StarTech.com

Hard-to-find made easy®

8-Port Gigabit Ethernet Switch (4-Port PoE+) - Managed

IES81GPOEW

*actual product may vary from photos

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

For the latest information, technical specifications, and support for this product, please visit www.StarTech.com/IES81GPOEW.

Manual Revision: 09/0916/2024

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.

Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe [A] est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

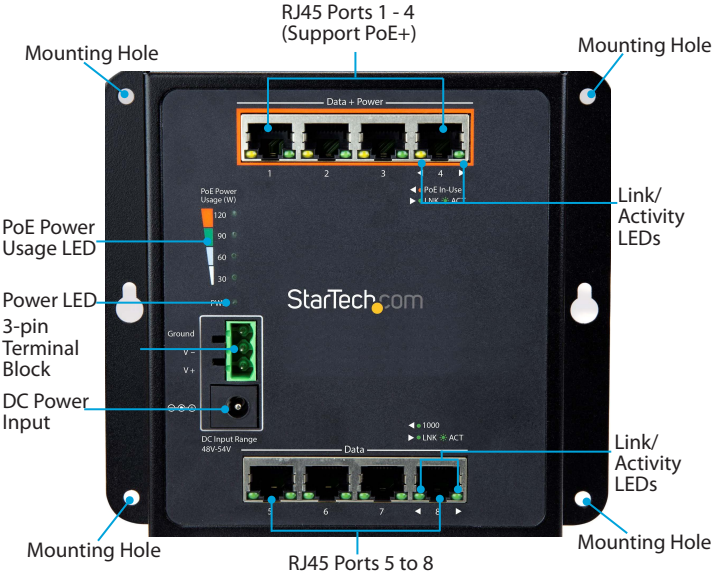
Use of Trademarks, Registered Trademarks, and other Protected Names and Symbols

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



Back View

Package Contents

- 1 x network switch
- 1 x terminal block connector
- 4 x screw anchors
- 4 x screws
- 4 x attaching pins
- 4 x locking pins
- 4 x washers
- 4 x magnets
- 1 x DIN rail
- 3 x DIN-rail screws
- 8 x RJ45 dust caps
- 1 x quick-start guide

Requirements

- Ethernet port connection
- RJ45 network cables
- PoE powered devices (optional)

This network switch is OS independent and doesn't require any additional drivers or software.

Requirements are subject to change. For the latest requirements, please visit www.StarTech.com/IES81GPOEW.

About the LED Indicators

This network switch features a **Link and Activity LED Indicator** for each of the eight RJ45 ports. There is also a **Power LED** located above the 3-Pin Terminal Block, and a **PoE Power Usage LED** that illuminates in 30 watt increments.

For more information about what the LED indicators signify, see the table below.

LED	Behavior	Significance
RJ45 Ports 1 - 4	Solid Green	Link was successfully established
	Blinking Green	Connected device is transferring data
	Solid Orange	Port is providing power
	Off	Connected device is not a PoE powered device
RJ45 Ports 5 - 8	Solid Green	Link was successfully established
	Blinking Green	Connected device is transferring data
	Solid Green	Connected device is transferring data at 1000Mbps
	Off	Link is down or connected device is transferring data at 10/100Mbps
Power LED indicator	Solid Green	Switch is receiving power

Wire the Power Inputs

You can use either an external power adapter or the terminal block to power the network switch. Alternatively, you can connect both an external power adapter and the terminal block to create a redundant power input.

Note: You should use wire ranging in size of 12 to 24 AWG.

Caution! Make sure that you ground the enclosure before you install the terminal block connector into the network switch.

1. Insert the grounding wire into the **Ground** port on the terminal block, and tighten the wire clamp screws.
2. Insert the positive DC power wire into the **V+** port on the terminal block connector, and tighten the wire clamp screws.
3. Insert the negative DC power wire into the **V-** port on the terminal block connector, and tighten the wire clamp screws.
4. Insert the terminal block connector into the **3-pin terminal block** on the network switch.

Reboot the Network Switch

The **Reset button** on the network switch is designed to reboot the network switch without turning the power on/off.

- To reboot the network switch, press the **Reset button**.

Reset to the default factory settings

You can use the **Reset button** to reset the network switch to the following default factory settings: **NOTE**: *The factory-default login is device-specific.*

Default user name: admin

Default password: "sw"+ the MAC Address UID (last 6 digits), lowercase

e.g. If your device MAC address is E8-EA-6A-A1**-**B2**-**C3**, then the factory default password is "**swa1b2c3**"*

These credentials apply to IES81GPOEW **Rev 03 and up. Older revisions use the Default Password "**admin**".*

Default IP address: 192.168.0.100

Subnet mask: 255.255.255.0

Default gateway: 192.168.0.254

- To reset to the default factory settings, press and hold the **Reset button** for more than 5 seconds.

When you press the **Reset button**, the **port LED indicators** illuminate. When the LEDs are no longer illuminated, the reset sequence is complete.

Installation

Install the Network Switch onto a Wall

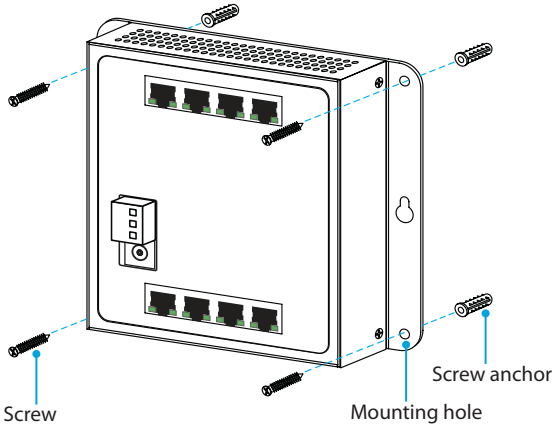
The mounting holes on the network switch are 8 mm in diameter, and the distance between the two holes is 133 mm.

1. Hold the network switch against the wall in the area that you want to install it, and use a pencil to trace the location of the four **Mounting Holes** onto the wall.
2. Use the **Mounting Holes** that you traced on the wall as a template and drill holes in the wall.
3. Insert the four **Screw Anchors** into the holes.

Note: Make sure that the **Screw Anchors** are flush against the wall.

4. Place the network switch against the wall and insert the four **screws** through the **Mounting Holes** on the switch and into the **Screw Anchors**. (*Figure 1*)
5. Tighten the **Screws**.

Figure 1



*actual product may vary from illustration

6. To power the switch, connect an external power adapter, wire the power inputs, or do both.

7. Connect RJ45 Cables to the **RJ45 Ports** on the network switch.

Install the Switch onto a Magnetic Surface

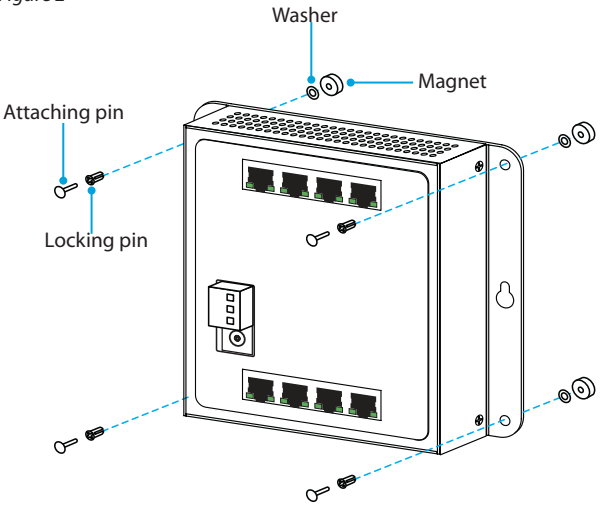
1. Push each of the **Attaching Pins** into a **Locking Pin**.

2. Insert the **Attaching** and **Locking Pins** into one of the **Mounting Holes** on the network switch, through a **Washer**, and into a **Magnet**.

Note: To prevent the magnets from becoming loose, make sure that you position the magnet so that the flat side is against the network switch.

3. Repeat step 2 for all of the **Mounting Holes** on the network switch. (*Figure 2*)

Figure 2



*actual product may vary from illustration

4. Attach the network switch to a magnetic surface.

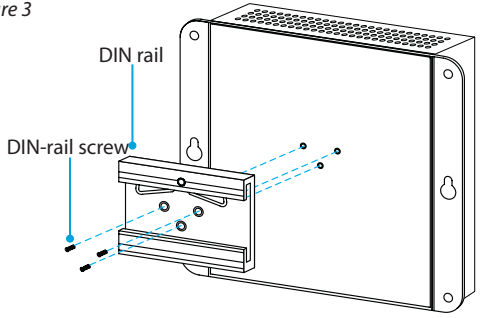
5. To power the switch, connect an external power adapter, wire the power inputs, or do both.

6. Connect RJ45 Cables to the **RJ45 Ports** on the enclosure.

Mount the Switch onto a DIN Rail

1. With the flat side of the **DIN Rail** positioned against the network switch, line up the holes on the **DIN Rail** with the holes on the switch.

Figure 3



2. Insert the **DIN-Rail screws** through the **DIN rail** and into the network switch. (*Figure 3*)

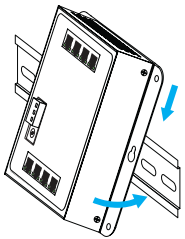
3. Tighten the screws.

4. Hook the **DIN Rail** onto the top of the track, and push it against the track. (*Figure 4*)

5. To power the switch, connect an external power adapter, wire the power inputs, or do both.

6. Connect the RJ45 Cables to the **RJ45 Ports** on the enclosure.

Figure 4



About the Web-Based GUI

This switch can be managed using it's web-based Graphical User Interface (GUI). You can access the GUI through any device that's connected to your network and equipped with a standard browser (e.g. Microsoft Internet Explorer, Google Chrome, etc.).

- The switch's default IP address is: 192.168.0.100
- The switch's default subnet mask is: 255.255.255.0
- The default username for the administrator account is: admin
- The default password for the administrator account is: "sw"+ the MAC Address UID (last 6 digits), lowercase
  *e.g. If your device MAC address is E8-EA-6A-A1-B2-C3, then the factory default password is "**swa1b2c3**".
  *These credentials apply to IES81GPOEW Rev 03 and up. Older revisions use the Default Password "**admin**".

In order for a device to access the switch's management GUI, the device must be connected to your network and assigned an IP address that's on the same subnet as the managed switch with an identical subnet mask.

For example: If the switch is set to its default IP address of 192.168.0.100, then the device that's accessing it must be assigned an IP address of 192.168.0.x (x is a number between 1 and 254, except 100). As the switch supports DHCP it's likely your computer will automatically be assigned an IP address in the same range, unless your device has a manually assigned IP address.

Notes:

- GUI is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.
- By default, many browsers (including Internet Explorer 8.0 or later) do not allow Java Applets to open sockets. If this is the case for your browser, you'll have to modify the browser setting to enable Java Applets to use network ports.

Accessing the Web-Based GUI

1. Open the web browser on a device that's connected to your network.
2. Enter the switch's default IP address (192.168.0.100) into the address bar and press Enter.
3. A login screen appears, enter the Username and Password (see above) for the switch's administrator account in the respective fields and click Login.
4. The GUI Home page is displayed.

Web-Based GUI Operation

This section outlines how to navigate the various sections of the web-based GUI and how to adjust the configuration settings.

Navigation Menu

The Navigation menu features several sections that can be accessed from anywhere within the web GUI and enable access to different features including Configuration Settings, Hardware Operation, and Port Status.

Port Status Panel

The Port Status Panel displays an individual image for each of the switch's ports that illustrates the current status of that port. Clicking on the port image will open a page displaying the port statistics.

The meaning of each port image is detailed below:

Disabled	Down	Link	PoE-in-use
			

Operational Buttons

The Operational buttons enable you to accomplish several tasks directly from the home page. An explanation of the functionality for each button is detailed below:

- **SAVE:** The **SAVE** button displays a sub-menu that enables you to save the **Running**, **Startup** and/or **Backup Configuration**, or **Reset** the switch to it's default settings. The sub-menu options are:
  - **Save Configurations to FLASH :** Opens the Configuration Manager. See "Configuration Manager" (p. 11) for further details.
  - **Restore to Defaults**: Resets the switch to factory settings.
- **LOGOUT:** The **LOGOUT** button securely exits the administrator account.
- **REBOOT:** The **REBOOT** button power cycles the switch, turning it off and on.
- **REFRESH:** The **REFRESH** button, reloads the page you're viewing.

Navigation Menu

The Navigation menu enables you to navigate throughout the various sections of the GUI:

- **System**
- **Port Management**
- **Link Aggregation**
- **VLAN**
- **Spanning Tree**
- **Multicast**
- **QoS**
- **Security**
- **Access Control List**
- **MAC Address Table**
- **LLDP**
- **Diagnostics**
- **RMON**
- **Maintenance**

Home Page

The Home page is the first page displayed upon login. It lists the product information and SKU and provides StarTech.com contact information.

Accessing the Configuration Manager

The **Configuration Manager** enables you to save the **Running**, **Startup** and **Backup** configurations.

1. Click the **Save** button to open the drop-down menu.
2. From the drop-down menu, click **Save Configurations to FLASH**. The **Configuration Manager** is displayed.

Applying Changes and Setting the Current Configuration

1. On the ***Save Configuration*** page, select a configuration option for:

- **Source File**: The running configuration.
  - **Running Configuration:** is the configuration sequence that's been most recently set to the switch. It's stored in the switch's RAM as running-config and will be lost upon reboot. The running configuration file can be saved from the switches RAM to the switch's flash memory, so that the running configuration can become the startup configuration.
  - **Startup Configuration**: is the configuration sequence used in the switch at startup. It's stored in the switch's flash memory as **startup.cfg**.
  - **Backup Configuration**: is stored in the system's Flash memory but is empty by default. You can save a backup configuration in the Backup Manager (Maintenance) file in Maintenance - Backup Manager.

1. Select a configuration option for:

- **Destination File**: The startup configuration.
  - **Startup Configuration**: is the configuration sequence used in the switch at startup. It's stored in the switch's flash memory as **startup.cfg**.
  - **Backup Configuration**: is stored in the system's Flash memory but is empty by default. You can save a backup configuration in the Backup Manager (Maintenance) file in Maintenance - Backup Manager.

2. Click the **Apply** button.

System Menu

From the **System** section of the main menu you can configure the switch's administrative settings. Within the **System** section the settings are organized into sub-sections. Each of these sub-sections and the type of configurations are listed below:

- **System Information** - The switch system information is provided here.
- **IP Configurations** - Configure the switch-managed IP information on this page.
- **IPv6 Configuration** - Configure the switch-managed IPv6 information on this page.
- **User Configuration** - Configure new User Name and Password on this page.
- **Time Settings** - Configure SNTP on this page.
- **Log Management** - The switch log information is provided here.

- **SNMP Management** - Configure SNMP on this page.

Editing System Parameters

1. On the ***System Information*** page, click on the **Edit** button next to the system parameter you wish to edit.
   - **System Name:** Enter a name for the system switch.
   - **System Location:** Enter a Location.
   - **System Contact:** Enter a system contact.
2. Enter the new value for the corresponding system parameter.

Viewing System Information

1. On the ***Main Menu***, click on the ***System Information.***
2. The ***Systems Information*** page will appear allowing you to view the following device information:
   - **System Name** - Displays the current system name.
   - **System Location** - Displays the current system location.
   - **System Contact** - Displays the current system contact.
   - **MAC Address** - Displays the switch's MAC address.
   - **IP Address** - Displays the switch's default IP address.
   - **Subnet Mask** - Displays the switch's subnet mask.
   - **Gateway** - Displays the switch's gateway.
   - **Loader Version -** Displays the loader version of the switch.
   - **Loader Date** - Displays the loader date of the switch.
   - **Firmware Version** - Displays the firmware version of the switch.
   - **Firmware Date** - Displays the firmware date of the switch.
   - **System Object ID** - Displays the system object ID of the switch.
   - **System Uptime** - Displays the period of time that the switch has been operational.
   - **PCN/HW Version** - Displays the hardware version of the switch.

IP Configurations

The **IP Configurations** page enables you to view or edit Internet Protocol (IPv4) settings such as IP address, subnet mask and gateway.

Apply Changes and Set IP Address Settings

1. On the ***IP Address Setting*** page, enter the following IP address settings:
   - **Mode:** Indicates and gives you the option to change the IP address mode operation.
     - • **Static:** Enables Static IP address operations. If Static is selected you will also have to manually set a static IP address, subnet mask, gateway address and DNS server addresses.
     - • **DHCP:** Enable DHCP client mode operation. When in DHCP client mode operation, the DHCP client will announce the configured System Name as hostname to provide DNS lookup for each connected device. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used.
   - **IP Address:** Enter the Network Switch's IP address.
   - **Subnet Mask:** Enter a subnet mask.
   - **Gateway:** Enter the router's IP address.
   - **DNS Server 1:** Enter the DNS 1 server's IP address.
   - **DNS Server 2:** Enter the DNS 2 server's IP address.
2. Click the **Apply** button, to apply the changes.

Viewing IP Address Settings

1. On the ***Main Menu***, click on the ***System*** and select ***IP Address*** from the drop-down list.
2. The ***IP Address Setting*** page will appear allowing you to view the following IP address information:
   - **DHCP State** - Displays the current DHCP state, either enabled or disabled.
   - **Static IP Address** - Displays the current IP address.
   - **Static Subnet Mask** - Displays the current subnet mask.
   - **Static Gateway** - Displays the current gateway.
   - **Static DNS Server 1:** Displays the current DNS server.
   - **Static DNS Server 2** - Displays the current DNS server.

Applying Changes and Setting IPv6 Address Settings

The **IPv6 Configuration** page enables you to view or edit Internet Protocol (IPv6) settings such as auto configuration, IPv6 address and gateway.

1. On the ***IP Address Setting*** page, enter the following IP address settings:

   - **Auto Configuration**: Enables IPv6 auto-configuration. If it fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds; the total time needed to complete auto-configuration can be significantly longer.
   - **IPv6 Address:** Displays and gives you the option to edit the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example: fe80::215:c5ff:fe03:4dc7. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only be used once.
   - **Gateway:** Displays and gives you the option to change the IPv6 address of the router.
   - **DHCPv6 Client**: Enables this switch to accept a configuration from a **Dynamic Host Configuration Protocol version 6 (DHCPv6)** server. By default, the switch does not perform DHCPv6 client actions. DHCPv6 clients request the delegation of long-lived prefixes that they can push to individual local hosts.

2. Click the **Apply** button, to apply the changes.

Viewing IPv6 Settings

1. On the ***Main Menu***, click on the ***System*** and select ***IP Address*** from the drop-down list.

2. The ***IP Address Setting*** page will appear allowing you to view the following IPv6 Information:

   - **Auto Configuration**: Displays the current auto configuration state.
   - **IPv6 In Use Address**: Displays the current IPv6 in-use address.
   - **IPv6 In Use Router:** Displays the current in-use gateway.
   - **IPv6 Static Address:** Displays the current IPv6 static address.
   - **IPv6 Static Router:** Displays the current IPv6 static gateway.
   - **DHCPv6 Client**: Displays the current DHCPv6 client status.

User Configuration

The **User Configuration** page enables you to view and delete users accounts and define, the new user account attributes such as privilege types and passwords.

Change Admin Password (Rev 01/02)

1. In the New User table, type "admin".
2. Enter a new password.

   Note: the admin account cannot be deleted. Once a new account with admin privileges is made, the admin account privileges can be set to User to restrict the account

Adding a New User

1. On the ***New User*** page, enter the following user information:
   - **Username:** The name identifying the user. The username is 32 characters in length. You can add up to a maximum of 8 users.
   - **Password Type**: Enables you to set whether the user account requires a password:
     - **Encrypted:** The user's password will be encrypted.
     - **Clear Text:** The user's password will not be encrypted.
     - **No Password:** The user does not require a password.
   - **Password:** Enter the user's password. The password must be 0-32 characters in length and is case sensitive.
     - **Clear Text:** If you selected clear text for the password type, only letters and numbers can be used.
     - **Encrypted:** If you selected encrypted for the password type, letters, numbers and special characters can also be used.
   - **Retype Password:** Confirms the user's password by re-entering the password.
   - **Privilege Type:** Defines whether a user can have write access to critical settings (Admin).
2. Click the **Apply** button, to apply the changes.

Viewing Existing User Profiles (Local User)

1. On the ***Main Menu***, click on the ***System*** and select ***User Configuration*** from the drop-down list.
2. The ***Local Users*** page will appear allowing you to view the following user information:
   - **Username** - Displays the user name.
   - **Password Type:** Displays the password type.
   - **Privilege Type:** Display the privilege type.
   - **Privilege Value:** Displays the privilege value.

Deleting a User Account

- On the ***Local User*** page, click the **Delete** button on the **Modify** field next to the user account you wish to delete.

Adjusting System Time Settings

From the **Time Settings** section of the main menu you can configure the system and network clock settings. **System Time** - Configure your system for local Simple Network Time Protocol (SNTP).

1. On the ***System Time Setting*** page, enter the following information:
   - **Enable SNTP**: Configure your system for external Simple Network Time Protocol (SNTP) supported by a third party.
     - **Enable:** When enabling SNTP mode operation, the agent forwards and transfers SNTP data between to the connected devices.
     - **Disabled:** When disabling SNTP mode operation, SNTP data will not be communicated.
   - **Manual Time:** Enables you to set your date and time manually for the following fields:
     - **Year:** Enter the current calendar year.
     - **Month:** Enter the current calendar month.
     - **Day:** Enter the current calendar day,
     - **Hours:** Enter the current hour.
     - **Minutes:** Enter the current minute(s).

- **Seconds:** Enter the current second(s).

- **Time Zone:** Enables you to select the time zone according to the physical location of the switch.
- **Daylight Saving Time:** Enables the clock to automatically adjust in accordance to Daylight Saving Time. Select **Disable** to prevent the clock from changing. Select **Recurring** to configure the auto adjustment to repeat every year. Select **Non-Recurring** to configure the adjustment to occur once. (Default: Disabled).
- **Daylight Saving Time Offset:** Enables you to enter the number of minutes to add during Daylight Saving Time change (Range: 1 to 1440).
- **Recurring From:** Enables you to define the week, day, hour and minute that Daylight Savings Time will start every year.
- **Recurring To:** Enables you to define the week, day, hour and minute that Daylight Savings Time will stop occurring every year.
- **Non-recurring From:** Enables you to define the week, day, hour and minute that Daylight Savings Time will start in a single-year cycle.
- **Non-recurring to:** Enables you to define the week, day, hour and minute that Daylight Savings Time will stop in a single-year cycle.

2. Click the **Apply** button, to apply the changes.

Viewing System Time Information

1. On the ***Main Menu***, click on the ***System*** and select ***System Time*** from the drop-down list.

2. The ***System Time Information*** page will appear allowing you to view the following user information:

- **Current Date/Time:** Displays the date and time that the system is currently set to.
- **SNTP**: Displays whether SNTP is enabled or disabled.
- **Time zone:** Displays the time zone that the system is currently set to.
- **Daylight Saving Time:** Displays whether Daylight Savings Time is enabled or disabled.
- **Daylight Saving Time Offset:** Displays the number of minutes that are added in the current Daylight Savings Time change.

- **From:** Displays the date and time that Daylight Savings Time will start.
- **To:** Displays the date and time that Daylight Savings Time will stop.

Adjusting SNTP Server Settings

You can use SNTP server settings to sync the switch's date and time settings to an external SNTP Server provider.

1. On the ***SNTP Server Settings*** page, enter the following information:
   - **SNTP Server Address:** Enables you to enter the IP address or domain of the SNTP server you'd like to sync with.
   - **Server Port:** Enables you to enter the port number that the SNTP server you're connecting to communicates on.
2. Click the **Apply** button, to apply the changes.

Viewing SNTP Server Information

1. On the ***Main Menu***, click on the ***System*** and select ***SNTP Server Settings*** from the drop-down list.
2. The ***SMTP Server Settings*** page will appear allowing you to view the following user information:
   - **SNTP Server Address:** Displays the current IP address or domain that's currently assigned to the switch.
   - **Server Port:** Displays the current port number that the SNTP server is currently set to communicates on.

Log Management

Log Management enables you to configure and limit system messages that are logged to Flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 6 to be logged to RAM. The following table lists the event levels of the switch:

Level	Severity Name	Description
7	Debug	Debugging messages
6	Information	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return) Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

Enabling/Disabling the Logging Service

The Logging Service can be turned on or off. When creating a new log you will need to enable the logging service before creating the log.

1. On the ***Logging Settings*** page, select one of the following radio buttons:
   - **Enable:** Enables the logging service on the switch.
   - **Disable:** Disables the logging service on the switch.
2. Click the **Apply** button.

Viewing Logging Service Status

To view the current status of the Logging Service system.

- On the ***Logging Information*** page, the **Information Value** field is show you the current state of the Logging Service (enabled or disabled).

Creating/Editing a Log

When adding a new log you must first enable **Logging Service** on the switch.

1. On the ***Local Logging Setting*** page, enter the following information:
   - **Target:** The target of the local log entry. The following target types are supported:
     - **Buffered**: Target the buffer of the local log.
     - **File**: Target the file of the local log.
   - **Severity:** The severity of the local log entry. The following severity types are supported:
     - **Emerg**: Emergency level of the system unstable for local log.
     - **Alert**: Alert level of the immediate action needed for local log.
     - **Crit**: Critical level of the critical conditions for local log.
     - **Error**: Error level of the error conditions for local log.
     - **Warning**: Warning level of the warning conditions for local log.
     - **Notice**: Notice level of the normal but significant conditions for local log.
     - **Info**: Informational level of the informational messages for local log.
     - **Debug**: Debug level of the debugging messages for local log.
2. Click the **Apply** button.

Deleting a Log

- On the ***Logging Information*** page, select the **Delete** button under the **Action** field, next to the log you wish to delete from the Switch.

Remote Syslog

The **Remote Syslog** page enables you to configure the logging of messages that are sent to syslog servers or other management stations.

Sending a Message to Syslog

1. On the ***Remote Logging Setting*** page, enter the following information:
   - **Server Address**: Provide the remote syslog IP address of the switch.
   - **Server Port**: Provide the port number of remote syslog server. (Default Port #: 514)
   - **Severity**: The severity of the local log entry. The following severity types are supported:
     - **Emerg**: Emergency level of the system unstable for local log.
     - **Alert**: Alert level of the immediate action needed for local log.
     - **Crit**: Critical level of the critical conditions for local log.
     - **Error**: Error level of the error conditions for local log.
     - **Warning**: Warning level of the warning conditions for local log.
     - **Notice**: Notice level of the normal but significant conditions for local log.
     - **Info**: Informational level of the informational messages for local log.
     - **Debug**: Debug level of the debugging messages for local log.
   - **Facility** - local user 0~7
2. Click the **Apply** button.

Deleting a Syslog Message

The ***Remote Logging Setting Status*** page, displays the settings for existing messages.

- On the ***Remote Logging Setting Status*** page, select the **Delete** button under the **Action** field, next to the Message you wish to delete from the Switch.

Viewing the Syslog Page

The Switch's Log overview is listed on this page. From the log overview you can filter logged items on a defined criteria.

1. On the ***Logging Filter Select*** page, enter the following information:
   - **Target**: The target of the local log entry. The following target types are supported:
     - **Buffered**: Target the buffer of the local log.
     - **File**: Target the file of the local log.
   - **Severity**: The severity of the local log entry. The following severity types are supported:
     - **Emerg**: Emergency level of the system unstable for local log.
     - **Alert**: Alert level of the immediate action needed for local log.
     - **Crit**: Critical level of the critical conditions for local log.
     - **Error**: Error level of the error conditions for local log.
     - **Warning**: Warning level of the warning conditions for local log.
     - **Notice**: Notice level of the normal but significant conditions for local log.
     - **Info**: Informational level of the informational messages for local log.
     - **Debug**: Debug level of the debugging messages for local log.
   - **Category**: The category of the log view includes: AAA, ACL, CABLE_DIAG, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP and STP.
2. Click the **View** button.
3. The ***Logging Information*** page will appear, listing the following log information:
   - **Target:** Displays the current log target.
   - **Severity:** Displays the current log severity.
   - **Category:** Displays the current log category.
   - **Total Entries:** Displays the current remote syslog facility.

Clearing/Refreshing the Syslog Page

1. On the ***Logging Messages*** page, you can clear/refresh the following log information:

   - **No.**: Displays the number for logs.
   - **Timestamp**: Displays the time of log.
   - **Category:** Displays the category type.
   - **Severity:** Displays the severity type.
   - **Message:** Displays the log message.

2. Click on the one of the buttons to perform one of the following functions:

Button	Function
Clear	Clears the log information on the ***Logging Messages*** page.
Refresh	Refreshes the log information on the ***Logging Messages*** page.

SNMP Management

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of three key components: Network management stations (NMS's), SNMP agents, Management information base (MIB) and network-management protocol:

- **Network management stations (NMSs)** - Sometimes called consoles, these devices execute management applications that monitor and control network elements.
- **Agents** - Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)** - An MIB is a collection of managed objects residing in a virtual information store.

- **Network-management protocol** - A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP operations

SNMP itself is a simple request/response protocol. NMS's can send multiple requests without receiving a response.

- **Get:** Allows the NMS to retrieve an object instance from the agent.
- **Set:** Allows the NMS to set values for object instances within an agent.
- **Trap:** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

Enabling/Disabling SNMP

On the **SNMP Global Setting** page you can enable and disable SNMP and view the current status.

1. On the ***SNMP Global Setting*** page, select one of the following radio buttons:
   - **Enable:** Enables SNMP on the switch.
   - **Disable:** Disables SNMP on the switch.
2. Click the **Apply** button.

Viewing SNMP Information

To view the current status of the SNMP system.

- On the ***SNMP Information*** page, the **Information Value** field is show you the current state of the SNMP system (enabled or disabled).

Adding an SNMP Entry

When adding a new log you must first enable **Logging Service** on the switch.

1. On the View Table Setting page, enter the following information:
   - **View Name**: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
   - **Subtree OID:** The OID defining the root of the subtree to add to the named view. The allowed string content a is digital number or asterisk (*).
   - **Subtree OID Mask:** The bitmask identifies which positions in the specified object identifier are to be regarded as "wildcards" for the purpose of pattern matching.
   - **View Type:** Indicates the view type that this entry should belong to. Possible view types are:
     - **Included:** An optional flag to indicate that this view subtree should be included.
     - **Excluded:** An optional flag to indicate that this view subtree should be excluded.
     - **General:** If a view entry's view type is 'excluded', it should exist in another view entry in which view type is 'included' and its OID subtree oversteps the 'excluded' view entry.
2. Click the **Add** button.

Viewing an SNMP Table Status

To view the current status of the SNMP Table.

- On the ***View Table Status*** page, the following SNMP information will be displayed:
  - **View Name:** Displays the current SNMP view.
  - **Subtree OID:** Displays the current SNMP subtree OID.
  - **OID Mask:** Displays the current SNMP OID mask.
  - **View Types:** Displays the current SNMP view type.

Deleting an SNMP Entry

- On the ***View Table Status*** page, select the **Delete** button under the **Action** field, next to the SNMP entry you wish to delete from the Switch.

SNMP Access Group

On this page you can configure SNMPv3 Access Group table. The entry index keys are **Group Name**, **Security Model** and **Security Level**.

Adding an SNMP Access Group

1. On the ***Access Group Setting*** page, enter the following information:
   - **Group Name:** A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16 characters.
   - **Security Model**: Indicates the security model that this entry should belong to. Possible security models are:
     - **V1:** Reserved for SNMPv1.
     - **V2c:** Reserved for SNMPv2c.
     - **V3:** Reserved for SNMPv3 or User-based Security Model (USM).
   - **Security Level:** Indicates the security model that this entry should belong to. The Security Level applies to SNNPv3 only. Possible security models are:
     - **Noauth:** None authentication and none privacy security levels are assigned to the group.
     - **Auth:** Authentication and none privacy.
     - **Priv:** Authentication and privacy.
   - **Read View Name**: Is the name of the view in which you can only see the contents of the agent. The allowed string length is 1 to 16 characters.
   - **Write View Name:** Is the name of the view in which you enter data and configure the contents of the agent. The allowed string length is 1 to 16 characters.
   - **Notify View Name:** Is the name of the view in which you specify a notify, inform, or trap.
2. Click on the **Add** button to add the new access group.

Deleting an SNMP Access Group

- On the ***Access Group Setting*** page, select the **Delete** button at the bottom of the page to delete the access group .
- You can also delete an access group on the ***Access Group Status*** page, by selecting the **Delete** button under the **Action** field, next to the access group you wish to delete from the Switch

Viewing Access Group Status

1. On the ***Access Group Status*** page, the following access group information will be displayed:

- **Group Name:** Displays the current SNMP access group name.
- **Security Model**: Displays the current security model.
- **Security Level**: Displays the current security level.
- **Read View Name**: Displays the current read view name.
- **Write View Name:** Displays the current write view name.
- **Notify View Name:** Displays the current notify view name.

SNMP Community

The SNMP Community settings can be configured and viewed on this page. The settings are sorted into two tables.

Adding SNMP Community Settings

1. On the ***Community Setting*** page, enter the following information:

- **Community Name:** Indicates the community read/write access string to permit access to SNMP agent. The allowed string length is 0 to 16 characters.
- **Community Mode:** Indicates the SNMP community supported mode.
  - Possible versions are:
    - **Basic:** Set SNMP community mode supported version 1 and 2c.
    - **Advanced:** Set SNMP community mode supported version 3.
- **Group Name:** A string identifying the group name that the entry belongs to. The allowed string length is 1 to 16 characters.
- **View Name**: A string identifying the view name that the entry belongs to. The allowed string length is 1 to 16 characters.
- **Access Right:** Indicates the SNMP community type operation. Possible types are:
  - **RO:** Read-Only: Set access string type in read-only mode.
  - **RW:** Read-Write: Set access string type in read-write mode.

2. Click the **Add** button to add the SNMP Community settings.

Viewing SNMP Community Settings

- On the ***Community Setting*** page, the following access group information will be displayed:
  - **Community Name** - Displays the current community type.
  - **Group Name** - Displays the current SNMP access group's name.
  - **View Name** - Displays the current view name.
  - **Access Right** - Displays the current access type.

Deleting SNMP Community Settings

- On the ***Community Setting*** page, by selecting the **Delete** button under the **Action** field, next to the SNMP community you wish to delete from the Switch.

SNMP User

Configure SNMPv3 users table on this page. Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, and notify view.

Adding an SNMP User

1. On the ***User Setting*** page, enter the following information:
   - **User Name:** Is a string identifying the user name that this entry should belong to. The allowed string length is 1 to 16.
   - **Group:** Is a string identifying the group name that this entry should belong to.
   - **Privilege Mode:** Indicates the security model that this entry should belong to.
     Possible security models are:
     - **NoAuth**: None authentication and none privacy.
     - **Auth**: Authentication and none privacy.
     - **Priv**: Authentication and privacy.
     - **Authentication Protocol** - Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
     - **None:** No authentication protocol.
     - **MD5**: An optional flag to indicate that this user is using MD5

authentication protocol.

- **SHA**: An optional flag to indicate that this user is using SHA authentication protocol.

- **Authentication Password**: Is a string identifying the authentication pass phrase. For both MD5 and SHA authentication protocols, the allowed string length is 8 to 16.
  - **Encryption Protocol**: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
  - **None**: No privacy protocol.
  - **DES**: An optional flag to indicate that this user is using DES authentication protocol.
- **Encryption Key**: A string identifying the privacy pass phrase. The allowed string length is 8 to 16 characters.

2. Click the **Add** button to add the SNMP User.

Viewing an SNMP User

1. On the ***User Setting*** page, the following access group information will be displayed:

- **User Name**: Display the current user name.
- **Group**: Displays the current group.
- **Privilege Mode**: Displays the current privilege mode.
- **Authentication Protocol**: Displays the current authentication protocol.
- **Encryption Protocol:** Displays the current encryption protocol.
- **Access Right:** Displays the current access right.

Deleting an SNMP User

- On the ***User Setting*** page, by selecting the **Delete** button under the **Action** field, next to the SNMP user you wish to delete from the Switch.

SNMPv1, 2 Notification Recipients

Configure SNMPv1 and 2 notification recipients on this page.

Adding SNMPv1 and 2 Notification Recipients

1. On the ***SNMPv1, 2 Host Setting*** page, enter the following information:

- **Server Address:** Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
- **SNMP Version:** Indicates the SNMP trap version supported.
  Possible versions are:
  - **SNMP v1**: Set SNMP trap supported version 1.
  - **SNMP v2c**: Set SNMP trap supported version 2c.
- **Notify Type**: Defines the type of notification, it can be set as **traps** or **informs**.
- **Community Name**: Indicates the community access string when sending an SNMP trap packet.
- **UDP Port**: Indicates the SNMP trap destination port. SNMP Agent will send an SNMP message via this port, the port range is 1~65535.
- **Time Out:** Indicates the SNMP trap inform time-out. The allowed range is 1 to 300.
- **Retries:** Indicates the SNMP trap inform retry times. The allowed range is 1 to 255.

2. Click on the Add button to add the new SNMPv1, 2 host entry.

Viewing SNMPv1 and 2 Notification Recipients

- On the ***SNMPv1, 2 Host Setting*** page, the following notification recipient information will be displayed:
  - **Server Address**: Displays the current server address.
  - **SNMP Version**: Displays the current SNMP version.
  - **Notify Type:** Displays the current notification type.
  - **Community Name:** Displays the current community name.
  - **UDP Port**: Displays the current UDP port.
  - **Time Out**: Displays the current time out.
  - **Retries**: Displays the current retry times.

Deleting SNMPv1 and 2 Notification Recipients

- On the ***SNMPv1, 2 Host Setting*** page, by selecting the **Delete** button under the **Action** field, next to the SNMP notification you wish to delete from the Switch.

Adding a New SNMPv3 Host Entry

1. On the ***SNMPv3 Host Setting*** page, enter the following information:
   - **Server Address:** Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
   - **Notify Type:** Defines the type of notification it can be set as **traps** or **informs**.
   - **User Name:** Indicates the user string when sending an SNMP trap packet.
   - **UDP Port:** Indicates the SNMP trap destination port. SNMP Agent will send the SNMP message via this port, the port range is 1~65535.
   - **Time Out**: Indicates the SNMP trap inform time-out. The allowed range is 1 to 300.
   - **Retries:** Indicates the SNMP trap inform retry times. The allowed range is 1 to 255.
2. Click on the **Add** button to add the new SNMPv3 host entry.

Viewing SNMPv3 Notification Recipients

- On the ***SNMPv3 2 Host Status*** page, the following notification recipient information will be displayed:
  - **Server Address**: Displays the current server address.
  - **SNMP Version**: Displays the current SNMP version.
  - **Notify Type:** Displays the current notification type.
  - **USer Name:** Display the current user name.
  - **UDP Port**: Displays the current UDP port.
  - **Time Out**: Displays the current time out.
  - **Retries:** Displays the current retry times.

Deleting SNMPv3 Notification Recipients

- On the ***SNMPv3 Host Status*** page, by selecting the **Delete** button under the **Action** field, next to the SNMP notification you wish to delete from the Switch.

SNMP Engine ID

Configure SNMPv3 Engine ID on this page. The entry index key is Engine ID. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Applying Changes to the SNMP Engine ID

1. On the ***Engine ID Setting*** page, enter the following information:
   - **Use Default:** Lets you define whether you'd like to use the default Engine ID (**Enabled**) or define your own (**Disabled**)
   - **Engine ID:** An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all zeros and all F's are not allowed.
2. Click on the **Apply** button to apply your changes to the SNMP engine ID.

Viewing SNMP Engine ID Status

- On the ***Engine ID Status*** page, the following engine ID information will be displayed:
  - **User Default**: Displays the current status.
  - **Engine ID**: Displays the current engine ID.

Adding an SNMP Remote Engine ID

You can configure SNMPv3 remote Engine ID on this page.

1. On the ***Remote Engine ID Setting*** page, enter the following information:
   - **Remote IP Address:** Indicates the SNMP remote engine ID address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
   - **Engine ID:** An octet string identifying the engine ID that this entry should belong to.
2. Click on the **Add** button to add the SNMP remote engine ID.

Viewing SNMP Remote Engine ID Status

- On the ***Remote Engine ID Status*** page, the following remote engine information will be displayed:
  - **Remote IP Address**: Displays the current remote IP address.
  - **Engine ID**: Displays the current engine ID.

Deleting an SNMP Remote Engine ID

- On the ***Remote Engine ID Status*** page, by selecting the **Delete** button under the **Action** field, next to the remote engine ID you wish to delete from the Switch.

Port Management

Use the Port Management Menu to display or configure the Managed Switch's ports.

Adding Port Configuration

Configures port configuration settings.

1. On the ***Port Settings*** page, enter the following information:

- **Port Select:** Enables you to choose the port number from this drop-down list.
- **Enabled:** Indicates the port state operation. Possible states are:
  - **Enabled**: Allows you to enable the selected port.
  - **Disabled**: Allows you to disable the selected port.
- **Speed:** Select an available link speed for the given switch port. Click on the drop-down menu to select a mode.
  - **Auto**: Setup Auto negotiation.
  - **Auto-10M**: Set up 10M Auto negotiation.
  - **Auto-100M**: Set up 100M Auto negotiation.
  - **Auto-1000M**: Set up 1000M Auto negotiation.
  - **Auto-10/100M**: Set up 10/100M Auto negotiation.
  - **10M**: Set up 10M Force mode.
  - **100M**: Set up 100M Force mode.
  - **1000M**: Set up 1000M Force mode.
- **Duplex**: Select an available link duplex for the given switch port. Click on the drop-down menu to select a mode.
  - **Auto**: Set up Auto negotiation.
  - **Full**: Force sets Full-Duplex mode.
  - **Half**: Force sets Half-Duplex mode.
- **Flow Control** - When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the

configured column to use flow control. This setting is related to the setting for Configured Link Speed.

- **Current Rx:** Indicates whether pause frames on the port are obeyed.
- **Current Tx:** Indicates whether pause frames on the port are transmitted.

2. Click on the **Apply** button to add the new port configuration.

Viewing a Port's Status

- On the ***Port Status*** page, the following port information will be displayed:
- **Port:** This is the logical port number for this row
  - **Description**: Indicates the port name (when clicked).
  - **Enable State**: Displays the current port state.
  - **Link Status**: Displays the current link status.
  - **Speed**: Displays the current speed status of the port.
  - **Duplex**: Displays the current duplex status of the port.
  - **Flow Control Configuration**: Displays the current flow control configuration of the port.
  - **Flow Control Status:** Displays the current flow control status of the port.

Editing a Ports Description

1. On the ***Port Status*** page, click on the **Edit** button next to the port description you wish to edit.
2. Enter the new port description.
3. Click the **Apply** button to apply the changes to the port description.

Port Counters

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

Viewing Port Counters

1. On the ***Port MIB Counters Settings*** page, select a port from the Port drop-down list.
2. Select a port counter **Mode** radio button. The **Mode** radio button determines the port counter information that is displayed:

- **All:** When this mode is selected all of the port counter information will be displayed.
- **Interface:**
  - **Received Octets**: Displays the total number of octets received on the interface, including framing characters.
  - **Received Unicast Packets:** Displays the number of subnetwork-unicast packets delivered to a higher-layer protocol.
  - **Received Unknown Unicast Packets:** Displays the number of packets received via the interface which is discarded because of an unknown or unsupported protocol.
  - **Received Discards Packets:** Displays the number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
  - **Transmit Octets:** Displays the total number of octets transmitted out of the interface, including framing characters.
  - **Transmit Unicast Packets:** Displays the total number of packets that higher-level protocols requested are transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
  - **Transmit Unknown Unicast Packets:** Displays the total number of packets that higher-level protocols requested are transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

- **Transmit Discards Packets**: The number of inbound packets which is chosen to be discarded even though no errors have been detected to prevent from being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
- **Received Multicast Packets**: Displays the number of packets, delivered by this sub-layer to a higher (sub-) layer, is addressed to a multicast address at this sub-layer.
- **Received Broadcast Packets**: The number of packets, delivered by this sub-layer to a higher (sub-) layer, addressed to a broadcast address at this sub-layer.
- **Transmit Multicast Packets:** The total number of packets that higher-level protocols requested are transmitted and are addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
- **Transmit Broadcast Packets:** The total number of packets that higher-level protocols requested are transmitted, and addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

- **Ethernet Link:**
  - **Alignment Errors:** Displays the number of alignment errors.
  - **FCS Errors:** Displays a count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
  - **Single Collision Frames:** The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
  - **Multiple Collision Frames:** Displays a count of successfully transmitted frames for which transmission is inhibited by more than one collision.
  - **Deferred Transmissions:** Displays a count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
  - **Late Collision:** The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
  - **Excessive Collision:** Displays a count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increase when the interface is operating in Full-Duplex mode.
  - **Frame Too Long:** Displays a count of frames received on a particular interface that exceeds the maximum permitted frame size.
  - **Symbol Errors:** The number of received and transmitted symbol errors.

- **Control In Unknown Opcodes:** Displays the number of received control unknown opcodes.
- **In Pause Frames:** The number of received pause frames.
- **Out Pause Frames:** The number of transmitted pause frames.

- **RMON:**
- **Drop Events:** Displays the total number of events in which packets were dropped due to lack of resources.
  - **Octets:** Displays the total number of octets received and transmitted on the interface, including framing characters.
  - **Packets:** Displays the total number of packets received and transmitted on the interface.
  - **Broadcast Packets:** Displays the total number of good frames received that were directed to the broadcast address.
    Note: This does not include multicast packets.
  - **Multicast Packets:** Displays the total number of good frames received that were directed to this multicast address.
  - **CRC / Alignment Errors:** Displays the number of CRC/alignment errors (FCS or alignment errors).
  - **Undersize Packets:** Displays the total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.
  - **Oversize Packets:** Displays the total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.
  - **Fragments:** Displays the total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
  - **Jabbers:** Displays the total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
  - **Collisions:** Displays the best estimate of the total number of collisions on this Ethernet segment.
  - **64 Bytes Frames:** The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
  - **65-127 Byte Frames:** 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames. The total number of frames (including bad packets) received and transmitted where the number

of octets falls within the specified range (excluding framing bits but including FCS octets).

Bandwidth Utilization

The Bandwidth Utilization page displays the percentage of the total available bandwidth being used on the ports. Bandwidth utilization statistics can be viewed using a line graph.

Viewing Port Utilization

1. On the ***Bandwidth Utilization*** page, click on the **Port Management** folder.
2. Click the **Bandwidth Utilization** link, the following information will be displayed:
   - **Refresh Period:** Allows you to select a period interval between last and next refresh either 2, 5, or 10 seconds.
   - **IFG:** Allow user to enable or disable this Inter Frame Gap (IFG).

Port Mirroring

This function provides monitoring of network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables you to keep close track of switch performance and alter it if necessary.

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

Note: The Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Mirror Application

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

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

Applying Changes to Port Mirroring Settings

1. On the Mirror Setting page, enter the following information:
   - **Session ID**: Enables you to select the port mirror session ID (possible IDs are 1 to 4).
   - **Monitor Session State:** Enable or disable the port mirroring function.
   - **Destination Port:** Select the port to mirror the destination port.
   - **Allow-ingress:** Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.
   - **Sniffer TX Ports:** Displays frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.
   - **Sniffer RX Ports:** Displays frames received at these ports that are mirrored to the mirroring port. Frames transmitted are not mirrored.
2. Click the **Apply** button to apply changes to the port mirroring settings.

Viewing Port Mirroring Status

- On the ***Port MIB Counters Settings*** page, the following port mirroring information will be displayed:
  - **Session ID**: Displays the session ID.
  - **Destination Port:** Displays the mirroring port entry.
  - **Ingress State**: Displays the ingress state.
  - **Source TX Port:** Displays the current TX ports.
  - **Source RX Port:** Displays the current RX ports.

Applying Changes to Jumbo Frame Settings

This page enables you to define the maximum frame size allowed for the switch port.

1. On the ***Jumbo Frame Setting*** page, enter the maximum frame size including FCS (in Bytes) in the **Jumbo Frame** field. The allowed range is 64 - 9216 Bytes.
2. Click on the **Apply** button to apply the Jumbo Frame size.

Viewing Jumbo Frame Size Setting

1. On the ***Jumbo Frame Config*** page, the current Jumbo Frame setting will appear listed under the **Jumbo Frame** field. The allowed range is 64 - 9216 Bytes.

Defining a Recovery Interval for Potential Errors

This page enables you to define the port error disable function.

1. On the ***Error Disabled Recovery*** page, enter the following information:
   - **Recovery Interval**: The period (in seconds) for which a port will be kept disabled in the event a port error is detected (and the port action shuts down the port).
   - **BPDU Guard**: Enable or disable the port error disabled function to check status by BPDU guard.
   - **Self Loop:** Enable or disable the port error disabled function to check status by self loop.
   - **Broadcast Flood:** Enable or disable the port error disabled function to check status by broadcast flood.
   - **Unknown Multicast Flood:** Enable or disable the port error disabled function to check status by unknown multicast flood.
   - **Unicast Flood:** Enable or disable the port error disabled function to check status by unicast flood.
   - **ACL:** Enable or disable the port error disabled function to check status by ACL.
   - **Port Security Violation:** Enable or disable the port error disabled function to check status by port security violation.
   - **DHCP Rate Limit:** Enable or disable the port error disabled function to check status by DHCP rate limit.
   - **ARP Rate Limit:** Enable or disable the port error disabled function to check status by ARP rate limit.
2. Click the **Apply** button to apply changes to the port error disabled settings.

Viewing Port Error Disabled Settings

- On the ***Error Disabled Information*** page, the following information will be displayed:
  - **Recovery Interval:** Displays the current recovery interval time.
  - **BPDU Guard**: Displays the current BPDU guard status.
  - **Self Loop:** Displays the current self loop status.
  - **Broadcast Flood:** Displays the current broadcast flood status.
  - **Unknown Multicast:** Displays the current unknown multicast flood status
  - **Unicast Flood:** Displays the current unicast flood status.

- **ACL:** Displays the current ACL status.
- **Port Security Violation:** Displays the current port security violation status.
- **DHCP Rate Limit:** Displays the current DHCP rate limit status.
- **ARP Rate Limit:** Displays the current ARP rate limit status.

Port Error Disabled

This page displays Errors that have been disabled on a port and the recovery options.

The ports can be disabled by some protocols such as BPDU Guard, Loopback and UDLD.

Viewing Port Error Status

- On the ***Port Error Disabled Status*** page, the following information will be displayed:
  - **Port Name** - Displays the port for error disable.
  - **Error Disable Reason** - Displays the error disabled reason of the port.
  - **Time Left (Seconds)** - Displays the time left in the error interval.

Protected Ports

When a switch port is configured to be a member of a protected group (also called Private VLAN), communication between protected ports within that group can be prevented. Two application examples of this feature are:

- Customers connected to an ISP can be members of the protected group, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other.

For a protected port group to be applied, the switch must first be configured for standard VLAN operation. Ports in a protected port group fall into one of these two groups:

- **Promiscuous** (Unprotected) ports are:
  - Ports from which traffic can be forwarded to all ports in the private VLAN.
  - Ports which can receive traffic from all ports in the private VLAN.
- **Isolated** (Protected) ports are:
  - Ports from which traffic can only be forwarded to promiscuous ports in

the private VLAN.

- Ports which can receive traffic from only promiscuous ports in the private VLAN.

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

Applying Protected Ports Settings

1. On the ***Protected Port Settings*** page, enter the following information:
   - **Port List**: Enables you to select the port from a drop-down list.
   - **Port Type:** Enables you to define whether your selected port is protected.
     - **Protected**: A single stand-alone VLAN that contains one promiscuous port and one or more isolated (or host) ports. This VLAN conveys traffic between the isolated ports and a lone promiscuous port.
     - **Unprotected**: A promiscuous port can communicate with all the interfaces within a private VLAN. This is the default setting.
2. Click on the **Apply** button to apply changes to the protected port.

Viewing Protected Ports Status

- On the Protected Port Status page, the following information will be displayed:
  - **Protected Ports:** Displays the current protected ports.
  - **Unprotected Ports:** Displays the current unprotected ports.

Energy Efficient Ethernet (EEE)

EEE is a power saving standard used to reduces power consumption during low periods of data activity or periods when no data is being transferred (transmitters in the port remain active when no data is being transferred). EEE communicates a protocol to the port enabling the port to function in a Low Power Idle Mode, conserving power during periods of low or no data activity. When a port needs to transmit data, EEE reactivates or wakes the port out of Low Power Idle Mode. The time it takes for EEE to transition the port out of Low Power Idle Mode is referred to as wake up time. Wake up time is defaulted to 17 - 30 µs depending on the link.

EEE devices must agree upon the value of the wake up time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wake up time information using the LLDP protocol. EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode. For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and cannot

be changed. The EEE port settings related to the current unit, as reflected by the page header.

When a port is in Low Power Idle Mode outgoing traffic is stored in a buffer until the port is powered up again. Power can be saved when traffic is buffered until a large amount of traffic can be transmitted.

Enabling/Disabling EEE Port Settings

1. On the ***EEE Port Settings*** page, enter the following information:
   - **Port**: Enables you to select the port from a drop-down list.
   - **Enable**: Enables you to turn EEE function on (enable) or off (disable).
2. Click on the **Apply** button to enable or disable the EEE function on the selected port.

Viewing EEE Port Status

- On the ***EE Enabled Status*** page, the following information will be displayed:
  - **Port**: Displays the switch port number of the logical port.
  - **EEE State**: Displays the current EEE state of the specified port.

Link Aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG can be of different media types (UTP/Fiber, or different fiber types) provided they operate at the same speed.

Aggregated Links can be assigned manually (Port Trunk) or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, duplex setting, etc.

The device supports the following Aggregation links :

- **Static LAGs (Port Trunk):** Force aggregated selected ports to be a trunk group.
- **Link Aggregation Control Protocol (LACP) LAGs:** LACP LAG negotiate

Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high-speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode. For more detailed information, refer to the IEEE 802.3ad standard.

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 8 consecutive ports into a single dedicated connection between any two of the **Switches** or other Layer 2 switches. However, before making any physical connections between devices, use the Link Aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, 100 Mbps fiber, etc.).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation, to avoid creating a data loop.

The Managed Switch allows a maximum of 8 Gigabit Ethernet ports to be aggregated at the same time (up to 8 groups). If the group is defined as an LACP static link aggregation group, any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, the number of ports must be the same as the group member ports.

Applying LAG Settings

The ***LAG Settings*** page allows configuring load balance algorithm settings.

1. On the ***LAG Settings*** page, select a Load Balance Algorithm mode:
   - **MAC Address**: The MAC address can be used to calculate the port for the frame.
   - **IP/MAC Address**: The IP and MAC address can be used to calculate the port for the frame.
2. Click on the **Apply** button to set the LAG.

Viewing LAG Setting

- On the ***LAG Information*** page, the following information will be displayed:
- **Load Balance Algorithm** - Displays the current load balance algorithm.

Applying LAG Management Settings

1. On the ***LAG Management*** page, enter the following information:
   - **LAG**: Select LAG number from this drop-down list.
   - **Name:** Indicates each LAG name.
   - **Type:** Indicates the trunk type. Possible options are:
     - **Static**: Force aggregated selected ports to be a trunk group.
     - **LACP**: LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.
   - **Ports:** Select the port number from this drop-down list to establish Link Aggregation.
2. Click on the **Apply** button to apply the changes to LAG management.

Viewing LAG Management Information

- On the LAG Management Information page, the following information will be displayed:
  - **LAG:** Displays the LAG number.
  - **Name:** Displays the current name.
  - **Type:** Displays the current type.
  - **Link State**: Displays the link state.

- **Active Member** - Displays the active member.
- **Standby Member** - Displays the standby member.

Editing LAG Management Settings

1. On the ***LAG Management*** page, click on the **Edit** button on the **Modify** field next to the LAG management you wish to edit.
2. Enter the new LAG information.
3. Click the **Apply** button to apply the changes to the LAG management.

Configuring LAG Port Setting

1. On the ***LAG Port Settings*** page, enter the following information:
   - **LAG Select**: Enables you to select your desired LAG number.
   - **Enable**: Defines the LAG state operation. Possible options are:
     - **Enabled**: Allows you to enable the LAG.
     - **Disabled**: Allows you to disable the LAG.
   - **Speed:** Select any available link speed for the given switch port. Click on the drop-down menu to select a mode.
     - **Auto**: Set up Auto negotiation.
     - **Auto-10M**: Set up 10M Auto negotiation.
     - **Auto-100M**: Set up 100M Auto negotiation.
     - **Auto-1000M**: Set up 1000M Auto negotiation.
     - **Auto-10/100M**: Set up 10/100M Auto negotiation.
     - **10M**: Set up 10M Force mode.
     - **100M**: Set up 100M Force mode.
     - **1000M**: Set up 1000M Force mode.
   - **Flow Control**: When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used.
2. Click on the **Apply** button to apply the LAG Port settings.

Viewing LAG Port Status

- On the ***LAG Port Status*** page, the following information will be displayed:
  - **LAG**: Displays the LAG number.

- **Description**: Displays the current description.
- **Port Type:** Displays the current port type.
- **Enable State:** Displays the current enable state.
- **Speed:** Displays the current speed.
- **Duplex:** Displays the current duplex mode.
- **Flow Control Config:** Displays the current flow control configuration.
- **Flow Control Status:** Displays the current flow control status.

Configuring LACP System Priority Settings

The ***LACP Settings*** page is used to configure the LACP system priority settings.

1. On the ***LACP Setting*** page, enter a system priority value (1 - 65525) in the **System Priority** field.
   - **System Priority** - A value which is used to identify the active LACP. The Managed Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
2. Click on the **Apply** button to apply the LACP setting changes.

Configuring LACP Port Setting

1. On the ***LACP Port Settings*** page, select a port from the **Port Selection** drop-down list that the LACP settings will apply to.
2. Enter a priority value in the **Priority** field.
   - **Priority**: Controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, this parameter will control which ports will be active and which ports will be in a backup role. A lower number means greater priority.
3. Select a **Timeout** method.
   - **Timeout**: The Timeout controls the period between BPDU transmissions. Short will transmit LACP packets each second, while Long will wait for 30 seconds before sending an LACP packet.
4. Click the **Apply** button to apply the LACP port settings.

Viewing LACP Port Information

- On the ***LACP Port Information*** page, the following information will be displayed:

- **Port Name**: The switch port number of the logical port.
- **Priority:** Displays the current LACP priority parameter.
- **Timeout:** Displays the current timeout parameter.

Viewing LAG Status

- On the ***LAG Status*** page, the following information will be displayed:
  - **LAG**: Displays the current LAG number.
  - **Name**: Displays the current LAG name.
  - **Type:** Displays the current trunk type.
  - **Link State:** Displays the current link state.
  - **Active Member:** Displays the current active member.
  - **Standby Member:** Displays the current standby member.

Viewing LACP Information

- On the ***LAG Information*** page, the following information will be displayed:
  - **LAG:** Displays the current LAG number.
  - **Port:** Displays the current port number.
  - **PartnerSysId:** The system ID of link partner. This field would be updated when the port receives LACP PDU from link partner.
  - **PnKey:** Port key of partner. This field would be updated when the port receives LACP PDU from link partner.
  - **AtKey:** Port key of actor. The key is designed to be the same as trunk ID.
  - **Sel:** The ports LACP selection status.
    - **S:** Means selected.
    - **U:** Means unselected.
    - **D:** Means standby.
  - **Mux**: LACP mux state machine status of the port.
    - **DETACH:** Means the port is in detached state.
    - **WAIT:** Means waiting state.
    - **ATTACH:** Means attach state.
    - **CLLCT:** Means collecting state.
    - **DSTRBT:** Means distributing state.

- **Receiv**: LACP receive state machine status of the port.
  - **INIT:** Means the port is in initialize state.
  - **PORTds:** Means port disabled state.
  - **EXPR:** Means expired state.
  - **LACPds:** Means LACP disabled state.
  - **DFLT:** Means defaulted state.
  - **CRRNT:** Means current state.
- **PrdTx:** LACP periodic transmission state machine status of the port.
  - **no PRD:** Means the port is in no periodic state.
  - **FstPRD:** Means fast periodic state.
  - **SlwPRD:** Means slow periodic state.
  - **PrdTX:** Means periodic TX state.
- **AtState:** The actor state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.
- **PnState:** The partner state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web will show "_"; if the contents are true, the Web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.

VLAN

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also segments the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the

same VLAN, regardless of where they are on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.

The Managed Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As a new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_ VLAN has a VID = 1.

IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This Managed Switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This Managed Switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard.
- Port overlapping, allowing a port to participate in multiple VLANs.
- End stations can belong to multiple VLANs.
- Passing traffic between VLAN-aware and VLAN-unaware devices.

IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging.:

- The untagging feature of IEEE 802.1Q VLAN allows the VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows the VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Terms:

- **Tagging**: The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging**: The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN Tags

There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the

VLAN information intact. This allows 802.1Q VLAN to span network devices (and the entire network, if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, as far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default". As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Assigning Ports to VLANs

Before enabling VLANs, you must first assign each port to the VLAN group(s) in which it will participate. By default, all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you

should add this port to the VLAN as an untagged port.

VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers.

Note: That if you implement VLANs which do not overlap but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

Re-Assigning a VLAN ID.

1. On the ***Management VLAN Setting*** page, select a management VLAN ID from the Management VLAN drop-down menu.
2. Click on the **Apply** button to assign the new VLAN ID.

Viewing the Status of the Management VLAN ID

- On the Management VLAN State page, the following information will be displayed:
  - **Config Name:** Displays the configuration name (Management VLAN).
  - **Config Value:** Displays the current management VLAN value.

Creating a VLAN

1. On the ***VLAN Setting*** page, enter the following information:

- **VLAN List**: Indicates the ID of this particular VLAN.
- **VLAN Action:** Allows users to add or delete VLANs.
- **VLAN Name Prefix:** Indicates the name of this particular VLAN.

2. Click on the **Apply** button to create the new VLAN

Viewing a VLAN

- On the ***VLAN Table*** page, the following information will be displayed:
  - **VLAN ID:** Displays the current VLAN ID entry.
  - **VLAN Name:** Displays the current VLAN ID name.
  - **VLAN Type:** Displays the current VLAN ID type.

Editing a VLAN

1. On the ***VLAN Table*** page, click on the **Edit** button on the **Modify** field next to the VLAN you wish to edit.

2. Enter the new VLAN information:

   - **VLAN List**: Indicates the ID of this particular VLAN.
   - **VLAN Action:** Allows users to add or delete VLANs.
   - **VLAN Name Prefix:** Indicates the name of this particular VLAN.

3. Click the **Apply** button to apply the changes to the selected VLAN.

Interface Settings

This page is used for configuring the switch port VLAN. The VLAN per Port Configuration Page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration Page. All untagged packets arriving to the device are tagged by the ports PVID.

Understand nomenclature of the Switch

- **IEEE 802.1Q Tagged and Untagged**: Every port on an 802.1Q compliant switch can be configured as tagged or untagged.
  - **Tagged**: Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet forwarding decisions.

- **Untagged**: Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

- **IEEE 802.1Q Tunneling (Q-in-Q)** - IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

The Managed Switch supports multiple VLAN tags and can therefore be used in MAN (Metro Access Network) applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the MAN space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customer's VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote customer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType 0x8100 or 0x88A8, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements are reduced.

Applying Changes to Interface Settings

1. On the ***Edit Interface Setting*** page, enter the following information:
   - **Port Select:** Select the VLAN port you wish to configure from the drop-down list.
   - **Interface VLAN Mode:** Set the port's Interface VLAN Mode by selecting either the access, trunk, hybrid or tunnel mode radio button.
     - **Trunk**: The port allows traffic of multiple VLANs.
     - **Access**: The port belongs to one VLAN only.
     - **Hybrid:** The port allows the traffic of multi-VLANs to pass in tag or untag mode.
     - **Tunnel**: Configures IEEE 802.1Q tunneling for a downlink port to another device within the customer network.
   - **PVID**: Allows you to assign PVID (Port VLAN ID) to the selected port. The PVID will be added to all untagged frames entering the ingress port. The PVID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped. The range for the PVID is: 1 - 4094.
   - **Accepted Type**: Determines what type of frames the port will accept. By default, the field is set to All.
     - **All:** All frames are accepted.
     - **Tag Only:** Only tagged frames are accepted.
     - **Untag Only:** Only untagged frames are accepted.
   - **Ingress Filtering** - If ingress filtering is enabled (i.e. checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.
   - **Uplink** - Enable/disable uplink function in trunk port.
   - **TPID** - Configure the type Tag Protocol ID (TPID) of the protocol of switch trunk port.
2. Click on the **Apply** button to apply the interface changes.

Viewing Port VLAN Status

- On the ***Port VLAN Status*** page, the following information will be displayed:
  - **Port:** Displays the switch port number of the logical port.

- **Interface VLAN Mode:** Displays the current interface VLAN mode.
- **PVID:** Displays the current PVID.
- **Accepted Frame Type:** Displays the current access frame type.
- **Ingress Filtering:** Displays the current ingress filtering.
- **Uplink:** Displays the current uplink mode.
- **TPID**: Displays the current TPID.

Port to VLAN

Use the VLAN Static Table to configure port members for the selected VLAN index. This page allows you to add and delete port members of each VLAN.

Adding a Port Member to a VLAN

1. On the ***Port to VLAN Settings*** page, enter the following information:

- **VLAN ID**: Select VLAN ID from this drop-down list to assign VLAN membership.
- **Port**: The switch port number of the logical port.
- **Interface VLAN Mode**: Displays the current interface VLAN mode.
  - **Membership:** Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP.
  - **Excluded**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged:** Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **PVID:** Displays the current PVID.

2. Click the **Apply** button to add the new port member to the VLAN.

Editing a Port Member from a VLAN

1. On the Port VLAN Membership Table page, click on the **Edit** button on the

Modify field next to the VLAN you wish to edit.

2. Enter the new port member information:

- **Port**: The switch port number of the logical port.
- **Mode:** Displays the current VLAN mode.
- **Administrative VLANs:** Displays all the VLANs the interface may be a member of.
- **Operational VLANs:** Displays all the VLANs the interface is current a member of.

3. Click the **Apply** button to apply the changes to the selected port member.

Protocol VLAN Group Setting

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this Managed Switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Configuring Protocol Based VLANs

It is recommended that a separate VLAN is configured for each major protocol running on your network.

1. Add VLAN groups for the protocol you are using.

2. On the ***Add Protocol VLAN Group*** page, enter the following information:

- **Group ID**: Protocol Group ID assigned to the Special Protocol VLAN Group.
- **Frame Type:** Frame Type can have one of the following values:
  - **Ethernet II**
  - **IEEE802.3_LLC_Other**
  - **RFC_1042**
- **Protocol Value (0x0600-0xFFFE)**: The valid value that can be entered in this text field depends on the option selected from the preceding Frame

Type selection menu.Valid values for Protocol Value/EtherType ranging from 0x0600-0xfffe.

3. Click the **Add** button to add the VLAN Group.
4. Next you need to map a protocol group to a VLAN.
5. On the ***Protocol VLAN Port Setting*** page, select a port from the **Port** drop-down list that you wish to assign the protocol group to.
6. Select the protocol group ID from the **Group** drop-down list.
7. On the **VLAN ID** field, enter a VLAN ID.
8. Click on the **Add** button to add the protocol group to the selected VLAN.

Viewing the Status of a VLAN Group

- On the ***Protocol VLAN Group Status*** page, the following information will be displayed:
  - **Group ID:** Displays the current group ID.
  - **Frame Type:** Displays the current frame type.
  - **Protocol Value:** Displays the current Protocol Value/EtherType.

Deleting a VLAN Group

- On the ***Protocol VLAN Group Status*** page, by selecting the **Delete** button under the **Action** field, next to the VLAN group you wish to delete from the Switch.

Mapping a Group to a VLAN Port

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

1. On the ***Protocol VLAN Port Settings*** page, enter the following information:
   - **Port:** Select a port from the drop-down list to assign a Protocol VLAN Group.
   - **Group:** Select a group ID from this drop-down list to assign a Protocol VLAN Group.
   - **VLAN:** Define a VLAN ID assigned to the Protocol VLAN Group.
2. Click on the **Add** button to map the group to a VLAN port.

Viewing a Protocol VLAN Port State

- On the ***Protocol VLAN Port Status*** page, the following information will be displayed:
- **Port:** Displays the current port.
- **Group ID:** Displays the current Group ID.
- **VLAN ID:** Displays the current VLAN ID.
- **Delete:** Click the Delete button to delete the group ID entry.

Deleting a Protocol VLAN Port

- On the ***Protocol VLAN Port State*** page, by selecting the **Delete** button under the **Delete** field, next to the VLAN port you wish to delete from the Switch.

GVRP Setting

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network.

VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Applying GVRP Global Settings

1. On the GVRP Global Setting page, enter the following information:
    - **GVRP:** Controls whether GVRP is enabled or disabled on this switch.
    - **Join Timeout**: The interval between transmitting requests/queries to participate in a VLAN group.
        - **Range**: 20-16375 centiseconds.
        - **Default**: 20 centiseconds.
    - **Leave Timeout**: The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group.
        - **Range:** 45-32760 centiseconds.
        - **Default:** 60 centiseconds.

- **LeaveAll Timeout:** The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
  - **Range:** 65-32765 centiseconds.
  - **Default:** 1000 centiseconds.

Note: Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer.

2. Click on the **Apply** button to apply the GVRP changes.

Viewing GVRP Settings

- On the ***GVRP Informations*** page, the following information will be displayed:
  - **GVRP Status**: Displays the current GVRP status.
  - **Join Timeout:** Displays the current join timeout parameter.
  - **Leave Timeout:** Displays the current leave timeout parameter.
  - **LeaveAll Timeout:** Displays the current leaveall timeout parameter.

Applying GVRP Port Setting

The GVRP Port Setting are assigned and viewed on this page.

1. On the ***Port Settings*** page, enter the following information:
   - **Port Select:** Choose the port from this drop-down list to assign protocol VLAN.
   - **GVRP Enabled:** Controls whether GVRP is enabled or disabled on port.
   - **Registration Mode:** By default GVRP ports are in normal registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the fixed mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in forbidden mode forward only for VLAN 1.
   - **VLAN Creation:** GVRP can dynamically create VLANs on switches for trunking purposes. By enabling GVRP dynamic VLAN creation, a switch will add VLANs to its database when it receives GVRP join messages about VLANs it does not have.
2. Click the **Apply** button to apply the port setting changes.

Viewing GVRP Port Status

- On the ***GVRP Port Status*** page, the following information will be displayed:
  - **Port**: Displays the switch port number for the logical port.
  - **Enable Status:** Displays the current GVRP port state.
  - **Registration Mode:** Displays the current registration mode.
  - **VLAN Creation Status:** Displays the current VLAN creation status.

Viewing GVRP VLAN Status

- On the ***GVRP VLAN Database*** page, the following information will be displayed:
  - **VLAN ID:** Displays the current VLAN ID.
  - **Member Ports:** Displays the current member ports.
  - **Dynamic Ports:** Displays the current dynamic ports.
  - **VLAN Type:** Displays the current VLAN type.

Clearing/Refreshing the GVRP Port Statistics Page

1. On the ***GVRP Port Statistics*** page, you can clear/refresh the following log information:
   - **Port:** The switch port number of the logical port.
   - **Join Empty (Rx/Tx):** Displays the current join empty (TX/RX) packets.
   - **Empty (Rx/Tx):** Displays the current empty (TX/RX) packets.
   - **Leave Empty (Rx/Tx):** Displays the current leave empty (TX/RX) packets.
   - **Join In (Rx/Tx):** Displays the current join in (TX/RX) packets.
   - **Leave In (Rx/Tx):** Displays the current leave in (TX/RX) packets.
   - **Leave All (Rx/Tx):** Displays the current leave all (TX/RX) packets.

2. Click on the one of the buttons to perform one of the following functions:

Button	Function
Clear	Clears the log information on the ***GVRP Port Statistics*** page.
Refresh	Refreshes the log information on the ***GVRP Port Statistics*** page.

Clearing/Refreshing the GVRP Port Error Statistics Page

1. On the ***GVRP Port Error Statistics*** page, you can clear/refresh the following log information:

   - **Port:** The switch port number of the logical port.
   - **Invalid Protocol ID:** Displays the current invalid protocol ID.
   - **Invalid Attribute Type:** Displays the current invalid attribute type.
   - **Invalid Attribute Value:** Displays the current invalid attribute value.
   - **Invalid Attribute Length:** Displays the current invalid attribute length.
   - **Invalid Event:** Displays the current invalid event.

2. Click on the one of the buttons to perform one of the following functions:

Button	Function
Clear	Clears the log information on the ***GVRP Port Error Statistics*** page.
Refresh	Refreshes the log information on the ***GVRP Port Error Statistics*** page.

Spanning Tree Protocol

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this Managed Switch include these versions:

- **STP:** Spanning Tree Protocol (IEEE 802.1D).
- **RSTP:** Rapid Spanning Tree Protocol (IEEE 802.1w).
- **MSTP:** Multiple Spanning Tree Protocol (IEEE 802.1s).

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious network performance degradation if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values:

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier.
- The path cost to the root associated with each switch port.
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch.
- The path cost to the root from the transmitting port.
- The port identifier of the transmitting port.

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

Using a stable STP topology makes the root port the fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a **Blocking** state to a **Forwarding** state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists in one of the following five states:

- **Blocking:** The port is blocked from forwarding or receiving packets.
- **Listening:** The port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.
- **Learning:** The port is adding addresses to its forwarding database, but not yet forwarding packets.
- **Forwarding**: The port is forwarding packets.
- **Disabled:** The port only responds to network management messages and must return to the blocking state first.

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking.
- From blocking to listening or to disabled.
- From listening to learning or to disabled.
- From learning to forwarding or to disabled.
- From forwarding to disabled.
- From disabled to blocking.

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or

more ports. The STP operates in much the same way for both levels.

Note: On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges. On the port level, STP sets the Root Port and the Designated Ports.

Switch User-Configurable STP Parameters

- **Bridge Identifier**: A combination of the user-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address. Default vaules 32768 + MAC.
- **Hello Time:** The length of time between broadcasts of the hello message by the switch. Default value 2 seconds.
- **Maximum Age Timer:** Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer. Default value 20 seconds.
- **Forward Delay Timer:** The amount of time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state. Default value 15 seconds.

Port User-Configurable STP Parameters

- **Port Priority:** A relative priority for each port. Lower numbers give a higher priority and a greater chance of a given port being elected as the root port. The default Value is 128.
- **Port Cost**: A value used by STP to evaluate paths. STP calculates path costs and selects the path with the minimum cost as the active path.
  - **Default Value for Fast Ethernet ports:** 200,000-100Mbps
  - **Default Value for Gigabit Ethernet Ports:** 20,000-1000Mbps

Default Spanning-Tree Configuration

- **Enable state:** STP disabled for all ports.
- **Port priority**: 128
- **Port cost**: 0
- **Bridge Priority:** 32,768

User-Changeable STP Parameters

The switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory, unless absolutely necessary to change. The user-changeable parameters in the switch are as follows:

- **Priority:** A priority for the switch can be set from 0 to 65535. 0 is equal to the highest priority.
- **Hello Time:** The **Hello Time** can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set **Hello Time** will be used if and when your Switch becomes the Root Bridge.

Note: The **Hello Time** cannot be longer than the **Max. Age**. Otherwise, a configuration error will occur.

- **Max. Age:** The **Max. Age** can be from 6 to 40 seconds. At the end of the **Max. Age**, if a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.
- **Forward Delay Timer:** The **Forward Delay Timer** can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

Note: Observe the following formulas when setting the above parameters:

- Max. Age _ 2 x (Forward Delay - 1 second)
- Max. Age _ 2 x (Hello Time + 1 second)

- **Port Priority:** Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.
- **Port Cost:** Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

STP Global Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the Switch. The Managed Switch supports the following Spanning Tree protocols:

- **Compatible -- Spanning Tree Protocol (STP):** Provides a single path between end stations, avoiding and eliminating loops.

- **Normal -- Rapid Spanning Tree Protocol (RSTP):** Detects and uses of network topologies that provide faster Spanning Tree convergence, without creating forwarding loops.
- **Extension – Multiple Spanning Tree Protocol (MSTP):** Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

Applying Changes to STP Global Settings

1. On the ***Global Setting*** page, enter the following information:
   - **Enable:** Enables or disables the STP function. The default value is Disabled.
   - **BPDU Forward:** Sets the BPDU forward method.
   - **PathCost Method**: The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
   - **Force Version:** The STP protocol version setting. Valid values are STP-Compatible, RSTP-Operation and MSTP-Operation.
   - **Configuration Name:** Identifier used to identify the configuration currently being used.
   - **Configuration Revision:** Identifier used to identify the configuration currently being used. Values allowed are 0 - 65535. The default value is 0.
2. Click on the **Apply** button to apply changes to the STP global settings.

Viewing STP Information

- On the ***STP Information*** page, the following information will be displayed:
  - **STP**: Displays the current STP state.
  - **BPDU Forward:** Displays the current BPDU forward mode.
  - **Cost Method:** Displays the current cost method.
  - **Force Version:** Displays the current force version.
  - **Configuration Name:** Displays the current configuration name.
  - **Configuration Revision:** Displays the current configuration revision.

Applying Changes to STP Port Setting

This page allows you to configure STP Port Settings on a per port basis.

1. On the STP Port Setting page, enter the following information:

   - **Port Select :** Select port number from this drop-down list.
   - **External Cost (0 = Auto):** Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
   - **Edge Port**: Controls whether the operEdge flag should start as being set or cleared (The initial operEdge state when a port is initialized).
   - **BPDU Filter:** Control whether a port explicitly configured as Edge will transmit and receive BPDUs.
   - **BPDU Guard:** Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.
   - **P2P MAC:** 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. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

     Note: This applies to physical ports only. Aggregations are always forced Point-to-Point.

   - **Migrate:** If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP compatible) to send on the selected interfaces. The default setting is unchecked.

2. Click on the **Apply** button to apply the port changes.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Recommended STP Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Default STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000

Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

Viewing STP Port Status

- On the STP Port Status page, the following information will be displayed:
  - **Port**: The switch port number of the logical STP port.
  - **Admin Enable**: Displays the current STP port mode status
  - **External Cost**: Displays the current external cost.
  - **Edge Port**: Displays the current edge port status.
  - **BPDU Filter**: Displays the current BPDU filter configuration.
  - **BPDU Guard**: Displays the current BPDU guard configuration.
  - **P2P MAC**: Displays the current P2P MAC status.

Applying Changes to CIST Instance Information Settings

1. On the ***CIST Instance Setting*** page, enter the following information:

- **Priority**: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
- **Max. Hops:** This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.
- **Forward Delay:** The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds The **d**efault value is 15. The value range is minimum the higher of 4 or [(Max. Message Age / 2) + 1] maximum 30.
- **Max Age:** The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds. The default value is 20. The value range is minimum the higher of 6 or [2 x (Hello Time + 1)] and maximum the lower of 40 or [2 x (Forward Delay -1)].

- **Tx Hold Count:** The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.
- **Hello Time:** The time that controls the switch to send out the BPDU packet to check STP current status. Enter a value between 1 - 10.

2. Click the **Apply** button to apply the changes to the CIST instance settings.

Viewing CIST Instance Information

- On the ***CIST Instance Information*** page, the following information will be displayed:
  - **Priority**: Displays the current CIST priority.
  - **Max Hop**: Displays the current Max. Hop.
  - **Forward Delay**: Displays the current forward delay.
  - **Max. Age**: Displays the current Max. Age.
  - **Tx Hold Count:** Displays the current Tx hold count.
  - **Hello Time:** Displays the current hello time.

Applying Changes to CIST Port Setting

This page allows you to configure CIST priority and cost on a per-port basis.

1. On the ***CIST Port Setting*** page, enter the following information:
   - **Port Select** : Select the port number from this drop-down list.
   - **Priority:** Controls the port priority. This can be used to control priority of ports that have an identical port cost. The default value is 128. The value range is 0-240, in steps of 16.
   - **Internal Path Cost (0 = Auto)**: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
2. Click on the **Apply** button to apply changed to the CIST port.

Viewing CIST Port Status

- On the ***CIST Port Status*** page, the following information will be displayed:
  - **Port**: The switch port number of the logical STP port.

- **Identifier (Priority / Port ID):** Displays the current identifier (Priority / Port ID).
- **External Path Cost Conf/Oper:** Displays the current external path cost conf/oper.
- **Internal Path Cost Conf/Oper:** Displays the current internal path cost conf/oper.
- **Designated Root Bridge:** Displays the current designated root bridge.
- **External Root Cost:** Displays the current external root cost.
- **Regional Root Bridge:** Displays the current regional root bridge.
- **Internal Root Cost:** Displays the current internal root cost.
- **Designated Bridge:** Displays the current designated bridge.
- **Internal Port Path Cost:** Displays the current internal port path cost.
- **Edge Port Conf/Oper:** Displays the current edge port conf/oper.
- **P2P MAC Conf/Oper:** Displays the current P2P MAC conf/oper.
- **Port Role:** Displays the current port role.
- **Port State:** Displays the current port state.

Applying Changes to MST Instance Configuration

This page allows the user to configure MST Instance Configuration.

1. On the ***MST Instance Setting*** page, enter the following information:
   - **MSTI ID:** Assign an MSTI ID. The range for the MSTI ID is 1-15.
   - **VLAN List (1-4096):** Assign a VLAN list to special MSTI ID. The range for the VLAN list is 1-4094.
   - **Priority:** Controls the bridge priority. Lower numerical 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.
2. Click on the **Apply** button to apply changes to the MST instance.

Viewing MST Instance Setting Information

- On the ***MST Instance Setting*** Information page, the following information will be displayed:
  - **MSTI**: Displays the current MSTI entry.
  - **Status**: Displays the current MSTI status.
  - **VLAN List:** Displays the current VLAN list.

- **VLAN Count:** Displays the current VLAN count.
- **Priority:** Displays the current MSTI priority.

Viewing MST Instance Status

- On the ***MST Instance Status*** page, the following information will be displayed:
  - **MSTI ID:** Displays the MSTI ID.
  - **Regional Root Bridge:** Displays the current designated root bridge.
  - **Internal Root Cost:** Displays the current internal root cost.
  - **Designated Bridge:** Displays the current designated bridge.
  - **Root Port:** Displays the current root port.
  - **Max. Age:** Displays the current Max. Age.
  - **Forward Delay:** Displays the current forward delay.
  - **Remaining Hops:** Displays the current remaining hops.
  - **Last Topology Change:** Displays the current last topology change.

MST Port Setting

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

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports. The aggregation settings are global.

Applying Changes to MST Port Configuration

On this page you can define the port configuration.

1. On the ***MST Port Setting*** page, enter the following information:
   - **MST ID**: Enter the special MST ID to configure path cost & priority.
   - **Port Select:** Select a port to configure, from this drop-down list.
   - **Priority:** Controls the port priority. This can be used to control priority of ports having identical port cost.
   - **Internal Path Cost (0 = Auto):** Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link

speed, using the 802.1D recommended values. Using the specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range for the MST port is 1 to 200000000.

2. Click on the **Apply** button to apply changes to the MST port.

Viewing MST Port Status

- On the ***MST Port Status*** page, the following information will be displayed:
  - **MSTI ID:** Displays the current MSTI ID.
  - **Port:** The switch port number of the logical STP port.
  - **Identifier (Priority / Port ID):** Displays the current identifier (priority / port ID).
  - **Internal Path Cost Conf/Oper**: Displays the current internal path cost configuration / operation.
  - **Regional Root Bridge:** Displays the current regional root bridget.
  - **Internal Root Cost:** Displays the current internal root cost.
  - **Designated Bridge:** Displays the current designated bridge.
  - **Internal Path Cost:** Displays the current internal path cost.
  - **Port Role:** Displays the current port role.
  - **Port State:** Display the current port state.

STP Statistics

This page displays STP statistics.

Viewing STP Statistics

- On the ***STP Statistics*** page, the following information will be displayed:
  - **Port**: The switch port number of the logical STP port.
  - **Configuration BPDUs Received:** Display the current configuration BPDUs received.
  - **TCN BPDUs Received:** Displays the current TCN BPDUs received.
  - **MSTP BPDUs Received:** Displays the current MSTP BPDUs received.
  - **Configuration BPDUs Transmitted:** Displays the configuration BPDUs transmitted.
  - **TCN BPDUs Transmitted:** Displays the current TCN BPDUs transmitted.

- **MSTP BPDUs Transmitted:** Displays the current BPDUs transmitted.

Multicast

Applying Changes to Properties Settings

1. On the ***Properties Setting*** page, enter the following information:
   - **Unknown Multicast Action** - Enables you to define the unknown multicast traffic method.
     - **Options include:** Drop, Flood or Send to router port.
   - **IPv4 Forward Method** - Configure the IPv4 multicast forward method.
   - **IPv6 Forward Method** - Configure the IPv6 multicast forward method.
2. Click on the **Apply** button to apply changes to the Properties settings.

Viewing Properties Information

- On the ***Properties Information*** page, the following information will be displayed:
  - **Unknown Multicast Action**: Displays the current unknown multicast action status.
  - **Forward Method For IPv4:** Displays the current IPv4 multicast forward method.
  - **Forward Method For IPv6:** Displays the current IPv6 multicast forward method.

IGMP Snooping

The Internet Group Management Protocol (IGMP) lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

About Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The Internet Group Management Protocol (IGMP) is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one

multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given subnetwork or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnetwork. If there are no members on a subnetwork, packets will not be forwarded to that subnetwork.

Applying Changes to IGMP Snooping Settings

This page allows you to configure IGMP Snooping settings.

1. On the ***IGMP Snooping*** page, enter the following information:
   - **IGMP Snooping Status:** Allows you to Enable or Disable IGMP Snooping. By default the status is set to Disabled.
   - **IGMP Snooping Version:** Allows you to set the IGMP Snooping Version.
     - **V2**: Allows you to set the IGMP Version to version 2.
     - **V3:** Allows you to set the IGMP Version to version 3.
   - IGMP Snooping Report Suppression: Allows you to Enable or Disable the IGMP Snooping Report. When the IGMP Snooping Report Suppression is set to Disabled all IGMP reports are sent to multicast-capable routers. By default the status is set to Disabled.
2. Click the **Apply** button to apply changes to the **IGMP Snooping Settings**.

Viewing IGMP Snooping Information

- On the ***IGMP Snooping Information*** page, the following information will be displayed:
  - **IGMP Snooping Status:** Displays the current IGMP Snooping Status (Enabled or Disabled).
  - **IGMP Snooping Version:** Displays the current IGMP Snooping Version (V2 or V3).
  - **IGMP Snooping V2 Report Suppression:** Displays whether IGMP Snooping version 2 report suppression is Enabled (suppressing the reports) or Disabled (not suppressing the reports).

Viewing IGMP Snooping Table

- On the ***IGMP Snooping Table*** page, the following information will be displayed:
  - **Entry No.:** Displays the current entry number.
  - **VLAN ID:** Displays the current VLAN ID.
  - **IGMP Snooping Operation Status:** Display the current IGMP Snooping operation status (Enabled or Disabled).
  - **Router Ports Auto Learn:** Displays the current router port auto learning setting.
  - **Query Robustness:** Displays the current query robustness. Increasing this value allows for more packet loss but also increase the subnetwork's leave latency. The Query Robustness value can be set from 2 - 10.
  - **Query Interval (sec.):** Displays the current query interval in seconds.
  - **Query Max Response Interval (sec.):** Displays the current query max response interval.
  - **Last Member Query Count:** Displays the current last member query count.
  - **Last Member Query Interval (sec.):** Displays the time in seconds, between group query messages).
  - **Immediate Leave:** Tracks hosts sending membership reports to determine when the last host on leaves a multicast group (Enabled or Disabled).

Editing IGMP Snooping Table Settings

- On the ***IGMP Snooping Table*** page, Click the **Edit** button, under the **Modify** field, to make changes to the IGMP Snooping Table settings.

IGMP Querier

Applying Changes to IGMP Querier Settings

An IGMP Querier is a router or multicast enabled switch that queries the LAN for group members. The Querier communicates query packets to all the switches connected to the network.

1. On the ***IGMP Querier Settings*** page, enter the following information:
   - **VLAN ID:** From the drop-down list, select the ID of the of the router or switch you wish to designate as the IGMP Querier.
   - **Querier State:** Indicates if the selected VLAN ID is set as the IGMP Querier (Enabled or Disabled). By default the setting is Disabled.
   - **Querier Version:** Allows you to set the IGMP Snooping Version. By default the setting is V2.
     - **V2** - Allows you to set the Querier Version to version 2.
     - **V3** - Allows you to set the Querier Version to version 3.
2. Click on the **Apply** button, to apply the IGMP Querier settings.

Viewing IGMP Querier Status

- On the ***IGMP Querier Status*** page, the following information will be displayed:
  - **VLAN ID:** Displays the current VLAN ID
  - **Querier State:** Displays the current querier state (Enabled or Disabled).
  - **Querier Status:** Displays the current querier status (Non-Querier or Querier)
  - **Querier Version:** Displays the current querier version (V2 or V3).
  - **Querier IP:** Displays the querier's IP address.

IGMP Static Group

Adding an IGMP Static Group:

For tighter control you can configure a multicast service on the Managed Switch. You will need to add all the ports connected to the hosts to a common VLAN and then assign the multicast service to that VLAN group.

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

1. On the ***Add IGMP Static Group*** page, enter the following information:
   - **VLAN ID:** From the drop-down list select a VLAN ID for the static group.
   - **Group IP Address:** Enter the IP address for the static group.
   - **Member Ports:** From the drop-down list select the port numbers you want to add to the static group.
2. Click the **Add** button, to add the new IGMP Static group.

Adding Additional Ports to an IGMP Static Group

1. On the ***Add IGMP Static Group*** page, select a VLAN for the desired static group from the **VLAN ID** drop-down list.
2. Select a port number from the **Member Ports** drop-down list.
3. Click the **Add** button to add the additional ports to the selected static group.

Viewing IGMP Static Group Information

- On the ***IGMP Static Group*** page, the following information will be displayed:
  - **VLAN ID:** Displays the static group's VLAN ID.
  - **Group IP Address:** Displays the static group's IP address.
  - **Member Ports:** Displays the ports that are connected to the static group.

Editing IGMP Static Group Information

- On the ***IGMP Static Group*** page, click the **Edit** button, to make changes to the IGMP Static Group settings.

Viewing IGMP Group Table Information

- On the ***IGMP Group Table*** page, the following information will be displayed:
  - **VLAN ID:** Displays the static group's VLAN ID.
  - **Group IP Address:** Displays the static group's IP address.
  - **Member Ports:** Displays the ports that are connected to the static group.
  - **Type:** Displays the member type either Static (e.g. Static Group) or Dynamic.
  - **Life:** Displays the static group's life in seconds.

IGMP Router

Adding a Router Port

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. If the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your Managed Switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the Managed Switch.

1. On the ***Add Router Port*** page, select the **VLAN ID**.
2. Select a router **Type** either:
   - **Static:** Select which ports you want to designate as a router port.
   - **Forbid**: Select which ports you do not want to designate as a router port.
3. Click the **Add** button to add the router port.

Adding Additional Ports to a Router Port

1. On the ***Add Router Port*** page, select a VLAN for the desired static group from the **VLAN ID** drop-down list.
2. Select a port type either **Static** or **Forbid** from the **Type** field.
3. Select a port number from the **Member Ports** drop-down list.
4. Click the **Add** button to add the additional ports.

Viewing Router Port Status

- On the ***Router Port Status*** page, the following information will be displayed:
  - **VLAN ID:** Displays the VLAN ID
  - **Static Ports:** Displays a list of ports that have been designated as a router port.
  - **Forbidden Ports:** Displays a list of ports that are designated as forbidden ports.

Editing/Deleting Router Ports

- On the ***Router Port Status*** page, click the **Edit or Delete** button under the **Modify** field, to make changes to the settings.

Viewing the Dynamic Router Table

- On the ***Dynamic Router Table*** page, the following information will be displayed:
  - **VLAN ID:** Displays the VLAN ID
  - **Port:** Displays a list of ports designated as dynamic router ports.
  - **Expiry Time (sec):** Displays the current expiration time in seconds.

Viewing the Static Router Table

- On the ***Static Router Table*** page, the following information will be displayed:
  - **VLAN ID:** Displays the VLAN ID
  - **Port Mask:** The port's port mask number indicating which channels are connected (1) and which are not connected (0).

Viewing the Forbidden Router Table

- On the ***Forbidden Router Table*** page, the following information will be displayed:
  - **VLAN ID:** Displays the VLAN ID
  - **Port Mask:** The port's port mask number indicating which channels are connected (1) and which are not connected (0).

Applying an IGMP Forward All

1. On the ***IGMP Forward All*** page, select a **VLAN ID** from the drop-down list.

2. Next to the corresponding **Port** switch port number, select a **Membership** type:
   - **Static:** The interface is a member of the IGMP.
   - **Forbidden:** The interface is forbidden from automatically joining the IGMP via Multicast VLAN Registration (MVR).
   - **None:** The interface is not a member of the VLAN. Packets associated with this VLAN are not transmitted by the interface.
3. Click the **Apply** button to apply your changes.

Clearing/Refreshing IGMP Snooping Statistics

1. On the ***IGMP Snooping Statistics*** page, you can clear/refresh the following information:
   - **Total RX:** Displays the total packets received.
   - **Valid RX:** Displays the amount of valid packets received.
   - **Invalid RX:** Displays the amount of invalid packets received.
   - **Other RX:** Displays the amount of other packets received.
   - **Leave RX:** Displays the amount of leave packets received
   - **Report RX:** Displays the amount of packet reports received
   - **General Query RX:** Displays the amount of general query packets received
   - **Special Group Query RX:** Displays the amount of special group query packets received.
   - **Special Group & Source Query RX:** Displays the amount of special group and source query packets received.
   - **Leave TX:** Displays the amount of leave packets transmitted.
   - **Report TX:** Displays the amount of report packets transmitted.
   - **General Query TX:** Displays the amount of general query packets transmitted.
   - **Special Group Query TX:** Displays the amount of special group query packets transmitted.
   - **Special Group & Source Query TX:** Displays the amount of special group and source query packets transmitted.

2. Click on the **Clear** button to clear the statistics data displayed.

or

3. Click on the **Refresh** button to refresh the statistics.

MLD Snooping

This page provides MLD Snooping related configuration. Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header.

Applying Changes to MLD Snooping

1. On the ***MLD Snooping*** page, enter the following information:
   - **MLD Snooping:** Allows you to disable or enable MLD Snooping functionality. The default value of this field is Disabled.
   - **MLD Snooping Version** - Sets the MLD Snooping operation version.
     - **v1**: Set MLD Snooping to support MLD version 1.
     - **v2**: Set MLD Snooping to support MLD version 2.
   - **MLD Snooping Report Suppression** - Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all MLD reports are sent as is to multicast-capable routers. The default is enabled.
2. Click the **Apply** button to implement your changes to MLD Snooping.

Viewing MLD Snooping Information

- On the ***MLD Snooping Informations*** page, the following information will be displayed:
  - **MLD Snooping Status** - Displays the current MLD snooping status.
  - **MLD Snooping Version** - Displays the current MLD snooping version.
  - **MLD Snooping Report Suppression** - Displays the current MLD snooping report suppression.

Clearing/Refreshing MLD Snooping Statics

1. On the ***MLD Snooping Statistics*** page, the following information will be displayed:

   - **Total Rx:** Displays the current total Rx.
   - **Valid Rx:** Displays the current valid Rx.
   - **Invalid Rx:** Displays the current invalid Rx.
   - **Other Rx:** Displays the current other Rx.
   - **Leave Rx:** Displays the current leave Rx.
   - **Report Rx:** Displays the current report Rx.
   - **General Query Rx:** Displays the current general query Rx.
   - **Special Group Query Rx:** Displays the current special group query Rx.
   - **Special Group & Source Query Rx:** Displays the current special group & source query Rx.
   - **Leave Tx:** Displays the current leave Tx.
   - **Report Tx:** Displays the current report Tx.
   - **General Query Tx:** Displays the current general query Tx.
   - **Special Group Query Tx:** Displays the current special group query Tx.
   - **Special Group & Source Query Tx:** Displays the current special group & source query Tx.

2. Click on the **Clear** button to clear the statistics data displayed.

   or

3. Click on the **Refresh** button to refresh the statistics.

Multicast Throttling Settings

Multicast throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either "deny" or "replace". If the action is set to deny, any new multicast join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

Once you have configured multicast profiles, you can assign them to interfaces on the Managed Switch. Also you can set the multicast throttling number to limit the number of multicast groups an interface can join at the same time.

Making Changes to the Max Groups and Action Settings:

1. On the ***Max Groups and Action Settings*** page, select an **IP Type** from this drop-down list.
2. Select a port from the **Port Select** drop down list.
3. Enter the maximum number of multicast groups an interface can join at the same time (0-256).
4. Select an **Action** radio button that will indicate what will happen when the maximum number of multicast groups is exceeded.
   - **Deny:** The new multicast group join report is dropped
   - **Replace:** The new multicast group replaces an existing group
5. Click the **Apply** button to apply changes to the max groups settings.

Viewing IGMP Port Max. Groups Information

- On the ***IGMP Port Max Group Informations*** page, the following information will be displayed:
  - **Port**: Displays the number of the logical port.
  - **Max. Groups:** Displays the current Max. Groups.
  - **Action:** Displays the current action.

Multicast Filter

In certain switch applications, the administrator may want to control the multicast services that are available to end users. For example, an IPTV service is based on a specific subscription plan. The multicast filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port.

Multicast filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A multicast filter profile can contain one or more, or a range of multicast addresses, but only one profile can be assigned to a port. When enabled, multicast join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the multicast join report is forwarded as normal. If a requested multicast group is denied, the multicast join report is dropped.

When you have created a Multicast profile number, you can then configure the

multicast groups to filter and set the access mode.

Command Usage

- Each profile has only one access mode, either permit or deny.
- When the access mode is set to permit, multicast join reports are processed when a multicast group falls within the controlled range.
- When the access mode is set to deny, multicast join reports are only processed when the multicast group is not in the controlled range.

Quality of Service

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multimedia, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to control a wide variety of network traffic by:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities for time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Providing predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improving performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reducing the need to constantly add bandwidth to the network.
- Managing network congestion.

Implementing QoS on Your Network:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.

4. Apply a QoS profile to a port(s).

The QoS page of the Managed Switch contains three types of QoS mode - the 802.1p mode, DSCP mode or Port-Base Priority Mode can be selected. Each of the three modes rely on predefined fields within the packet to determine the output queue.

- **802.1p Tag Priority Mode:** The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **IP DSCP Mode:** The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- **Port-Base Priority Mode:** Any packet received from the specified high priority port will be treated as a high priority packet.

The Managed Switch supports eight priority level queue, the queue service rate is based on the WRR (Weighted Round Robin) and WFQ (Weighted Fair Queuing) alorithm. The WRR ratio of high-priority and low priority can be set to 4:1 and 8:1.

Security

This section lets you control access to the switch, including the user access and management control.

The Security Page contains links to the following main topics:

- 802.1x
- Radius Server
- TACACS+ Server
- AAA
- Access
- Management Access Method
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- DoS
- Strom Control

802.1X

In the 802.1X world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the Switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

RADIUS Server

This page is used to configure the RADIUS server connection session parameters.

Configuring Use Default Parameters

1. On the ***Use Default Parameters*** page, enter a **Retries** value in seconds. Retries refers to the amount of time the switch waits for a reply from a RADIUS server before retransmitting a request.

2. Enter a **Timeout for Reply** value. This value is the number of times a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be offline.

3. Enter a **Dead Time** value. This value is the period (in seconds) during which the switch will not send new requests to a server that has failed to respond to a previous request.

4. Enter a Key String value. This value a secret key shared between RADIUS server and the Switch.

5. Click the **Apply** button to apply changes to the RADIUS server table.

Adding a New Radius Server

This screen allows you to setup a new RADIUS server.

1. On the ***New RADIUS Server*** page, select a **Server Definition**.
2. Enter the **Server IP** address of the RADIUS server.
3. Enter the **Authentication Port.** This port is used as the UDP port on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
4. Enter an **Acct Port.** This port is used to set the UDP port on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
5. Enter a **Key String,** the key shared between the RADIUS Authentication Server and the Switch.

   - or -

6. Select **Use Default** to use a Default key string.
7. Enter a **Timeout for Reply** value. The value is the maximum time to wait for a reply from a server.

   - or -

8. Select **Use Default** to use a Default setting.

   Note: If the server does not reply within this timeframe, we will consider it to be dead and continue with the next enabled server. In order to cope with lost frames, the timeout interval is divided into three subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.

9. Enter the number of **Retries** to wait for a reply from a RADIUS server before retransmitting the request.

   - or -

10. Select **Use Default** to use a Default setting.
11. Enter a **Server Priority** value.

12. Enter a **Dead Time** value. The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

13. Select a **Usage Type radio button:**

- Login
- 802.1X
- All

14. Click the Add button to add the new RADIUS server.

Editing/Deleting a Login Authentication List

1. On the ***Login Authentication List*** page, the following information is displayed:

- **IP Address:** Displays the current IP address.
- **Auth Port:** Displays the current auth port.
- **Acct Port:** Displays the current acct port.
- **Key:** Displays the current key.
- **Timeout:** Displays the current timeout.
- **Retries:** Displays the current retry times.
- **Priority:** Displays the current priority.
- **Dead Time:** Displays the current dead time.
- **Usage Type:** Displays the current usage type.
- **Modify:** Click to edit login authentication list parameter.

2. Click on the **Edit** button to edit any of the authentication list parameters.

- or -

3. Click on the **Delete** button to an authentication list parameter.

Configuring TACACS+ Server Session Parameters

This page is to configure the TACACS+ server connection session parameters.

1. On the **Use Default Parameter** page, enter a **Key String.** A secret key shared between the TACACS+ server and the switch.
2. Enter a **Timeout for Reply** value. The number of times a TACACS+ request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit, it is considered to be dead.
3. Click the **Add** button to apply the changes.

Adding a New TACACS+ Server

1. On the ***New TACACS+ Server*** page, enter a **Server Definition**.
2. Enter the **Server IP** address of the TACACS+ server.
3. Enter the **Server Port,** Network (TCP) port of TACACS+ server used for authentication messages.
4. Enter a **Server Key.** The key is shared between the TACACS+ Authentication Server and the switch.

   - or -

5. Select **Use Default** to use a Default setting.
6. Enter a **Server Timeout** value. The number of seconds the switch waits for a reply from the server before it resends the request.

   - or -

7. Select **Use Default** to use a Default setting.
8. Enter a **Server Priority**.
9. Click on the Add button to add the new TACACS+ Server.

Editing/Deleting a TACACS+ Server Authentication List

1. On the ***Login Authentication List*** page, the following information is displayed:
   - **IP Address**: Displays the current IP address.
   - **Port:** Displays the current port.
   - **Key:** Displays the current key.

- **Timeout:** Displays the current timeout.
- **Retries:** Displays the current retry times.
- **Priority:** Displays the current priority.
- **Modify:** Click to edit login authentication list parameter.

2. Click on the **Edit** button to edit any of the authentication list parameters.

   - or -

3. Click on the **Delete** button to an authentication list parameter.

AAA

Authentication, authorization, and accounting (AAA) provides a framework for configuring access control on the Managed Switch. The three security functions can be summarized as follows:

- **Authentication** - Identifies users that request access to the network.
- **Authorization** - Determines if users can access specific services.
- **Accounting** - Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are then applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group; if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The Managed Switch supports the following AAA features:

- Accounting for IEEE 802.1X authenticated users that access the network through the Managed Switch.
- Accounting for users that access management interfaces on the Managed Switch through the Telnet.
- Accounting for commands that users enter at specific CLI privilege levels. Authorization of users that access management interfaces on the Managed Switch through the Telnet.

Configuring AAA on the Managed Switch:

1. Configure RADIUS and TACACS+ server access parameters. See "Configuring Local/ Remote Logon Authentication".

2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.

3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use. Apply the method names to port or line interfaces.

Access

This section enables you to control remote access to the Switch, including the different access methods. From this section you can control:

- **Telnet**
- **SSH**
- **HTTP**
- **HTTPS**

Managed Access Method

This section enables you to define the rules for accessing the switch. From this section you can define:

- Profile Rules
- Access Rules

DHCP Snooping

The addresses assigned to DHCP clients on unsecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall. When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP

messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.

- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to/from the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- Filtering rules are implemented as follows:
  - If global DHCP snooping is disabled, all DHCP packets are forwarded.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded to a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.
  - If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:
  - If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
  - If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.

- If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
- If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet from a server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

- Additional considerations when the switch itself is a DHCP client – The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server. Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Applying DHCP Snooping Setting

- On the ***DHCP Snooping Setting*** page, Select either to **Enable** or **Disable** DHCP Snooping on the Swtich:
  - **Enabled:** Enables DHCP Snooping. When enabled, DHCP messages will only be sent to trusted ports and will only allow reply packets from trusted ports.
  - **Disabled:** Disables DHCP Snooping.

Viewing DHCP Snooping Informations

- On the ***DHCP Snooping Informations*** page, the following information is displayed:
  - **Information Name:** Displays the title of the field "DHCP Snooping".
  - **Information Value:** Displays the DHCP Snooping status (**Enabled** or **Disabled**).

DHCP Snooping VLAN Setting

Command Usage

- When DHCP snooping is globally enabled on the specified VLAN, DHCP packet filtering will be performed on any suspicious ports within the VLAN.
- DHCP snooping can be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally enabled.
- When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

Applying DHCP Snooping VLAN Setting

1. On the ***DHCP Snooping VLAN Setting*** page, Enter a **VLAN List.** A list of VLAN IDs that DHCP Snooping VLAN will apply to.
2. Select a **Status** either **Enable** or **Disable,** DHCP Snooping VLAN:
   - **Enabled:** Enables DHCP Snooping on the VLAN. When enabled, DHCP messages will only be sent to trusted ports and will only allow reply packets from trusted ports.
   - **Disabled:** Disables DHCP Snooping on the VLAN.
3. Click on the **Apply** button to apply the DHCP Snooping VLAN Settings.

Setting up DHCP Snooping VLAN

1. On the ***DHCP Snooping VLAN Setting*** page, select the **Enabled** radio button.

Note: Select the **Disabled** radio button to disable DHCP Snooping VLAN.

2. Click the **Apply** button.

Viewing DHCP Snooping VLAN Setting

- On the ***DHCP Snooping VLAN Setting*** page, the following information will be displayed:
  - **VLAN List:** Displays a list of VLAN IDs.
  - **Status:** Displays the status of DHCP Snooping VLAN (**Enable** or **Disable**).

Port Setting

Allows you to configure whether a port is trusted or untrusted.

Command Usage

- A trusted port is a port that is configured to receive messages only from within the network.
- An untrusted port is a port that is configured to receive messages from outside the network or firewall.
- When DHCP snooping is enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.
- When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with the port will be removed.

Applying DHCP Snooping Port Settings

1. On the ***DHCP Snooping Port Setting*** page, select a **Port** From the drop-down list.
2. Select a DHCP Snooping port **Type** radio button:
   - **Trusted:** Receives messages from within the network.
   - **Untrusted:** Receives messages from outside the network or firewall.
3. Select whether to Enable or Disable **Chaddr Check,** Client Hardware Address (CHADDR) Checking on the selected port.
4. Click the **Apply** button to apply the DHCP Spooning Port settings.

Viewing DHCP Snooping Port Settings

- On the ***DHCP Snooping Port Settings*** page, the following information will be displayed:
  - **Port:** Displays the port number the DHCP Snooping settings are applied to.
  - **Type:** Displays the port status type (trusted or untrusted)
  - **Chaddr Check:** Displays whether CHADDR checking is enabled or disabled on the corresponding port.

Clearing DHCP Snooping Statistics Page

1. On the ***DHCP Snooping Statistics*** page, the following information can be cleared/refreshed:
   - **Port:** Displays the port number the DHCP Snooping settings are applied to.
   - **Forwarded:** Displays the number of packets forwarded.
   - **Chaddr Check Dropped:** Displays the number of CHADDR checks dropped.
   - **Untrusted Port Dropped:** Displays the number of untrusted ports dropped.
   - **Untrusted Port with Option82 Dropped:** Displays the number of untrusted ports with Option82 configured that were dropped.
   - **Invalid Dropped:** Displays the number if invalid ports dropped.
2. Click the **Clear** button to clear the current information from the ***DHCP Snooping Statistics*** page.

   - or -

3. Click the **Refresh** button to refresh the information on the ***DHCP Snooping Statistics*** page.

Database Agent

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 database entries (bindings).

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DCHP spoofing attacks.

When reloading, the switch reads the binding file to rebuild the DHCP snooping binding database. The switch keeps the file current by updating it when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database and entries in the binding file. The frequency at which the file is updated is based on a configurable delay (**Timeout**), and the updates are batched. If the file is not updated in a specified time (set by the **Write-Delay** and **Abort-Timeout** values), the update stops.

Configuring DHCP Snooping Database

1. On the ***DHCP Snooping Database*** page, select a **Database Type** from the drop-down list.
2. Enter a **File Name.** The file name will be used as a bindings backup file name.
3. Enter the **Remote Server's** IP address.
4. Enter a **Write Delay** value. This value is the amount of time (in seconds) the binding file backup will be delayed.
5. Enter a **Timeout** value. This value is the amount of time (in seconds) to delay the binding file backup after the binding database changes.
6. Click the **Apply** button to apply all of the changes.

Viewing DHCP Snooping Database Information

- On the ***DHCP Snooping Database Informations*** page, the following information will be displayed:
  - **Database Type:** Displays the selected database type.
  - **FileName:** Displays the binding backup file name.
  - **Remote Server:** Displays the remote server's IP address.
  - **Write Delay:** Displays the amount of time (in seconds) the binding file backup will be delayed.
  - **Timeout:** Displays the amount of time (in seconds) to delay the binding file backup after the binding database changes.

Configuring DHCP Snooping Rate Limit Settings

Allows you to define the number of packets that are transmitter or received per second through trusted and untrusted ports.

1. On the ***DHCP Rate Limit Setting*** page, select a **Port** from the drop-down list that you want to apply the DHCP Rate Limit settings to.
2. Select a port **State** either (**Default** or **User Defined**).
3. Enter a **Rate Limit (pps):** Enter the number of packet transmitted or received per second. By default this field is set to **Unlimited**.
4. Click the **Apply** button to apply all of the changes.

Viewing DHCP Rate Limit Settings

- On the ***DHCP Rate Limit Config*** page, the following information will be displayed:
  - **Port Name:** Displays the name of the port the DHCP rate limit is applied to.
  - **Rate Limit (pps):** Displays the packets per second rate limit.

Option82 Global Setting

DHCP Option82 is a relay mechanism for sending information about the switch and its DHCP clients to DHCP servers. It allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks from attached clients on DHCP services, such as IP spoofing, client identifier spoofing, MAC address spoofing, and address exhaustion.

The DHCP Option82 enables a DHCP relay agent to insert specific information into a DHCP request packet when forwarding client DHCP packets to a DHCP server, and remove the specific information from a DHCP reply packet when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

- **Circuit ID (option 1):** The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on.
- **Remote ID (option 2):** The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is VLAN ID, Module ID and Port Number.

Configuring Option82 Global Setting

1. On the ***Option82 Global Setting*** page, select the remote ID **State** (**Default** or **User Defined**):
   - **Default:** Uses the default VLAN MAC format.
   - **User Defined:** Uses user defined remote ID content.
2. Click the **Apply** button.

Viewing Option82 Global Settings

- On the ***Option82 Global Setting*** page, the following information will be displayed:
  - **Option82 Remote ID:** Displays the Option82 remote ID.

Option82 Port Settings

This function is used to set the retransmitting policy of the system for the received DHCP request message which contains Option82.

Configuring Option82 Port Settings

1. On the ***Option82 Port Setting*** page, select a **Port** number to apply the Option82 settings to.
2. Select to either enable or disable Option82 settings on the selected port.
3. Select an **Allow Untrusted** mode from the drop-down list:
   - **Drop:** If a message is using Option82 the system will drop it without processing the message.
   - **Keep:** The system will keep any message segments using Option82 and forward it to the server to process.
   - **Replace:** The system will replace the Option82 segment in the message with its own Option82 segment and forward it to the server to process.
4. Click the **Apply** button.

Viewing Option82 Port Setting

- From the ***Option82 Port Settings*** page, the following information will be displayed:
  - **Port:** Displays the port number.
  - **Enable:** Displays whether Option82 is enabled or disabled on the selected port.
  - **Allow Untrusted:** Displays the allow untrusted mode (**Drop**, **Keep**, or **Replace**).

Configuring Option82 Circuit-ID Settings

Allows you to define the parameters for circuit-id sub-option.

1. On the ***Option82 Port Circuit-ID Setting*** page, select a **Port** number from the drop-down list to apply the Option82 Circuit-ID settings to.
2. Select a **VLAN ID**.
3. Select a **Circuit ID** radio button. The Circuit ID allows you to use the default Option82 circuit ID or enter a user defined circuit ID.
   - **Default:** Uses the default circuit ID.
   - **User-Define:** Enter a user defined circuit ID.
4. Click the **Apply** button.

Viewing Configuring Option82 Port Circuit-ID Settings

- On the ***Option82 Port Setting*** page, the following information will be displayed:
  - **Port:** Displays the port number.
  - **VLAN:** Displays the VLAN ID.
  - **Circuit ID:** Displays the circuit ID.

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. This page provides ARP Inspection related configuration.

Configuring Dynamic ARP Inspection Settings

1. On the ***DAI Setting*** page, select whether to enable or disable Global Dynamic ARP Inspection.
2. Click the **Apply** button.

Viewing DAI Informations

- From the ***DAI Informations*** page, the following information will be displayed:
  - **DAI:** Displays the current DAI status (**Enabled** or **Disabled**).

Configuring Dynamic VLAN Settings

1. On the ***DAI Informations*** page, enter a VLAN numbers within the VLAN List field.
2. Select a **Status** either enable or disable Dynamic VLAN on the corresponding VLAN ID.
3. Click the **Apply** button.

Viewing DAI VLAN Setting

- On the ***DAI VLAN Settings*** page, the following information will be displayed
  - **VLAN LIST:** Displays the VLAN ID.
  - **Status:** Displays whether Dynamic ARP Inspection is enabled or disabled on the corresponding VLAN ID.

Configuring DAI Port Settings:

1. On the ***DAI Port Setting*** page, select the port(s) you want to apply the DAI port settings to apply to.
2. Select a **Type** either **Un Trusted** or **Trusted.**
3. Select whether to enable or disable **Src-Mac Chk:**
   - If enabled, the system compares the source MAC address in the Ethernet header to the sender MAC address in the ARP body. If the MAC addresses are different the system tags it as invalid and drops the packets. This check is performed on both ARP requests and responses.
4. Select whether to enable or disable **Dst-Mac Chk.**
   - If enabled, the system compares the destination MAC address in the Ethernet header to the target MAC address in the ARP body. If the MAC addresses are different the system tags it as invalid and drops the packets. This check is performed on ARP responses.

5. Select whether to enable or disable **IP Chk.**

   - If enabled, the system will check the source and destination IP addresses on the ARP packets. All zero, all ones or multicast IP addresses are considered invalid and the corresponding packets are dropped.

6. Select whether to enable or disable **IP Allow Zero.**

   - If enabled, the system checks all-zero IP addresses.

7. Click the **Apply** button.

Viewing DAI Port Setting

- On the ***DAI Port Setting*** page, the following information will be displayed:
  - **Port:** Displays the port number the DAI settings are applied to.
  - **Type:** Displays the port type as either **Trusted** or **Untrusted**.
  - **Src-Mac Chk:** Displays whether **Src-Mac Chk** is enabled or disabled on the corresponding port.
  - **Dst-Mac Chk:** Displays whether **Dst-Mac Chk** is enabled or disabled on the corresponding port.
  - **IP Chk:** Displays whether **IP Chk** is enabled or disabled on the corresponding port.
  - **IP Allow Zero:** Displays whether **IP Allow Zero** is enabled or disabled on the corresponding port.

Clearing/Refreshing the Dynamic ARP Inspection Statistics

1. On the ***Dynamic ARP Inspection Statistics*** page, the following information will be displayed:

   - **Port:** Displays the port number the DAI settings are applied to.
   - **Forwarded:** Displays the number of ports that are forwarded to the corresponding port.
   - **Source MAC Failures:** Displays the number of MAC failures on the corresponding port.
   - **SIP Validation:** Displays the number of Session Initiation Protocol (SIP) validations on the corresponding port.
   - **DIP Validation:** Displays the number of DIP validations on the

corresponding port.

- **IP-MAC Mismatch Failures:** Displays the number of IP-MAC mismatch failures on the corresponding port.

2. Click the **Clear** button to clear the data.

   - or -

3. Click the **Refresh** button to refresh the data.

Configuring ARP Rate Limit Setting

1. On the ***ARP Rate Limit Setting*** page, select the port you want the ARP Rate Limit to apply to.
2. Select a rate limit **State** either **Defined** or **User-Define.**
   - If a **User-Define State** is selected, enter the packets per second.
3. Enter an ARP **Rate Limit** to restrict the number of packets per second. By default the rate is unlimited.
4. Click the **Apply** button.

Viewing ARP Rate Limit Config

- On the ***ARP Rate Limit Config*** page, the following information will be displayed:
  - **Port:** Displays the port the Address Resolution Protocol (ARP) rate limit applies to.
    - **State:** Displays the ARP rate limit or user defined ARP rate limit.
  - **Rate Limit (pps):** Displays the ARP rate limit in packets per second.

IP Source Guard

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

After receiving a packet, the port looks up the key attributes (including IP address, MAC address and VLAN tag) of the packet in the binding entries of the IP Source Guard. If there is a matching entry, the port will forward the packet. Otherwise, the port will abandon the packet.

IP Source Guard filters packets based on the following types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry

Configuring IP Source Guard Port Settings

1. On the ***IP Source Guard Port Setting*** page, select the port you want to apply the IP Source Guard Port settings to.
2. Select whether to enable or disable IP Source Guard Port settings on the corresponding port.
3. Select a **Verify Source** method to filter the inbound traffic by:
   - **None:** Disables IP source guard filtering on the Managed Switch.
   - **IP:** Traffic filtering based on IP address stored in the binding table.
   - **IP and MAC:** Traffic filtering based on IP address or MAC address stored in the binding table.
4. Enter a **Max Binding Entry** from the drop-down list, that can be secured on the corresponding port.
   - If a **User-Define State** is selected, enter the packets per second.
5. Click the **Apply** button.

Viewing IP Source Guard Port Information

- On the ***IP Source Guard Port Information*** page, the following information will be displayed:
  - **Port:** Displays a list of ports that IP Source Guarding applies to.
  - **Status:** Displays the status of the port either **Enabled** or **Disabled**.
  - **Verify Source:** Displays the source verification type either **None**, **IP**, **IP and MAC**.
  - **Max Binding Entry:** Displays the maximum number of IP guards that can be secured on the corresponding port.
  - **Current Binding Entry:** Displays the port's current binding entry.

Adding an IP Source Guard Static Binding Entry

1. On the ***IP Source Guard Binding Table Status*** page, select the port you want to apply the IP Source Guard Binding Table Settings to.
2. Enter a **VLAN IP** Address.
3. Enter a **MAC Address**.
4. Enter an **IP Address**.
5. Click the **Add** button.

Viewing IP Source Binding Table Status

- On the ***IP Source Guard Binding Table Status*** page, the following information will be displayed:
  - **Port:** Displays the port that the Source Binding applies to.
  - **VLAN:** The port's VLAN IP address.
  - **MAC Address:** The port's MAC address.
  - **IP Address:** The port's IP address.
  - **Type:** Displays the port's entry type.
  - **Lease Time:** Displays the lease time.
  - **Action:** Select the Delete button to delete the corresponding IP Source Binding table setup.

Deleting an IP Source Guard Static Binding Entry

- On the I***P Source Binding Table Status*** page, select the **Delete** button next to the corresponding IP Source Guard Static Binding set up you want to delete.

Port Security

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

The Limit Control module is one of the modules that utilize a lower-layer module while the Port Security module manages MAC addresses learned on the port.

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

Applying Port Security

1. On the ***Port Security Status*** page, select a port number you want to apply port security to.
2. Select whether to **Enable** or **Disable** port security.
3. Enter a MAC address limit for the corresponding port, on the **Mac L2** field.
4. Select which Action to take when the number of MAC addresses on the port exceeds the **Mac L2** field limit.
   - **Forward:** This setting does not go over the MAC address limit set of the corresponding port and no further actions are taken.
   - **Shutdown:** If the MAC address exceeds the limit the port will shut down, all secured MAC addresses will be removed and no new ones will be learned. To reconnect the port you need to either disable and re-enable limit control on the port or the switch and click the **Reopen** button.
   - **Discard:** If the MAC address exceeds the limit, the port will not learn any new MAC addresses and drop the packet.
5. Click the **Apply** button.

Port: From the drop-down list, select a port you want to set up security settings on.

Security: Allows you to enable or disable the security settings on the corresponding port.

Mac L2: Allows you to set the limit of MAC Addresses that can be secured on the corresponding port.

Action: Allows you to set an action if the MAC L2 limit is reached:

Viewing Port Security Status

- On the ***Port Security Status*** page, the following information will be displayed:
  - **Port Name:** Displays the port number the security is set up on.
  - **Enable State:** Displays whether the port is **Enabled** or **Disabled**.
  - **L2 Entry Num:** Displays the maximum number of MAC addresses that can be on the corresponding port at one time.
  - **Action:** Displays the action that will apply if the port exceeds the MAC address limit either **Forwarded**, **Shutdown**, or **Discard**.

DoS

A Denial of Service (DoS) attack is a simple but destructive attack on the internet. A server under DoS attack will drop normal user data packets due to non-stop processing of the attacker's data packet, leading to the denial of the service, and worse can lead to leak of sensitive data of the server.

Security Feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against DoS attacks while having no influence on the linear forwarding performance of the switch.

Applying Global DoS Settings

1. On the ***Global DoS Settings*** page, select the DoS settings you want to apply:
   - **DMAC = SMAC:** Allows you to enable or disable the DoS check mode for DMAC = SMAC attacks.
   - **Land:** Allows you to enable or disable the DoS check mode for Land attacks.
   - **UDP Blat:** Allows you to enable or disable the DoS check mode for UDP Blat attacks.
   - **TCP Blat:** Allows you to enable or disable the DoS check mode for TCP Blat attacks.
   - **POD:** Allows you to enable or disable the DoS check mode for POD attacks.
   - **IPv6 Min Fragment:** Allows you to enable or disable the DoS check mode for IPv6 Min Fragment attacks and enter the minimum fragment value.
   - **ICMP Fragments:** Allows you to enable or disable the DoS check mode for ICMP Fragment attacks.

- **IPv4 Ping Max Size:** Allows you to enable or disable the DoS check mode ping test to determine MTU size on the router.
- **IPv6 Ping Max Size:** Allows you to enable or disable the DoS check mode ping test to determine MTU size on the router.
- **Ping Max Size Setting:** Allows you to enter a maximum ping size in Bytes.
- **Smurf Attack:** Allows you to enable or disable the DoS check mode for Smurf attacks and enter a Netmask Length.
- **TCP Min Hdr Size:** Allows you to enable or disable TCP Min Hdr size and enter a minimum TCP Hdr size.
- **TCP-SYN (SPORT<1024):** Allows you to enable or disable DoS check mode for TCP SYN.
- **Null Scan Attack:** Allows you to enable or disable DoS check mode for Null Scan attacks.
- **X-mas Scan Attack:** Allows you to enable or disable DoS check mode for X-mas Scan attacks.
- **TCP SYN-FIN Attack:** Allows you to enable or disable DoS check mode for TCP SYN-FIN attacks.
- **TCP SYN-RST Attack:** Allows you to enable or disable DoS check mode for TCP SYN-RST attacks.
- **TCP Fragment (Offset = 1):**Allows you to enable or disable DoS check mode for TCP Fragment (Offset =1).

2. Click the **Apply** button.

Viewing DoS Information

- On the ***DoS informations*** page, the following information will be displayed:
  - **DMAC = SMAC:** Displays whether the DoS check mode for DMAC = SMAC attacks is enabled or disabled.
  - **Land:** Displays whether the DoS check mode for Land attacks is enabled or disabled.
  - **UDP Blat:** Displays whether the DoS check mode for UDP Blat attacks is enabled or disabled.
  - **TCP Blat:** Displays whether the DoS check mode for TCP Blat attacks is enabled or disabled.

- **POD:** Displays whether the DoS check mode for POD attacks is enabled or disabled.
- **IPv6 Min Fragment:** Displays whether the DoS check mode for IPv6 Min Fragment is enabled or disabled.
- **ICMP Fragments:** Displays whether the DoS check mode for ICMP Fragments is enabled or disabled.
- **IPv4 Ping Max Size:** Displays whether the DoS check mode for IPv4 Ping Max Size is enabled or disabled.
- **IPv6 Ping Max Size:** Displays whether the DoS check mode for IPv6 Ping Max Size is enabled or disabled.
- **Ping Max Size Setting:** Displays the Ping Max Size in bytes.
- **Smurf Attack:** Displays whether the DoS check mode for Smurf attacks is enabled or disabled.
- **TCP Min Hdr Size:** Displays whether the DoS check mode for TCP Min Hdr Size is enabled or disabled.
- **TCP SYN (SPORT < 1024):** Displays whether the DoS check mode for TCP SYN (SPORT <1024) is enabled or disabled.
- **Null Scan Attack:** Displays whether the DoS check mode for Null Scan attacks is enabled or disabled.
- **X-mas Scan Attack:** Displays whether the DoS check mode for X-mas Scan attacks is enabled or disabled.
- **TCP SYN-FIN Attack:** Displays whether the DoS check mode for TCP SYN-FIN attacks is enabled or disabled.
- **TCP SYN-RST Attack:** Displays whether the DoS check mode for TCP SYN-RST attacks is enabled or disabled.
- **TCP Fragment (Offset = 1):** Displays whether the DoS check mode for TCP Fragment (Offset = 1) is enabled or disabled.

Applying STP Port Settings

1. On the ***STP Port Setting*** page, select a port number you want to apply STP Port settings to.
2. On the **DoS Protection** field, select whether to enable or disable STP port settings.
3. Click the **Apply** button.

Viewing DoS Port Status

- On the ***DoS Part Status*** page, the following information will be displayed:
  - **Port Select:** Displays a list of port numbers.
  - **DoS Protection:** Displays whether STP Port Settings are enabled or disabled on the corresponding port.

Storm Control

Storm Control settings allow you to configure settings that affect the three types of Storm Control, unknown unicast storm rate control, unknown multicast storm rate control, and a broadcast storm rate control. These Storm Control types only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

Applying Storm Control Settings

1. On the ***Storm Control Global Setting*** page, select a **Unit** of measure either:
   - **pps**: Packets per second
   - **bps:** Bits per second
2. On the **Preamble & IFG** field, select whether to exclude or include Inter-Frame Gap (IFG).
3. Click the **Apply** button.

Viewing Storm Control Global Information

- On the ***Storm Control Global Information*** page, the following information will be displayed:
  - **Unit:** Displays the unit of measure selected to measure the Storm Control Rate.
  - **Preamble & IFG:** Displays whether or not IFG is excluded or included.

Applying Storm Control Port Settings

1. On the ***Storm Control Setting*** page, select the **Port** the Storm Control settings will apply to.
2. Select a **Port State,** allows you to disable or enable storm control on the selected port.
3. Select an **Action** from the drop-down list, that occurs when the Storm Control rate is exceeded on the selected port:
   - **Shutdown**
   - **Drop**
4. Select a **Type Enabled**:
   - **Broadcast:** A packets is transmitted from one sender to multiple receivers.
   - **Unknown unicast:** A packets is transmitted from one sender to one receiver.
   - **Unknown multicast:** A packets is transmitted from multiple sends to multiple receivers.
5. Enter the **Rate (kbps/pps)**, which allows you to set the maximum number of packets per second (pps) transmitted. By default this field is set to 10000.

Viewing Storm Control Information

- On the ***Storm Control Information*** page, the following information is displayed:
  - **Port:** The number of the port that the storm control setting are applied to.
  - **Port State:** Displays whether the **Storm Control** settings are **Enabled** or **Disabled** on the corresponding port.
  - **Broadcast (kbps):** Displays whether **Broadcast** is **Enabled** or **Disabled** and the **Rate** maximum packets per second transmitted.
  - **Unknown Multicast (kbps):** Displays whether **Unknown Multicasat** is **Enabled** or **Disabled** and the **Rate** maximum packets per second transmitted.
  - **Unknown Unicast (kbps):** Displays whether **Unknown Unicast** is **Enabled** or **Disabled** and the **Rate** maximum packets per second transmitted.

- **Action:** Displays the **Action** that will occur when the maximum **Rate** has been exceeded:
  - Shutdown
  - Drop

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs (Access Control Entries), containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

The ACL page contains links to the following main topics:

- **MAC-based ACL** - Configuration MAC-based ACL setting.
- **MAC-based ACE** - Add / Edit / Delete the MAC-based ACE setting.
- **IPv4-based ACL** - Configuration IPv4-based ACL setting.
- **IPv4-based ACE** - Add / Edit / Delete the IPv4-based ACE setting.
- **IPv6-based ACL** - Configuration IPv6-based ACL setting.
- **IPv6-based ACE** - Add / Edit / Delete the IPv6-based ACE setting.
- **ACL Binding** - Configure the ACL parameters (ACE) of each switch port.

Adding an MAC-Based ACL List

1. On the **MAC-Based ACL** page, enter an **ACL Name**.
2. Click on the **Add** button to add the new **ACL List**.

Deleting an ACL List

- On the ***ACL Table*** page, click on the **Delete** button next to the **ACL List** you wish to delete.

Adding MAC Based ACE

1. On the **MAC-Based ACE** page, select the MAC Based ACE settings you want to apply:
   - **ACL Name:** From the drop-down list, select an ACL List that you wish to apply the ACE parameters to.
   - **Sequence:** Allows you to change the sequence numbers assigned to rules within the MAC ACL list. 1 is the first rule that will be processed in the sequence.
   - **Action:** Select the ACE forwarding action
     - **Permit:** Any frames that match the ACE parameters are forwarded.
     - **Deny:** Any frames that match the ACE parameters are dropped.
     - **Shutdown:** Port shutdown is disabled.
   - **DA MAC:** Select a DA MAC filter to apply to the ACE.
     - **Any:** Filters all MAC Addresses.
     - **User Defined:** Allows you to apply a filter to the MAC Address entered in the DA MAC Value field.
   - **DA MAC Value:** This field appears when a DA MAC value of **User Defined** is selected, Enter the MAC Address you wish to filter.
   - **DA MAC Mask:** The DA MAC Mask is a 12 digit code made up of 0s and 1s.
     - **0:** The corresponding MAC address will be included.
     - **1:** The corresponding MAC address will be ignored.

- **SA MAC:** Select a SA MAC filter to apply to the ACE.
  - **Any:** Filters all MAC Addresses.
  - **User Defined:** Allows you to apply a filter to the MAC Address entered in the SA MAC Value field.
- **SA MAC Value:** This field appears when a SA MAC value of **User Defined** is selected, enter the MAC Address you wish to filter.
- **SA MAC Mask:** The SA MAC Mask is a 12 digit code made up of 0s and 1s.
  - **0:** The corresponding MAC address will be included.
  - **1:** The corresponding MAC address will be ignored.
- **VLAN ID:** Displays the VLAN ID.
- **802.1p:** Select whether to **Include** the 802.1p value.
- **802.1p Value:** Allows you to enter a 802.1p value (0-7).
- **802.1p Mask:** Allows you to enter the 802.1p mask that is applied to the VPT (Virtual Path Terminator) tag.
- **EtherType:** Allows you to enter an Ether Type. The Ether Type is between the range (0x05DD - 0xFFFF).

2. Click the **Add** button.

Viewing MAC-Based ACE

- On the ***MAC-Based ACE Table*** page, the following information will be displayed:
  - **ACL Name:** Displays the selected ACL List name.
  - **Sequence:** Displays the ACL Rules sequence number.
  - **Action:** Displays the ACE forwarding action, either **Permit**, **Deny**, or **Shutdown**.
  - **Destination MAC Address:** Displays the destination MAC address.
  - **Destination MAC Address Mask:** Displays the destination MAC address.
  - **Source MAC Address:** Displays the source MAC address.
  - **Source MAC Address Mask:** Displays the source MAC address mask.
  - **VLAN ID:** Displays the VLAN ID
  - **802.1p:** Displays the 802.1p value.

- **802.1p Mask:** Displays the 802.1p mask
- **EtherType:** Displays the Ethernet type.

Editing/Deleting a MAC based ACL Entry

- On the **MAC-Based ACE Table** page. Click the **Edit** button next to the ACL entry you wish to edit.

  - or -

  Click on the **Delete** button to delete the corresponding ACL entry.

Adding an IPv4 Based ACL List

1. On the **IPv4-Based ACL** page, enter an **ACL Name**.
2. Click on the **Add** button to add the new **I**Pv4- based **ACL** list.

Viewing IPv4 Based ACL Table

- On the ***ACL Table*** page, the following information will be displayed:
  - **ACL NAME:** Displays the IPv4 based ACL list name.
  - **Delete:** Allows you to delete the corresponding IPv4 based ACL list.

Deleting an IPv4 Based ACL List

- On the **ACL Table** page, click the **Delete** button next to the IPv4 based ACL list you wish to delete.

Adding an IPv4 Based ACE Table Settings

1. On the **IPv4 Based ACE Table** page, select the IPv4 Based ACE Table settings you wnt to apply:
   - **ACL Name:** From the drop-down list, select the IPv4 based ACL list you wish to apply ACE parameters to.
   - **Sequence:** Allows you to change the sequence numbers assigned to rules within the IPv4 based ACL list. 1 is the first rule that will be processed in the sequence.
   - **Action:** Select the ACE forwarding action:
     - **Permit:** Any frames that match the ACE parameters are forwarded.
     - **Deny:** Any frames that match the ACE parameters are dropped.
     - **Shutdown:** Port shutdown is disabled.

- **Protocol:** Select a protocol filter for the corresponding ACE.
  - **Any(IP):** If selected no IP protocol is specified.
  - **Select from list:** Allows you to specify a specific IP protocol e.g. ICMP.
  - **Protocol ID to match:** If you have selected an IP protocol on the **Select from list** drop-down, enter an IP protocol ID.
- **Source IP Address:** Allows you to select a source IP address filter.
  - **Any:** If selected no source IP address is specified.
  - **User Defined:** If selected the **Source IP Address Value** field will appear, allowing you to enter a source IP address.
- **Source IP Address Value:** Allows you to enter a source IP address. This field appears when the **User Defined** radio button is selected under the **Source IP Address** field.
- **Source IP Wildcard Mask:** Allows you to enter a source IP mask in dotted decimal notation (e.g. 0.0.172.1). This field appears when the **User Defined** radio button is selected under the **Source IP Address** field.
- **Destination IP Address:** Allows you to select a destination IP address filter.
  - **Any:** If selected no source IP address is specified.
  - **User Defined:** If selected the **Destination IP Address Value** field will appear, allowing you to enter a destination IP address.
- **Destination IP Address Value:** Allows you to enter a destination IP address. This field appears when the **User Defined** radio button is selected under the **Destination IP Address** field.
- **Destination IP Wildcard Mask:** Allows you to enter a destination IP mask in dotted decimal notation (e.g. 0.0.172.1). This field appears when the **User Defined** radio button is selected under the **Destination IP Address** field.
- **Source Port Range:** Allows you to select a source port filter.
  - **Any:** If selected uses a generated source port value.
  - **Single:** Allows you to enter a specific source port value (0 - 65535).
  - **Range:** Allows you to enter a source port value range (0-65535).
-

- **Destination Port:** Allows you to select a destination port filter.
  - **Any:** If selected uses a generated destination port value.
  - **Single:** Allows you to enter a specific destination port value (0 - 65535).
  - **Range:** Allows you to enter a destination port value range (0-65535).
- **TCP Flag:**
  - **Urg:** The urgent (Urg) TCP flag indicates that data within a segment is urgent. Urg segments are processed immediately.
    - **Set:** When this option is selected all incoming data segments with a Urg flag are considered urgent.
    - **Unset:** When this option is selected all incoming data segments with a Urg flag are not considered urgent.
    - **Don't Care:** When this option is selected all data segments are considered urgent.
  - **Ack:** The acknowledgement (Ack) TCP flag indicates that a data segment was received. When a data segment is received the host will send a Ack data segment to the sender indicating that the sent data segment was successfully received.
    - **Set:** When this option is selected an Ack data segment will be sent to the sender indicating that the data source was received.
    - **Unset:** When this option is selected no Ack data segment will be sent.
    - **Don't Care:** When this option is selected an Ack data segment will be sent for all received data segments.
  - **Psh:** The push (Psh) TCP flag indicates to the receiver not to buffer the data segment but to process them as soon as they are received.
    - **Set:** When this option is selected all incoming Psh data segments will be processed once received.
    - **Unset:** When this option is selected all incoming Psh data segments will be buffered.
    - **Don't Care:** When this option is selected all incoming data segments will be processed once received.

- **Rst:** The reset (Rst) TCP flag indicates to the sender that the connection to the host has been reset.
  - **Set:** When this option is selected any data segment received that have a Rst flag will reset the connection.
  - **Unset:** When this option is selected no Ack data segment will be sent.
  - **Don't Care:** When this option is selected an Ack data segment will be sent for all received data segments.
- **Syn:** The synchronisation (Syn) TCP flag establishes the initial connection between the sender and receiver.
  - **Set:** When this option is selected any data segment received that have a Syn flag will establish initial connection.
  - **Unset:** When this option is selected no data segment received that has a Syn flag will indicated to the receiver that the sender is trying to establish a connection.
  - **Don't Care:** When this option is selected all data segments are considered Syn data segments.
- **Fin:** The Finished (Fin) TCP flag terminates the connection between the sender and receiver.
  - **Set:** When this option is selected any data segment received that have a Fin flag will indicate to the receiver that the connection was terminated.
  - **Unset:** When this option is selected data segments received that have a Fin flag will not terminate the connection.
  - **Don't Care:** When this option is selected all data segments are considered Fin data segments.
- **Type of Service:** Select and ACE service type
  - **Any:** If selected any ACE service type will be used.
  - **DSCP:** If selected the **DSCP Value** field will appear, allowing you to enter a source IP address. The value range is 0 - 63.
  - **IP Precedence:** If selected the **IP Precedence** field will appear, allowing you to enter an IP Precedence value. The value range is 0 - 7.
-

- **ICMP:** Select and Internet Control Message Protocol (ICMP) for the corresponding ACE.
  - **Any:** No specific ICMP filter is selected.
  - **List:** Allows you to select an ICMP filter from the drop-down list.
  - **Protocol ID:** Allows you to enter a protocol ID filter for the corresponding ACE. If selected a Protocol ID field will appear. The protocol ID range is 0 - 255.
- **ICMP Code:** Allows you to specify an ICMP code.
  - **Any:** No specific ICMP code is used.
  - **User Defined:** Allows you to define the ICMP code.

2. Click the **Add** button.

Viewing the IPv4 Based ACE Table

- On the ***IPv4 Based ACE Table*** page, the following information will be displayed:
  - **ACL Name:** Displays the ACL Name.
  - **Sequence:** Displays the current sequence.
  - **Action:** Displays the current action.
  - **Protocol:** Displays the current protocol.
  - **Source IP Address:** Displays the current source IP address.
  - **Source IP Address Wildcard Mask:** Displays the current IP address wildcard mask
  - **Destination IP Address:** Displays the current destination IP address.
  - **Destination IP Address Wildcard Mask:** Displays the current destination IP address wildcard mask.
  - **Source Port Range:** Displays the current source port range.
  - **Destination Port Range:** Displays the current destination port range.
  - **Flag Set:** Displays the current TCP flag and value.
  - **DSCP:** Displays the current Differentiated Services Code Point (DSCP).
  - **IP Precedence:** Displays the current IP Precedence value.
  - **ICMP Type:** Displays the current ICMP type.

- **ICMP Code:** Displays the current ICMP code.

Editing/Deleting an IPv4 ACE Table

- On the **IPv4 Based ACE Table** page, click the **Edit** button next to the ACL entry you wish to edit.

  - or -

  Click on the **Delete** button to delete the corresponding ACL entry.

Naming an IPv6 Based ACL List

1. On the **ACL Table** page, enter an IPv6 based ACL list name in the **ACL Name** field.
2. Click the **Add** button to create the new IPv6 based ACL list entry you wish to edit.

Deleting an IPv6 Based ACL List

- On the **ACL Table** page, click on the **Delete** button to delete the corresponding ACL entry.

Adding an IPv6 - Based ACE List

1. On the ***IPv6-Based ACE*** page, enter the required information into the following fields:
   - **ACL Name:** Select and ACL Name from the drop-down list. The parameters selected will apply to the ACL list selected.
   - **Sequence:** Indicate the sequence that the ACL list will be processed (range 1 - 2147483647).
   - **Action:** Select the ACE forwarding action:
     - **Permit:** Any frames that match the ACE parameters are forwarded.
     - **Deny:** Any frames that match the ACE parameters are dropped.
     - **Shutdown:** Port shutdown is disabled.
   - **Protocol:** Select a protocol filter for the corresponding ACE.
     - **Any(IP):** If selected no IP protocol is specified.
     - **Select from list:** Allows you to specify a specific IP protocol e.g. ICMP.
   - **Source IP Address:** Allows you to select a source IP address filter:
     - **Any:** If selected no source IP address is specified.

- **User Defined:** If selected the **Source IP Address Value** field will appear, allowing you to enter a source IP address.

- **Source IP Address Value:** Allows you to enter a source IP address. This field appears when the **User Defined** radio button is selected under the **Source IP Address** field.
- **Source IP Prefix Length:** Allows you to enter an SIP prefix length in dotted decimal notation. This field appears when the **User Defined** radio button is selected under the **Source IP Address** field. **Destination IP Address:** Allows you to select a destination IP address filter:
- **Destination IP Address Value:** Allows you to enter a destination IP address. This field appears when the **User Defined** radio button is selected under the **Destination IP Address** field.
- **Destination IP Wildcard Mask:** Allows you to enter a destination IP mask in dotted decimal notation (e.g. 0.0.172.1). This field appears when the **User Defined** radio button is selected under the **Destination IP Address** field.
- **Source Port:** Allows you to select a source port filter:
  - **Any:** If selected uses a generated source port value.
  - **Single:** Allows you to enter a specific source port value (0 - 65535).
  - **Range:** Allows you to enter a source port value range (0-65535).
- **Destination Port:** Allows you to select a destination port filter:
  - **Any:** If selected uses a generated destination port value.
  - **Single:** Allows you to enter a specific destination port value (0 - 65535).
  - **Range:** Allows you to enter a destination port value range (0-65535).
- **TCP Flags:**
  - **Urg:** The urgent (Urg) TCP flag indicates that data within a segment is urgent. Urg segments are processed immediately.
    - **Set:** When this option is selected all incoming data segments with a Urg flag are considered urgent.
    - **Unset:** When this option is selected all incoming data segments with a Urg flag are not considered urgent.
    - **Don't Care:** When this option is selected all data segments are considered urgent.

- **Ack:** The acknowledgement (Ack) TCP flag indicates that a data segment was received. When a data segment is received the host will send a Ack data segment to the sender indicating that the sent data segment was successfully received.
  - **Set:** When this option is selected an Ack data segment will be sent to the sender indicating that the data source was received.
  - **Unset:** When this option is selected no Ack data segment will be sent.
  - **Don't Care:** When this option is selected an Ack data segment will be sent for all received data segments.
- **Psh:** The push (Psh) TCP flag indicates to the receiver not to buffer the data segment but to process them as soon as they are received.
  - **Set:** When this option is selected all incoming Psh data segments will be processed once received.
  - **Unset:** When this option is selected all incoming Psh data segments will be buffered.
  - **Don't Care:** When this option is selected all incoming data segments will be processed once received.
- **Rst:** The reset (Rst) TCP flag indicates to the sender that the connection to the host has been reset.
  - **Set:** When this option is selected any data segment received that have a Rst flag will reset the connection.
  - **Unset:** When this option is selected no Ack data segment will be sent.
  - **Don't Care:** When this option is selected an Ack data segment will be sent for all received data segments.
- **Syn:** The synchronisation (Syn) TCP flag establishes the initial connection between the sender and receiver.
  - **Set:** When this option is selected any data segment received that have a Syn flag will establish initial connection.
  - **Unset:** When this option is selected no data segment received that has a Syn flag will indicated to the receiver that the sender is trying to establish a connection.
  - **Don't Care:** When this option is selected all data segments are considered Syn data segments.

- **Fin:** The Finished (Fin) TCP flag terminates the connection between the sender and receiver.
  - **Set:** When this option is selected any data segment received that have a Fin flag will indicate to the receiver that the connection was terminated.
  - **Unset:** When this option is selected data segments received that have a Fin flag will not terminate the connection.
  - **Don't Care:** When this option is selected all data segments are considered Fin data segments.
- **Type of Service:** Select and ACE service type:
  - **Any:** If selected any ACE service type will be used.
  - **DSCP:** If selected the **DSCP Value** field will appear, allowing you to enter a source IP address. The value range is 0 - 63.
  - **IP Precedence:** If selected the **IP Precedence** field will appear, allowing you to enter an IP Precedence value. The value range is 0 - 7.
- **ICMP:** Select and Internet Control Message Protocol (ICMP) for the corresponding ACE.
  - **Any:** No specific ICMP filter is selected.
  - **List:** Allows you to select an ICMP filter from the drop-down list.
  - **Protocol ID:** Allows you to enter a protocol ID filter for the corresponding ACE. If selected a Protocol ID field will appear. The protocol ID range is 0 - 255.
- **ICMP Code:** Allows you to specify an ICMP code.
  - **Any:** No specific ICMP code is used.
  - **User Defined:** Allows you to define the ICMP code.

2. Click the **Add** button.

Editing/Deleting an IPv4 ACE Table

- On the **IPv4 Based ACE Table** page. Click the **Edit** button next to the ACL entry you wish to edit.

  - or -

  Click on the **Delete** button to delete the corresponding ACL entry.

Binding an ACL List to a Port

An ACL can be bound to a port or multiple ports. When an ACL is bound to a port the ACE rules associated with the ACL are applied to the interface or interfaces bound to it.

- **Binding Port:** Select a port from the drop-down list to bind the ACL rules to.
- **ACL Select:** Select an ACL list from the drop-down list.

1. On the **ACL Binding** page, select a port from the **Binding Port** drop-down list.
2. Select an **ACL Type** radio button:
   - MAC-Based ACL
   - IPv4 Based ACL
   - IPv6 Based ACL
3. Select an ACL list type from the **ACL Select** drop-down lists. This ACL list will apply to the port selected in step 1.
4. Click the **Apply** button.

MAC Address Table

Switching of frames is based on the destination MAC address contained in the frame. The Managed Switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the destination MAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the destination MAC address and switch ports.

The frames also contain a MAC address (source MAC address), which shows the MAC address of the equipment sending the frame. The source MAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding source MAC address has been seen after a configurable age time.

Configuring a Static MAC Setting

1. On the **Static MAC Settings** page, enter a **MAC Address**.
   - **MAC Address:** The ports physical MAC address
2. Select a VLAN from the **VLAN** drop-down list.
3. Select a port from the **Binding Port** drop-down list.
4. Click the **Add** button.

Viewing Static MAC Status

- On the ***Static MAC Status*** page, the following information will be displayed:
  - **No.:** Indicates the line item in numerical order.
  - **MAC Address:** Displays the MAC address
  - **VLAN:** Displays the VLAN setting.
  - **Port:** Displays the port.

Deleting Static MAC Settings

- On the **Static MAC Status** page, click the **Delete** button next to the static MAC setting you wish to delete.

MAC Filtering Setting

MAC filtering allows you to setup a list of accepted MAC addresses which are allowed access and a list of unaccepted MAC addresses which are denied access.

Adding a New MAC Filtering Setting

1. On the **Static MAC Status** page, enter a MAC address.
2. Select a VLAN from the **VLAN** drop-down list.
3. Click the **Add** button.

Viewing Static MAC Status

- On the ***Static MAC Status*** page, the following information will be displayed:
  - **No.:** Indicates the line item in numerical order.
  - **MAC Address:** Displays the MAC address
  - **VLAN:** Displays the VLAN setting.

- **Action:** Allows you to delete the static MAC entry.

Applying a Dynamic Address Setting

1. On the **Dynamic Address Setting** page, enter an **Aging Time** (10 - 630 seconds).
   - **Aging Time:** Enter the amount of time a MAC address can sit dormant (no active traffic) Once this interval is reached the MAC address will be deleted.
2. Click the **Apply** button.

Viewing Dynamic Address Status

- On the ***Dynamic Address Setting*** page, the following information will be displayed:
  - **Information Name:** Displays the field title (**Aging Time**).
  - **Information Value:** Displays the current aging time in seconds.

Editing/Viewing/Clearing the Dynamic MAC Table

Dynamic Learned routing automatically edits table changes based on the best data transfer paths.

1. On the ***Dynamic Learned*** page, enter the following information:
   - **Port:** Select a port from the drop-down list.
   - **VLAN:** Select a VLAN from the drop-down list.
   - **MAC Address:** Enter the ports physical MAC Address.
2. Click the **View** button to refresh the page.

   - or -

   Click on the **Clear** button to delete the field on the **Dynamic MAC Table** page.

Adding a Dynamic MAC Address to the Static MAC Address table

1. On the MAC Address Information page, the following information will be displayed:
   - **Type:** Indicates whether the MAC address entry is **Dynamic** or **Static**.
   - **Port:** Displays the ports associated with the MAC address.

2. Click on the Add to Static MAC Table button next to the dynamic MAC address you wish to add to the static MAC table.

LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Applying LLDP Global Settings

1. On the **Global Settings** page, select the LLDP settings you want to apply:

- **Enabled:** Allows you to Globally Enable or Disable the LLDP settings.
- **LLDP PDU Disable Action:** Allows you to set an LLDP PDU setting:
  - **Filtering:** If selected deletes all LLDP PDUs.
  - **Bridging:** If selected transmits LLDP PDUs in the same VLAN
  - **Flooding:** If selected transmits LLDP PDUs for all ports.
- **Transmission Interval:** Enter a transmission interval. The transmission interval is the interval between LLDP Frame transmissions. The default interval is set to 30 seconds. The Interval range is 5 - 32768 seconds. The transmission interval multiplied by the hold time multiplier value must be less than or equal to 65536 and/or the transmission internal must be greater than or equal to the delay interval multiplied by 4.
- **Holdtime Multiplier:** Enter a hold time multiplier value. The hold time multiplier value is multiplied by the transmission interval and determines how long information in an LLDP frame is considered valid. Valid values are 2 - 10.

- **Re initialization Delay:** Enter a re initialization delay value. The re initialization delay value Is the amount of time a shutdown frame and a new LLDP Initialization. Valid values are 1 - 10 seconds.
- **Transmit Delay:** Enter a transmission delay value. The transmission delay value is the time between when a configuration changed occurs and when the LLDP frame is transmitted. The transmit delay value cannot be larger than the 1/4 the transmission interval. Valid values are 1 - 8192 seconds. The transmit delay value multiplied by 4 must be less than or equal to the transmission interval.
- **LLDP-MED Fast Start Repeat Count:** Enter a LLPD-MED fast start repeat count value. The LLDP-MED fast start repeat count value indicates the number of packets that are sent during the LLDP-MED fast start. Valid values are 1 - 10 packets. The default setting is 3 packets.

2. Click the **Add** button.

Viewing LLDP Global Settings

- On the LLDP Global Config page, the following information will be displayed:
  - LLDP Enabled: Displays the current LLDP Status.
  - **LLDP PDU Disable Action:** Displays the current LLDP PDU disable action.
  - **Transmission Interval:** Displays the current transmission interval.
  - **Holdtime Multiplier:** Displays the current hold time multiplier.
  - **Re initialization Delay:** Displays the current re initialization delay value.
  - **Transmit Delay:** Displays the transmit delay value.
  - **LLDP-MED Fast Start Report Count:** Displays the current LLDP-MED fast start report count value.

Applying LLDP Port Configuration

1. On the **LLDP Port Configuration** page, select a port from the drop-down list.
2. Select a LLDP message **State**:
   - **Tx Only (Transmit only):** Enable or Disable Transmitting LLDP messages.
   - **Rx Only (Receive only):** Enable or Disable Receiving LLDP messages.
   - **TxRx (Transmit and receive):** Enable or Disable both Transmitting and Receiving LLDP messages.
   - **Disable:** Disable LLDP
3. Click the **Apply** button.

Applying LLDP TLV Selection

1. On the **Optional TLVs Selection** page, select a **Port** from the drop-down list.
2. Select an Optional TLV Select type, information that is included or excluded when LLDP information is transmitted:
   - **System Name:** Includes the system name when transmitting LLDP information.
   - **Port Description:** Includes the port description when transmitting LLDP information.
   - **System Description:** Includes the system description when transmitting LLDP information.
   - **System Compatibility:** Includes the system compatibility when transmitting LLDP information.
   - **802.3 MAC-PHY:** Includes 802.3 MAC-PHY information when transmitting LLDP information.
   - **802.3 Link Aggregation:** Includes 802.3 link aggregation information when transmitting LLDP information.
   - **802.3 Maximum Frame Size:** Includes 802.3 maximum frame size when transmitting LLDP information.
   - **Management Address:** Includes the management address when transmitting LLDP information.
   - **802.1 PVID: I**ncludes 802.1 PVID information when transmitting LLDP information.

3. Click the **Apply** button.

Viewing LLDP Port Status

- On the ***LLDP Port Status*** page, the following information will be displayed:
  - **Port:** Displays the port number.
  - **State:** Displays the TVL state on the corresponding port.
  - **Selected Optional TLVs:** Displays the optional TLV.

Applying a VLAN Name TLV VLAN

1. On the **VLAN Name TLV VLAN Selection** page, select a port from the **Port Select** drop-down list.
2. Select a VLAN from the **VLAN Select** drop-down list.
3. Click on the **Apply** button.

Viewing LLDP Port VLAN TLV Status

- On the ***LLDP Port VLAN TLV*** Status page, the following information will be displayed:
  - **Port:** Displays the port number.
  - **Selected VLAN:** Displays the current VLAN

Viewing Local Device Summary

The Local Device Summary page displays information about the **Switch** (e.g. MAC address, chassis ID, management IP address, etc.)

- On the ***Local Device Summary*** page, the following information will be displayed:
  - **Chassis ID Subtype:** Displays the **Switches** current chassis ID subtype
  - **Chassis ID:** Displays the **Switch's** current chassis ID.
  - **System Name:** Displays the **Switch's** current system name.
  - **System Description:** Displays the **Switch's** current system description.
  - **Capabilities Supported:** Displays the current capabilities supported by the **Switch**.
  - **Capabilities Enabled:** Displays the current capabilities enabled on the **Switch**.

- **Port ID Subtype:** Displays the Switches current port ID subtype.

Accessing Detailed Port Status Information

1. On the **Local Device Summary** page, select the radio button next to a port.
2. Click the **Detail** button to access a more port status information on the selected port.

Viewing, Deleting, and Refreshing LLDP Remote Devices

1. On the **LLDP Remote Device** page, select a **Sel** radio button next to a port.
   - **Sel:** The **Sel** radio button allows you to select a specific port in order to either access detailed information, delete, or refresh the port.
2. Click the **Detail** button to access a more port status information on the selected port.

   - or -

   Click on the **Refresh** button to refresh the port information on the **LLDP Remote Device** page.

   - or -

   Click on the **Delete** button to delete the field entries on the **LLDP Remote Device** page.
3. On the ***LLDP Remote Device*** page, the following information will be displayed:
   - **Local Port:** Displays the local port number.
   - **Chassis ID Subtype:** Displays the local port's current chassis ID subtype.
   - **Chassis ID:** Displays the local port's current chassis ID.
   - **Port ID Subtype:** Displays the port's current port ID subtype.
   - **Port ID:** Displays the remote port's ID (ID of the neighbor port).
   - **System Name:** Displays the neighbor unit's system name.
   - **Time to Live:** Time to Live (TTL) is a value in seconds from 0 - 65,000. The TTL is part of an LLDP packet. When a device receives an LLDP packet a timer is started when the timer reaches the time indicated in the TTL, the LLDP device will delete the store packet information. This guarantees that only valid information is stored.

MED Network Policy

MED Network Policy work with interactive voice and or video services that have specific real time network policy requirements.

Setting the LLDP MED Policy for Voice Application

1. On the **Voice Auto Mode Configuration** page, select a method for determining the voice VLAN ID:
   - **Auto:** Will automatically detect the voice VLAN ID.
   - **Manual:** Allows you to manual set the voice VLAN ID.
2. Click on the **Apply** button.

Applying Network Policy Configuration

1. On the **Network Policy Configuration** page, select the settings you wish to apply:
   - **Network Policy Number:** Select a network policy number from the drop-down list:
     - **1:** Layer 2 VLAN ID (IEEE 802.1Q-2003)
     - **2:** Layer 2 priority value (IEEE 802.1D-2004)
     - **3:** Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)
   - **Application:** Select an application type from the drop-down list:
     - **Voice:** Used for dedicated IP Telephony headsets and other similar appliances that support interactive voice services.
     - **Voice Signaling:** Used for network topologies that require a different policy for voice signaling than for voice media.
     - **Guest Voice:** Supports a separate limited feature set, for guest users.
     - **Guest Voice Signaling:** Used for network topologies that require a different policy for guest voice signaling than for guest voice.
     - **Softphone Voice:** Used for Softphone applications on a PC or laptop. These endpoints typically use a untagged VLAN or single tagged data specific VLAN.
     - **Video Conferencing:** Used for dedicated video conference device which supports real time interactive video/audio services.

- **App Streaming Video:** Used for broadcast or multicast video streaming.
- **Video Signaling:** Used for topologies that require a separate for video signaling than for video media.

- **VLAN ID:** The port VLAN ID.
- **VLAN Tag:** Indicates whether the selected application type is using an untagged VLAN or tagged VLAN.
  - **Untagged:** Indicates that the application type is using an untagged VLAN frame format and does not include a tag header.
  - **Tagged:** Indicates that the application type is using a tagged VLAN from format and includes a tag header and a priority tagged frames.
- **L2 Priority:** Allows you to set the Layer 2 priority level. The L2 priority level ranges from 0 - 7, where 0 is the default priority level.
- **DSCP Value:** Allows you to set a Differentiated Services Code Point (DSCP). The DSCP value ranges from 0 - 63, where 0 is the default value.

2. Click on the **Apply** button.

Viewing LLDP MED Network Policy Table

- On the LLDP MED Network Policy Table page, the following information will be displayed:
  - **Network Policy Number:** Displays the current network policy number.
  - **Application:** Displays the current application type **Voice**, **Voice Signaling**, **Guest Voice**, **Guest Voice Signaling**, **Softphone Voice**, **Video Conferencing**, **App Streaming Video**, or **Video Signaling**.
  - **VLAN ID:** Displays the current VLAN ID.
  - **VLAN Tag:** Displays whether the application type is using a **Tagged** or **Untagged** VLAN.
  - **L2 Priority:** Displays the current L2 priority level (0 - 7).
  - **DSCP Value:** Displays the current DSCP value (0 - 63).

Deleting an LLDP MED Network Policy Table Entry

1. On the **LLDP MED Network Policy Table** page, select the radio button next to the LLDP MED Network Policy entry you wish to delete.

2. Click on the **Delete** button.

Applying Port LLDP MED Configuration

1. On the **Port LLDP MED Configuration** page, select the port you wish to apply the MED port settings to.
2. Configure the following port settings:
   - **MED Enable:** Allows you to Enable or Disable the LLDP MED Settings on the selected port.
   - **MED Optional TLVs:** Select an MED optional TLV setting:
     - **Network Policy:** If selected advertises network policy configuration information, which aids in VLAN discovery and diagnosis.
     - **Location:** If selected advertises location details.
     - **Inventory:** If selected advertises device details e.g. manufacturer, model, software version, etc.
   - **MED Network Policy:** Allows you to select an MED Network policy from the drop-down list.
3. Click on the **Apply** button.

Viewing LLDP MED Port Setting Table

- On the ***LLDP MED Port Setting Table*** page, the following information will be displayed:
  - **Interface:** Displays the port number.
  - **LLDP MED Status:** Displays whether the LLDP MED Status is set to enable or disabled.
  - **User Defined Network Policy:**
    - **Active:** Displays whether the active status of yes or no.
    - **Application:** Displays the application type.
    - **Location:** Displays the current location.
    - **Inventory:** Displays the current inventory.

Applying MED Location Configuration

1. On the **MED Location Configuration** page, select the port you wish to apply the MED port settings to.
2. Configure the following port settings:
   - **Location Coordinate:** Enter the location of the device (coordinates).
   - **Location Civic Address:** Enter the device's street address.
   - **Location ECS ELIN:** Enter the device's ECS ELIN location.
3. Click on the **Apply** button.

Viewing LLDP MED Port Location Table

- On the ***LLDP MED Port Location Table*** page, the following information will be displayed:
  - **Port:** Displays the port number.
  - **Coordinate:** Displays the devices current coordinates.
  - **Civic Address:** Displays the device's street address.
  - **ECS ELIN:** Displays the device's ECS ELIN location.

Viewing the LLDP Port Overloading Table

- On the ***LLDP Port Overloading Table*** page, the following information will be displayed:
  - **Interface:** From the drop-down list, select the port you wish to apply the LLDP Port Overloading Table settings to.
  - **Total (Bytes):** Displays the amount of LLDP information in bytes that is sent within a packet.
  - **Left to Send (Bytes):** Displays the amount of LLDP Information in bytes that needs to still be transmitted by a packet.
  - **Status:** Displays the current TVL status.
  - **Mandatory TVLs:** Displays the number of mandatory TLVs that were **Transmitted** or **Overloaded**.
  - **MED Capabilities:** Displays the number of capability packets that were **Transmitted** or **Overloaded**.
  - **MED Location:** Displays the number of location packets that were

Transmitted or **Overloaded**.

- **MED Network Policy:** Displays the number of network policy packets that were **Transmitted** or **Overloaded**.
- **MED Extended Power via MDI:** Displays the number of extended power MDI packets that were **Transmitted** or **Overloaded**.
- **802.3 TVLs:** Displays the number of 802.1 TLVs that were **Transmitted** or **Overloaded**.
- **Optional TVLs:** Displays the number of optional TVLs that were **Transmitted** or **Overloaded**.
- **MED Inventory:** Displays the number of MED TLVs that were **Transmitted** or **Overloaded**.
- **802.1 TLVs:** Displays the number of 802.1 TLVs that were **Transmitted** or **Overloaded**.

Clearing or Refreshing LLDP Global Statistics

1. On the **LLDP Global Statistic** page, click the **Clear** button to clear the LLDP statistic information.

   - or -

2. Click on the **Refresh** button to refresh the LLDP Statistics information.

3. On the ***LLDP Global Statistic*** page, the following information will be displayed:

   - **Insertions:** Displays the number of new LLDP entries since the last time the switch was rebooted.
   - **Deletions:** Displays the number of LLDP entries deleted since the last time the switch was rebooted.
   - **Drops:** Displays the number of LLDP entries that were dropped because the entry table did not have the required space.
   - **Age Outs:** Displays the number of LLDP entries delete due to Time to Live expiration.

Viewing LLDP Port Statistics

- On the ***LLDP Port Statistics*** page, the following information will be displayed:
  - **Port:** Displays the port number that the LLDP frame are transmitted and/or received.
  - **TX Frames**:
    - **Total:** Displays the number of LLDP frames transmitted on the corresponding port.
  - **RX Frames:**
    - **Total:** Displays the number of LLDP frames received on the corresponding port.
    - **Discarded:** Displays the number of LLDP frames discarded by the corresponding port. If a LLDP frame is discarded, the frame will require a new entry.
    - **Error:** Displays the number of LLDP frames with errors.
  - **RX TLVs**:
    - **Discarded:** Displays the number of LLDP frames that contain malformed Type Length Values (TLVs).
    - **Unrecognized:** Displays the number of LLDP frames with unknown TLVs.
  - **RX Age Outs:**
    - **Total:** Displays the number of LLDP frames that were aged out.

Diagnostics

This section provides Physical layer and IP layer network diagnostics tools for troubleshooting. The diagnostic tools are designed for network managers to help them quickly diagnose problems between two points to better service customers.

Use the Diagnostics menu items to display and configure basic administrative details of the Managed Switch. Under System, the following topics are provided to configure and view:

This section has the following items:

- Cable Diagnostics
- Ping Test
- IPv6 Ping Test
- Trace Route

Cable Diagnostics

Cable Diagnostics allows you to perform tests on copper cables. The tests detect the cable's length and operating conditions. The tests also allow you to identify common faults that can occur on CAT5 Twisted pair cabling.

After the Cable Diagnostics is complete a link is re-established and the following function are available again:

- Coupling between cable pairs
- Cable pair termination
- Cable length

Note: Cable Diagnostics can only be performed on cables 15 to 100 meters in length.

Running a Copper Cable Test

1. On the **Select the port on which to run the copper test** page, select a port from the drop-down list.
2. Click on the **Copper Test** button to run the copper cable test on the selected port.
3. Once the copper test is complete you will receive the following information in a test results section:
   - **Port:** Displays the port that the copper cable test was performed on.

- **Channel A - D:** Displays the current channel status (A - D).
- **Cable Length A - D:** Displays the current cable length (A - D).
- **Results:** Displays the result from the copper cable test.

Ping

The Ping option allows you to send an ICMP-PING packet to test IP connectivity issues.

Transmitting ICMP Packets

1. On the **Ping Test Setting** page, enter the following ping settings:

- **IP Address:** The IP address the ICMP-PING packet was sent to.
- **Count:** Enter the number of echo requests send as part of the ICMP-PING (1 - 5) the default setting is 4.
- **Interval (in sec):** Enter the interval time in seconds between a send ICMP packet and when the next packet is sent (1 - 5 seconds) the default setting is 1 second.
- **Size (in bytes):** The payload size of the ICMP packet in bytes. The values range from 8bytes to 5120bytes, the default setting is 56bytes.
- **Ping Results:** Displays the current ping results (sequence number and roundtrip time). This page will automatically refresh until responses to all packets are received are until a timeout occurs.

2. Click on the **Apply** button to transmit the ICMP packets.

IPv6 Ping Test

The Ping option allows you to send an ICMPv6-PING packet to test IP connectivity issues.

Transmitting ICMPv6 Packets

1. On the **Ping Test Setting** page, enter the following ping settings:

- **IP Address:** The IP address the ICMPv6-PING packet was sent to.
- **Count:** Enter the number of echo requests send as part of the ICMPv6-PING (1 - 5) the default setting is 4.

- **Interval (in sec):** Enter the interval time in seconds between a send ICMPv6 packet and when the next packet is sent (1 - 5 seconds) the default setting is 1 second.
- **Size (in bytes): T**he payload size of the ICMPv6 packet in bytes. The values range from 8bytes to 5120bytes, the default setting is 56bytes.
- **Ping Results:** Displays the current ping results (sequence number and roundtrip time). This page will automatically refresh until responses to all packets are received are until a timeout occurs.

2. Click on the **Apply** button to transmit the ICMPv6 packets.

Trace Router

The Trace Route function tests network accessibility and locates any network failures away the gateways which data packets are sent from the source device to the destination.

Applying Trace Route Settings

1. On the **Trace Route Setting** page, enter the following settings:
   - **IP Address:** Enter the destination IP Address.
   - **Max Hop:** The total amount of network device data is passed through, as the data is sent from source to destination (2 - 255). the default setting is 30.
   - **Trace Route Results:** Displays the trace route test results.
2. Click on the **Apply** button to run the trace route test.

RMON

RMON is the most important expansion of the standard SNMP. RMON is a set of MIB definitions, used to define standard network monitor functions and interfaces, enabling the communication between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

RMON1 MIB consists of 10 groups. The switch supports the most frequently used group 1, 2, 3 and 9:

- **Statistics** - Maintain basic usage and error statistics for each subnet monitored by the Agent.
- **History** - Record periodical statistic samples available from Statistics.
- **Alarm** - Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON Agent records.
- **Event** - A list of all events generated by RMON Agent.

Alarm depends on the implementation of Event. Statistics and History display some current or historical subnet statistics. Alarm and Event provide a method to monitor any integer data change in the network, and provide alerts upon abnormal events (sending Trap or record in logs)

Clearing RMON Statistics

1. On the **Port GE1 RMON Statistics** page, click the **Clear** button to clear the RMON statistic information.

2. The following information is displayed:

   - **Port:** Allows you to select the port you wish to view the RMON statistics on, from the drop-down list.
   - **Drop Events:** The number of events where packets were dropped by the probe due to the lack of resources.
   - **Octets:** the number of octets of data (including bad packets) received.
   - **Packets:** The number of packets (including bad, broadcast, and multicast packets) received.
   - **Boardcast Packets:** the number of good packets received addressed to the broadcast address.
   - **Multicast Packets:** The number of packets received addressed to the multicast address.

- **CRC / Alignment Errors:** The number packets received that had a length between 64 - 1518 octets (excluding framing bits, but including FCS octets).
- **Undersize Packets:** The number of packets received that were less than 64 octets.
- **Fragments:** The number of frames received with invalid CRC and were less than 64 octets.
- **Jabbers:** The number of frames received with invalid CRC and were larger than 64 octets.
- **Collisions:** The number of estimated collisions that occurred on the corresponding Ethernet segment.
- **64 Bytes Frame:** The number of packets (including bad packets) received that were 64 octets.
- **65 - 127 Byte Frames:** The number of packets (including bad packets) received that were between 65 - 127 octets.
- **128 - 255 byte Frames:** The number of packets (including bad packets) received that were between 128 - 255 octets.
- **256 - 511 byte Frames:** The number of packets (including bad packets) received that were between 256 - 511 octets.
- **513- 1023 bytes Frames:** The number of packets (including bad packets) received that were between 512 - 1023 octets.
- **1024 - 1518 bytes Frames:** The number of packets (including bad packets) received that were between 1024 - 1518 octets.

Creating a New Index or Modifying an Existing Index RMON Event

1. On the **RMON Event** page, select an **Select Index** method (create a new index, or modify an existing index) from the drop-down list.
2. Enter an **Index** value, ranging from 1 - 65535.
3. Select a RMON event notification **Type**.
   - **None:** The number of octets received including characters.
   - **Log:** The number of uni-cast packets delivered to a high-layer protocol.
   - **SNMP Trap:** The number of broad-cast and multi-cast packet delivered to a high-layer protocol.

- **Log and Trap:** The number of inbound packets discarded including normal packets.

4. Enter the **Community** location where trap (discarded inbound) packets are sent. The string length is 0 - 127, the default setting is public.
5. Enter an **Owner** of the RMON event. The string length is 0 - 127, the default setting is null.
6. Enter a **Description** for the RMON event. The string length is 0 - 127, the default is null.
7. Click on the **Apply** button to either add a new index or modify an existing index.

Viewing RMON Event Information

- On the ***RMON Event*** page, the following information will be displayed:
  - **Index:** Displays the current index value.
  - **Event Type:** Displays the current RMON event notification type (None, Log, SNMP Traps, or Log and Trap)
  - **Community:** Displays the current location where trap packets are sent.
  - **Description:** Displays the current RMON event description.
  - **Last Sent Time:** Displays the last time an RMON event was sent.
  - **Owner:** Displays the current RMON event owner.
  - **Action:** Allows you to delete the current RMON event entry.

Deleting an RMON Event Entry

- On the **RMON Event** page, click on the **Delete** button to delete the current RMON event entry.

Viewing the RMON Event Log Table

- On the RMON Event Log Table page, the following information will be displayed:
  - **Event Index:** Select an RMON event index from the drop-down list.
  - **Index:** Displays the index of the selected RMON event entry.
  - **Log Time:** Displays the log time of the selected RMON event entry.
  - **Description:** Displays the description of the selected RMON event entry.

Creaitng a New RMON Alarm or Modifying an Existing RMON Alarm

1. On the **RMON Alarm** page, select an alarm option from the drop-down list:
   - **Create New**
   - **Modify Existing**
2. Enter the following information in the corresponding fields:
   - **Index:** Enter an index value ranging from 1 - 65535.
   - **Sample Port:** Select the port that the RMON Alarm will apply to from the drop-down list.
   - **Sample Variable:** Select a variable to sample:
   - **Drop Events:** The number of RMON events where packets were dropped due to a lack of resources.
     - **Octets:** The number of received and transmitted bytes, includes FCS and excludes framing.
     - **Pkts:** The number of frames received and transmitted.
     - **Broadcast Pkts:** The number of good frames received by the broadcast address, does not include multicast packets.
     - **Multicast Pkts:** The number of good frames received by the multicast address.
     - **CRC Align Errors:** The number of CRC/alignment errors.
     - **Under Size Pkts:** The number of frames received that were less than 64 octets (excluding framing bits but including FCS octets).
     - **Over Size Pkts:** The number of frames received that were longer than 1518 octets (excluding framing bits but including FCS octets).
     - **Fragments:** The number of frames received that were less than 64 octets and had either an FCS or alignment issue.
     - **Jabbers:** The number of frames received that were longer than 1518 octets and had either an FCS or alignment issue.
     - **Collisions:** The number of collisions on the Ethernet segment.
     - **Pkts 64 Octets:** The number of frames (including bad packets) received and transmitted that were 64 octets in length.

- **Pkts 158 to 255 Octets:** The number of frames (including bad packets) received and transmitted that were between 158 to 255 octets.
- **Pkts 256 to 511 Octets:** The number of frames (including bad packets) received and transmitted that were between 256 to 511 octets.
- **Pkts 512 to 1023 Octets:** The number of frames (including bad packets) received and transmitted that were between 512 to 1023 octets.
- **Pkts 1024 to 1518 Octets:** The number of frames (including bad packets) received and transmitted that were between 1024 to 1518 octets.

- **Sample Interval:** The sample interval between 1 - 2147483647.
- **Sample Type:** The sample method used for calculating the value that is compared against the threshold value.
  - **Absolute:** Uses the absolute sample value.
  - **Delta:** Uses the difference between sample values.
- **Rising Threshold:** The rising threshold value 0 - 2147483647.
- **Falling Threshold:** The falling threshold value 0 - 2147483647.
- **Rising Event:** The event that is activated when the rising threshold value is reached.
- **Falling Event:** The event that is activated when the falling threshold value is reached.
- **Owner:** The owner of the RMON alarm.

3. Click on the **Apply** button to either add a new alarm or modify an existing alarm.

Viewing RMON Alarm Information

- On the ***RMON Alarm*** page, the following information will be displayed:
  - **Index:** Displays the index of the alarm control entry
  - **Sample Port:** Displays the current sample port.
  - **Sample Variable:** Displays the current sample variable.
  - **Sample Interval:** Displays the current sample interval.
  - **Sample Type:** Displays the current sample alarm.
  - **Rising Threshold:** Displays the rising threshold value.
  - **Falling Threshold:** Displays the falling threshold value.

- **Rising Event:** Display the rising event that is activated once the rising threshold is met.
- **Falling Event:** Display the falling event that is activated once the falling threshold is met.
- **Owner:** Displays the owner of the RMON Alarm entry.

Deleting an RMON Alarm Entry

- On the **RMON Alarm** page, click on the **Delete** button to delete the current RMON alarm entry.

Creaitng a New RMON History or Modifying an Existing RMON History

1. On the **RMON History** page, select a history option from the drop-down list:
   - **Create New**
   - **Modify Existing**
2. Enter the following information in the corresponding fields:
   - **Index:** Enter a RMON history value ranging from 1 - 65535.
   - **Sample Port:** Select the port that the RMON history entry will apply to from the drop-down list.
   - **Bucket Requested:** Indicate the maximum number of entries that can be stored in RMON history. The range is 1 - 50, the default value is 50.
   - **Intervals:** Indicate the RMON history sampling interval in seconds. The range is 1 - 3600, the default value is 1800 seconds.
   - **Owner:** The owner for the RMON history entry.
3. Click on the **Apply** button to either add a new history entry or modify an existing history entry.

Viewing RMON History

- On the ***RMON History*** page, the following information will be displayed:
  - **Index:** Displays the index selected for the RMON history entry.
  - **Data Source:** Displays the current data source.
  - **Bucket Requested:** Displays the current bucket value.
  - **Interval:** Displays the current interval value.

- **Owner:** Displays the current owner of the RMON history entry.

Deleting an RMON History Entry

- On the **RMON History** page, click on the **Delete** button to delete the current RMON history entry.

Applying the RMON History Index

1. On the **RMON History Table** page, select a RMON history index from the drop-down list.
   - RMON History: Allows you to select a RMON history index from the drop-down list.
2. Click on the **Apply** button.

Power over Ethernet

The switch can be used to easily build a powered centrally-controlled IP phone system, IP camera system and AP group for the enterprise. For instance, cameras / APs can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without a power-socket limitation, the switch makes the installation of cameras or WLAN APs easier and more efficient.

System Configuration

In a Power over Ethernet system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure, to powered devices (PDs), which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system with a PSU is capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the function of the majority of the ports, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current. The input power consumption is equal to the system's aggregated power consumption. The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected. When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority and maximum allowable power per port.

Power over Ethernet Configuration

This section enables you to inspect and configure the current PoE configuration and usage settings.

PoE Configuration

Making Changes to the Power over Ethernet Configuration

1. On the PoE Configuration page, from the drop-down list, select a System PoE Admin Mode:.
   - **System PoE Admin Mode:** Allows a user to enable or disable PoE function. It will cause all of PoE ports to supply or not to supply power.
2. From the drop-down list select a **PoE Management Mode**:
   - **PoE Management Mode:** There are six modes for configuring how the ports/PDs may reserve power and when to shut down ports.
     - **Classification mode:** The system reserves PoE power for PD according to PoE class level.
     - **Consumption mode:** The system offers PoE power according to PD real power consumption.
     - **Allocation mode:** Allows users allow to assign how much PoE power to each port and the system will reserve PoE power to PD.
3. Enter a **Temperature Threshold.** This allows the user to set a temperature protection threshold value. If the system temperature is overly high, the system will lower the total PoE power budget automatically.PoE Temperature Display the PoE Chip Temperature
4. The **PoE Temperature** field will display the current temperature of the **Switch**.
5. Enter a **Power Budget** value. This value allows the user to configure PoE power budget on the **Switch**.
6. Click the **Apply** button.

Making Changes to Power Allocation

1. On the ***Power Allocation*** page, from the drop-down list, select a PoE Mode for the corresponding port:
   - **Enable:** Enables PoE function.
   - **Disable:** Disables PoE function.
   - **Schedule:** Enables PoE function in schedule mode.
2. From the drop-down list select a **Schedule** profile mode:
   - **Profile 1**
   - **Profile 2**
   - **Profile 3**
   - **Profile 4**
3. From the drop-down list select the corresponding port's PoE port **Priority.** The priority is used in case the total power consumption exceeds the total power budget. In this case the port with the lowest priority will be turned off, and offer power to the port of higher priority:
   - **Low**
   - **High**
   - **Critical**
4. The **PD Class** field will display the class of the PD assigned to the port, as established in PoE Management Mode section of the PoE Configuration table.
5. The **Current Used [mA]** field will displays how much current the PD currently is using.
6. The **Power Used [W]** field will displays how much power the PD currently is using.
7. Enter a **Power Allocation** value. The maximum value must be less than 36 watts, per port. Total port values must be less than the Power Reservation value. Once power overload is detected, the port will automatically shut down and remain in detection mode until PD's power consumption is lower than the power limit value.
8. Click the **Apply** button.

Power over Ethernet Status

- The PoE Status page provides and on-screen report for the PoE status per port.

PoE Schedule

This page allows the user to a define PoE schedule and schedule power recycling.

Besides being used for IP Surveillance, the Managed PoE switch is suitable for creating any PoE network including VoIP and Wireless LAN. The PoE switch can effectively control the power supply besides its capability of giving power. The "PoE schedule" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is effective in helping SMBs or enterprise to save power and money.

Scheduled Power Recycling

The Managed PoE switch allows each of the connected PoE IP cameras to reboot at a specified time each week. Therefore, it will reduce the chance of IP camera crashes resulting from buffer overflow.

Press the **Add New Rule** button to start setting the PoE Schedule function. You have to set a PoE schedule to profile and then go back to PoE Port Configuration, and select **Schedule Mode** from per-port **PoE Mode** option to enable you to indicate which schedule profile could be applied to the PoE port.

- Press the **Delete** button to delete an existing rule.
- Press the **Modify** button to change an existing rule.

- The page includes the following fields:
  - **Profile:** Set the schedule profile mode. Possible profiles are: Profile1, Profile2, Profile3, Profile4.
    - **Week Day:** Allows user to set a week day for defining PoE function by enabling it on the day.
    - **Start Hour:** Allows the user to set the hour the PoE function starts.
    - **Start Min:** Allows the user to set the minute the PoE function starts.
    - **End Hour:** Allows the user to set the hour PoE function ends.
    - **End Min:** Allows the user to set the minute PoE function ends.
  - **Reboot Enable:** Allows user to enable or disable the whole PoE port reboot by PoE reboot schedule. Please note that if you want PoE schedule and PoE reboot

schedule to work at the same time, please use this function, and don't use the Reboot Only function. This function enables an administrator to reboot a PoE device at an indicated time if required.

- **Reboot Only** - Allows a user to reboot PoE function by PoE reboot schedule. Please note that if an administrator enables this function, the PoE schedule will not set a time to the profile. This function is just for the PoE port to reset at an indicated time.
- **Reboot Hour** - Allows a user to set what hour PoE reboots. This function is only for the PoE reboot schedule.
- **Reboot Min** - Allows a user to set what minute PoE reboots. This function is only for the PoE reboot schedule.

PoE Alive Check Configuration

The switch can be configured to monitor connected PD's status in real-time via ping action. Once the PD stops working and responding, the PoE Switch is going to restart PoE port power, and force a reboot of the PD.

This page provides you with details on how to configure PD Alive Check.

Applying Alive Check Configuration

1. On the ***PD Alive Check*** page, select a **Port** from the drop-down list.
2. Select a **Mode.** A mode allows users to enable or disable the PD Alive Check function on a per-port basis. By default, all ports are disabled.
3. Enter an **Interval Time (10 - 300s)**. This field allows a user to set how long a system should issue a ping request to PD, for detecting whether PD is alive or dead. Interval time range is from 10 seconds to 300 seconds.
4. Select a **Retry Count (1 - 5).** This field allows a user to set the number of times a system tries to ping the PD. For example, if we set count 2, it means that if system retries ping to the PD and the PD doesn't response continuously, the PoE port will be reset.

5. Select an **Action.** This field allows user to set which action will be applied if the PD is without any response. The PoE Switch Series offers the following 3 actions:
   - **PD Reboot**: It means the system will reset the PoE port that is connected to the PD.
   - **PD Reboot & Alarm**: It means the system will reset the PoE port and issue an alarm message via Syslog.
   - **Alarm**: It means the system will issue an alarm message via Syslog.
6. Enter a **Reboot Time (30 - 180s).** This field allows a user to set the PoE device rebooting time as there are so many kinds of PoE devices on the market and they have a different rebooting time.
7. Click on the **Apply** button.

Viewing changes to the PD Alive-Check

1. On the PD Alive Check Configuration page, the following information will be displayed:
   - **Port:** The number of the port.
   - **Mode:** Displays whether the PD Alive Check function is enabled or disabled on a per-port basis. By default, all ports are disabled.
   - **Ping PD IP Address:** Displays the PoE device IP address.
     - Click the **Edit** button to manually edit the IP address.
   - Internal Time: Displays how long system should issue a ping request to PD for detecting whether PD is alive or dead.
   - Retry Count: Displays the number of times system retries ping to PD.
   - **Action:** Displays which action will be applied if the PD is without any response
   - Reboot Time: Displays the PoE device rebooting time as there are so many kinds of PoE devices on the market and they have a different rebooting time.

Maintenance

Use the Maintenance menu items to display and configure basic configurations of the Managed Switch. Under maintenance, the following topics are provided to back up, upgrade, save and restore the configuration. This section has the following items:

- **Factory Default** - Enables you to reset the configuration of the Switch on this page.
- **Reboot Switch** - Enables you to restart the Switch on this page. After restart, the switch will boot normally.
- **Backup Manager** - Enables you to back up the Switch configuration.
- **Upgrade Manager** - Enables you to upgrade the switch configuration.
- **Dual Image** - Enables you to select an active or backup image on this page.

Factory Default

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. After the **Factory** button is pressed and the Switch is rebooted, the system will load the default IP settings as follows:

- **Default IP address**: 192.168.0.100
- **Subnet mask**: 255.255.255.0
- **Default Gateway**: 192.168.0.254
- **Other setting value**: disable (none).

To reset the Managed Switch to the factory default setting, you can also press the hardware reset button at the front panel about 10 seconds.

After the device is rebooted you can log into the web GUI using the web interface within the same subnet of 192.168.0.xx.

Reboot Switch

The Reboot page enables you to reboot the device from a remote location. Once the **Reboot** button is pressed, the user has to login to the Web interface for about 60 seconds.

Rebooting the Switch

1. On the ***Reboot*** page, click the **Reboot** button.

2. Once the **Reboot** button is selected the user must log back into the ***Web Interface*** for 60 seconds.

Backup Manager

This function allows backup of the current image or configuration of the Managed Switch to the local management station.

Backing up an Image

1. On the ***Backup Manager*** page, select a **Backup Method** from the drop-down list.

2. Enter a **Server IP** address.

3. Select a Backup Type:

   - **Image**
   - **Running Configuration**
   - **Startup Configuration**
   - **Backup Configuration**
   - **Flash Log**
   - **Buffered Log**

4. If **Image** is selected as a **Backup Type**, select an **Image type:**

   - **Active**
   - **Backup**

5. Click the **Backup** button. The image has now been backed up.

Upgrade Manager

This function enables you to reload the current image or configuration to the switch as a local management solution. You can also upgrade the Switch if new firmware becomes available.

Upgrading or reloading a Firmware Image

1. On the ***Upgrade Manager*** page, select an **Upgrade Method** from the drop-down list.
2. Enter the **Server IP** address.
3. Enter a **File Name.** The name of firmware image or configuration.
4. Select an **Upgrade Type:**
   - **Image**
   - **Start Configuration**
   - **Backup Configuration**
   - **Running Configuration**
5. Select an **Image type**:
   - **Active**
   - **Backup**
6. Click the **Upgrade** button. The firmware image on the switch will now be replaced with the destination file.

Dual Image

This page provides information about the active and backup firmware images in the device, and allows you to revert to the backup image. The web page displays two tables with information about the active and backup firmware images.

Applying an Image

1. On the Dual Image Configuration page, select your desired active or backup image from the **Active Image** drop-down menu.
2. Click the **Apply** button. Your image will now be applied.

Viewing Dual Image Information

- On the ***Images Information*** page, the following information will be displayed:
  - **Flash Partition** - Displays the current flash partition.
  - **Image Name** - Displays the current image name.
  - **Image Size** - Displays the current image size.
  - **Created Time** - Displays the created time.

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.

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.