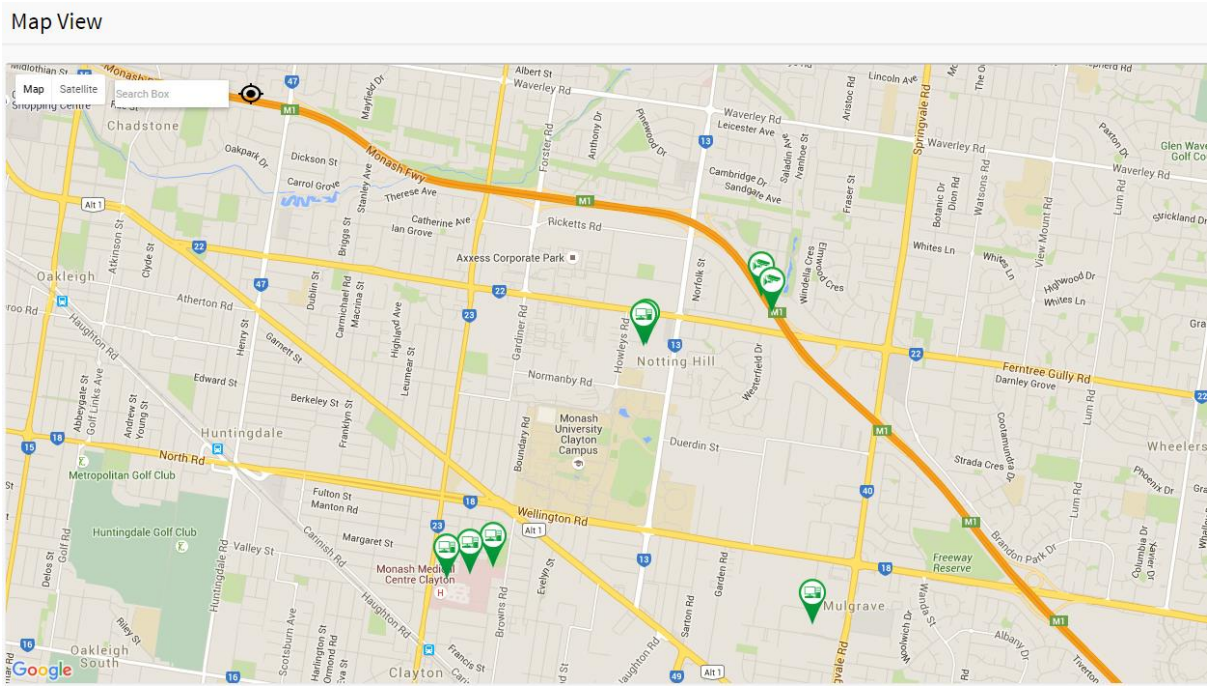
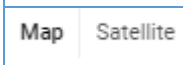


Fig: DMS Map View

Buttons	Description
	Use the directional pad to scroll up, down, left, or right.
	Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.
	Saves a picture of the Topology in either SVG, PNG or PDF Format.
	Select the device category.
	Search for device by typing IP/MAC address or Model/Device name.
	To Toggle between Map and Satellite views
	To center in on your current location.

DMS Maintenance

Floor Image

In this page, an administrator can add or delete a custom map or floor image

Information

To Configure the DMS Floor Image Information via the Web Interface

1. Click **DMS Tab** > **Maintenance > Floor Image**
2. To add a new Image select **Choose File** then Navigate to the file.
3. Enter a **Name** into the Name field and then select **Add**
4. To delete a Floor Image, tick the Select box and then click **Delete**.

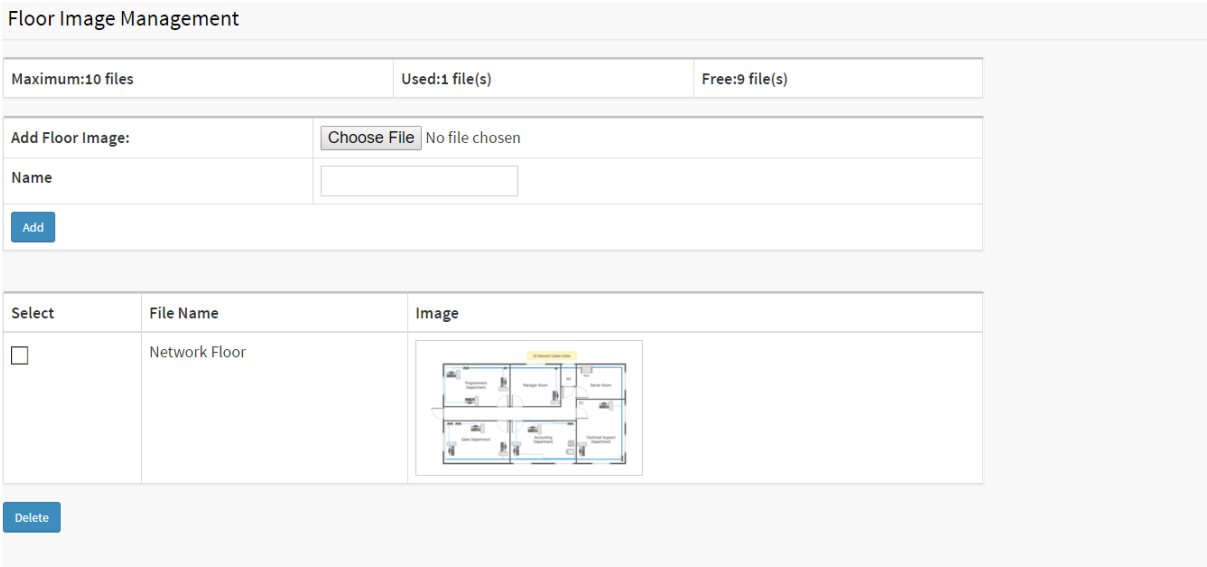


Fig: DMS Floor Image

Diagnostics

In this page, you can troubleshoot any issue you have with devices connected to the network. This feature is designed primarily for administrators to verify and test the link routes between the switch and the device. A troubleshooting solution is provided by the system so that administrators can detect where the problem lies. Note that the topology of network needs to be saved for this function to work properly.

Information

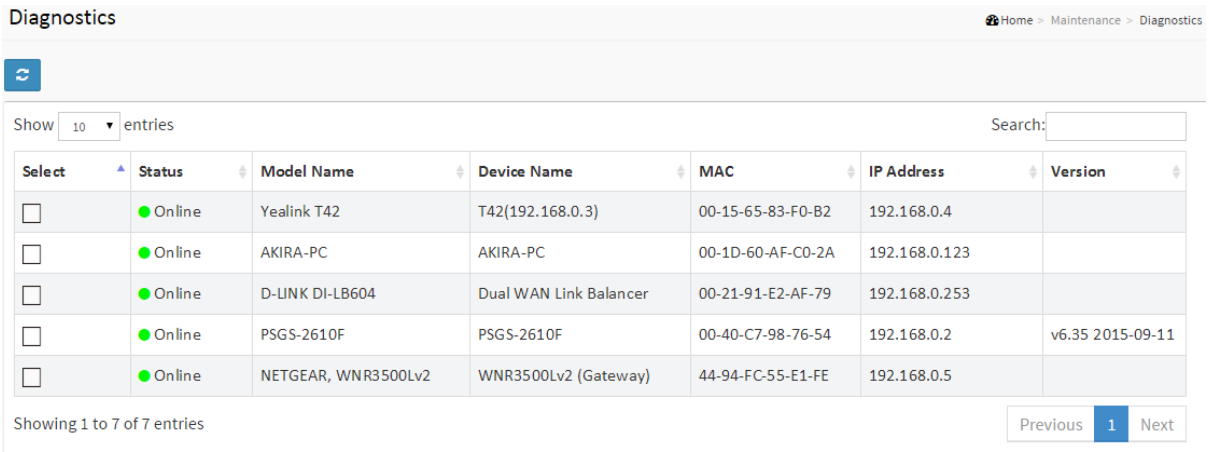
To view the DMS Diagnostic Information via the Web Interface

1. Click **DMS Tab** > **Maintenance > Diagnostics**

2. Select the device to you wish to start the Diagnostics operations on by ticking the Select box to the left hand side

3. This will check the DMS connection and cable status between the switch and the device you selected in the above step.

4. To probe another device, select the **Another Try** option at the top of the screen.



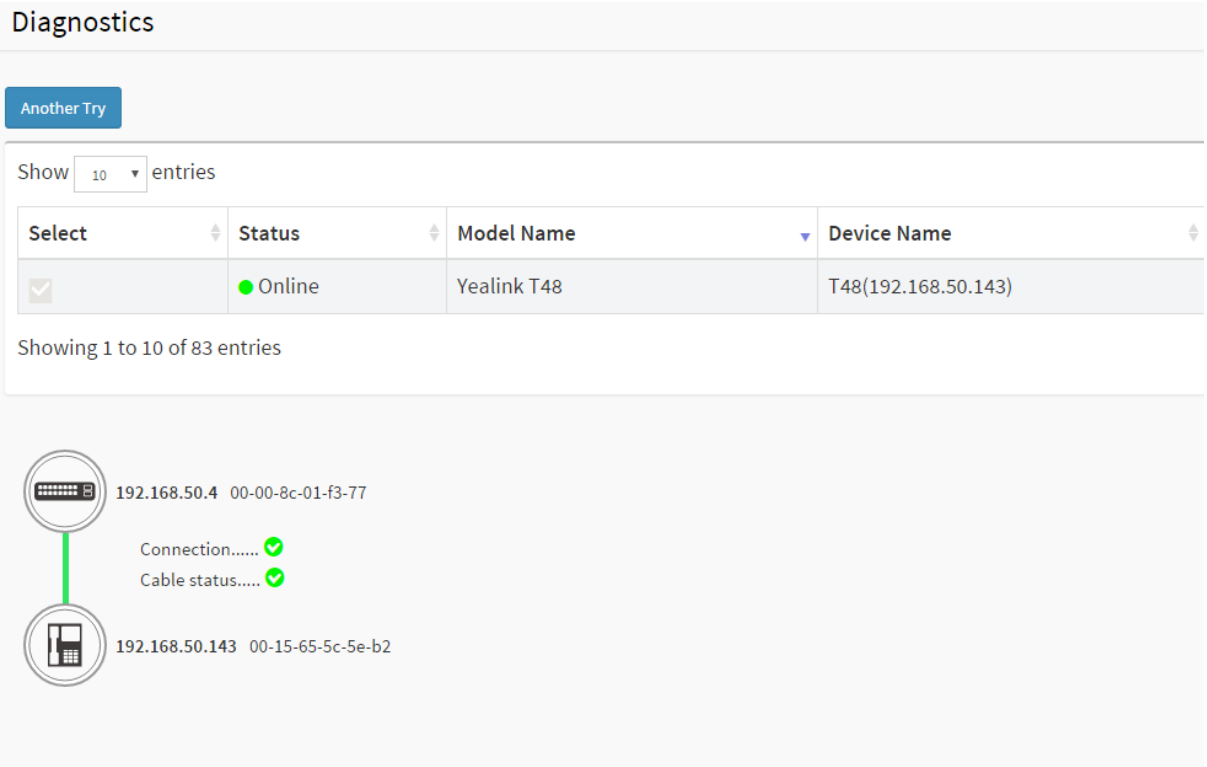


Fig: the DMS Diagnostics Section.

Traffic Monitor

This page displays visual chart of network traffic of all the devices managed by the AS Series switch.

Information

To view the DMS Traffic Monitor Information via the Web Interface

1. Click **DMS Tab** > **Maintenance > Traffic Monitor**
2. Select the Time frame you wish to look Analyse by selecting either **Day** or **Week**
3. To view individual Port statistics, click on the bar graph to the corresponding port number (EG port 2)
4. This will either break down the Individual port graph by Hour (if Day is selected), or by Day if Week is selected.

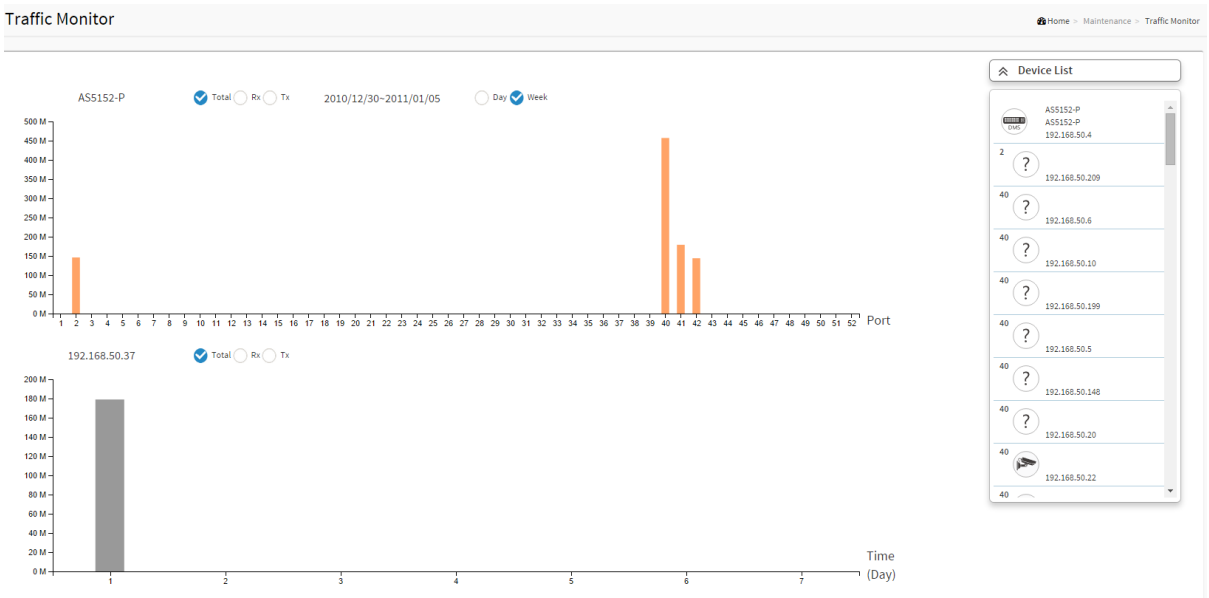


Fig: DMS Traffic Monitor

9. Software Features

Layer 3 Lite Switching	
IPv4 Static Routes	IPv4 Unicast: Static routing
IPv6 Static Routes	IPv6 Unicast: Static routing
DHCP Server	Built in DHCP Server, allowing IP Address assignment to DHCP clients. Configurable DHCP Options.
Layer 2+ Switching	
Spanning Tree Protocol	Provides Redundant links and prevents network loops. Supports; Standard Spanning Tree 802.1d Rapid Spanning Tree (RSTP) 802.1w Multiple Spanning Tree (MSTP) 802.1s
Port Aggregation	Link Aggregation Control Protocol (LACP) IEEE 802.3ad Up to 14 groups Up to 4 ports per group
VLAN	Supports up to 4K VLANs simultaneously (4096 VLAN IDs) Port-based VLAN 802.1Q tag-based VLAN MAC-based VLAN Management VLAN Private VLAN Edge (PVE) Q-in-Q (double tag) VLAN Voice VLAN GARP VLAN Registration Protocol (GVRP)
IGMP	IGMP Snooping, Querier and Proxy support; Controls and manages the flooding of multicast packets in a layer 2 network, supports 1024 multicast groups
MLD	Version 1 and 2, Snooping for IPv6; Controls and manages the flooding of IPv6 multicast packets in a layer 2 network
Loop Protection	Alternative to STP, Prevents network loops
Device Management System	
Graphical Monitoring	Provides a graphical representation of your network displaying all devices that are connected. Three different layouts are available: Topology View - Logical diagram of your physical devices, includes

	information such as port numbers, devices connected, devices disconnected, allows access to device web management etc. Floor View - Allows you to upload floor plan of your building, allowing you to place devices in their physical positions. Map View - Google Maps type view, allowing you to place devices in their physical locations, perfect for IP Cameras that are installed schools, streets etc.
Device Management	Easy access to management of IP Phones, IP Cameras, Wireless Access Points and Switches via their built in web manager.
Traffic Monitoring	Visual display of traffic on your switch, per port analysis.
Troubleshooting	Network diagnostic between switch and connected device.
Find My Switch	Same functionality as the Find My Switch App. Allows you to click on a switch in your network, select find my switch and all LED's on the front panel of the switch will light allowing you to find your switch in racks that are full of devices and at most times difficult to locate.
Quality of Service (QoS)	
Hardware Queues	Supports 8 Hardware Queues
Scheduling	Strict Priority and weighted round-robin (WRR) Queue assignment based on DSCP and Class of Service (COS)
Classification	Port based 802.1p VLAN priority based IPv4/IPv6 precedence / DSCP based Differentiated Services (DiffServ) Classification and tag re-marking ACLs
Rate Limiting	Ingress policer Egress shaping and rate control
Security	
Secure Shell (SSH)	SSH secures Telnet traffic in or out of the switch, supports SSH v1 and v2
Secure Sockets Layer (SSL)	SSL encrypts http traffic, allows secure access to the web GUI
IEEE 802.1X	IEEE802.1X: RADIUS authentication, authorization and accounting, MD5 hash, guest VLAN, single/multiple host mode and single/multiple sessions Supports IGMP-RADIUS based 802.1X Dynamic VLAN assignment

Private VLAN Edge	PVE (also known as protected ports) provides L2 isolation between clients in the same VLAN. Supports multiple uplinks
Port Security	Locks MAC addresses to ports, and limits the number of learned MAC address
IP Source Guard	Prevents illegal IP address from accessing specific ports on the switch
RADIUS / TACACS+	Supports RADIUS and TACACS+ authentication. Switch as a client
Storm Control	Prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm
DHCP Snooping	Eliminates unauthorized DHCP Servers from offering IP Addresses to DHCP clients
ACLs	Supports up to 512 entries. Drop or rate limitation based on: Source and destination MAC, VLAN ID or IP address, protocol, port, Differentiated services code point (DSCP) / IP precedence TCP/ UDP source and destination ports 802.1p priority Ethernet type Internet Control Message Protocol (ICMP) packets TCP flag
Management	
Web GUI	Built-in switch configuration utility for browser-based device configuration; IPv4 and IPv6 HTTP, HTTPS
CLI	Configure/manage switch in command line mode; Telnet, SSH, Console
Remote Monitoring (RMON)	Embedded RMON agent supports RMON groups 1,2,3,9 (history, statistics, alarms, and events) for enhanced traffic management, monitoring and analysis
UPnP	Supports UPnP to enable device to device interoperability
s-Flow	Supports s-Flow monitoring
IEEE 802.1ab (LLDP)	Used by network devices for advertising their identities, capabilities, and neighbors on an IEEE 802ab local area network Support LLDP-MED extensions
Dual Firmware Images	Independent primary and secondary firmware images

Multiple Configuration Files	Multiple versions of configuration can be saved on the switch. Config files can be backed exported and imported.
SNMP	SNMP version1, 2c and 3 with support for traps, and SNMP version 3 user-based security model (USM)
Power over Ethernet (PoE)	
Port Configuration	Supports per port PoE configuration; Set Priority; maximum power, enable/disable PoE
PoE Scheduling	Supports per port PoE scheduling to turn on/off the PoE devices (PDs)
PD Auto Checking	Check the link status of PDs. Reboot PDs if there is no response
Power Delay	Can setup time based delays on PD's to reduce PoE power overload due to power spike on boot up of PD
Diagnostics	
IPv4 Ping	Used to test connectivity to IPv4 devices
IPv6 Ping	Used to test connectivity to IPv6 devices
VeriPHY	Cable diagnostics to determine correct pin out and cable length
Traceroute	used to determine route to IP Address to Hostname

10. Specifications

AS Series Model	AS5010-P	AS5026-P	AS5048-P	AS5128-P	AS5152-P
Interface					
Total Ports, comprising	10x GbE	26x GbE	48x GbE	28x GbE	52x GbE
UTP (10/100/1000Mbps)	8	24	44	24	48
UTP/(100M/1G) SFP	2	2	4	-	-
SFP+ (1G/10G)	-	-	-	4	4
Power Over Ethernet					
Total IEEE 802.3af/at PoE Ports	8	24	48	24	48
PoE compliant Ports	UTP Ports 1-8	UTP Ports 1-24	UTP Ports 1-48	UTP Ports 1-24	UTP Ports 1-48
Max AF/AT Power Per Port (watts)	15.4W 802.3af / 30W 802.3at				
Maw PoE Per Port (Full Load)	16.25W	7.7W	7.7W	7.7W	7.7W
Total Power Budget (watts)	130W	185W	370W	185W	370W
PoE Pins	1, 2, 3 & 6				
Hardware Performance					
Jumbo Frames	9K	9K	10K	10K	10K
MAC Table	8K	8K	32K	32K	32K
Switching Capacity	20Gbps	52Gbps	96Gbps	128Gbps	176Gbps
Forwarding Capacity	14.88 mpps	38.68 mpps	71.42 mpps	95.23 mpps	130.94 mpps
Latency	1GB Copper: < 2.7ms, 1GB SFP: < 1.1ms	1GB Copper: < 3ms, 1GB SFP: < 1.9ms	1GB Copper: < 3ms, 1GB SFP: < 1.9ms	1GB Copper: < 3.9ms, 1GB SFP: < 3.2ms; 10GB SFP: < 2.2µs	1GB Copper: < 3.9ms, 1GB SFP: < 6.1ms, 10GB SFP: < 4.7µs
Memory and Processor					

SDRAM	128MB	128MB	128MB	128MB	128MB
Flash	32MB	32MB	32MB	32MB	32MB
Environmental Specifications					
Dimensions (W x H x D mm)	220 x 44 x 242	442 x 44 x 211	442 x 44 x 385	442 x 44 x 211	442 x 44 x 385
Weight	2.3Kg	3.1Kg	5.8Kg	2.5Kg	5.8Kg
Case	Desktop / 1RU rackmount (mounting kit included), all metal case				
Temperature	0° to 40° operating; -20° to 70° storage				
Humidity	10% to 90% , relative, non-condensing				
Power Supply	100-240VAC 50-60Hz, internal , universal				
Certification	CE Mark, FCC Part 15 (CFR47) Class A, RCM				