Hard-to-find made easy®

10-Port L2 Managed Gigabit Ethernet Switch with 2 SFP Slots - Rack Mountable

IES101002SFP

*actual product may vary from photos

DE: Bedienungsanleitung - de.startech.com
FR: Guide de l'utilisateur - fr.startech.com
ES: Guía del usuario - es.startech.com
IT: Guida per l'uso - it.startech.com
NL: Gebruiksaanwijzing - nl.startech.com
PT: Guia do usuário - pt.startech.com

For the latest information, technical specifications, and support for this product, please visit www.startech.com/IES101002SFP.

Manual Revision: 08/07/2015

FCC Compliance 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 when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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.

Changes or modifications not expressly approved by StarTech.com could void the user's authority to operate the equipment.

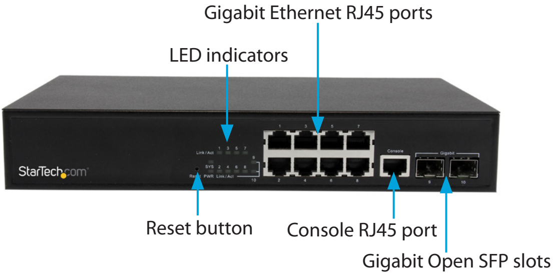
Use of Trademarks, Registered Trademarks, and other Protected Names and Symbols

This manual may make reference to trademarks, registered trademarks, and other protected names and/or symbols of third-party companies not related in any way to StarTech.com. Where they occur these references are for illustrative purposes only and do not represent an endorsement of a product or service by StarTech.com, or an endorsement of the product(s) to which this manual applies by the third-party company in question. Regardless of any direct acknowledgement elsewhere in the body of this document, StarTech.com hereby acknowledges that all trademarks, registered trademarks, service marks, and other protected names and/or symbols contained in this manual and related documents are the property of their respective holders.

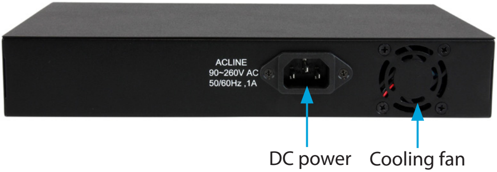
Table of Contents

Product diagram

Front view



Rear view



Introduction

This switch is a Web Smart switch equipped with 8 ports 10/100/1000BaseT(X) and 2 ports Gigabit SFP open slots, and provides a broad range of features for Layer2 switching. It was designed for easy installation and high performance in an environment where the traffic is on the network and the number of users increases continuously. The smart and efficient power design is designed to improve power usage.

Packaging contents

- 1 x 10-port Gigabit Ethernet switch with 2 open SFP slots
- 2 x mounting brackets (1 set)
- 3 x power cords (NA/UK/EU)
- 1 x instructional manual (CD)
- 1 x instruction manual

Features

Feature	Description
Dual images	Prevents any kind of upgrading process failure
IPv4	Supports IPv4 addressing, management, and Quality of Service (QoS)
IPv6	Supports IPv6 addressing, management, and Multicast Listener Discovery (MLD) snooping
	Supports local and remote Syslog Server with 3 levels (Info, Warning, and Error)
Power saving	LED power management 802.3az EEE
Security	Private VLAN (static) Access Control Lists (ACLs) for filtering, policing, and port copy, including an ACL wizard

Authentication	Telnet, Web - user name and password Telnet - Secure Shell (SSH) Simple Network Management Protocol (SNMP) v1/v2c - community strings SNMP version 3 - MD5 or SHA password Port-based 802.1x
Port limiting	Input rate limiting per port (manual setting or ACL)
Port configuration	Speed, duplex mode, flow control, maximum transmission unit (MTU), and power saving mode
Port mirroring	1 session, up to 10 source port to 1 analysis port per session
Port aggregation	IEEE 802.3ad link aggregation, static, and Link Aggregation Control Protocol (LACP)
Spanning Tree Algorithm	Supports standard Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP)
IEEE 802.1D bridge	Supports dynamic data switching and learning addresses
Quality of Service	Traffic classes (1, 2, or 4/8 active priorities) Storm control for UC, MC, and BC
DHCP	Client
Configuration	Save and restore configuration
Firmware	Supports upgrade and firmware image switch using Web and console port
CLI command	Supports command line interface (CLI) commands with console port (Baudrate: 115200, DataBit: 8, Parity: N, StopBit1)

Specifications

Standard

- IEEE 802.3ad link aggregation
- IEEE 802.3x flow control
- IEEE 802.1x Port-based Network Access Control
- IEEE 802.1Q VLAN tagging
- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- 24 integrated IEEE 802.3ab-compliant 10/100/1000BASE-T Ethernet

MIBs

- RFC 1213 MIB-II
- RFC 3411 SNMP Management Frameworks
- RFC 3621 LLEP-MED power
- RFC 3635 Ethernet-like MIB
- RFC 4188 Bridge MIB
- IEEE 802.1AB LLDP MIB
- RFC 3621 Power Ethernet

Performances

Information

- MAC address: 8 K, 4 K VLAN support
- Packet memory: 4 Mb of integrated shared memory
- Jumbo frame: 9.6 K
- Transmission method: Store and forward

LED indicators

The LED indicators present real-time information about systematic operation status. The following table provides descriptions of LED statuses and meanings.

LED	Status	Description
Power	On	System is on
	Off	System is off
Link or activity	Blinking	Activating link and data
	Off	Port is disabled or disconnected

Web management

The following section describes the features of the Web Smart switch, including instructions on how to configure each feature using the Web interface.

Configure the switch for the first time

Note: You can use the LED activity to check the status of the switch while you configure it.

To configure the switch, complete the following steps:

1. Place the switch close to the computer that you're using to complete the configuration.
2. Connect an Ethernet cable from the port of your computer to any of the ports on the front panel of the switch.
3. Turn on the switch and observe the LED activity to confirm that the switch is connected.
4. Change your computer's IP address so that it's the same subnet as the switch's.

   The following table describes the default login information:

IP address	192.168.2.1
IP mask	255.255.255.0
IP router	0.0.0.0
Username	admin
Password	

5. On your computer, open a Web browser and navigate to **192.168.2.1**.
6. In the **Username** field, type **admin**.
7. Leave the **Password** field blank, and click **OK**.

Change your password

After you set up the switch for the first time, before you configure the switch, you should change the password.

To change your password, complete the following steps:

1. On your computer, open a Web browser and navigate to **192.168.2.1**.
2. In the **Username** field, type **admin**.
3. Leave the **Password** field blank, and click **OK**.
4. Click **Security**.
5. Click **Switch**.
6. On the **Password** tab, enter the old and new passwords.

About the setting options in the Web management UI

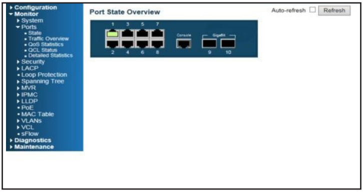
The Web management UI includes several elements that you can use to configure the settings for your switch. These UI elements include text fields, drop-down lists, radio buttons, and check boxes.

Note: When you change any of the setting options, remember to click **Save** to apply your changes.

The following table describes some of the options that are available on the main screen of the Web management UI:

Button	Description
Save	Apply your changes to the switch.
Reset	Restore the settings to what they were before you saved the changes.
?	View the Help information for the screen that you’re currently on.
🚪	Log out of the Web management UI.

When you log in to the Web management UI, the default screen that you see is the Port State Overview screen:



Ports 1 to 8 are Gigabit Ethernet ports, and ports 9 and 10 are the SFP slots. When the port image is green, it means that the port is connected.

By default, Auto-refresh mode is turned off. When Auto-refresh mode is turned on, the state of the ports is automatically refreshed every 5 seconds. To turn on **Auto-refresh** mode, select the **Auto-refresh** check box. To manually update the state of the ports, click **Refresh**.

To view detailed statistics about any of the ports, click the corresponding image of the port.

There is a menu located on the left side of the main Web management screen that includes numerous menu options organized under four categories: Configuration, Monitor, Diagnostic, and Maintenance.

About the menu options in the Configuration drop-down list

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **System** > <*menu option*>.

Menu option	Description
Information	Specify the system contact, name, location, and time zone offset.
IP	Configure the IPv4 (static IP address and DHCP client), and the VLAN ID settings.
IPv6	Configure the IPv6 (static IP address and DHCP client) settings.
NTP	Configure the NTP server setting (maximum: 5).
Time	Set the time zone and daylight saving time.
Log	Configure the Remote System Log Server, including the 3 levels: Info, Warning, and Error.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Power Reduction** > <*menu option*>.

Menu option	Description
LED	Reduce the LED intensity during specified hours, and configure the link change at error settings.
EEE (Energy Efficient Ethernet)	Turn on and turn off EEE, and configure the EEE urgent queues.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > <*menu option*>.

Menu option	Description
Ports	Configure the connection settings of the ports.
Loop Protection	Set the ports to shut down if the ports are stuck in a loop.
MVR	Configure the Multicast VLANs Registration.
MAC Table	Configure the aging time, dynamic learning, and static addresses.
Mirroring	Specify the source and destination port for mirroring.
UPnP	Turn on and turn off the UPnP, and configure the TTL and AD settings.
sFlow	Turn on sFlow and configure the flow and counter samplers for each port.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** <*menu option*>.

Menu option	Description
Users	Create user accounts and passwords, and set privilege levels.
Aud Method	Configure the authentication method for console and web access using the local database and RADIUS.
SSH	Turn on and turn off SSH.

HTTPS	Turn on and turn off HTTPS and specify the auto-redirect setting.
Access Management	Turn on and turn off Access Management, set the IP address range for HTTP and HTTPS, and specify the SNMP and TELNET/SSH access.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > *<menu option>*.

Menu option	**Description**
System	Configure SNMP, version (v1, v2c, and v3), read and write community, and Trap.
Communities	Specify the community for SNMPv3 and the source IP address.
Users	Configure the SNMPv3 user.
Groups	Configure the SNMP group.
Views	Configure the View Name and type.
Access	Configure the access authority.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **RMON** > *<menu option>*.

Menu option	**Description**
Statistics	Configure the RMON statistics table.
History	Configure the RMON history table.
Alarm	Configure the RMON alarm table.
Event	Configure the RMON event table.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > *<menu option>*.

Menu option	Description
Limit Control	Limit the numer of users on a specific port.
NAS	Configure the Network Access Server.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **ACL** > *<menu option>*.

Menu option	Description
Ports	Specify the ACL parameters of each switch port.
Rate Limiters	Specify the rate limiters for the switch ACL.
Access Control List	View the Access Control List.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **DHCP** > *<menu option>*.

Menu option	Description
Snooping	Turn on and turn off DHCP snooping.
Relay	Turn on and turn off DHCP relay and set up the relay server.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **IP Source Guard** > *<menu option>*.

Menu option	Description
Configuration	Turn on and turn off the IP Source guard and set up the maximum number of dynamic clients for each port.
Static Table	Manually insert the IP Source guard table.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **ARP Inspection** > *<menu option>*.

Menu option	Description
Configuration	Turn on and turn off the Global ARP inspection.
Static Table	Manually insert the ARP Inspection table.

To access the menu option, on the left side of the main screen of the Web management UI, click **Configuration** > **Security** > **AAA**.

Menu option	Description
AAA	Configure the Authentication Servers.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Aggregation** > *<menu option>*.

Menu option	Description
Static	Configure the aggregation mode and group.
LACP	View the current LACP port configurations and if neccesary, change them.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Spanning Tree** > *<menu option>*.

Menu option	Description
Bridge Settings	Configure the global bridge setting for STP and RSTP, and configure the edge port setting for BPDU filtering, BPDU guard, and port error recovery.
MSTI Mapping	Map VLANs to a specific MSTP instance.
MSTI Priorities	Specify the priority for each MSTI.
VLAN Membership	Configure the VLAN groups.

Ports	Specify the default PVID and VLAN attributes.
CIST Ports	Configure the interface settings for STA.
MSTI Ports	Configure the interface settings for an MST instance.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **IPMC** > **IGMP Snooping** > *<menu option>*.

Menu option	**Description**
Basic configuration	Configure the global and port settings for multicast filtering.
VLAN Configuration	Configure the IGMP Snooping for each VLAN interface.
Port Group Filtering	Configure ports to a specific filtering group.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **IPMC** > **MLD Snooping** > *<menu option>*.

Menu option	**Description**
Basic configuration	Configure the global and port settings for multicast filtering.
VLAN Configuration	Configure the IGMP Snooping for each VLAN interface.
Port Group Filtering	Configure ports to a specific filtering group.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **LLDP** > *<menu option>*.

Menu option	**Description**
LLDP	Configure the global parameters and the optional TLVs for a port.
LLDP-MED	Configure the LLDP-MED attributes.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **VLANs** > *<menu option>*.

Menu option	Description
VLAN Memberships	Specify the VLAN groups.
Ports	Configure the VLAN setting for each port.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Private VLANs** > *<menu option>*.

Menu option	Description
PVLAN Membership	Specify the PVLAN groups.
Port isolation	Configure the port isolation.

To access the menu option, on the left side of the main screen of the Web management UI, click **Configuration** > **VCL** > *<menu option>*.

Menu option	Description
MAC-based VLANs	Map a specific source MAC Address to a VLAN.
IP Subnet-based VLAN	Assign a subnet IP to a specific VLAN.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **VCL** > **Protocol-based VLAN** > *<menu option>*.

Menu option	Description
Protocol to Group	Create a specific protocol group.
Group to VLAN	Map a specific protocol group to a VLAN.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **Voice VCL** > <*menu option*>.

Menu option	**Description**
Configuration	Configure the global settings, allow or block Voice VLAN by port setting.
OUI	Configure the Voice VLAN and OUI mapping table.

To access the menu options, on the left side of the main screen of the Web management UI, click **Configuration** > **QoS** > <*menu option*>.

Menu option	**Description**
Port Classification	Configure the QoS Ingress Classification settings for all ports.
Port Policing	Configure the QoS Ingress Port policers to limit traffic flows by a specific rate.
Port Scheduler	See an overview of the egress priority status for each port, and set the egress queue mode and sharper.
Port Shaping	See an overview of the egress sharper for each port, and set the egress queue mode and sharper.
Port Tag Remarking	See an overview of the egress tag remarking, and set the tag remarking mode.
Port DSCP	Configure the egress translation and classification, and set the egress DSCP rewrite value.
DSCP-Based QoS	Configure the Ingress classification setting for DSCP-based QoS.
DSCP Translation	Set the translation of Ingress classification and the egress DP lv.
DSCP Classification	Map the DSCP value to the QoS class and DP level.
QoS Control List	Configure the QoS Control Entry based on parameters such as VLAN ID, UDP/TCP port, IPv4 DSCP, or tag priority.
Storm Control	Set the limitation for broadcast, unicast, and multicast traffic.

About the menu options in the Monitor drop-down list

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **System** > *<menu option>*.

Menu option	Description
Information	View the system contact, name, location, system time, firmware version, and the MAC address for the switch.
CPU load	View the CPU load by realtime SVG graph.
Log	View logged messages with the selected level (Info, Warning, Error, and All).
Detailed Log	View the fully logged message.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Ports** > *<menu option>*.

Menu option	Description
State	View a graphic image of the front panel of the switch to see the current port states.
Traffic Overview	View the basic port statistics.
QoS Statistics	View the total of incoming and outgoing egress queues.
QCL Status	View the status of the QoS Control Lists.
Detailed Statistics	View the detailed port statistics.

To access the menu option, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > *<menu option>*.

Menu option	Description
Access Management Statistics	View the incoming management packets, including HTTP, HTTPS, SNMP, TELNET, and SSH.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **Port Security** > *<menu option>*.

Menu option	Description
Switch	View the module legend and the status of each port, including the MAC address learning and the maximum allowed MAC count.
Port	View the MAC address, VLAN ID, state, time of addition, and the age and hold of the timer for each port.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **NAS** > *<menu option>*.

Menu option	Description
Switch	View the authentication service status and information for each port.
Port	View the authentication statistics, port status, and authentication method.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > *<menu option>*.

Menu option	Description
ACL Status	View the ACL status by different ACL users.
ARP Inspection	View the dynamic ARP inspection table, sorted by port number, VLAN ID, MAC address, and IP address.
IP Source Guard	View the IP Source Guard table, sorted by port number, VLAN ID, and IP address.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **DHCP** > *<menu option>*.

Menu option	Description
Snooping Statistics	View the statistics for each packet type.
Relay Statistics	View the DHCP relay statistics.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > **AAA** > *<menu option>*.

Menu option	Description
RADIUS Overview	View the status of the associated authentication RADIUS servers.
RADIUS Details	View the traffic and status of each of the associated RADIUS servers.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Security** > **Switch** > **RMON** > *<menu option>*.

Menu option	Description
Statistics	View an overview of the RMON Statistics entries.
History	View an overview of the RMON History entries.
Alarm	View an overview of the RMON Alarm entries.
Event	View an overview of the RMON Event table entries.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **LACP** > *<menu option>*.

Menu option	Description
System Status	View the LACP information for each local port, including the Aggr ID, Partner system ID, and Partner key.
Port Status	View the key, Aggr ID, Partner system ID, and Partner port for each local port.
Port Statistics	View the statistics for LACP protocol messages.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > *<menu option>*.

Menu option	Description
Loop Protection	View the loop status for each port.
MAC Table	View the Dynamic and Static MAC address table.
sFlow	View the receiver and per-port sFlow statistics.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **Spanning Tree** > *<menu option>*.

Menu option	Description
Bridge Status	View the STP detailed bridge status, CIST Ports, and Aggregations state.
Port Status	View the CIST role, State, and uptime for each port.
Port Statistics	View the statistics for the RSTP, STP, and TCN packets.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **MVR** > *<menu option>*.

Menu option	Description
Statistics	View the IGMP/MLD statistics used by the MVR.
MVR Channel Groups	View the MVR channel information, including the VLAN ID groups and port members.
MVR SFM Information	View the Source-Filtered Multicast information, including the Source-Specific Multicast information.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **IPMC** > **IGMP Snooping** > *<menu option>*.

Menu option	**Description**
Status	View the statistics related to IGMP packets passed upstream to the IGMP Querier or downstream to multicast clients.
Groups Information	View information about the IGMP snooping groups.
IPv4 SFM Information	View information about the IGMP Source-Filtered Multicast, including Source-Specific Multicast.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **IPMC** > **MLD Snooping** > *<menu option>*.

Menu option	**Description**
Status	View the MLD snooping status and statistics.
Groups Information	View the MLD group table, which is sorted by VLAN ID and then by group.
IPv6 SFM Information	View the MLD Source-Filtered Multicast information table, including the Source-Specific Multicast information.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **LLDP** > *<menu option>*.

Menu option	**Description**
Neighbours	View the LLDP information for the remote device that is connected to a port on the switch.
LLDP-MED Neighbours	View the information for the remote device that is advertising LLDP-MED.
EEE	View an overview of the EEE information exchanged by LLDP.
Port Statistics	See an overview of all of the LLDP traffic.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **VLANs** > *<menu option>*.

Menu option	Description
VLAN Membership	View the port members for a specific VLAN ID.
VLAN Port	View the VLAN Port Status for a Static user.

To access the menu options, on the left side of the main screen of the Web management UI, click **Monitor** > **VCL** > *<menu option>*.

Menu option	Description
MAC-based VLAN	View the MAC-based VLAN entries configured by various MAC-based VLAN users.

About the menu options in the Diagnostics drop-down list

To access the menu options, on the left side of the main screen of the Web management UI, click **Diagnostics** > *<menu option>*.

Menu option	Description
Ping	Test a specific IP address by using the ping function.
Ping6	Test a specific IPv6 address by using the ping function.

About the menu options in the Maintenance drop-down list

To access the menu options, on the left side of the main screen of the Web management UI, click **Maintenance** > *<menu option>*.

Menu option	Description
Restart Device	Restart the switch.
Factory Defaults	Restore all of the settings to the factory default settings.

About the menu options in the Maintenance drop-down list

To access the menu options, on the left side of the main screen of the Web management UI, click **Maintenance** > **Software** > *<menu option>*.

Menu option	Description
Upload	Use the Web UI to update the firmware for the switch.
Image Select	Select a recovery firmware to use to start the switch.

About the menu options in the Maintenance drop-down list

To access the menu options, on the left side of the main screen of the Web management UI, click **Maintenance** > **Configuration** > *<menu option>*.

Menu option	Description
Save	Save the configuration to your local PC.
Upload	Restore the previous configuration from a file.

Changing the Configuration settings

Change the System Information settings

1. On the main screen of the Web management UI, click **Configuration** > **System** > **Information**.
2. Do any of the following:
   - To specify an administrator for the switch, in the **System Contact** field, enter a name (maximum length is 255 characters).
   - To specify a name for the switch, in the **System Name** field, enter a name (maximum length is 255 characters).
   - To specify the location that the switch is in, in the **System Location** field, enter a location (maximum length is 255 characters).

Change the System IP settings

The following table describes the System IP settings that you can change:

Option	Description
DHCP Client	Enable the DHCP client or disable the DHCP client and use a static IP address.
IP Address	Sets the static IP address of the switch, if not acting as a DHCP client. The default IP is 192.168.2.1.
IP Mask	The mask used to determine which subnet the switch belongs to.
IP Router	The IP address of the gateway.
VLAN ID	The VLAN that the switch is associated with. The VLAN ID needs to match your management's PC/NB VLAN ID. The range is between 1 and 4096 and the default VLAN ID is 1.
DNS Server	A domain name server that resolves client host name to IP address requests.
DNS Proxy	Enable this feature to maintain a DNS database.
Renew	Use to renew a DHCP lease.

To configure the static IP address and enable the DHCP client, do the following:

1. On the main screen of the Web management UI, click **Configuration** > **System** > **IP**.
2. Do one of the following:
   - To enable the DHCP client, select the **DHCP** check box.
   - To disable the DHCP client and use a static IP address, clear the **DHCP** check box.
3. In the **Configured** column, complete the **IP Address**, **IP Mask**, **IP Router**, and **SNTP Server IP** fields.
4. To renew the IP Address, click **Renew**.
5. To maintain a local DNS database, select the **DNS Proxy** check box.
6. To apply the changes that you made, click **Save**.

To restore the previous settings, click **Restore**.

Change the System IPv6 settings

The following table describes the System IPv6 settings that you can change:

Option	Description
Auto Configuration	Enable the DHCP client, or disable the DHCP client and use a static IP address.
Address	The IPv6 address must adhere to the IPv6 Addressing Architecture format. The IPv6 address is in 128-bit records represented as 8 fields of up to 4 hexadecimal digits with a colon separating each field.
Prefix	Specify the IPv6 prefix for your switch. The allowed range is between 1 and 128.
Router	Specify the IPv6 gateway for your switch.

1. On the main screen of the Web management UI, click **Configuration** > **System** > **IPv6**.
2. Do one of the following:
   - To enable Auto Configuration, select the **Auto Configuration** check box.
   - To disable Auto Configuration, clear the **Auto Configuration** check box.
3. In the **Configured** column, complete the **Address** field.

4. If necessary, complete the **Router** field.
5. To renew the IPv6 Address, click **Renew**.
6. To apply the changes that you made, click **Save**.

To restore the previous settings, click **Restore**.

Change the NTP Configuration settings

The following table describes the NTP Configuration settings that you can change:

Option	Description
Mode	Enable or disable NTP Client mode.
Server 1 to 5	Specify the IPv4 or IPv6 of up to 5 NTP servers.

1. On the main screen of the Web management UI, click **Configuration** > **System** > **NTP**.
2. Do one of the following:
    - To enable NTP Client mode, in the **Mode** drop-down list, click **Enabled**.
    - To disable NTP Client mode, in the **Mode** drop-down list, click **Disabled**.
3. In the **Server** fields, enter the IP address of the NTP Server.
4. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Time settings

The following table describes the Time settings that you can change:

Option	Description
Time Zone	Select a time zone from a list of world-wide time zones.
Acronym	Enter an acronym for the time zone that you selected. You can use up to 16 alphanumeric characters and the acronym can contain "-", "_", and ".".
Daylight Saving Time	Set the daylight saving time to recur every year or to just occur once.
Month	Specify the month to start and end daylight saving time.

Date	Specify the day to start and end daylight saving time.
Year	Specify the year to start and end daylight saving time.
Hours	Specify the hour to start and end daylight saving time.
Minutes	Specify the minute to start and end daylight saving time.
Offset	Specify the number of minutes to add during daylight saving time. The range is between 1 and 1440 minutes.

To configure the time settings, do the following:

1. On the main screen of the Web management UI, click **Configuration** > **System** > **Time**.
2. In the **Time Zone** drop-down list, click a time zone.
3. In the **Acronym** field, enter an acronym to describe the time zone that you selected.
4. To enable daylight saving time, in the **Daylight Saving Time** drop-down list, click **Enabled**.
5. Do one of the following:
    - To set the daylight saving time to repeat every year, in the **Daylight Saving Time** drop-down list, click **Recurring**.
    - To set the daylight saving time to only occur once, click **Non-Recurring**.
6. To configure the date to start daylight saving time, do the following:
    - In the **Month** drop-down list, click a month.
    - In the **Date** drop-down list, click a day of the month.
    - In the **Year** drop-down list, click a year.
    - In the **Hours** drop-down list, click an hour.
    - In the **Minutes** drop-down list, click a numeric value.
7. To configure the date to end daylight saving time, repeat step 6.
8. To enter the number of minutes to add during daylight saving time, in the **Offset** field, enter a numeric value.
9. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Log settings

The following table describes the Log settings that you can change:

Option	Description
Server Mode	Enable or disable remote system logging.
Server Address	Specify the IP address of the server used for remote system logging.
Syslog Level	Select one of the following logging event levels: Info, Warning, or Error.

1. On the main screen of the Web management UI, click **Configuration** > **System** > **Log**.
2. Do one of the following:
    - To enable Server mode, in the **Server Mode** drop-down list, click **Enabled**.
    - To disable Server mode, in the **Server Mode** drop-down list, click **Disabled**.
3. In the **Server Address** field, enter the IP address of the server.
4. Do one of the following:
    - To send info, warnings, and errors, in the **Syslog Level** drop-down list, click **Info**.
    - To send warnings and errors, in the **Syslog Level** drop-down list, click **Warning**.
    - To send errors, in the **Syslog Level** drop-down list, click **Error**.
5. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the LED settings

The following table describes the LED settings that you can change to reduce the LED intensity during specified hours to save power.

Option	Description
Time	Specify the length of time to change the LED itensity for.
Intensity	Set the LED intensity percentage level. There are 10 levels of LED intensity, increasing by 10% intensity with each level. 0% intensity level means the LED is turned off and 100% intensity means the LED is at full power.

On time at link change	Set the duration of time that the LED operates at full power when a link change occurs.
On at errors	Set the LED to operate at full power when an error occurs.

1. On the main screen of the Web management UI, click **Configuration** > **Power Reduction** > **LED**.
2. In the **Time** drop-down list, click a time.
3. In the **Intensity** drop-down list, click a percentage value.
4. To add the LED rule to the switch, click **Add**.
5. To set the duration of time that the LED operates at full power when a link change occurs, in the **Sec.** field, enter a numeric value.
6. To set the LED to operate at full power when an error occurs, select the **On at errors** check box.
7. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the EEE settings

The following table describes the EEE (Energy Efficient Ethernet) settings that you can change:

Option	**Description**
Enable	Enable or disable EEE for each port.
EEE Urgent Queue	Set queues to activate the transmission of frames as soon as any data is available. If not set, the queue will postpone the transmission until 3 000 bytes are ready to be transmitted.

Note: If a port is greyed out on the **EEE Configuration** screen, it means that the port isn't EEE capable and can't be set.

1. On the main screen of the Web management UI, click **Configuration** > **Power Reduction** > **EEE**.
2. To enable EEE for a port, select the **Enabled** check box next to the port that you want to enable.
3. If necessary, select the **EEE Urgent Queues** check box next to a port.
4. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port settings

On the Port Configuration screen, you can specify the parameters for each port, including enabling and disabling ports, setting port speeds such as auto, half-duplex, full-duplex, and more. You can also set the frame size, specify the collision policy and power control. See the table below for more information about the settings that you can change.

Option	Description
Link	View the status of each port.
Speed	View the current speed in the Current column. Choose between seven options in the Configured column.
Flow Control	View the flow control state of Rx and Tx in the Current columns. You can also enable Flow Control to eliminate packet loss.
Maximum Frame Size	Specify the maximum frame size allowance to transfer for each port.
Excessive Collision Mode	Configure the behavior for port transmit collisions.
Power Control	Set the options for automatic power saving mode.

1. On the main screen of the Web management UI, click **Configuration** > **Ports**.
2. Do one of the following:
    - To disable the port interface, in the **Configured** drop-down list, click **Disabled**.
    - To enable auto-negotiation, in the **Configured** drop-down list, click **Auto**.
    - To set the switch to support 10 Mbps half-duplex, in the **Configured** drop-down list, click **10Mbps HDX**.
    - To set the switch to support 10 Mbps full-duplex, in the **Configured** drop-down list, click **10Mbps FDX**.
    - To set the switch to support 100 Mbps half-duplex, in the **Configured** drop-down list, click **100Mbps HDX**.
    - To set the switch to support 100 Mbps full-duplex, in the **Configured** drop-down list, click **100Mbps FDX**.
    - To set the switch to support 1 Gbps full-duplex, in the **Configured** drop-down list, click **1Gbps FDX**.

3. To enable flow control, select the **Configured** check box.
4. To specify the maximum frame size allowance to transfer for each port, in the **Maximum Frame Size** field, enter a numeric value.
5. To change the settings for the excessive collision mode, in the **Excessive Collision Mode** drop-down list, click an option.
6. To change the options for the automatic power saving mode, do one of the following:
    - To set the switch to detect unused Ethernet ports on network devices and power them down, in the **Power Control** drop-down list, click **ActiPHY**.
    - To use an intelligent algorithm that actively adjusts the power level needed based on cable length, in the **Power Control** drop-down list, click **PerfectReach**.
    - To enable both ActiPHY and PerfectRead, in the **Power Control** drop-down list, click **Enabled**.
    - To disable the power saving mode, in the **Power Control** drop-down list, click **Disabled**.
7. To save your changes, click **Save**.
8. To manually reload the information on the screen, click **Refresh**.

To restore the previous settings, click **Reset**.

Change the User settings

On the User Configuration screen, you can configure the user name and password authority for different privilege levels. See the table below for more information about the settings that you can change.

Option	Description
User Name	Enter a user name that is up to 31 characters long (letters, numbers, and underscores are allowed).
Password	Enter a password that is up to 31 characters long for a user.
Privilege Level	Set a privilege level for a user between the range of 1 and 15.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **Users**.
2. Complete the **User Name**, **Password**, and **Password (again)** fields.

3. In the **Privilege Level** drop-down list, click a level option.
4. To save your changes, click **Save**.
5. To cancel your changes, click **Cancel**.

To restore the previous settings, click **Reset**.

Change the Privilege Levels settings

On the Privilege Levels screen, you can set the privilege level required to read or configure a software module or system setting. See the table below for more information about the settings that you can change.

Option	Description
Group Name	The name used to identify the privilege group.
Privilege Level	Set a privilege level for a user between the range of 1 and 15.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **Privilege Levels**.
2. Do any of the following:
   - For any of the group names, in the **Configuration Read-only** drop-down list, click a privilege level.
   - For any of the group names, in the **Configuration/Execute Read/Write** drop-down list, click a privilege level.
   - For any of the group names, in the **Status/Statistics Read-only** drop-down list, click a privilege level.
   - For any of the group names, in the **Status/Statistics Read/Write** drop-down list, click a privilege level.
3. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Authentication Method settings

On the Authentication Method Configuration screen, you can specify the authentication method for access management using console, telnet, ssh, and Web. Access can be controlled by local (password) or remote access authentication (RADIUS server). See the table below for more information about the settings that you can change.

Option	Description
Client	Specify the authentication method for the administrator.
Authentication Method	Select 1 of 4 authentication methods.
Fallback	Set the switch to check by local password if fallback is checked when radius server authentication fails.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **Auth Methods**.
2. For any of the client types, do the following:
    - To disable access via specified management interface, in the **Authentication Method** drop-down list, click **None**.
    - To check by password, in the **Authentication Method** drop-down list, click **Local**.
    - To authenticate using the RADIUS server, in the **Authentication Method** drop-down list, click **RADIUS**.
    - To authenticate using the TACACS+ server, in the **Authentication Method** drop-down list, click **TACACS+**.
3. If necessary, select the **Fallback** check box for any of the client types.
4. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Set up the Secure Shell management interface

On the SSH Configuration screen, you can enable SSH. SSH service on this switch only supports password authentication. It can be authenticated by RADIUS, TACACS+, or locally.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SSH**.
2. Do one of the following:
    - To enable SSH, in the **Mode** drop-down list, click **Enabled**.
    - To disable SSH, in the **Mode** drop-down list, click **Disabled**.
3. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Enable HTTPS

On the HTTPS Configuration screen, you can enable or disable HTTPS and Automatic Redirect mode. When Automatic Redirect mode is enabled, the Web browser is automatically redirected to an HTTPS connection when both HTTPS and Automatic Redirect modes are enabled.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **HTTPS**.
2. Do one of the following:
   - To enable HTTPS, in the **Mode** drop-down list, click **Enabled**.
   - To disable HTTPS, in the **Mode** drop-down list, click **Disabled**.
3. If HTTPS is enabled, do one of the following:
   - To enable Automatic Redirect, in the **Mode** drop-down list, click **Enabled**.
   - To disable Automatic Redirect, in the **Mode** drop-down list, click **Disabled**.
4. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Configure the access management settings

On the Access Management Configuration screen, you can create a list of up to 16 IP addresses or IP address groups that allow access management through the HTTP/HTTPS/SNMP/TELNET/SSH.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **Access Management**.
2. Do one of the following:
   - To enable access management, in the **Mode** drop-down list, click **Enabled**.
   - To disable access management, in the **Mode** drop-down list, click **Disabled**.
3. If access management is enabled, click **Add New Entry**.
4. Set up a list of rules for HTTP/HTTPS, SNMP, TELNET/SSH.
5. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Configure the SNMP settings

On the SNMP System Configuration screen, you can configure the SNMP settings, including community name, trap host, public traps, and so on. See the table below for more information about the settings that you can change.

Option	Description
Mode	Enable or disable the SNMP service.
Version	Specify the SNMP version (SNMP v1, SNMP v2c, or SNMP v3).
Read Community	Specify the community that has read access.
Write Community	Specify the community that has read/write access.
Engine ID	View the SNMP v3 engine ID (only available for SNMP v3).
Trap Mode	Enable or disable the SNMP traps.
Trap Version	Specify the trap version (SNMP v1, SNMP v2c, or SNMP v3).
Trap Community	Specify the community string for SNMP trap packets.
Trap Destination Address	Specify the IP address of the server to receive trap packets.
Trap Authentication Failure	Enable trap authentication failure to issue a notification message to the trap destination address whenever a SNMP request fails.
Trap Link-up and Link-down	Enable trap link-up and link-down to issue a notification message to the trap destination address whenever a port link is established or broken.
Trap Inform Mode	Enable trap inform mode to send a notification as an inform message (only available for SNMP v2c and SNMP v3). This mode can guarantee that the message is received.
Trap Inform Timeout	Set the length of time in seconds to wait for ACK.
Trap Inform Retry Times	Set the maximum number of retry times before timeout.
Trap Probe Security Engine ID	Specify whether or not to use the engine ID of the SNMP trap probe in trap and inform messages (only available for SNMP v3).

Trap Security Engine ID	View the SNMP trap security engine ID (only available for SNMP v3).
Trap Security Name	View the trap security name (only available for SNMP v3).

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > **System**.
2. To enable SNMP mode, in the **Mode** drop-down list, click **Enabled**.
3. In the **Version** drop-down list, click a version.
4. If required, in the **Read Community** and **Write Community** fields, change the community access.
5. To enable the switch to send SNMP traps, in the **Trap Mode** drop-down list, click **Enabled**.
6. In the **Trap Version** drop-down list, click a version.
7. Complete the **Trap Community**, **Trap Destination Address**, and **Trap Destination IPv6 Address** fields.
8. To enable the switch to send a notification message to trap destination address when an SNMP request fails, in the **Trap Authentication Failure** drop-down list, click **Enabled**.
9. To enable the switch to send a notification message to trap destination address when a port link is established or broken, in the **Trap Link-up and Link-down** drop-down list, click **Enabled**.
10. To enable the switch to send a notification as an inform message, in the **Trap Inform Mode** drop-down list, click **Enabled**.
11. Complete the **Trap Inform Timeout (seconds)** and **Trap Inform Retry Times** fields.
12. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the SNMPv3 community configuration settings

The table below describes the settings that you can change on the SNMPv3 Community Configuration screen.

Option	**Description**
Community	Specify the community string to allow access to the SNMP agent (range is between 1 and 32).

Source IP	Specify the IP address of the SNMP client.
Source Mask	Specify the subnet mask of the SNMP client.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > **Communities**.
2. Do any of the following:
   - Complete the **Source IP** and **Source Mask** fields.
   - To delete a community, select the **Delete** check box next to the community that you want to remove.
   - To add a new community string, click **Add New Entry** and complete the instructions on the screen.
3. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the SNMPv3 User settings

On the SNMPv3 User Configuration screen, you can specify an engine ID, user name, and security level, as well as set the authentication and privacy level for each SNMPv3 user. See the table below for more information about the settings that you can change.

Option	Description
Engine ID	View the engine identifier for the SNMP agent (only available for SNMPv3).
User Name	Specify a unique user name (between 1 and 32 characters long) for the SNMP.
Security Level	Set 1 of 3 security levels: • NoAuth, NoPriv (no authentication and encryption applied during the communication). • Auth, NoPriv (the communication has authentication applied to it, but not encryption). • Auth, Priv (both authentication and encryption are applied during the communication).
Authentication Protocol	Set the method for authentication (None, MD5, or SHA).
Authentication Password	Set a password between 1 and 32 text characters long.

Privacy Protocol	Set the encryption algorithm (none or 56-bit DES).
Privacy Password	Set a privacy passphrase between 8 and 40 characters long).

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > **Users**.
2. Click **Add New User**.
3. In the **Engine ID** field, enter a remote engine ID.
4. Complete the **User Name**, **Security Level**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password** fields.
5. To save your changes, click **Save**.
6. To delete a user configuration, in the **Delete** column, select the check box next to the entry that you want to remove.

To restore the previous settings, click **Reset**.

Change the SNMPv3 Group settings

On the SNMPv3 Group Configuration screen, you can define a specific SNMPv3 group and restrict the access policy to read and write views. See the table below for more information about the settings that you can change.

Option	Description
Security Model	Select 1 of 3 user security models: v1, v2, and USM (User-based Security Model).
Security Name	Set a security name between 1 and 32 characters in length that is used to connect to the SNMP agent.
Group Name	Enter a name for the SNMP group.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > **Groups**.
2. To create a new group, click **Add New Entry**.
3. In the **Security Model** column, select a model type.
4. In the **Security Name** column, select a name.
5. In the **Group Name** field, enter a name for the group.
6. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the SNMPv3 View settings

On the SNMPv3 View Configuration screen, you can define the restricts access policy for a specific MIB tree. The default_view includes access ability for the whole MIB tree. See the table below for more information about the settings that you can change.

Option	Description
View Name	Specify a name between 1 and 32 characters long for the SNMP view.
View Type	Set whether the OID is included or excluded for a specific SNMP view.
OID Subtree	Specify the object identifiers of branches within the MIB tree.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > **Views**.
2. To create a new view, click **Add New Entry**.
3. In the **View Name** column, enter a name for the SNMP view.
4. In the **View Type** drop-down list, click a view type.
5. In the **OID Subtree** column, enter an identifier of the OID subtree.
6. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the SNMPv3 Access settings

On the SNMPv3 Access Configuration screen, you can define the access rights for a portion of the MIB tree. See the table below for more information about the settings that you can change.

Option	Description
Group Name	Specify a name between 1 and 32 characters long for the SNMP group.
Security Model	Select 1 of 3 user security models: v1, v2, and USM (User-based Security Model).

Security Level	Set 1 of 3 security levels: • NoAuth, NoPriv (no authentication and encryption applied during the communication). • Auth, NoPriv (the communication has authentication applied to it, but not encryption). • Auth, Priv (both authentication and encryption are applied during the communication).
Read View Name	Select a view name for read access.
Write View Name	Select a view name for write access.

Note: You can have more than one access policy for an SNMPv3 group.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **SNMP** > **Access**.
2. To create a new access profile, click **Add New Entry**.
3. In the **Group Name** column, enter a name for the SNMP group.
4. In the **Security Model** column, select a security model type.
5. In the **Security Level** column, select a security level type.
6. In the **Read View Name** drop-down list, click a view name.
7. In the **Write View Name** drop-down list, click a view name.
8. To save your changes, click **Save**.
9. To delete an access configuration, in the **Delete** column, select the check box next to the configuration that you want to remove.

To restore the previous settings, click **Reset**.

Change the RMON Statistics settings

On the RMON Statistics Configuration screen, you can configure the page to set the ID for MIBs and to store real-time LAN statistics, including utilization, collisions, and CRC errors. See the table below for more information about the settings that you can change.

Option	**Description**
Delete	Delete the entry of MIBs.
ID	Configure the index for the statistics. The index range is between 1 and 65535.
Data Source	View the port ID that you want to monitor. The number corresponds to the port number.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **RMON** > **Statistics**.
2. To create a new MIBs, click **Add New Entry**.
3. In the **ID** field, enter an ID number.
4. In the **Data Source** field, enter a port number.
5. To delete the MIBs entry, click **Delete** next to the MIBs that you want to delete.
6. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the RMON History settings

On the RMON History Configuration screen, you can see an overview of the history of selected LAN statistics, including utilization, collisions, and CRC errors. See the table below for more information about the settings that you can change.

Option	Description
Delete	Delete the History configuration entry.
ID	Configure the index for the group of statistics. The index range is between 1 and 65535.
Data Source	View the port ID that you want to monitor. The number corresponds to the port number.
Interval	Specify the interval in seconds for sampling the History statistics data. The range is from 1 to 3600 and the default value is 1800 seconds.
Buckets	The maximum number of entries to collect.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **RMON** > **History**.
2. To create a new rule, click **Add New Entry**.
3. In the **ID** field, enter an ID number.
4. In the **Data Source** field, enter the port ID of the port that you want to monitor.
5. In the **Interval** field, enter a numeric value.
6. In the **Buckets** field, enter a numeric value.
7. To save your changes, click **Save**.
8. To delete a rule, click **Delete** next to the rule that you want to delete.

To restore the previous settings, click **Reset**.

Change the RMON Alarm settings

On the RMON Alarm Configuration screen, you can set the threshold to use for sending the SNMP trap. See the table below for more information about the settings that you can change.

Option	Description
ID	Configure index of the entry. The index range is between 1 and 65535.
Interval	Set the interval in seconds for sampling and comparing the rising and falling threshold. The range is 1 to 2^31-1.
Variable	Specify the variable to be sampled. Choose from the following variables: • InOctets (the number of the octets received on the interface, including framing characters). • InUcastPkts (the number of the unicast packets delivered to a high-layer protocol). • InNUcastPkts (the number of the broadcast and multicast packets delivered to a higher-layer protocol). • InDiscards (the number of inbound packets that are discarded, even if the packets are normal). • InErrors (the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol). • InUnknown Protocols (the number of the inbound packets that were discarded because of the unknown or unsupported protocols). • OutOctets (the number of octets transmitted out of the interface, including framing characters). • OutUcastPakts (the number of unicast packets that request to transmit). • OutNUcastPkts (the number of broadcast and multicast packets that request to transmit). • OutDiscards (the number of outbound packets that are discarded even if the packets are normal). • OutErrors (the number of outbound packets that couldn't be transmitted because of errors). • OutQlen (the length, in packets, of the output packet queue).

Delete	Delete the RMON Alarm configuration entry.
Sample Type	Select the method of sampling the selected variable and calculating the value to be compared against the threshold. Possible sample types include Absolute (directly get the sample) and Delta (calculate the difference between samples).
Value	View the value of the statistic during the last sampling period.
Startup Alarm	Specify the method of sampling the selected variable and calculating the value to be compared against the thresholds. Sample types include the following: • Rising (the alarm is triggered when the first value is larger than the rising threshold). • Falling (the alarm is triggered when the first value is less than the falling threshold). • RisingOrFalling (the alarm is triggered when the first value is larger than the rising threshold or less than the falling threshold).

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **RMON** > **Alarm**.
2. To create a new rule, click **Add New Entry**.
3. Complete the **ID**, **Interval**, **Variable**, **Rising Threshold**, **Rising Index**, **Falling Threshold**, and **Falling Index** fields.
4. In the **Sample Type** drop-down list, click a sample type.
5. In the **Startup Alarm** drop-down list, click a sample type.
6. To save your changes, click **Save**.
7. To delete a rule, click **Delete** next to the rule that you want to delete.

To restore the previous settings, click **Reset**.

Change the RMON Event settings

On the RMON Event Configuration screen, you can set up a trigger when an alarm trigger occurs. See the table below for more information about the settings that you can change.

Menu option	Description
Delete	Delete the Event configuration entry.
ID	Configure the index of the entry. The index range is between 1 and 65535.
Desc	View the event identifier. The string length is between 0 and 127, and the default is null string.
Type	Indicates the notification of the event. Notification types include the following: • none (the total number of octets received on the interface, including framing characters). • log (the number of unicast packets delivered to a higher-layer protocol). • snmtrap (the number of broadcast and multicast packets delivered to a higher-layer protocol). • logandtrap (the number of inbound packets that are discarded even if the packets are normal).
Community	Specify the community when the trap is sent. The string length is from 0 to 127 and the default is Public.
Event Last Time	View the value of sysUpTime at the time the event entry last generated an event.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Switch** > **RMON** > **Event**.
2. To create a new rule, click **Add New Entry**.
3. Complete the **ID**, **Desc**, and **Community** fields.
4. In the **Type** drop-down list, click an event type.
5. To save your changes, click **Save**.
6. To delete a rule, click **Delete** next to the rule that you want to delete.

To restore the previous settings, click **Reset**.

Change the Port Security Limit Control settings

On the Port Security Limit Control Configuration screen, you can limit the number of users who are accessing a specific port. Users are identified by a MAC address or VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users that can be on a port, and if the number is exceeded, action is taken. See the table below for more information about the settings that you can change.

Menu option	Description
Mode	Enable or disable limit control.
Aging Enabled	When selected, secure MAC addresses are subject to aging.
Aging Period	Specify the aging period. Set a value between 10 and 10,000,000 seconds.
Port	View the port number.
Mode	Enable or disable Limit Control for a specific port. **Note:** This field and the Global Mode must be set to Enabled for Limit Control to be enabled.
Limit	Set the maximum number of MAC addresses that can be secured on the port. The number can't exceed 1024 and 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 enabled with Port Security. Since all ports draw from the same pool, it may happen that a configured maximum can't be granted if the remaining ports have already used all of the available MAC addresses.
Action	If the limit is reached, the switch can take one of the following actions: • none (doesn't allow more than Limit MAC addresses on the port, but takes 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.)

Action	There are three ways to reopen a port: 1. Turn on the switch. 2. Disable and enable the **Limit Control** on the port or the switch again. 3. Click the **Re-open** button. • Trap&Shutdown (if Limit+ 1 MAC address is seen on the port, both the Trap and the Shutdown actions described above will be taken).
State	View the current state of the port as seen from the Limit Control's point of view. The state can be one of four values: • Disabled (Limit Control is either globally disabled or disabled on the port). • Ready (the limit isn't reached yet). This can be shown for all actions. • Limit Reached (indicates that the limit is reached on this port, and 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, and 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 can reopen it by clicking this button. For other methods, refer to the Shutdown in the Action section. **Note:** Clicking the **Re-open** button refreshes the page and any unsaved changes will be lost.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **Limit Control**.
2. In the **Mode** drop-down list, click a mode.
3. Select the **Aging Enabled** check box.
4. In the **Aging Period** field, enter an aging period in seconds.
5. Set each port's configuration, including **Mode**, **Limit**, and **Action**.
6. If the state of a port is **Shutdown**, to enable the port again, click **Reopen**.
7. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Network Access settings

On the Network Access Server Configuration screen, you can configure network authentication settings. See the table below for more information about the settings that you can change.

Menu option	Description
Mode	Indicates if Network Access Server (NAS) is globally enabled or disabled on the switch. If disabled, all ports are allowed forwarding of frames.
Re-authentication Enabled	If checked, successfully authenticated supplicants/ clients are re-authenticated after the interval specified by the Re-authentication Period. For 802.1X-enabled ports, re-authentication can be used to detect if a new device is plugged into a switch port, or if a supplicant/client is no longer attached. For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It doesn’t involve communication between the switch and the client, and therefore doesn’t imply that a client is still present on a port.
Re-authentication Period	If Re-authentication is enabled, this value determines the length of time after which a connected client must be re-authenticated. Values are in the range of 1 to 3600 seconds.
EAPOL Timeout	Determines the time for re-transmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This setting is not applicable for MAC-based ports

Aging Period

This setting applies to the following modes:

1) Single 802.1X

2) Multi 802.1X

3) MAC-Based Auth.

The Port Security Module scans for activity on the MAC addresses at regular intervals and frees up resources if no activity is seen within a given period of time. This parameter controls the interval at which the ports are scanned, and can be set to a number between 10 and 1000000 seconds.

If re-authentication is enabled and the port is in an 802.1X-based mode, the Aging Period isn't relevant since clients that are no longer attached to the port will be removed upon the next re-authentication. If re-authentication is not enabled, the only way to free resources is by aging the entries.

Hold Time

For ports in MAC-based Auth. mode, re-authentication doesn't initiate direct communication between the switch and the client. As such, re-authentication won't detect whether or not the client is still attached, and the only way to free up resources is to age the entry.

This setting applies to the following modes, when Port Security is used to secure MAC addresses:

1) Single 802.1X

2) Multi 802.1X

3) MAC-Based Auth.

If a client is denied access or 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 doesn't 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 Enable	RADIUS-assigned QoS lets you centrally control the traffic class to which traffic coming from a successfully authenticated client is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. The RADIUS-Assigned QoS Enabled check box provides a quick way to globally enable/disable RADIUS-server assigned QoS class functionality. When checked, the individual port's ditto setting determines whether RADIUS-assigned QoS is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN lets you centrally control the VLAN on which a successfully authenticated client 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. The RADIUS-Assigned VLAN Enabled check box provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual port's ditto setting determines 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 timeout as set by the network administrator. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The Guest VLAN Enabled check box provides a quick way to globally enable or disable Guest VLAN functionality. When checked, the individual port's 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 VLAN ID is set to if the port is moved into the Guest VLAN. This value can only be changed if the Guest VLAN option is enabled globally. Valid values are in the range of 1 to 255.
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on 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 by default), the switch will only enter the Guest VLAN if an EAPOL frame has been received on the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port. This value can only be changed if the Guest VLAN option is enabled globally.
Port Configuration	
Port	The port number to which the configuration below applies.
Admin State	If NAS is enabled globally, 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 deny network access to any client on the port.
[Port-Based 802.1X]	In 802.1X terminology, the user is called the 'supplicant', the switch is the 'authenticator', and the RADIUS server is the 'authentication server'. The authenticator forwards requests and responses between the supplicant and the authentication server.

[Single 802.1x]	Only one supplicant can be authenticated on the port at any time. 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 the first supplicant fails to authenticate, the second supplicant is then considered.
[Multi 802.1X]	One or more supplicants can be authenticated on the same port at any 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 toward the supplicant, since that would cause all supplicants attached to the port to reply to the requests sent from the switch.
[MAC-based Auth]	Unlike port-based 802.1X, MAC-based authentication is not a standard, rather a best-practice method adopted by the industry. In MAC-Based authentication terminology, users are called "clients", and the switch acts as the supplicant on behalf of clients. The initial frame sent by a client is snooped by the switch, which in turn uses the client's MAC address as both user name and password in the subsquent EAP exchanged with the RADIUS server. The 6-byte MAC address is converted to a string of hexadecimal digits, formatted as "xx-xx-xx-xx-xx-xx". 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 or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch.
[RADIUS-Assigned QoS Enabled]	This feature can be enabled or disabled for a given port.
[RADIUS-Assigned VLAN Enabled]	This feature can be enabled or disabled for a given port.

[Guest VLAN Enabled]	This feature can be enabled or disabled for a given port.
Port State	The current state of the port:
[Globally Disabled]	802.1X and MAC-based authentication are globally disabled.
[Link Down]	802.1X and MAC-based authentication is enabled, but no link on the given port.
[Authorized]	The port is in Force Authorized mode, or a single-supplicant mode and the supplicant is authorized.
[Unauthorized]	The port is in Force Unauthorized mode, 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, X clients are currently authorized and Y are unauthorized.
Restart	Restart client authentication using the following methods:
[Reauthenticate]	Schedules reauthentication to whenever the quiet period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This setting only affects authenticated clients on the port and will not deauthorize clients.
[Reinitialize]	Forces a reinitialization of the clients on the port and immediately reauthenticates. The clients will transfer to the unauthorized state while the reauthentication is in progess.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **NAS**.
2. Configure the **System Configuration** settings as needed.
3. Configure the **Port Configuration** settings as needed.
4. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Ports settings

On the ACL Ports Configuration screen, you can specify the assigned port reactions when specific frames are matched. These behaviors include **Port Redirect**, **Mirror**, **Logging**, and **Shutdown**.

To access the **ACL Ports Configuration** screen, click **Configuration** > **Security** > **Network** > **ACL** > **Ports**.

Menu option	Description
Port	Identifies the port to which the settings contained in the same row will apply.
Policy ID	Specify the Policy ID to apply to this port (range: 0 to 255).
Action	Permit or deny the forwarding if policy is Matched. (**Permit** selected by default.)
Rate Limiter ID	Specify a Rate Limiter ID. The mapping table is on the **Rate Limiters** page. **Disabled** by default. Value range: 1 to 16.
Port Redirect	Select the port to which frames are redirected. Allowed values are **Disabled** (default value) or a **specific port number**. This value can't be set when **Action** is permitted.
Mirror	Specify the 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**.
Shutdown	Specify the operation of this port. The allowed values are:
[Enabled]	If a frame is received on the port. The port will be disabled.
[Disabled]	Port shutdown is disabled. The default value is **Disabled**.
State	Specify the port state of this port. The allowed values are:
[Enabled]	To reopen ports by changing the volatile port configuration of the ACL user module.
[Disabled]	To close ports by changing the volatile port configuration of the ACL user module. The default value is **Enabled**.
Counter	Counts the number of frames that match this ACE.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **ACL** > **Ports**.
2. Assign a **Policy ID** to a given port and set the related ACE parameters. Options include **Action**, **Rate Limiter ID**, **Port Redirect**, **Mirror**, **Logging**, **Shutdown**, and **State**.
3. Do any of the following:

- To refresh the counter of frames tht matched the policy, click **Refresh**.
- To clear the counter of frames matching the policy, click **Clear**.

4. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Rate Limiters settings

On the ACL Rate Limiter configuration screen, you can configure up to 16 Rate Limit options. See the table below for more information about the settings that you can change.

To access the **Rate Limiter** configuration screen, click **Configuration** > **Security** > **Network** > **ACL** > **Rate Limiters**.

Menu option	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row (range is 1 to 16).
Rate	The dropping threshold. Allowed values include 0 to 3276700 in pps or 0, 100, 2*100, 3*100…100000 in kbps.
Unit	Specify the rate unit. The allowed values are:
[pps]	Packets per second
[kbps]	Kbits per second

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **ACL** > **Rate Limiter**.
2. Configure the **Rate Limiter** settings as needed.
3. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Access Control List settings

You can use the **Access Control List** screen to define the ACE settings on the switch. Each row describes the ACE that is defined. You can define filtering rules for an ACL policy, for a specific port, or for all ports. See the table below for more information about the settings that you can change.

To access the **Access Control List** screen, click **Configuration** > **Security** > **Network** > **ACL** > **Access Control List**.

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

Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled
Mirror	Specifiy the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror 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**.
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.
[e]	Edits the ACE row.
[↑]	Moves the ACE up the list.
[↓]	Moves the ACE down the list
[X]	Deletes the ACE.
[+]	The lowest plus sign adds a new entry at the botton of the ACE listings.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **ACL** > **Access Control List**.
2. Do any of the following:

- To add a new ACE, click the **plus** button.
- To modify the ACE row, click the **e** button.
- To clean the counter of frames matching the policy, click the **Clear** button.
- To delete all of the ACE rows, click the **Remove All** button.
- To automatically refresh the page, click the **Auto-refresh** button.

3. To save your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Snooping Configuration settings

You can use the **DHCP Snooping Configuration** screen to filter IP traffic on insecure ports for which the source address can't be identified using DHCP snooping.

To access the **DHCP Snooping Configuration** screen, click **Configuration** > **Security** > **Network** > **DHCP** > **Snooping**.

Menu option	Description
Snooping mode	
Snooping mode	Indicates the status of DHCP snooping mode operation. Possible modes are:
[Enabled]	Enables DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow packets from trusted ports.
[Disabled]	Disables DHCP snooping mode operation.
Port mode configuration	
Port mode	Indicates the DHCP snooping port mode.
Configuration	Possible port modes are:
[Trusted]	Configures the port as a trusted source of the DHCP messages.
[Untrusted]	Configures the port as an untrusted source of the DHCP messages.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **DHCP Snooping**.
2. Do one of the following:

- Select **Enabled Snooping Mode**.
- Select **Disabled Snooping port**.

3. Select either **Trusted** or **Untrusted for each port**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**

Change the Relay settings

Using the **DHCP Relay Configuration** screen, you can configure DHCP relay service for attached host devices. If a subnet doesn't include a DHCP server, you can relay DHCP client requests to a DHCP server on another subnet.

To access the **DHCP Relay Configuration** screen, click **Configuration** > **Security** > **Network** > **DHCP** > **Relay**.

Menu option	Description
Relay mode	Indicates the DHCP relay mode operation. Possible modes are:
[Enable]	Enables DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. The DHCP broadcast message won't be flooded for security considerations.
[Disable]	Disables DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain.
Relay Information mode	DHCP **Option 82** is the "DHCP Relay Agent Information Option". Option 82 was designed to allow a **DHCP Relay Agent** to insert circuit specific information into a request that is being forwarded to a **DHCP server**. The option works by setting two sub-options: Circuit ID and Remote ID. Possible modes are:
[Enable]	Enables DHCP relay information mode. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server, and removes it from a DHCP message when transferring to a DHCP client. It only works when DHCP relay operation mode is enabled.
[Disable]	Disables DHCP relay information mode.

Relay Information Policy	Indicates the DHCP relay information policy option. When DHCP relay information mode operation is enabled, if an agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The Replace option is invalid when relay information mode is disabled. Possible policies are:
[Replace]	Replace the original replay 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 replay information is received.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **DHCP** > **Relay**.
2. Set the **Relay Mode** to either **Enabled** or **Disabled**.
3. Specify the **Relay Server** address.
4. Set **Relay Information Mode** to either **Enabled** or **Disabled**.
5. Specify **Policy Settings**.
6. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the IP Source Guard settings

You can use the **IP Source Guard** table (manually insert MAC Address table) or **DHCP Snooping** table (dynamic MAC address table) to filter IP traffic on switch ports.

To access the **IP Source Guard** screen, click **Configuration** > **Security** > **Network** > **IP Source Guard**.

Menu option	Description
IP Source Guard mode	
Mode	Enable or Disable the Global IP Source Guard. All configured ACEs will be lost when Mode is set to Enabled.
Port mode configuration	
Port mode	Specifies the ports on which IP Source Guard is enabled. Only when both Global Mode and Port Mode are enabled on a given port is IP Source Guard enabled on that port.
Max Dynamic	Specify the maximum number of dynamic clients that can be learned on a given port. This value can be 0, 1, 2, or Unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only the IP packets that are matched in static entries on the specific port are forwarded.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **IP Source Guard** > **Configuration**.
2. Set the **IP Source Guard** mode to either **Enabled** or **Disabled**.
3. Set the **IP Source Guard** mode for each port, as well as the **Max Dynamic Clients** allowed.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Static Table settings

You can create a Static Port-VLAN-IP Address-MAC address mapping table for IP Source Guard usage. The following table describes the options for configuring the mapping table:

Menu option	Description
Delete	Select to delete the entry. It will be deleted during the next save.
Port	The logical port of the settings.
VLAN ID	The VLAN ID for the setting.
IP address	Allowed source IP address.
Mac address	Allowed source Mac address.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **IP Source Guard** > **Static Table**.
2. Select **Add New Entry**.
3. Enter the desired information for the following fields: **Port number**, **VLAN ID**, **IP Address**, and **Mac Address**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Configuration settings

ARP Inspection is a method of protecting against certain man-in-the-middle attacks. It will validate the ARP request and response packet by intercepting with information from the MAC-to-IP database (dynamic: DHCP Snooping table, static: Static table).

Menu option	Description
Mode	Enable the Global ARP Inspection or disable the Global ARP Inspection.
Port mode configuration	Specify which ports ARP Inspection is enabled on. ARP will only be enabled on ports on which Global Mode and Port Mode are enabled.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **Network** > **ARP Inspection** > **Configuration**.
2. Set the **ARP Inspection Configuration** mode to either **Enabled** or **Disabled**.

3. Select **Enabled** or **Disabled** for each port.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Static ARP Inspections Table settings

Use the Static ARP Inspection table to create a database for validation.

The switch first compares ARP packets to any entries specified in the static ARP table. If no static entry matches the packets, then the DHCP snooping bindings database determines their validity.

Menu option	Description
Delete	Clicking the Delete button will remove the entry during the next save.
Port	The logical port for the settings.
VLAN ID	The VLAN ID for the settings.
Mac address	Designates the Allowed Source MAC address in ARP request packets.
IP address	Designates the Allowed Source IP address in ARP request packets.

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **ARP Inspection** > **Static Table**.
2. To create a new Static ARP inspection record for a given port, click **Add New Entry**.
3. Enter the appropriate values for **Port number**, **VLAN ID**, **IP Address**, and **Mac Address**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Authentication Server Configuration settings

Use the **Authentication Server Configuration** screen to build up an authenticated mechanism with RADIUS server.

To access the **Authentication Server Configuration** screen, click **Configuration** > **Security** > **AAA**.

Menu option	Description
Common Server Configuration	
Timeout	The maximum waiting time to wait for a reply from server (range is 3 to 3600 seconds).
Dead time	The time after which the switch considers an authentication server to be dead if it does not reply (range is 0 to 3600 seconds).
RADIUS Authentication Server Configuration	
Enable	Enable the RADIUS Authentication Server by selecting this check box.
IP Adress	IP address of the RADIUS server.
Port	The UDP port to use on the RADIUS authentication Server.
Secret	Encryption key (maximum characters is 29).

1. On the main screen of the Web management UI, click **Configuration** > **Security** > **AAA**.
2. Specify the parameters of the **Radius Authentication Server**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Static settings

You can create a static trunk group (multiple links between devices to work as one virtual aggregated link), using the **Aggregation Mode Configuration** screen.

To locate the screen, click **Configuration** > **Port Trunking** > **Static**.

Menu option	Description
Hash Code contributors	
Source MAC address	The Source MAC address can be used to calculate the destination port for the frame. Select to enable the use of the Source MAC address, or unselect 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. Select to enable the use of the Destination MAC Address, or unselect 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. Select to enable the use of the IP Address, or unselect to disable. By default, IP Address is enabled.
TCP/IP port number	The TCP/IP port number can be used to calculate the destination port for the frame. Select to enable the use of the TCP/IP Port Number, or unselect to disable. By default, TCP/UDP Port Number is enabled.
Aggregation Group Configuration	
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.

1. On the main screen of the Web management UI, click **Configuration** > **Aggregation** > **Static**.
2. In the section titled **Hash Code Contributors**, configure the desired load-balancing method using the provided check boxes. Parameters include **Source MAC Address**, **Destination MAC Address**, **IP Address**, and **TCP/UDP Port Number**.
3. Assign port members to their specific trunking group.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the LACP settings

Using the **LACP Port Configuration** screen, you can enable LACP on selected ports, and also configure key and LACP mode.

To locate the screen, click **Configuration** > **Port Trunking** > **Static**.

Menu option	**Description**
Port	Port identifier.

LACP enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when two or more ports are connected to the same partner. LACP can have up to 12 LLAGs per switch and GLAGs per stack..
Key	The Key value incurred by the port.(Range is 1 to 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. The same key setting ports can participate in the same aggregation group.
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.
Timeout	The Timeout controls the period between BPDU transmissions. "Fast" will transmit LACP packets each seconds, while "Slow" will wait for 30 seconds before sending an 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.

1. On the main screen of the Web management UI, click **Configuration** > **Aggregation** > **LACP**.
2. Enable LACPS on all of the ports in an LAG.
3. Divide the LAG by a different key.
4. Set the **Role** of at least one port to **Active**.
5. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Loop Protection settings

You can access the **Loop Protection** screen by clicking **Configuration** > **Loop Protection**.

Menu option	Description
General Settings	
Enable loop protection	Controls whether loop protection is enabled.
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 loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart).
Port Configuration	
Port	Port identifier.
Enable	Control whether loop protection is enabled on this switch port.
Action	Configure the action performed when a loop protection is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log, or Log only.
Tx mode	Control whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs.

1. On the main screen of the Web management UI, click **Configuration** > **Loop Protection**.
2. Enable **Loop Protection**, configure **Transmission Time** and **Shutdown Time**.
3. Specify the reaction for each port when loop protection is detected.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Spanning Tree settings

The Spanning Tree algorithm enables the switch to cooperate with other bridging devices by detecting and disabling network loops and providing backup links between switches, bridges, and routers.

You can access the **Spanning Tree** screen by clicking **Configuration** > **Spanning Tree** > **Bridge Settings**.

Menu option	**Description**
Basic Settings	
Protocol version	The STP protocol version setting, the Valid values are STP(IEEE 802.1D) and RSTP(IEEE 802.1w).
Bridge priority	Controls the bridge priority; low numeric values have higher priority.
Forward delay	The delay used by STP Bridges to transit Root and Designated Ports to forwarding (used in STP compatible mode). (Range is 4 to 30 seconds.)
Max age	The Maximum age of information transmitted by the Bridge when it is the Root Bridge. (Range is 6 to 40 seconds.) Max Age must be ≤ (Forward delay -1) x 2.
Maximum hop count	This setting defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. (Range is 6 to 40 hops.)
Advanced settings	
Edge Port BPDU filtering	Control whether the 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 BPDUs. The port will enter the error-disables state and will be removed from the active topology.
Port Error Recovery	Control whether a port in the error-disable state will automatically be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled from normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time to pass before a port in the error-disabled state can be enabled. (Range is 30 to 86400 seconds.)

1. On the main screen of the Web management UI, click **Configuration** > **Spanning Tree** > **Bridge Settings**.
2. Configure the required attributes.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the MSTI Mapping settings

Use the **MSTI Mapping** screen to inspect the current STP MSTI bridge instance priorities configuration and change them if necessary.

You can access the screen by clicking **Configuration** > **Spanning Tree** > **MSTI Mapping**.

Menu option	**Description**
Configuration Identification	
Configuration name	The name identifying the VLAN-to-MSTI mapping. Bridges must share the name and revision (see below), as well as VLAN-to-MSTI mapping configuration, in order to share spanning trees for MSTIs (intra-region). The name can be at most 32 characters.
Configuration revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI Mapping	
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs that aren't explicitly mapped.
VLANs mapped	The list of VLANs mapped to the MSTI. The VLANs can be given as a single VLAN (xx, xx being between 1 and 4094), or a range(xx-yy), each of which must be separated with a 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 to 40.

1. On the main screen of the Web management UI, click **Configuration** > **Spanning Tree** > **MSTI** > **Mapping**.
2. Configure the **Identification** and **MSTI Mapping** tables.
3. Specify the reaction for each port when loop protection is detected.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the MSTI Priorities settings

Use the **MSTI Priorities** screen to configure the bridge priority for the CIST and any configured MSTI. RSTP recognizes each MST Instance as a single bridge node.

You can access the screen by clicking **Configuration** > **Spanning Tree** > **MSTI Priorities**.

Menu option	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priorities	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.

1. On the main screen of the Web management UI, click **Configuration** > **Spanning Tree** > **MSTI Priorities**.
2. Set the **Priority** value for **CIST** and **MSTI1-MSTI7**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the CIST ports settings

Using the **STP CIST Ports Configuration** screen, you can configure STA attributes for interfaces when the Spanning Tree mode is set to STP or RSTP, or for Interfaces in the CIST. STA interface attributes include Path Cost, Priority, Edge Port, Automatic Detection of an edge port, and PtP link type.

You can access the screen by clicking **Configuration** > **Spanning Tree** > **Bridge Ports**.

Menu option	Description
CIST Aggregation Port Configuration	
STP Enable	Controls whether STP is enabled on this switch port.

Path Cost	Control the Path Cost incurred by this port. The "Auto" setting will set the path cost as appropriate by physical link speed, using the 802.1D recommended values. Using "specific" settings, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Low path cost ports are chosen as forwarding ports in favour of higher path cost ports. (Range is 1 to 200000000.)
Priority	Control the port priority. This can be used to control priority of the ports having identical port cost.
Admin Edge	Enable this option if this port is connected to an end node or at the end of the bridge.
Auto Edge	Control whether automatic edge detection is enabled on a bridge port.
Restricted role	If enabled, cause the port not to be selected as Root port for the CIST, even if it has the best spanning tree priority vector. This features is also known as Root Guard.
Restricted TCN	If enabled, this 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 external bridges 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.
BDPU Guard	If enabled, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status doesn't affect this setting.
Point-to-Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. The transition to the forwarding state is faster for point-to-point LANs than for shared media.

1. On the main screen of the Web management UI, click **Configuration** > **Spanning Tree** > **CIST Ports**.

2. Configure the required attributes.

3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the MSTI Ports settings

The MSTI ports configuration screen allows the user to inspect the current STP MSTI port configurations and possibly change them as well. An MSTI port is a virtual port, which is instantiated separately for each active CIST(physical) port for each MSTI instance configured on and applicable to the port.The MSTI instance must be selected before displaying actual MSTI port configuration options.

Menu option	**Description**
MSTI Aggregated Ports Configuration	
Port	The switch port number of the corresponding STP CIST(and MSTI) port.
Path Cost	Control the Path Cost incurred by this port. The "Auto" setting will set the path cost as appropriate by physical link speed, using the 802.1D recommended values. Using "specific" settings, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Low path cost ports are chosen as forwarding ports in favour of higher path cost ports. (Range is 1 to 200000000.)
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.

1. On the main screen of the Web management UI, click **Configuration** > **Spanning Tree** > **MSTI Ports**.
2. Select **MSTI** and then click the **get** button.
3. Set the STA parameters for ports.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the MVR settings

You can enable multicast traffic forwarding on the multicast VLANs by using the MVR configuration screen. In a multicast television application, a PC, a network television, or set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port.

When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast VLAN are called MVR source ports. It allows you to create at maximum eight MVR VLANs, with corresponding channel settings for each Multicast VLAN. At maximum, there will be a total of 256 group addresses for channel settings.

Menu option	Description
MVR Mode	Enable or 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. **Warning:** It's not recommended to have MVR source ports 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 alphanumeric characters. When the optional MVR VLAN name is given, it should contain at least one letter. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new enteries.
Mode	Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR memership 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	Defines 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 beside the Edit symbol.
Port	The logical port for the setting.
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles.
[Inactive]	The designated port does not participate in MVR operations.
[Source]	Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
[Receiver]	Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.
[Be Caution]	MVR source ports are not recommended to be overlapped with management VLAN ports. Select the port rule by clicking the Role symbol to switch the setting. "I" indicates Inactive, "S" indicates source, and "R" indicates Receiver. The default Role is Inactive.

1. On the main screen of the Web management UI, click **Configuration** > **MVR**.
2. Enable MVR globally on the switch, and select **MVR VLAN**.
3. Set the **VLAN** interface setting.
4. If necessary, you can select **Enable "fast leaving**" for each port.
5. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the IGMP Snooping Configuration settings

Multicasting is used to support real-time applications such as video-conferencing or streaming audio. A multicast server doesn't have to establish a separate connection to each client; it only broadcasts its service to the network. Using this approach will significantly increase broadcast traffic on the network. This switch can use IGMP to filter multicast traffic. IGMP snooping can be used to passively monitor or snoop the packets exchanging between multicast hosts and clients. Then it can set its filters. You can use the IGMP Snooping Configuration page to configure Global and Port Related settings to control the forwarding of multicast traffic. This can decrease broadcast traffic to improve the network performance.

You can access the screen by clicking **Configuration** > **IPMC** > **IGMP Snooping** > **Basic Configuration**.

Menu option	Description
Global Configuration	
Snooping Enabled	Control whether the IGMP snooping is enabled.
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range.
Leave Proxy Enable	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.
Port Related Configuration	
Port	Port identifier.
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	Set this to Enable to limit the number of multicast groups to which a switch port can belong.

1. On the main screen of the Web management UI, click **Configuration** > **IPMC** > **IGMP Snooping** > **Basic Configuration**.
2. Specify the required **IGMP Snooping** settings.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the VLAN Configuration settings

Each page shows up to 99 entries from the VLAN table, the 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 one with the lowest VLAN ID found in the VLAN table will be displayed first.

You can access the screen by clicking **Configuration** > **IPMC** > **IGMP Snooping** > **VLAN**.

Menu option	**Description**
Delete	Select to delete the entry. The desginated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN.
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, and Forced IGMPv3. The default compatibility value is IGMP-Auto.
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, and the default robustness variable is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds. Default query interval is 125 seconds.

QRI	Query Response Interval. The maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, and the 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, and the default last member query intervall is 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, and the default unsolicited report interval is 1 second.

1. On the main screen of the Web management UI, click **Configuration** > **IPMC** > **IGMP Snooping** > **VLAN Configuration**.
2. To add a new entry, click **Add New IGMP VLAN**.
3. To update the displayed table starting from that or the next closest VLAN table match, click **Refresh**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Group Filtering settings

Use the Port Group Filtering Configuration screen to filter specific multicast traffic.

You can access the screen by clicking **Configuration** > **IPMC** > **IGMP Snooping** > **VLAN Configuration**.

Menu option	**Description**
Delete	Check to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
Filtering Groups	The IP Multicast Group that will be filtered.
Add New Filtering Group	Click **Add New Filtering Group** to add a new entry to the Group Filtering table. Specify the Port, and Filtering Group of the new entry.

1. On the main screen of the Web management UI, click **Configuration** > **IPMC** > **IGMP Snooping** > **Port Group Filtering**.
2. Click **Add New Filtering Group**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Basic Configuration settings

Multicast Listener Discovery snooping is available on IPv6 network and performs a similar function to IGMP for IPv4.

You can access the screen by clicking **Configuration** > **IPMC** > **MLD Snooping** > **Basic**.

Menu option	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 to run the SSM service model for the groups in the address range.
Leave Proxy Enabled	Enable MLD leave Proxy. This feature can be used to avoid fowarding 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.
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave Throttling	Enable the fast leave on the port. Enable to limit the number of multicast groups to which a switch port can belong.

1. On the main screen of the Web management UI, click **Configuration** > **IPMC** > **MLD Snooping** > **Basic Configuration**.

2. Compile the MLD-related parameters.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the VLAN Configuration settings

Use the MLD Snooping VLAN Configuration screen to configure MLD snooping and query for a VLAN interface.

You can access the screen by clicking **Configuration** > **IPMC** > **MLD Snooping** > **VLAN Configuration**.

Menu option	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MLD Snooping Enabled	Enable per-VLAN MLD Snooping. Up to 32 VLANs can be selected for MLD Snooping.
MLD Querier Compatibility	Enable the IGMP Querier in the VLAN Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is "MLD-Auto", "Forced-MLDv1", and "Forced MLDv2". The default compatibility value is "MLD-auto".
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255, default robustness variable value is 2.
QI	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 - 31744 seconds, default query interval is 125 seconds.
QRI	Query Response Interval. The maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

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

1. On the main screen of the Web management UI, click **Configuration** > **IPMC** > **MLD Snooping** > **VLAN Configuration**.
2. To create a new MLD VLAN entry, click **Add New MLD VLAN**.
3. To update the displayed table starting from that or the next closest VLAN table match, click **Refresh**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the MLD Configuration settings

Use the MLD Snooping Port Group Filtering Configuration screen to filter specific multicast traffic.

You can access the screen by clicking **Configuration** > **IPMC** > **MLD Snooping** > **Port Group Filtering**.

Menu option	**Description**
Delete	Select to delete the entry. The designated entry will be deleted during the next save.
Port	The logical port for the settings.
Add New Filtering Group	Add a new filtering group.

1. On the main screen of the Web management UI, click **Configuration** > **IPMC** > **MLD Snooping** > **Port Group Filtering**.
2. To add a new entry, click **Add New Filtering Group**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the LLDP settings

Use the LLDP Configuration screen to set the timing parameters for LLDP advertisements and the device information which is advertised.

You can access the screen by clicking **LLDP** > **LLDP**.

Menu option	**Description**
LLDP Parameters	
Tx Interval	The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up to date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 to 32768 seconds.
Tx Hold	Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 to 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 to 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 neighbouring units, signalling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 to 10 seconds.
LLDP Port Configuration	
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 neighbour units is analyzed.
[Tx only]	The switch will drop LLDP information received from neighbours, but will send out LLDP information.
[Disabled]	The switch will not send out LLDP information, and will drop LLDP information received from neighbours.
[Enabled]	The switch will send out LLDP information, and will analyze LLDP information received from neighbours.
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 neighbours' table are decoded. All other TLVs are discarded (unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics). CDP TLVs are mapped onto LLDP neighbours' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours' table. 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 neighbours table. If all ports have CDP awareness disabled, the switch forwards CDP frames received from neighbour devices. If at least one port has CDP awareness enabled all CDP frames are terminated by the switch. **Note:** When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
Port Descr	Optional TLV: When selected, the "port description" is included in LLDP information transmitted.

Sys Name	Optional TLV: When selected, the "system name" is included in LLDP information transmitted.
Sys Capa	Optional TLV: When selected, the "system capability" is included in LLDP information transmitted.
Mgmt Addr	Optional TLV: When selected, the "management address" is included in LLDP information transmitted.

1. On the main screen of the Web management UI, click **Configuration** > **LLDP** > **LLDP**.
2. Set the **LLDP Parameters**.
3. Configure the **LLDP Mode**, **CDP aware**, and **Optional TLVs** parameters.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the LLDP-MED settings

Use the LLDP-MED Configuration screen to set the device information which is advertised for other devices.

You can access the screen by clicking **LLDP** > **LLDP-MED**.

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

Fast start repeat count	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 neighbour has been detected in order share LLDP-MED information as fast as possible to new neighbours. Because there is a risk of an LLDP frame being lost during transmission between neighbours, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbours receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.
Coordinates Location	
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 diretion to either East of the prime meridian or West of the prime meridian.

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

Leading street direction	Leading street direction – Example : N
Trailing street suffix	Trailing street suffix – Example: SW
Street suffix	Street suffix – Example: Ave, Platz.
House no.	House number – Example : 21
House no. suffix	House number suffix. Examples: 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, suit) – 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	Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CMAM or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.
Policies	

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. Policies are only intended for use with applications that have specific "real-time" network policy requirements, such as interactive voice and/or video service. The network policy attributes advertised are: 1. Layer 2 VLAN ID (IEEE 802.1Q) 2. Layer 2 priority value (IEEE 802.1D) 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 type above)
Delete	Select to delete the policy, it will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and will be used when selecting the policies that will 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 signalling (conditional)	For use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice	Support a separate "limited feature-set" voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling (conditional)	For use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the Guest Voice application policy.
5. Softphone Voice	For use by softphone application 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 appliance 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 (conditional)	For use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all of 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 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 the default priority as defined in IEEE 802.1D-2004.
DSCP	DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents the default DSCP value as defined in RFC 2475.

Change the MAC Table settings

Use the MAC Address Table Configuration screen to configure dynamic address learning or to assign static addresses to specific ports.

You can access the screen by clicking **Configuration** > **MAC Table**.

Menu option	Description
Aging Configuration	
Disable Automatic Aging	Do not automatically remove default dynamic entries from the MAC Table after the Aging Time expires.
Aging Time	Specify the number of seconds for the aging time (range is from 10 to 1000000).
MAC Table Learning	
Auto	If the learning mode for a port is greyed out, then another module is in control of the mode and you can't change it. For example, one possible module is MAC-Based Authentication under 802.1X. Perform learning automatically as soon as a frame with an unknown SMAC is received.
Disable	Do not perform learning.
Secure	Only static MAC entries are learned; all other frames are dropped. **Note:** Make sure that the link that manages the switch is added to the Static MAC Table before you change to secure learning mode. Otherwise, the management link is lost and can only to restored by using another non-secure port or by connecting to the switch via the serial interface.

1. On the main screen of the Web management UI, click **Configuration** > **MAC Table**.
2. Configure the MAC Table.
3. If necessary, change the aging time.
4. Specify the learning method for each port.
5. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the VLAN Memberships settings

VLAN provides greater network performance by reducing broadcast traffic. It also provides a high level of network security because traffic must pass through a configured Layer 3 link to reach a different VLAN.

You can monitor and modify the VLAN Membership Configuration for the switch here. Up to 4096 VLANs are supported.

You can access the screen by clicking **Configuration** > **VLANs** > **VLAN Membership**.

Menu option	Description
Delete	Delete a VLAN entry during the next save.
VLAN ID	Specify the ID of this particular VLAN (range is from 1 to 4096).
VLAN Name	Specify the name of the VLAN. The VLAN name can be null. If it is not null, it must contain letters or numbers. You must include at least one letter in a non-null VLAN name. You can edit the VLAN name for the existing VLAN entries or you can add it to the new entries. (Range is from 0 to 32 characters.)
Port Members	A row of check boxes for each port appears for each VLAN ID. Check the box to include a port in a VLAN. Place an X in the box to include a port in a forbidden port list. Uncheck the box to remove a port from a VLAN.

1. On the main screen of the Web management UI, click **Configuration** > **VLANs** > **VLAN Membership**.
2. If necessary, change the default VLAN ID=1.
3. To create a new VLAN group with ID, name, and port members, click **Add New Entry**.
4. To refresh the display table starting from the first entry of the VLAN table, click **Refresh**.
5. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Ports settings

Use the VLAN Port Configuration page to set VLAN attributes for specific interfaces, including processing frames with embedded tags, ingress filtering, accepted frame types, and the Port VLAN ID.

You can access the screen by clicking **Configuration** > **VLANs** > **Ports**.

Menu option	**Description**
EtherType for Custom S-ports	Specify the EtherType used for Custom S-ports. This is a global setting for all the Custom S-ports.
Port	Specify the logical port number of this row.
Port Type	Specify the port type: Unaware, Customer port (C-port), Service Port (S-port), Or Custom Service port (S-custom-port). If the Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress filtering	Enable ingress filtering on a port. This parameter affects VLAN ingress processing. If you enable ingress filtering and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled.
Frame Type	Specify whether the port accepts all frames or only tagged or untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on this port are discarded.
Port VLAN mode	Configure VLAN mode to "None" or Specific." None: a VLAN tag with classified VLAN ID is inserted in frames transmitted on the port.This mode is normally used for ports connected to VLAN-aware switches. Specific: a Port VLAN ID can be configured. Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.
Port VLAN ID	Specify the VLAN identifier for the port (range is from 1 to 4095, and the default is 1). **Note:** The port must be a member of the same VLAN as the Port VLAN ID.
Tc Tag	Specify the egress tagging of a port. Untag_pvid - All VLANs except the configured PVID are tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

1. On the main screen of the Web management UI, click **Configuration** > **VLANs** > **Ports**.
2. Configure the required settings for each interface.
3. To refresh the display table starting from the first entry of the VLAN table, click **Refresh**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change PVLAN Membership settings

A private VLAN provides port-base security and isolation between ports within an assigned VLAN. Data traffic on ports assigned to a private VLAN can only be forwarded to or from uplink ports. Ports isolated in the private VLAN are designated as downlink ports and can only communicate to uplink ports with the same private VLAN.

Use the private VLAN Membership Configuration page to assign ports to a specific private VLAN.

You can access the screen by clicking **Configuration** > **Private VLANs** > **PVLAN Membership**.

Menu option	**Description**
Delete	Delete a private VLAN entry. The entry is deleted during the next save.
Private VLAN ID	Specify the ID of this particular private VLAN.
Port Members	Specify whether ports are members of a private VLAN. A row of check boxes for each port appears 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, uncheck the box. By default, no ports are members, and all boxes are unchecked.

1. On the main screen of the Web management UI, click **Configuration** > **Private VLANs** > **PVLAN Membership**.
2. To add or delete members of any existing PVLAN, or to create a new PVLAN, click **Add New Private VLAN**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Isolation settings

Use the Port Isolation Configuration screen to prevent communications between customer ports within the same private VLAN.

You can access the screen by clicking **Configuration** > **Private VLANs** > Port Isolation.

Menu option	Description
Port Members	Enable port isolation for ports. A check box appears for each port of a private VLAN. When you check a box, port isolation is enabled for the corresponding port. When you uncheck a box, port isolation is disabled for the corresponding port. By default, port isolation is disabled on all ports.

1. On the main screen of the Web management UI, click **Configuration** > **Private VLANs** > **Port Isolation**.
2. Make sure that the checked ports are isolated from each other.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the MAC-based VLAN settings

Use MAC-Based VLAN Membership Configuration to configure VLAN based on MAC addresses. It assigns a VLAN ID for the ingess untagged frame by the source MAC address. If it doesn't match the database, it is assigned by Port VLAN ID.

You can access the screen by clicking **Configuration** > **VCL** > **MAC-based VLAN**.

Menu option	Description
Delete	To delete a MAC-based VLAN entry, check this box and press save. The entry is deleted in the stack.
MAC Address	Specify the MAC Address.
VLAN ID	Specify the VLAN ID.
Port Members	Specify whether to include a port in a MAC-based VLAN. A row of check boxes for each port appears 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, uncheck the box. By default, no ports are members, and all boxes are unchecked.

1. On the main screen of the Web management UI, click **Configuration** > **VCL** > **MAC-based VLAN**.
2. To add a new entry, click **Add New Entry**.
3. Insert the MAC Address and VLAN ID and select the applied ports.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Protocol to Group settings

This function can assign a specific protocol frame into a VLAN group. When a frame is received in a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

You can access the screen by clicking **Configuration** > **VCL** > **Protocol-based VLAN** > **Protocol to Group**.

Menu option	**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 **Note:** After you change the Frame Type field, valid values of the following text field vary depending on the frame type that you selected.
Value	The value that you can enter in the text field depends on the Frame Type. Below is the criteria for three different Frame Types:
[For Ethernet]	When Ethernet is selected as a Frame Type, you can specify an EtherType value. Valid values for EtherType range from 0x0600-0xffff. A valid value in this case is comprised of two different sub-values:
[For LLC]	a. DSAP: 1-byte long string(0x00-0xff) b. SSAP: 1-byte long string(0x00-0xff) A valid value in this case is also composed of two different sub-values:

[For SNAP]	a. OUI: OUI (Organizationally Unique Identifier) is a value in the format xx-xx-xx where each pair (xx) in the string is a hexadecimal value, ranging from 0x00-0xff. b. PID: If the OUI is the 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 the value of the OUI field is 00-00-00, then the value of PID will be the EtherType (0x0600-0xffff). And if the value of OUI is other than 00-00-00, then a valid value for PID will be any value from 0x000 to 0xffff.
Group Name	A valid Group Name is a unique 16-character-long string, consisting of a combination of letters (a-z or A-Z) and integers (0-9). **Note:** Special characters and underscores (_) are not allowed.

1. On the main screen of the Web management UI, click **Configuration** > **VCL** > **Protocol-Based VLAN** > **Protocol to Group**.
2. To add a new entry, click **Add New Entry**.
3. Select the **Frame Type**, **Etype value**, and **Group Name**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Group to VLAN settings

The Group Name to VLAN Mapping Table allows you to add new protocols to Group Name (unique for each group) mapping entries, as well as allow you to see and delete already mapped entries for the switch.

You can access the screen by clicking **Configuration** > **VCL** > **Protocol-based VLAN** > **Group to VLAN**.

Menu option	**Description**
Delete	To delete a Group Name 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 up to 16 characters, which consists of a combination of letters (a-z or A-Z) and integers (0-9). No special character is allowed. Whichever Group Name you map to a VLAN must be present in the Protocol to Group mapping table and must not be already used by any other existing 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, uncheck the box. By default, no ports are members and all boxes are unchecked.

1. On the main screen of the Web management UI, click **Configuration** > **VCL** > **Protocol-Based VLAN** > **Protocol to Group**.
2. To add a new entry, click **Add New Entry**.
3. Select **Frame Type**, **Etype Value**, and **Group Name**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the IP subnet-based VLAN settings

You can configure the IP subnet-based VLAN entries 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.

You can access the screen by clicking **Configuration** > **VCL** > **IP Subnet-based VLAN**.

Menu option	**Description**
Delete	To delete a IP subnet-based VLAN entry, check this box and click save.
VCE ID	Indicates the index of the entry. It is user configurable. Its value ranges from 0-128. If a VCD ID is 0, the application auto-generates the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN entries 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 an 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.

1. On the main screen of the Web management UI, click **Configuration** > **VCL** > **IP Subnet-based VLAN**.
2. To add a new entry, click **Add New Entry**.
3. Set the **VCE ID**, **IP Address**, **subnet Mask**, **VLAN ID**, and **port members**.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Voice VLAN Configuration settings

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

You can access the screen by clicking **Configuration** > **Voice VLAN** > **Configuration**.

Menu option	Description
Mode	Indicates the Voice VLAN mode operation. You must disable the MSTP feature before you enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are: Enable: 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.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.
Port Mode	Indicates the Voice VLAN port mode. Possible port modes are: Disabled: Do not join the 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 the Voice VLAN.
Port Discovery Protool	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. You should enable the LLDP feature before you configure the discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart the auto-detect process. Possible discovery protocols are: OUI: Detect telephony device by OUI address. LLDP: Detect telephony device by LLDP. Both: Both OUI and LLDP.

1. On the main screen of the Web management UI, click **Configuration** > **Voice VLAN** > **Configuration**.
2. Configure any required changes to VoIP setting for the switch or the specific port.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the OUI settings

Use the Voice VLAN OUI Table to set the identity of the Table of VoIP devices in this switch. The maximum number of entries is 16. Modifying The OUI table will restart the auto-detection of OUI process.

You can access the screen by clicking **Configuration** > **Voice VLAN** > **OUI**.

Menu option	Description
Delete	Select 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	Specify the description of OUI address. It describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

1. On the main screen of the Web management UI, click **Configuration** > **Voice VLAN** > **OUI**.
2. To add a new entry, click **Add New Entry**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Classification settings

Use the QoS Ingress Port Configuration screen to set the basic QoS parameters for a port, including the default traffic class, DP Level (IEEE 802.1p), user priority and the drop eligible indicator.

You can access the screen by clicking **Configuration** > **QoS** > **Port classification**.

Menu option	Description
Port	The port number that the configuration below applies to.
QoS Class	Controls the default QoS class, (in other words, the QoS class for frames that are 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. **Note:** If the QoS class has been dynamically changed, then the actual QoS class is shown in parentheses after the configured QoS class.
DP Level	Controls the default Drop Precedence Level. All frames are classified to a DP level. If the port is VLAN aware, the frame is tagged and Tag Class is enabled. Then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default DP level. The classified DP level can be overruled by a QCL entry.

PCP	Controls the default Priority Code Point (PCP). All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default Drop Eligible Indicator (DEI) for untagged frames. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	Shows the classification mode for tagged frames on this port. Disabled: Use the default QoS class and DP level for tagged frames. Enabled: Use the 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 QoS class and DP level.

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Port Classification**.
2. Set the QoS Class priority for each port, DP Level and PCP, DEI for untagged frames.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Policing settings

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 video usually maintains a steady rate of traffic.

You can access the screen by clicking **Configuration** > **QoS** > **Port Policing**.

Menu option	**Description**
Port	The port number that the configuration below applies to.

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

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Port Policing**.
2. Evoke which port needs to enable the QoS Ingress Port Policers and type the Rate limit condition.
3. Scroll down to select the Rate unit.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Scheduler settings

Use the QoS Egress Port Schedulers to show an overview of the Egress Port Scheduling Table, including queue mode and weight. Click Port number to configure.

You can access the screen by clicking **Configuration** > **QoS** > **Port Scheduler**.

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

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Port Scheduler**.
2. On the **Overview** screen, click **port number into Scheduler** setting for a specific port.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Shaping settings

Use the QoS Egress Port shapers to show an overview of the QoS Egress Port Shapers. Include rate of each queue and port. Click the port number to configure.

You can access the screen by clicking **Configuration** > **QoS** > **Port Shaping**.

Menu option	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.
Qn	Shows "disabled" or actual queue shaper rate. For example, 800 Mbps.
Port	Shows "disabled" or actual queue shaper rate. For example, 800 Mbps.

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Port Shaper**.
2. On the **Overview** screen, click port number for the **Shaping** settings for each specific port.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port Tag Remarking settings

Use the QoS Egress Port Tag Remarking screen to show an overview of QoS Egress Port Tag Remarking mode. Click the port number to configure.

You can access the screen by clicking **Configuration** > **QoS** > **Port Tag Remarking**.

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

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Port Tag Remarking**.
2. On the **Overview** screen, click the port number for the **Tag Remarking** settings for each specific port.
3. To apply your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the Port DSCP settings

Use the QoS Port DSCP Configuration page to configure Ingress translation and classification settings and Egress re-writing of Differential Services Code Point (DSCP) values.

You can access the screen by clicking **Configuration** > **QoS** > **Port DSCP**.

Menu option	**Description**
Port	The Port column shows the list of ports thatyou can configure DSCP Ingress and Egress settings for.
Ingress	In Ingress settings, you can change Ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. Translate 2. Classify
[Translate]	To enable the Ingress Translation, select the check box.
[Classify]	The classification for a port can have four different values: Disable: No Ingress DSCP Classification DSCP=0: Classify if incoming (or translated, if enabled) DSCP value is 0. Selected: Classify only the selected DSCP values for which classification is enabled as specified in the DSCP Translation settings. All: Classify all DSCP values.

Egress	Port Egress Rewriting can be one of the following: Disable: No egress rewrite. Enable: Rewrite enabled without remapping. Remap DP Unaware: DSCP from the analyzer is remapped and the frame is remarked with the remapped DSCP value. The remapping DSCP value is always taken from the "DSCP Translation->Egress Remap DP0" table. Remap DP Aware: DSCP from the analyzer is remapped and the frame is remarked with the remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the "DSCP Translation->Egress Remap DP0" table or from the "DSCP Translation->Egress Remap DP1" table.

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Port DSCP**.
2. Set the required **Ingress** and **Egress** parameters.
3. To apply your changes, click **Save**.

To restore the previous settings, click **Reset**.

Change the DSCP-Based QoS settings

Use the DSCP-Based QoS Ingress Classification screen to configure the basic QoS DSCP based QoS Ingress Classificaton settings for all switches.

You can access the screen by clicking **Configuration** > **QoS** > **DSCP-Based QoS**.

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

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **DSCP-Based QoS**.
2. Specify whether the DSCP value is trusted or not and set the corresponding QoS value and DP level for ingress frames.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the DSCP Translation settings

Use the DSCP Translation screen to configure DSCP Translation for Ingress traffic or DSCP remapping for Egress traffic.

You can access the screen by clicking **Configuration** > **QoS** > **DSCP Translation**.

Menu option	Description
DSCP	The maximum number of supported DSCP values is 64 and the valid range of DSCP values is from 0 to 63.
Ingress	Ingress-side DSCP can be first translated to a new DSCP before using the DSCP value for the QoS class and DPL map. There are two configuration parameters for DSCP Translation: 1. Translate 2. Classify
Egress	The following are the configurable parameters for the egress side: 1. Remap DP0: Controls the remapping for frames with DP level 0. 2. Remap DP1: Controls the remapping for frames with DP level 1.

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **DSCP Translation**.
2. Set the required Ingress translation and Egress remapping parameters.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the DSCP Classification settings

Use the DSCP Classification screen to map DSCP values to a QoS class and drop precedence level.

You can access the screen by clicking **Configuration** > **QoS** > **DSCP Classification**.

Menu option	Description
QoS Class	Actual QoS class.
DPL	Actual Drop Precedence Level.
SCP	Select the classified DSCP value (0 to 63).

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **DSCP Classification**.
2. Map **DSCP values** to a corresponding **QoS class** and **DP level**.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the QoS Control List settings

Use the QoS Control List Configuration screen 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.

You can access the screen by clicking **Configuration** > **QoS** > **QoS Control List**.

Menu option	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
SMAC	Display the OUI field of Source MAC address, for example, the first three octet (byte) of MAC address.
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range of 1to 4095 or Any.
PCP	Priority Code Point: Valid values for 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.

Frame Type	Indicates the type of frame to look for on incoming frames. Possible frame types are: Any: The QCE will match all frame type. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPv4 frames. IPv6: The QCE will match only IPv6 frames
DMAC	Specify the type of Destination MAC addresses for incoming frames. Possible values are: Any: All types of Destination MAC addresses are allowed. Unicast: Only Unicast MAC addresses are allowed. Multicast: Only Multicast MAC addresses are allowed. Broadcast: Only Broadcast MAC addresses are allowed. The default value is 'Any'.
DEI	Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1, or Any.
Action	Indicates the classification action taken on an ingress frame if the configured parameters are matched with the frame's content. There are three action fields: Class: Classified QoS class. DPL: Classified Drop Precedence Level. DSCP: Classified DSCP value.
Modification Buttons	[+] Insert a new QCE before the current row. [e] Edit the QCE row. [↑] Move the QCE up the list. [↓] Move the QCE down the list. [X] Delete the QCE. [+] The lowest plus sign adds a new entry at the bottom of the QCE listings.

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **QoS Control List**.
2. Click the **+** button to add a new QoS control list.
3. Scroll all of the parameters and evoke the port member to join the QCE rules
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Storm Control settings

Use the Storm Control Configuration screen to set limitation of broadcast, multi-cast, and unknown uni-cast traffic to control traffic storms when the device is malfunctioning. Traffic storm can degrade the network performance or halt the network.

You can access the screen by clicking **Configuration** > **QoS** > **Storm Control**.

Menu option	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, 1024K, 2048K, 4096K, 8192K, 16384K, or 32768K.

1. On the main screen of the Web management UI, click **Configuration** > **QoS** > **Storm Control**.
2. Enable Storm Control for Broadcast, Multi-cast, and unknown uni-cast, and scroll down to select the Rate value.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the Mirror Configuration settings

Use the Mirror Configuration screen to mirror traffic from any source port to a target port.

You can access the screen by clicking **Configuration** > **Mirroring**.

Menu option	Description
Port	The logical port for the settings is 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, the mode for the selected mirror port is limited to Disabled or Rx only.

1. On the main screen of the Web management UI, click **Configuration** > **Mirroring**.
2. Select the destination port that all mirrored traffic is sent to.
3. Set the mirror mode on and of the source ports that will be mirrored.
4. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the UPnP settings

Use The UPnP Configuration page to setup UPnP. Universal Plug and Play is a set of protocols that allows devices to deploy easily.

You can access the screen by clicking **Configuration** > **UPnP**.

Menu option	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 of 1 to 255.
Advertising Duration	The duration, carried in SSDP packets, is used to inform a control point or control points how often 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, it is recommended to refresh advertisements 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.

1. On the main screen of the Web management UI, click **Configuration** > **UPnP**.
2. Set the required UPnP related parameters.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Change the sFlow settings

sFlow is an industry standard technology for monitoring switched networks through the random sampling of packets on switch ports and time-based sampling of port counts. The sampled packets and counters are sent as sFlow UDP datagrams to a central network traffic monitoring server. The central server is called an sFlow receiver or sFlow collector. This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (also known as the sFlow collector) and configuration of the per-port flow and counter samplers.

You can access the screen by clicking **Configuration** > **sFlow**.

Menu option	Description
Receiver Configuration	
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 unconfigured/unclaimed, Owner contains <none>. If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>. If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver. If sFlow is configured through SNMP, all controls except for the Release-button are disabled to avoid inadvertent reconfiguration.
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 it is 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 clock 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.The valid range is 200 to 1468 bytes, with the default being 1400 bytes.
Port Configuration	
Port	The port number that the configuration below applies to.
Flow Sampler Enabled	Enables/disables flow sampling on this port.

Flow Sampler Sampling	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. The valid range is 14 to 200 bytes, with the 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.

1. On the main screen of the Web management UI, click **Configuration** > **sFlow**.
2. Set the required sFlow related parameters.
3. To save your settings, click **Save**.

To restore the previous settings, click **Reset**.

Changing the Monitor settings

This section describes how to monitor all of the basic functions, including configuration, the system log, traffic views, and the switch or port states.

Change the Information settings

Use the System Information screen to verify the firmware and hardware versions. It also displays the system contact, device name, location, and system uptime.

You can access the screen by clicking **Monitor** > **System** > **Information**.

Menu option	**Description**
Contact	Displays the system contact configured in Configuration | System | Information | System Contact.
Name	Displays the system name configured in Configuration | System | Information | System Name.
Location	Displays the system location configured in Configuration | System | Information | System Location.
MAC Address	Displays the MAC Address of the switch.
Chip ID	Displays the Chip ID of the switch.
System Date	Displays the current (GMT) system time and date. The system time is obtained through the timing server running on the switch, if any.
System Uptime	Displays the period of time that the device has been operational.
Software Version	Displays the software version of the switch.
Software Date	Displays the date when the switch software was produced.

1. On the main screen of the Web management UI, click **Monitor** > **System** > **Information**.
2. To manually refresh the page information, click **Refresh**.
3. To automatically update the page information, select the **Auto-refresh** check box.

Change the CPU Load settings

This screen displays the CPU load, using an SVG graph. The load is measured as average over the last 100 ms, 1 second, and 10 seconds intervals. The last 120 samples are graphed and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support SVG format. Consult the SVG wiki for more information on browser support.

1. On the main screen of the Web management UI, click **Monitor** > **System** > **CPU Load**.
2. By default, the **Auto-refresh** check box is selected to automatically update the page information.

Change the Log settings

Use the System Log Information page to display event messages.

You can access the screen by clicking **Monitor** > **System** > **Log**.

Menu option	Description
ID	Event log ID (>=1).
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.
Buttons	Auto-refresh: Select this check box to enable an automatic refresh of the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system 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.

<table>
<tr><td>Buttons (cont'd)</td><td>>>: Updates the system log entries, starting from the last entry currently displayed.
>>|: Updates the system log entries, ending at the last available entry ID.</td></tr>
</table>

1. On the main screen of the Web management UI, click **Monitor** > **System** > **Log**.
2. Specify the different level to show for the log.
3. To automatically update the system log, select the **Auto-refresh** check box.
4. To clear the log, click **Clear**.

Change the Detailed Log settings

Use the Detailed System log information screen to display the detail event log.

You can access the screen by clicking **Monitor** > **System** > **Detailed Log**.

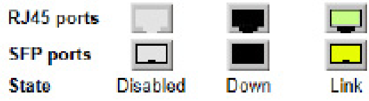
<table>
<tr><th>Menu option</th><th>Description</th></tr>
<tr><td>ID</td><td>The event log ID.</td></tr>
<tr><td>Message</td><td>The detailed message of the system log entry.</td></tr>
<tr><td>Buttons</td><td>Refresh: Updates the system log entries, starting from the current entry ID.
|<<: Updates the 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.</td></tr>
</table>

1. On the main screen of the Web management UI, click **Monitor** > **System** > **Detailed Log**.
2. Specify the detailed system log.

Change the Detailed Log settings

The Port State screen provides an overview of the current state of all ports. You can click a port's icon to get detailed statistics for the port.

You can access the screen by clicking **Monitor** > **Ports** > **State**.

Menu option	Description
Port State	The port states are as follows:  RJ45 ports SFP ports State Disabled Down Link
Buttons	Auto-refresh: Select this check box to enable an automatic refresh of the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. On the main screen of the Web management UI, click **Monitor** > **Ports** > **State**.
2. Display the current state of each port.
3. To automatically update the switch's port state, select the **Auto-refresh** check box.

Change the Traffic Overview settings

Use the Port Statistics Overview screen to display an overview of incoming and outgoing packets for each port.

You can access the screen by clicking **Monitor** > **Ports** > **Traffic Overview**.

Menu option	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 process.
Buttons	Auto-refresh: Select this check box to enable an automatic refresh of the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system log entries.

1. On the main screen of the Web management UI, click **Monitor** > **Ports** > **Traffic Overview**.
2. To automatically update the switch's port state, select the **Auto-refresh** check box.
3. To reset all of the data, click **Clear**.

Change the QoS Statistics settings

Use the Queuing Counters screen to display the number of packets processed by each port.

You can access the screen by clicking **Monitor** > **Ports** > **QoS Statistics**.

Menu option	**Description**
Port	The logical port for the settings contained in the same row.
Qn	There are eight QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.
Buttons	Auto-refresh: Select this check box to enable an automatic refresh of the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system log entries.

1. On the main screen of the Web management UI, click **Monitor** > **Ports** > **QoS Statistics**.
2. To reset all of the data, click **Clear**.

3. To automatically update the switch's port state, select the **Auto-refresh** check box.

Change the QCL Status settings

Use the QoS Control List Status to show the QCE configured for different users or software modules, and see whether there is a conflict.

You can access the screen by clicking **Monitor** > **Ports** > **QCL Status**.

Menu option	Description
Users	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame	Indicates the type of frame to look for on incoming frames. Possible frame types are: Any: The QCE will match all frame types. Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC: Only (LLC) frames are allowed. SNAP: Only (SNAP) frames are allowed. IPv4: The QCE will match only IPV4 frames. IPv6: The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on an ingress frame if the configured parameters match the frame's content. There are three action fields: Class: Classified QoS class; if a frame matches the QCE, the frame will be put in the queue. DPL: Drop Precedence Level; if a frame matches the QCE, then the DP level is set to the value displayed under the DPL column. DSCP: If a frame matches the QCE, then DSCP is classified with the value displayed under the DSCP column.

Conflict	Displays the conflict status of QCL entries, as hardware resources are shared by multiple applications. Resources required to add a QCE might not be available. In this case it shows the conflict status as **Yes**; otherwise, it is always **No**. You can resolve a conflict by pressing the **Resolve Conflict** button. This releases the hardware resources required to add a QCL entry.
Buttons	In the QCL status drop-down list, click a status. Auto-refresh: Select this check box to enable an automatic refresh of the page at regular intervals. Refresh: Click to release the resources required to add a QCL entry. You can use this button when the conflict status for any QCL entry is Yes. Resolve Conflict: Flushes all of the system log entries.

1. On the main screen of the Web management UI, click **Monitor** > **Ports** > **QCL Status**.
2. In the drop-down list, click the user type to display.
3. If any of the entries show a conflict, click **Resolve Conflict** to resolve the conflict. Click **Refresh** to make sure that the conflict was resolved.

Change the Detailed Statistics settings

Use the Detailed Port Statistics screen to display detailed statistics on the network. All values have been accumulated since the system bootup.

You can access the screen by clicking **Monitor** > **Ports** > **Detailed Statistics**.

Menu option	**Description**
Receive Total and Transmit Total	
Rx and Tx packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	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	
Rx Drops	The number of frames dropped due to lack of received 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 a valid CRC.
Rx Oversize	The number of long[2] frames received with a valid CRC.
Rx Fragments	The number of short[1] frames received with an invalid CRC.
Rx Jabber	The number of long[2] frames received with an invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
[1] Short frames are frames that are smaller than 64 bytes. [2] Long frames are frames that are longer than the configured maximum frame length for this port.	
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.

Buttons	Auto-refresh: Select this check box to enable an automatic refresh of the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Resolve Conflict: Flushes all of the system log entries.

1. On the main screen of the Web management UI, click **Monitor** > **Ports** > **Detailed Statistics**.
2. Select a port number to display the detailed statistics for the port.

Change the ACL Status settings

Use the Access Management Statistics screen to monitor management traffic through five interfaces, including HTTP, HTTPS, SNMP, TELNET, and SSH.

You can access the screen by clicking **Monitor** > **Ports** > **ACL Status**.

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

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Access Management Statistics**.
2. To refresh the screen periodically, click **Auto-refresh**.

Change the Switch settings

This screen shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from 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 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.

You can access the screen by clicking **Monitor** > **Security** > **Network** > **Port Security** > **Switch**.

Menu option	**Description**
User Module Legend	
User Module Name	The full name of a module that may request Port Security services.
Abbr	A one-letter abbrevation of the user module. This is used in the Users column in the port status table.
Port Status	
Port	The port number that the status applies to. Click the port number to see the status for this paritcular 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. A letter indicates that the user module abbreviated by that letter 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.

State (cont'd)	Limit Reached: The Port Security service is enabled by at least the Limit Control user module. Also, 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 exceed. No MAC addresses can be learned on that port until it is administratively re-opened on the Limit Control configuration Webpage.
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 shows a dash (-). If the Limit Control user module is not enabled on the port, the Limit column shows a dash (-).

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **Port Security** > **Switch**.
2. To refresh the screen periodically, click **Auto-refresh**.

Change the Port settings

Use the Port Security Port Status screen to view the entries that are authorized by port security, including the MAC Address, VLAN ID, Time of Addition, and Aging time or Hold state.

You can access the screen by clicking **Monitor** > **Security** > **Network** > **Port Security** > **Port**.

Menu option	**Description**
MAC Address and VLAN ID	Indicates 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 is not 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 periodically checks that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the Mac address is removed from the MAC table. Otherwise, a new age period begins. If aging is disabled or a user module has decided to hold the MAC address idenfinitely, a dash (-) is shown.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **Port Security** > **Port**.
2. To refresh the page periodically, select the **Auto-refresh** check box.

Change the Switch settings

Use the Network Access Server Switch Status screen to show the port status for authentication services, including the 802.1X security state, last source address, last ID, QoS Class, and Port VLAN ID.

You can access the screen by clicking **Monitor** > **Security** > **Network** > **NAS** > **Switch**.

Menu option	**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	Specifies the user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication. Also specifies 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. If the Port VLAN ID is not overridden by NAS, the field is blank. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **NAS** > **Switch to display information about Port status for authentication services**.
2. To refresh the screen periodically, click **Auto-refresh**.

Change the NAS Statistics Port settings

Use the NAS Statistics Port screen to show the authentication statistics for a specific port.

You can access the screen by clicking **Monitor** > **Security** > **Network** > **NAS** > **Port**.

Menu option	**Description**
Port State	
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port Vlan ID

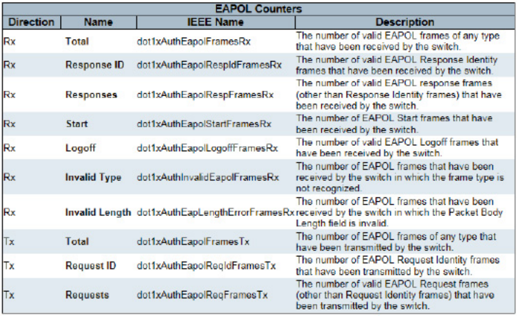
The VLAN ID that NAS has put the port in. If the Port VLAN ID is not overridden by NAS, then the field is blank. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

EAPOL Counters

The supplicant frame counters pictured below are available for the following adminstrative states:

- Force Authorized
- Force Unauthorized
- Port-Based 802.1x
- Single 802.1X
- Multi 802.1X



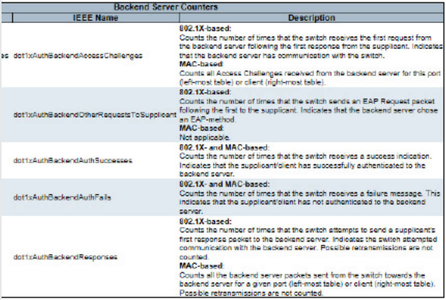
EAPOL Counters

Direction	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Backend Server Counters

The backend (RADIUS) frame counters pictured below are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.



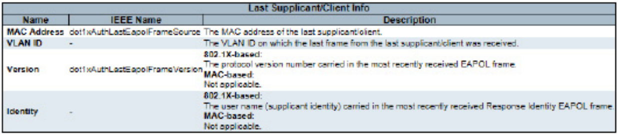
Backend Server Counters

	IEEE Name	Description
es	dot1xAuthBackendAccessChallenges	**802.1X-based:** Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based:** Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based:** Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based:** Not applicable.
	dot1xAuthBackendAuthSuccesses	**802.1X- and MAC-based:** Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
	dot1xAuthBackendAuthFails	**802.1X- and MAC-based:** Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
	dot1xAuthBackendResponses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/ Client Info

Information about the last supplicant/client that attempted to authenticate is pictured below. This information is available for the following adminstrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.



Last Supplicant/Client Info

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based:** The protocol version number carried in the most recently received EAPOL frame. **MAC-based:** Not applicable.
Identity	-	**802.1X-based:** The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based:** Not applicable.

Selected Counters

Selected Counters	The Selected Counters table is visible when the port is in one of the following adminstrative states: • Multi 802.1X • MAC-based Auth. The table is identical to and is placed next to the Port Counters table. It won't display any information 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	
Identity	Displays 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 displays **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 displays **No clients attached**.
VLAN ID	This column holds the VLAN ID of the corresponding client that is currently secured through the Port Security module.
State	The client can be authenticated or unauthenticated. In authenticated state, it is allowed to forward frames on the port, while in unauthenticated state it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails, the client will remain in the unauthenticated state until the Hold Time expires.
Last Authentication	Shows the date and time of the last successful or unsuccessful authentication of the client.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **NAS** > **Switch to display information about Port status for authentication services**.
2. To periodically refresh the page information, click **Auto-refresh**.

Change the ACL Status settings

Each row describes the defined ACE (Access Control Entry). It's a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACE is 256 on each switch.

You can access the screen by clicking **Monitor** > **System** > **Network** > **ACL Status**.

Menu option	**Description**
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress ports. Port: The ACE will match a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. **Note:** an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.

Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When a **Disabled** message is displayed, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Indicates frames matching the ACE are redirected to the port number. The allowed values are **Disabled** or a specific port number. When a **Disabled** message is displayed, the port redirect 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**.
CPU	Indicates the forward packet that matched the specific ACE to CPU.
CPU Once	Indicates the forward first packet that matched the specific ACE to CPU.
Counter	Indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE was not applied to the hardware due to hardware limitations.
Buttons	In the QCL status drop-down list, click a status. Auto-refresh: Select this check box to automatically refresh the page. Automatic refresh occurs at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **ACL Status**.
2. In the drop-down list, click a software module.

Change the Snooping Statistics settings

Use the DHCP Snooping Port Statistics page to show statistics for various types of DHCP protocol packets.

You can access the screen by clicking **Monitor** > **Security** > **Network** > **DHCP** > **Snooping Statistics**.

Menu option	Description
Rx and Tx Discover	Indicates the number of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	Indicates the number of offer (option 53 with value 2) packets received and transmitted.
Rx and Tx Request	Indicates the number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	Indicates the number of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	Indicates the number of ACK (option 53 with value 5) packets received and transmitted.
Rx and Tx NAK	Indicates the number of NAK (option 53 with value 6) packets received and transmitted.
Rx and Tx Release	Indicates the numer of release (option 53 with value 7) packets received and transmitted.
Rx and Tx Inform	Indicates the number of Inform (option 53 with value 8) packets received and transmitted.
Rx and Tx Query	Indicates the number of Query (option 53 with value 10) packets received and transmitted.
Rx and Tx Unassigned	Indicates the number of Unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Unknown	Indicates the number of Unknown (option 53 with value 12) packets received and transmitted.
Rx and Tx Active	Indicates the number of Active (option 53 with value 13) packets received and transmitted.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **DHCP** > **Snooping Statistics**.
2. In the drop-down list, click a port number.

Change the Relay Statistics settings

Use the DHCP Relay Statistics screen to show statistics for the DHCP Relay service supported by this switch and DHCP Relay clients.

You can access the screen by clicking **Monitor** > **Security** > **Network** > **DHCP** > **Relay Statistics**.

Menu option	**Description**
Server Statistics	
Transmit to Server	Indicates the number of packets that are relayed from client to server.
Transmit Error	Indicates the number of packets that resulted in errors while being sent to clients.
Receive from Server	Indicates the number of packets received from the server.
Receive Missing Agent Option	Indicates the number of packets received without agent information options.
Receive Missing Circuit ID	Indicates the number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	Indicates the number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	Indicates the number of packets whose Circuit ID option did not match the known circuit ID.
Receive Bad Remote ID	Indicates the number of packets whose Remote ID option did not match the known Remote ID.
Client Statistics	
Transmit to Client	Indicates the number of relayed packets from the server to the client.
Transmit Error	Indicates the number of the packet that resulted in an error while being sent to the servers.
Receive from Client	Indicates the number of received packets from the server.
Receive Agent Option	Indicates the number of received packets with a relay agent information option.
Replace Agent Option	Indicates the number of packets which were replaced with a relay agent information option.

Keep Agent Option	Indicates the number of packets whose relay agent information was retained.
Drop Agent Option	Indicates the number of packets that were dropped which were received with relay agent information.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **DHCP** > **Relay Statistics**.
2. To automatically refresh the screen, select the **Auto-refresh** check box.

Change the ARP Inspection settings

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

You can access the screen by clicking **Monitor** > **Security** > **Network** > **ARP Inspection**.

Menu option	**Description**
Port	Indicates the switch port number for which the entries are displayed.
VLAN ID	Indicates the VLAN ID in which the ARP traffic is permitted.
MAC Address	Indicates the user MAC address of the entry.
IP Address	Indicates the user IP address of the entry.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **ARP Inspection**.
2. Change the entry number to display more entries.
3. To automatically refresh the screen, select the **Auto-refresh** check box.

Change the IP Source Guard settings

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

You can access the screen by clicking **Monitor** > **Security** > **Network** > **IP Source Guard**.

Menu option	Description
Port	Indicates the switch port number for which the entries are displayed.
VLAN ID	Indicates the VLAN ID in which the ARP traffic is permitted.
MAC Address	Indicates the source MAC address.
IP Address	Indicates the user IP address of the entry.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Network** > **ARP Inspection**.
2. Change the entry number to display more entries.
3. To automatically refresh the screen, select the **Auto-refresh** check box.

Change the RADIUS Overview settings

Use the RADIUS Overview screen to display a list of configured RADIUS servers.

You can access the screen by clicking **Monitor** > **Security** > **AAA** > **RADIUS Overview**.

Menu option	Description
#	Indicates the RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	Indicates the IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.

Status	Indicates the current status 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.
Buttons	In the QCL status drop-down list, click a status. Auto-refresh: Select this check box to automatically refresh the page. Refresh: Updates the system log entries, starting from the current entry ID.

Change the RADIUS Details settings

Use the RADIUS Details page to display statistics for RADIUS servers.

You can access the screen by clicking **Monitor** > **Security** > **AAA** > **RADIUS Details**.

Menu option	**Description**
Receive packets	Indicates the counters of Receive Packets, including the following parameters: (Access Accepts, Access Rejects, Access Challenges, Malformed Access Responses, Bad Authenticators, Unknown Types, Packets Dropped).
Transmit packets	Indicates the counters of Transmit Packets, including the following parameters: (Access Requests, Access Retransmissions, Pending Requests, Timeouts).

Other Info.	IP Address: Shows the IP Address of the RADIUS server State: Shows the state of the RADIUS server Round-Trip Time: Shows the handshake time between the RADIUS server and clients
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system log entries.

Change the RMON Statistics settings

This screen provides an overview of RMON Statistics entries.

You can access the screen by clicking **Monitor** > **Security** > **Switch** > **RMON** > **Statistics**.

Menu option	Description
ID	Indicates the index of Statistics entry.
Data Source (if Index)	Indicates the port ID which wants to be monitored.
Drop	Indicates the total number of events in which packets were dropped by the probe due to lack of resources.
Octets	Indicates the total number of octets of data (including those in bad packets) received on the network.
Pks	Indicates the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	Indicates the total number of good packets received that were directed to the broadcast address.
Multi-cast	Indicates the total number of good packets received that were directed to a multicast address.
CRC Errors	Indicates the total number of packets received that had a length (excluding framing bits, but including FCS octets) of 64 to 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	Indicates the total number of packets received that were less than 64 octets.
Over-size	Indicates the total number of packets received that were longer than 1518 octets.
Frag.	Indicates the number of frames whose size is less than 64 octets received with an invalid CRC.
Jabb.	Indicates the number of frames whose size is larger than 64 octets received with an invalid CRC.
Coll.	Indicates the best estimate of the total number of collisions on this Ethernet segment.
64	Indicates the total number of packets (including bad packets) received that were 64 octets in length.
64~127	Indicates the total number of packets (including bad packets) received that were 65 to 127 octets in length.
128~255	Indicates the total number of packets (including bad packets) received that were 128 to 255 octets in length.
256~511	Indicates the total number of packets (including bad packets) received that were 256 to 511 octets in length.
512~1023	Indicates the total number of packets (including bad packets) received that were 512 to 1023 octets in length.
1024~1588	Indicates the total number of packets (including bad packets) received that were 1024 to 1588 octets in length.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Switch** > **RMON** > **Statistics**.
2. To automatically refresh the screen, select the **Auto-refresh** check box.

Change the RMON History settings

This screen provides an overview of RMON History entries.

You can access the screen by clicking **Monitor** > **Security** > **Switch** > **RMON** > **History**.

Menu option	Description
History Index	Indicates the index of the history control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	Indicates the value of sysUPTime at the start of the interval over which this sample was measured.
Drop	Indicates the the total number of events in which packets were dropped by the probe due to lack of resources.
Octets	Indicates the total number of octets of data (including those in bad packets) received on the network.
Pks	Indicates the total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	Indicates the total number of good packets received that were directed to the broadcast address.
Multi-cast	Indicates the total number of good packets received that were directed to a multicast address.
CRC Errors	Indicates the total number of packets received that had a length (excluding framing bits but including FCS octets) of 64 to1518 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	Indicates the total number of packets received that were less than 64 octets.
Over-size	Indicates the total number of packets received that were longer than 1518 octets.
Frag.	Indicates the number of frames which size is less than 64 octets received with an invalid CRC.

Jabb.	Indicates the number of frames which size is larger than 64 octets received with an invalid CRC.
Coll.	Indicates the best estimate of the total number of collisions on this Ethernet segment.
Utilization	Indicates the best estimate of the mean physical layer network utilization on this interface during this sampling interval in hundredths of a percent.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Switch** > **RMON** > **History**.
2. To automatically update the screen information, select the **Auto-refresh** check box.

Change the Alarm settings

This screen provides an overview of RMON Alarm entries.

You can access the screen by clicking **Monitor** > **Security** > **Switch** > **RMON** > **Alarm**.

Menu option	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	Indicates the method of sampling of the selected variable, and calculates the value to be compared against the thresholds.
Value	Indicates the value of the statistic during the last sampling period.
Startup Alarm	Indicates the alarm that may be sent when this entry is first set to valid.
Rising Threshold	Indicates the rising threshold value.
Rising Index	Indicates the rising event index.
Falling Threshold	Indicates the falling threshold value.
Falling Index	Indicates the falling event index.

1. On the main screen of the Web management UI, click **Monitor** > **Security** > **Switch** > **RMON** > **Alarm**.
2. To automatically update the page information, select the **Auto-refresh** check box.

Change the System Status settings

Use the LACP System Status screen to display an overview of LACP groups.

You can access the screen by clicking **Monitor** > **LACP** > **System Status**.

Menu option	**Description**
Aggr ID	Indicates the Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as i**sid:aggr-id** and for GLAGs as **aggr-id**.
Partner System ID	Indicates the system ID (MAC address) of the aggregation partner.
Partner Key	Indicates the key that the partner has assigned to this aggregation ID.
Last Changed	Indicates the time since this aggregation changed.
Local Ports	Indicates which ports are a part of this aggregation for this switch.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. To see an overview of the LACP group active on the switch, on the main screen of the Web management UI, click **Monitor** > **LACP** > **System Status**.

Change the Port Status settings

Use the LACP Port Status screen to display information on the LACP groups active on each port.

You can access the screen by clicking **Monitor** > **LACP** > **Port Status**.

Menu option	Description
Port LACP	Indicates the switch port number. **Yes** indicates that LACP is enabled and the port link is up. **No** indicates that LACP is not enabled or that the port link is down. **Backup** indicates that the port could not join the aggregation group but will join if other ports leave. Meanwhile its LACP status is disabled
Key	Indicates the key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	Indicates the Aggregation ID assigned to this aggregation group.
Partner System ID	Indicates the partner's System ID (MAC address).
Partner Port	Indicates the partner's port number connected to this port.
Partner Prio	Indicates the partner's port priority.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID

1. To display the LACP status for local ports, on the main screen of the Web management UI, click **Monitor** > **LACP** > **Port Status**.

Change the Port Statistics settings

Use the LACP Port Statistics screen to display statistics on LACP control packets across each port.

You can access the screen by clicking **Monitor** > **LACP** > **Port Statistics**.

Menu option	**Description**
Port	Indicates the switch port number.
LACP Received	Indicates how many LACP frames have been received at each port.
LACP Transmitted	Indicates how many LACP frames have been sent from each port.
Discarded	Indicates how many unknown or illegal LACP frames have been discarded at each port.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system log entries.

1. To display all of the LACP port statistics for local ports, on the main screen of the Web management UI, click **Monitor** > **LACP** > **Port Statistics**.

Change the Loop Protection settings

Use the Loop Protection Status screen to display the loop status.

You can access the screen by clicking **Monitor** > **Loop Protection**.

Menu option	**Description**
Port	Indicates the switch port number of the logical port.
Action	Indicates the currently configured port action.
Transmit	Indicates the currently configured port transmit mode.
Loops	Indicates the number of loops detected on this port.

Status	Indicates the current loop protection status of the port.
Loop	Indicates whether a loop is currently detected on the port.
Time of Last Loop	Indicates the time of the last loop event detected.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. To display all of the LACP port statistics for each port, on the main screen of the Web management UI, click **Monitor** > **Loop Protection**.

Change the Bridge Status settings

Use the Monitor menu to display Spanning Tree bridge status, CIST port status for physical ports on the current switch, and statistics for STP packets. Use the STP Detailed Bridge Status screen to display STA information on the global bridge and individual ports.

You can access the screen by clicking **Monitor** > **Spanning Tree** > **Bridge Status**.

Menu option	**Description**
Bridge Instance	Indicates the bridge instance. For example, CIST, MST1, and so on.
Bridge ID	Indicates the bridge ID of the Bridge instance.
Root ID	Indicates the bridge ID of the currently elected root bridge.
Root Port	Indicates the switch port currently assigned the root port role.
Root Cost	Indicates the root path cost. For the root bridge, this is zero. For all of the other bridges, this is the sum of the port path costs on the lowest cost path to the root bridge.
Regional Root	Indicates the Bridge ID of the currently elected regional root bridge inside the MSTP region of this bridge (for the CIST instance only).
Internal Root Cost	Indicates the regional root path cost. For the regional root bridge this is zero. For all of the other CIST instances in the same MSTP region, it is the sum of the internal port path costs on the lowest cost path to the internal root bridge (for the CIST instance only).

Topology Flag	Indicates the current state of the topology change flag of this bridge instance.
Topology Change Count	Indicates the number of times where the topology change flag has been set during a one-second interval.
Topology Last	Indicates the time that has passed since the topology flag was last set.
CIST Ports & Aggregations State	
Port	Indicates the switch port number of the logical STP port.
Port ID	Indicates the port ID as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
Role	Indicates the current STP port role. The port role can be one of the following values: AlternatePort, BackupPort, RootPort, and DesignatedPort.
State	Indicates the current STP port state. The port state can be one of the following values: Discarding, Learning, Forwarding.
Path Cost	Indicates the current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.
Edge	Indicates the current STP port (operational) Edge Flag. An Edge Port is a switch port in which no bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State since there is no possibility of it participating in a loop.
Point2Point	Indicates the current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
Uptime	Indicates the time since the bridge port was last initialized.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. To display the information, on the main screen of the Web management UI, click **Monitor** > **Spanning Tree** > **Bridge Status**.

Change the Port Status settings

Use the STP Port Status screen to display the STP CIST port status for physical ports.

You can access the screen by clicking **Monitor** > **Spanning Tree** > **Port Status**.

Menu option	Description
Port	Indicates the switch port number of the logical STP port.
CIST Role	Indicates the current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, BackupPort, RootPort, and DesignatedPort Disabled.
CIST State	Indicates the current STP port state of the CIST port. The port state can be one of the following values: Discarding, Learning, Forwarding.
Uptime	Indicates the time since the bridge port was last initialized.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. To display the STP Port Status, on the main screen of the Web management UI, click **Monitor** > **Spanning Tree** > **Port Status**.

Change the Port Statistics settings

Use the STP Port Statistics screen to display statistics on Spanning Tree Protocol packets across each port.

You can access the screen by clicking **Monitor** > **Spanning Tree** > **Port Statistics**.

Menu option	Description
Port	Indicates the switch port number of the logical STP port.
RSTP	Indicates the number of RSTP Configuration BPDU's received/transmitted on the port.
STP	Indicates the number of legacy STP Configuration BPDU's received/transmitted on the port.

TCN	Indicates the number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	Indicates the number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	Indicates the number of illegal Spanning Tree BPDUs received (and discarded) on the port.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system log entries.

1. To display the STP Port Statistics, on the main screen of the Web management UI, click **Monitor** > **Spanning Tree** > **Port Statistics**.

Change the Statistics settings

Use the MVR Group Information screen to display statistics for IGMP protocol message used by the MVR.

You can access the screen by clicking **Monitor** > **MVR** > **Statistics**.

Menu option	**Description**
VLAN ID	Indicates the Multicast VLAN ID.
IGMP/MLD Queries Received	Indicates the number of Received Queries for IGMP and MLD, respectively.
IGMP/MLD Queries Transmitted	Indicates the number of Transmitted Queries for IGMP and MLD, respectively.
IGMPv1 Joins Received	Indicates The number of Received IGMPv1 Join messages.
IGMPv2/MLDv1 Reports Received	Indicates the number of Received IGMPv2 Join and MLDv1 Report messages. respectively.
IGMPv3/MLDv2 Reports Received	Indicates the number of Received IGMPv1 Join and MLDv2 Report messages, respectively.
IGMPv2/MLDv1 Leaves Received	Indicates the number of Received IGMPv2 Leave and MLDv1 Done messages, respectively

IGMPv3/MLDv2 Reports Received	Indicates the number of Received IGMPv1 Join and MLDv2 Report messages, respectively.
IGMPv2/MLDv1 Leaves Received	Indicates the number of Received IGMPv2 Leave and MLDv1 Done messages, respectively.

1. To display information for MVR Statistics, on the main screen of the Web management UI, click **Monitor** > **MVR Statistics**.

Change the MVR Channel Groups settings

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

You can access the screen by clicking **Monitor** > **MVR** > **MVR Channel Groups**.

Menu option	Description
VLAN ID	Indicates the VLAN ID of the group.
Groups	Group ID of the group displayed.
Port Members	Indicate the ports under this group.

1. To display the MVR Channel Groups information, on the main screen of the Web management UI, click **Monitor** > **MVR Channel Groups**.

Change the MVR SFM Information settings

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

You can access the screen by clicking **Monitor** > **MVR** > **MVR SFM Information**.

Menu option	Description
VLAN ID	Indicates the VLAN ID of the group.
Groups	Indicates the group ID of the group displayed.
Port	Indicates the switch port number.

Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be **Include** or **Exclude**.
Source Address	Indicates the IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128. When there is not any source filtering address, the text **None** is displayed in the **Source Address** field.
Type	Indicates the type (**Allow** or **Deny**).
Hardware Filter/ Switch	Indicates whether the data plan destined to the specific group address from the source IPv4/IPv6 address could be handled by the chip or not.

1. To display the MVR SFM Information, on the main screen of the Web management UI, click **Monitor** > **MVR SFM Information**.

Change the Snooping Status settings

Use the IGMP SNOOPING screen to display IGMP Snooping statistics, router port status, and group information. Use the IGMP Snooping Status page to display IGMP querier status, and snooping statistics for each VLAN.

You can access the screen by clicking **Monitor** > **IPMC** > **IGMP Snooping** > **Status**

Menu option	**Description**
VLAN ID	Indicates the VLAN ID of the entry.
Querier Version	Indicates the current Working Querier Version.
Host Version	Indicates the current Working Host Version.
Querier Status	Indicates the Querier status as **ACTIVE** or **IDLE**. **DISABLE** denotes that the specific interface is administratively disabled.
Queries Transmitted	Indicates the number of Transmitted Queries.
Queries Received	Indicates the number of Received Queries.
V1 Reports Received	Indicates the number of Received V1 Reports.
V2 Reports Received	Indicates the number of Received V2 Reports.

V3 Reports Received	Indicates the number of Received V3 Reports.
V2 Leaves Received	Indicates the number of Received V2 Leaves.
Router Port	Indicates 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 that the specific port is configured to be a router port. Dynamic denotes that the specific port is learnt to be a router port. Both denote that the specific port is configured or learnt to be a router port.
Port	Indicates the switch port number.
Status	Indicates whether a specific port is a router port or not.
Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. Clear: Flushes all of the system log entries.

1. To display the IGMP Snooping Status information, on the main screen of the Web management UI, click **Monitor** > **IPMC Snooping** > **Status**.

Change the Groups Information settings

Use the IGMP Snooping Group Information screen to display the port member of each service group.

You can access the screen by clicking **Monitor** > **IPMC** > **IGMP Snooping** > **Groups Information**.

Menu option	**Description**
VLAN ID	Indicates the VLAN ID of the entry.
Groups	Indicates the group address of the displayed group.
Port Members	Indicates the ports under this group.

Buttons	Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID. |<< : Updates the table starting with the first entry in the IGMP group table. <<: Updates the table starting with the entry after the last entry current displayed.

1. To display the group port members, on the main screen of the Web management UI, click **Monitor** > **IPMC** > **IGMP Snooping** > **Groups**.

Change the IPv4 SFM Information settings

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, followed by port. Different source addresses belonging to the same group are treated as a single entry.

You can access the screen by clicking **Monitor** > **IPMC** > **IGMP Snooping** > **Groups Information**.

Menu option	**Description**
VLAN ID	Indicates the VLAN ID of the entry.
Group	Indicates the group address of the displayed group.
Port	Indicates the switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be **Include** or **Exclude**.
Source Address	Indicates the IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the Type: **Allow** or **Deny**.
Hardware Filter/ Switch	Indicates whether the data plane destined to the specific group address from the source IPv4 address could be handled by the chip or not.

1. To display the IGMP SFM information, on the main screen of the Web management UI, click **Monitor** > **IPMC** > **IGMP Snooping** > **IPv4 SFM Information**.

Change the MLD Status settings

This screen provides MLD Snooping status.

You can access the screen by clicking **Monitor** > **IPMC** > **MLD** > **Status**.

Menu option	Description
VLAN ID	Indicates the VLAN ID of the entry.
Querier Version	Indicates the current Working Querier Version.
Host Version	Indicates the current Working Host Version.
Querier Status	Indicates the Querier status as **ACTIVE** or **IDLE**. **DISABLE** denotes that the specific interface is administratively disabled.
Queries Transmitted	Indicates the number of Transmitted queries.
Queries Received	Indicates the number of Received Queries.
V1 Reports Received	Indicates the number of Received V1 Reports.
V2 Reports Received	Indicates the number of Received V2 Reports.
V1 Leaves Received	Indicates the number of Received V1 Leaves.
Router Port	Indicates which ports act as router ports. A router port is a port on the ethernetswitch that leads toward the Layer 3 multicast device or IGMP querier. **Static** denotes that the specific port is configured to be a router port. **Dynamic** denotes that the specific port is learned to be a router port. **Both** denote that the specific port is configured or learned to be a router port.
Port	Indicates the switch port number.

Status	Indicates whether the specific port is a router port or not.

1. To view the IGMP Snooping Status, on the main screen of the Web management UI, click **Monitor** > **System** > **Information**.

Change the Groups Information settings

Use the MLD Snooping Group Information screen to display the port member of each service group.

You can access the screen by clicking **Monitor** > **IPMC** > **MLD** > **Groups Information**.

Menu option	**Description**
VLAN ID	Indicates the VLAN ID of the entry.
Groups	Indicates the group address of the group displayed.
Port Members	Indicates ports under this group.

Change the IPv6 SFM Information settings

Entries in the MLD SFM Information Table are shown on this screen. 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, followed by port. Different source addresses belonging to the same group are treated as a single entry.

You can access the screen by clicking **Monitor** > **IPMC** > **MLD** > **IPv6 SFM Information**.

Menu option	**Description**
VLAN ID	Indicates the VLAN ID of the entry.
Group	Indicates the group address of the group displayed.
Port	Indicates the switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be **Include** or **Exclude**.
Source Address	Indicates the IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.

Type	Indicates the Type: **Allow** or **Deny**.
Hardware Filter/ Switch	Indicates whether the data plane destined to the specific group address from the source IPv4 address could be handled by the chip or not.

1. To view the MLD SFM information, on the main screen of the Web management UI, click **Monitor** > **System** > **Information**.

Change the Neighbours settings

Use the LLDP Neighbour Information screen to show information about LLDP neighbour devices connected directly to the switch.

You can access the screen by clicking **Monitor** > **LLDP** > **Neighbours**.

Menu option	**Description**
Local Port	Indicates the port on which the LLDP frame was received.
Chassis ID	Indicates the Chassis ID is the identification of the neighbour's LLD frames.
Port ID	Indicates the Port ID is the identification of the neighbour port.
Port Description	Indicates the Port Description advertised by the neighbour unit.
System Name	Indicates the System name advertised by the neighbour unit.

System Capabilities	Indicates the System Capabilities describing the neighbour 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 a **(+)**. If the capability is disabled, the capability is followed by a **(-)**.
Management Address	Management Address is the neighbour unit’s address that is used for higher layer entities to assist discovery by the network management. For instance, this could hold the neighbour’s IP Address.

1. To view the information about LLDP Neighbours, on the main screen of the Web management UI, click **Monitor** > **LLDP** > **Neighbours**.

Change the LLDP-MED Neighbours settings

Use the LLDP-MED Neighbour Information screen to show information about the remote device which is connected to the switch and advertises LLDP-MED TLVs.

You can access the screen by clicking **Monitor** > **LLDP** > **LLDP-MED Neighbours**.

Menu option	**Description**
Port	Indicates 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.

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 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, inventory management.

LLDP-MED Capabilities	LLDP-MED Capabilities describes the neighbour 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 indicates 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 by the operational MAU type field value rather than by auto-negotiation.
Auto-negotiation Capabilities	Auto-negotiation Capabilities show the link partners MAC/ PHY capabilities.

1. To view information about the LLDP-MED neigbors, on the main screen of the Web management UI, click **Monitor** > **LLDP** > **LLED-MED**.

Change the EEE settings

EEE power savings can be achieved at the expense of traffic latency. This latency occurs because the circuits EEE turns 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 wake up time they need.

You can access the screen by clicking **Monitor** > **LLDP** > **EEE**.

Menu option	**Description**
Local Port	Indicates the port on which the LLDP frame was received.
Tx Tw	Indicates the link partner's maximum time that the transmit path can hold-off sending data after deassertion of LPI.
Rx Tw	Indicates the link partner's time that the receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.
Fallback Receive TW	Indicates the link partner's fallback 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	Indicates the link partner's Echo Tx Tw value. The respective echo values is defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner has received, registered, and processed its most recent 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	Indicates the link partner's Echo Rx Tw value.
Resolved Tx Tw	Indicates the resolved Tx Tw for this link. **Note:** Not the link partner. Indicates the resolved value that is the actual **tx wakeup time** used for this link (based on EEE information exchanged via LLDP).
Resolved Rx Tw	Indicates the resolved Rx Tw for this link. **Note:** Not the link partner. Indicates 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: Indciates the switch and link partner have not agreed on wakeup times. Green: Indicates switch and link partner have agreed on wakeup times.

1. To view information about the LLDP EEE neighbours, on the main screen of the Web management UI, click **Monitor** > **LLDP** > **EEE**.

Change the Port Statistics settings

This screen provides an overview of all LLDP traffic. 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.

You can access the screen by clicking **Monitor** > **LLDP** > **Port Statistics**.

Menu option	**Description**
Global Counters	
Neighbour entries were last changed	Indicates the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbour Entries Added	Indicates the number of new entries added since switch reboot.
Total Neighbour Entries Deleted	Indicates the number of new entries deleted since switch reboot.
Total Neighbour Entries Dropped	Indicates the number of LLDP frames dropped due to the entry table being full.
Total Neighbour Entries Aged Out	Indicates the number of entries deleted due to Time-To-Live expiring.
Local Counters	
Local Port	Indicates the port on which LLDP frames are received or transmitted.
Tx Frames	Indicates the number of LLDP frames transmitted on the port.
Rx Frames	Indicates the number of LLDP frames received on the port.
Rx Errors	Indicates the number of received LLDP frames containing some kind of error.
Frames Discard	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 Neighbours" 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	Indicates the number of well-formed TLVs, but with an unknown type value.
Org. Discarded	Indicates the number of organizationally received TLVs.
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

1. To view information about the LLDP traffics, on the main screen of the Web management UI, click **Monitor** > **LLDP** > **Port Statistics**.

Change the MAC Table settings

Entries in the MAC Table are shown on this screen. The MAC Table contains 8192 entries, and is sorted first by VLAN ID, then followed by MAC Address.

You can access the screen by clicking **Monitor** > **MAC Table**.

Menu option	Description
Type	Indicates whether the entry is a static or a dynamic entry.
MAC Address	Displays the MAC Address of the switch.
VLAN	Indicates the VLAN ID of the entry.
Port Members	Indicates the ports that are members of the entry.

1. To view the Static MAC Address and Dynamic MAC address entries, on the main screen of the Web management UI, click **Monitor** > **MAC Table**.

Change the VLAN Membership settings

Use Monitor screens for VLANs to display port members of VLANs and its VLAN attributes corresponding to each port. Use VLAN Membership Status for a specific user's page to display the status and report information of all VLANs status and reports.

You can access the screen by clicking **Monitor** > **VLANs** > **VLAN Membership**.

Menu option	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: 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. MSTP: The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, a checkmark image is displayed. If a port is included in a Forbidden port list, an image of an x is displayed. If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then the conflict port is displayed as follows: Xc
VLAN Membership	The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN User (selection will be allowed by a Combo Box). When ALL VLAN Users are selected, it will 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	Select VLAN users in the drop-down list. Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. To view the VLAN Membership Status for specific users, on the main screen of the Web management UI, click **Monitor** > **VLANs** > **VLAN Membership**.

Change the VLAN Port settings

Use the VLAN Port Status for a specific user's page to display the status information of all VLAN Ports status.

You can access the screen by clicking **Monitor** > **VLANs** > **VLAN Port**.

Menu option	Description
Port	Indicates the logical port for the settings contained in the same row.
PVID	Indicates the VLAN identifier for that port. The allowed values are 1 through to 4095. The default value is 1.
Port Type	Indicates 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.
Ingress Filtering	Indicates 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	Indicates whether the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Tx Tag	Indicates egress filtering frame status whether tagged or untagged.
UVID	Indicates UVID (untagged VLAN ID). A Port's UVID determines the packet's behaviour at the egress side.
Conflicts	Indicates the status of Conflicts and whether they exist 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	Select VLAN users in the drop-down list. Auto-refresh: Select the Auto-refresh check box to automatically refresh the page at regular intervals. Refresh: Updates the system log entries, starting from the current entry ID.

1. To view the VLAN Port information, on the main screen of the Web management UI, click **Monitor** > **VLANs** > **VLAN Port**.

Change the MAC-Based VLAN settings

Use the MAC-Based VLAN Membership Status for User Static to show the MAC Address to VLAN mapping entries.

You can access the screen by clicking **Monitor** > **VCL** > **MAC-based VLAN**.

Menu option	Description
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	Indicates the Port Members of the Mac-based VLAN entry.

1. To view the MAC Address to VLAN Mapping entries, on the main screen of the Web management UI, click **Monitor** > **VCL** > **MAC-based VLAN**.

Change the sFlow settings

This screen shows receiver and per-port sFlow statistics.

You can access the screen by clicking **Monitor** > **sFlow**.

Menu option	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 Timeout	Indicates the IP address or hostname of the sFlow receiver. Indicates the number of seconds remaining before sampling stops and the current sFlow owner is released.
Tx successes	Indicates the number of UDP datagrams successfully sent to the sFlow receiver.
Tx Errors	Indicates 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	Indicates the total number of flow samples sent to the sFlow receiver.
Counter Samples	Indicates the total number of counter samples sent to the sFlow receiver.
Port Statistics	
Port	Indicates the port number for which the following statistics applies.

Rx and Tx Flow Samples	Indicates 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. Rx flow samples contain the number of packets that were sampled upon reception (ingress) on the port. Tx flow samples contain the number of packets that were sampled upon transmission (egress) on the port.
Counter Samples	Indicates the total number of counter samples sent to the sFlow receiver originating from this port.

1. To view the sFlow Statistics infromation, on the main screen of the Web management UI, click **Monitor** > **sFlow**.

Testing the connectivity of the network

This section provides information about IPv4 ping to test the connectivity of the network.

Change the Ping settings

Use the ICMP Ping screen to send ICMP request packets to another connected point to check if it's connected.

You can access the screen by clicking **Diagnostics** > **Ping**.

Menu option	Description
IP Address	Indicates the destination IP Address.
Ping Length	Indicates the payload size of the ICMP packet. Values range from 2 to 1452 bytes.
Ping Count	Indicates the count of the ICMP packet. Values range from 1 to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 to 30 seconds.

1. To run the testing, on the main screen of the Web management UI, click **Diagnostics** > **Ping**.

Change the Ping6 settings

Use the ICMP Ping screen to send ICMPv6 request packets to another connected point to check if it's connected.

You can access the screen by clicking **Diagnostics** > **Ping6**.

Menu option	Description
IP Address	Indicates the destination IP Address.
Ping Length	Indicates the payload size of the ICMP packet. Values range from 2 to 1452 bytes.
Ping Count	Indicates the count of the ICMP packet. Values range from 1 to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 to 30 seconds.

1. To run the testing, on the main screen of the Web management UI, click **Diagnostics** > **Ping6**.

About device maintenance

This section describes how to restart the device, reload the device to default factory settings, save or restore the configuration, as well as upgrading and swapping firmware.

Restart the device

Use the Restart Device screen to restart the switch.

1. To restart the KVM switch, on the main screen of the Web management UI, click **Maintenance** > **Restart Device**.
2. In the confirmation dialog box, do one of the following:
    - To restart the device, click **Yes**.
    - To cancel the restart process, click **No**.

Restore the factory default settings

Use the Factory Defaults screen to reset the switch to default factory settings.

1. To restore the KVM switch to the default factory settings, on the main screen of the Web management UI, click **Maintenance** > **Faculty Defaults**.
2. In the confirmation dialog box, do one of the following:
    - To restore the factory settings, click **Yes**.
    - To cancel the restore process, click **No**.

Update your firmware

1. To update your firmware, on the main screen of the Web management UI, click **Maintenance** > **Software** > **Upload**.
2. Click **Browse** and navigate to the location of the image.
3. Click **Upload**.

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

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

Change the Image Select settings

Use the Software Image Selection screen to swap the firmware to an alternative image.

You can access the screen by clicking **Maintenace** > **Software** > **Image Select**.

Menu option	Description
Image	Indicates the flash index name of the firmware image. The name of primary (preferred) image is **image**, the alternate image is named **image.bk**.
Version Date	Indicates the version of the firmware image. Indicates the date where the firmware was produced.
Buttons	To use the alternate image, click **Activate Alternate Image**. Depending on the system state, this button may be disabled. To cancel the activation of the backup image and to navigate away from the screen, click **Cancel**.

1. To swap to an alternative image, on the main screen of the Web management UI, click **Maintenance** > **Software** > **Image Select**.

Save the switch configuration to an XML file

1. To save the switch configuration to an XML file, on the main screen of the Web management UI, click **Maintenance** > **Configuration** > **Save**.
2. Click **Save Configuration**.

When you click Save Configuration, a file-saving dialog opens and the default name is **config.xml**.

Restore the switch to a backup configuration

1. To restore the switch to a backup configuration from an XML file, on the main screen of the Web management UI, click **Maintenance** > **Configuration** > **Upload**.
2. Click **Browse** and navigate to the location of the image.
3. Click **Upload**.

After the configuration file is uploaded, a page says that the configuration upload done.

4. To apply the configuration, reset the switch.

Technical Support

StarTech.com's lifetime technical support is an integral part of our commitment to provide industry-leading solutions. If you ever need help with your product, visit **www.startech.com/support** and access our comprehensive selection of online tools, documentation, and downloads.

For the latest drivers/software, please visit **www.startech.com/downloads**

Warranty Information

This product is backed by a two-year warranty.

In addition, StarTech.com warrants its products against defects in materials and workmanship for the periods noted, following the initial date of purchase. During this period, the products may be returned for repair, or replacement with equivalent products at our discretion. The warranty covers parts and labor costs only. StarTech.com does not warrant its products from defects or damages arising from misuse, abuse, alteration, or normal wear and tear.

Limitation of Liability

In no event shall the liability of StarTech.com Ltd. and StarTech.com USA LLP (or their officers, directors, employees or agents) for any damages (whether direct or indirect, special, punitive, incidental, consequential, or otherwise), loss of profits, loss of business, or any pecuniary loss, arising out of or related to the use of the product exceed the actual price paid for the product. Some states do not allow the exclusion or limitation of incidental or consequential damages. If such laws apply, the limitations or exclusions contained in this statement may not apply to you.

StarTech.com

Hard-to-find **made easy**®

Hard-to-find made easy. At StarTech.com, that isn't a slogan. It's a promise.

StarTech.com is your one-stop source for every connectivity part you need. From the latest technology to legacy products — and all the parts that bridge the old and new — we can help you find the parts that connect your solutions.

We make it easy to locate the parts, and we quickly deliver them wherever they need to go. Just talk to one of our tech advisors or visit our website. You'll be connected to the products you need in no time.

Visit www.startech.com for complete information on all StarTech.com products and to access exclusive resources and time-saving tools.

StarTech.com is an ISO 9001 Registered manufacturer of connectivity and technology parts. StarTech.com was founded in 1985 and has operations in the United States, Canada, the United Kingdom and Taiwan servicing a worldwide market.