User Manual

Product Model: DES-1210-10/ME, DES-1210-26/ME, DES-1210-28/ME L2 Managed Metro Ethernet Switch

Release: R6.02

Table of Contents

About This Guide

This guide provides instructions to install the D-Link DES-1210 Metro Ethernet Managed Switch and to configure with HTTP step-by-step.

Note: The model you have purchased may appear slightly different from the illustrations shown in the document. Refer to the Product Instruction and Technical Specification sections for detailed information about your switch, its components, network connections, and technical specifications.

This guide is mainly divided into three parts:

1. Hardware Installation: Step-by-step hardware installation procedures.
2. Getting Started: A startup guide for basic switch installation and settings.
3. Configuration: Information about the function descriptions and configuration settings.

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to DES-1210 Metro Ethernet Managed Switch, and “switch” (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms “switch”, “bridge” and “switching hubs” interchangeably, and both are commonly accepted for Ethernet switches.

A **NOTE** indicates important information that helps a better use of the device.

A **CAUTION** indicates potential property damage or personal injury.

Copyright and Trademarks

Information in this document is subjected to change without notice.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

1 *Product Introduction*

- **Switch Description**
- **Front Panel Description**
- **LED Indicators**
- **Rear Panel Description**
- **Side Panel Description**
- **Gigabit Combo Ports**

Switch Description

The DES-1210 Metro Ethernet Managed switch is equipped with **Copper ports** (10/100Mbps) and **SFP ports** (100/1000Mbps) that can be used to attach various networking devices to the network like Computers, Notebooks, Print Servers, Network Attached Storage devices, IP Cameras, VoIP PBX devices, and other Switches. The Small Form Factor Portable (SFP) combo ports can be used together with fiber-optical transceivers in order to connect various other networking devices, using a fiber-optic connection, to the network at Gigabit Ethernet speeds over great distances.

This DES-1210 Metro Ethernet Managed switch provides unsurpassed performance, fault tolerance, scalability, robust security, standard-based interoperability and impressive technology to future-proof departmental and enterprise network deployments.

It allows IGMP Snooping and Authentication, QoS, Bandwidth Control, ACL and many security functions. It can be managed by Web UI, or commands via Telnet.

The DES-1210 Metro Ethernet Managed features the following list of switches:

Switch	Description
DES-1210-10/ME	8 10/100Mbps Copper Ports, 2 Combo 10/100/1000Mbps Copper / 100/1000Mbps SFP Ports, and One RJ-45 Console Port for out-of-band CLI configuration.
DES-1210-26/ME	24 10/100Mbps Copper Ports, 2 Combo 10/100/1000Mbps Copper / 100/1000Mbps SFP Ports, and One RJ-45 Console Port for out-of-band CLI configuration.
DES-1210-28/ME	24 10/100Mbps Copper Ports, 2 100/1000Mbps SFP Ports, 2 Combo 10/100/1000Mbps Copper / 100/1000Mbps SFP Ports, and One RJ-45 Console Port for out-of-band CLI configuration.

These switches have a combination of 1000BASE-T ports and SFP ports that may be used in to uplink various network devices to the Switch, including PCs, hubs and other switches to provide a gigabit Ethernet uplink in full-duplex mode. The SFP (Small Form Factor Portable) combo ports are used with fiber-optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances.

Front Panel Description

The front panel of the **DES-1210-10/ME** switch consists out of the following:

- 8 10/100Mbps Copper Ports
- 2 Combo 10/100/1000Mbps Copper / 100/1000Mbps SFP port
- One RJ-45 Console Port
- LEDs for Power, Console, Link/Act for port 1 to 8, and Link/Act/Speed for port 9 and 10

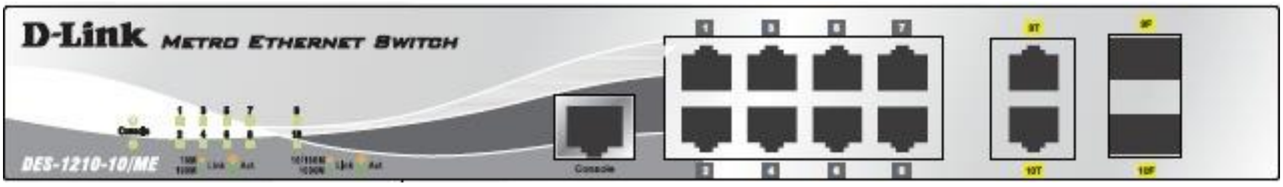


Figure 1.1 – DES-1210-10/ME Front Panel

NOTE: The MiniGBIC ports are shared with normal RJ-45 ports 9 and 10. When MiniGBIC port is used, the RJ-45 port cannot be used.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DES-1210-26/ME** switch consists out of the following:

- 24 10/100Mbps Copper Ports
- 2 Combo 10/100/1000Mbps Copper / 100/1000Mbps SFP port
- One RJ-45 Console Port
- LEDs for Power, Console, Link/Act for port 1 to 24, and Link/Act/Speed for port 25 and 26

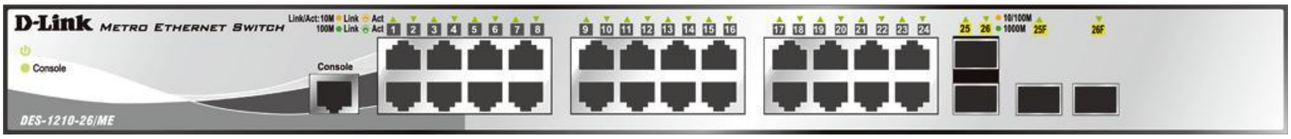


Figure 1.2 – DES-1210-26/ME Front Panel

NOTE: The MiniGBIC ports are shared with normal RJ-45 ports 25 and 26. When MiniGBIC port is used, the RJ-45 port cannot be used.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

The front panel of the **DES-1210-28/ME** switch consists out of the following:

- 24 10/100Mbps Copper Ports
- 2 Combo 10/100/1000Mbps Copper / 100/1000Mbps SFP port
- 2 100/1000Mbps SFP Ports
- One RJ-45 Console Port
- LEDs for Power, Console, Link/Act for port 1 to 24, and Link/Act/Speed for port 25 and 26

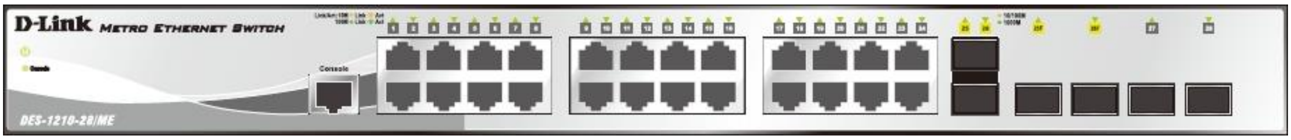


Figure 1.3 – DES-1210-28/ME Front Panel

NOTE: The MiniGBIC ports are shared with normal RJ-45 ports 25 and 26. When MiniGBIC port is used, the RJ-45 port cannot be used.

⚠ **CAUTION:** The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

LED Indicators

The Switch supports LED indicators for Power, Console, Fan, and Link/Act or Link/Act/Speed for each port. The following shows the LED indicators for the DES-1210 Metro Ethernet Managed Switch along with an explanation of each indicator.

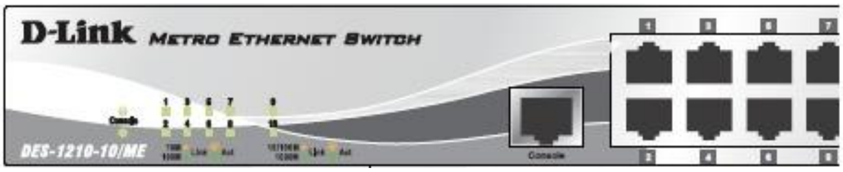


Figure 1.4 –LED Indicators on DES-1210-10/ME

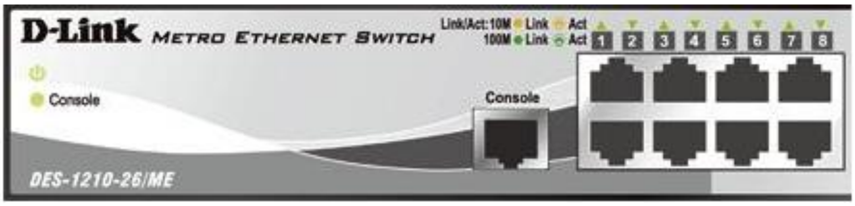


Figure 1.5 –LED Indicators on DES-1210-26/ME

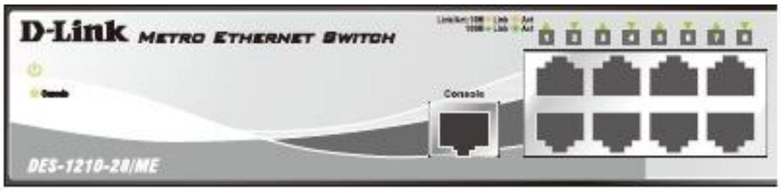


Figure 1.6 –LED Indicators on DES-1210-28/ME

Location	LED Indicative	Color	Status	Description
Per Device	**Power**	Green	Solid Light	Power on.
			Light off	Power off.
	Console	Green	Solid Light	Console on.
			Blinking	POST is in progress.
			Light off	Console off.
LED Per 10/100Mbps Copper Port	**Link/Act**	Green	Solid Green	When there is a secure 10/100Mbps Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 10/100Mbps Ethernet connected port.
			Light off	No link.
LED Per 10/100/1000Mbps Copper Port	**Link/Act/Speed**	Green/Amber	Solid Green	When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 1000Mbps Ethernet connected port.

			Solid Amber	When there is a secure 10/100Mbps Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 10/100Mbps Ethernet connected port.
			Light off	No link.
LED Per 100/1000Mbps SFP Port	**Link/Act/Speed**	Green/Amber	Solid Green	When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 1000Mbps Ethernet connected port.
			Solid Amber	When there is a secure 100Mbps Ethernet connection (or link) at any of the ports.
			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 100Mbps Ethernet connected port.
			Light off	No link.

Rear Panel Description

The rear panel of the Switch contains an AC power connector. The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 to 240 VAC at 50 to 60 Hz. Connect the Kensington-compatible security lock, at the rear of the switch, to a secure immovable device(only for DES-1210-10/ME). Insert the lock into the notch and turn the key to secure the lock(only for DES-1210-10/ME).

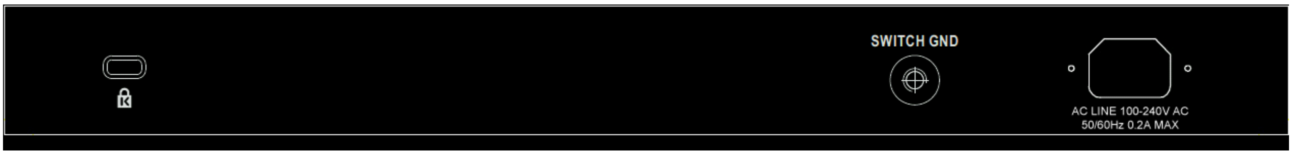


Figure 1.7 –Rear panel view of the DES-1210-10/ME

Figure 1.8 –Rear panel view of the DES-1210-26/ME

Figure 1.9 –Rear panel view of the DES-1210-28/ME

Side Panel Description

The left- and right-hand panels of the Switch have heat vents to dissipate heat. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

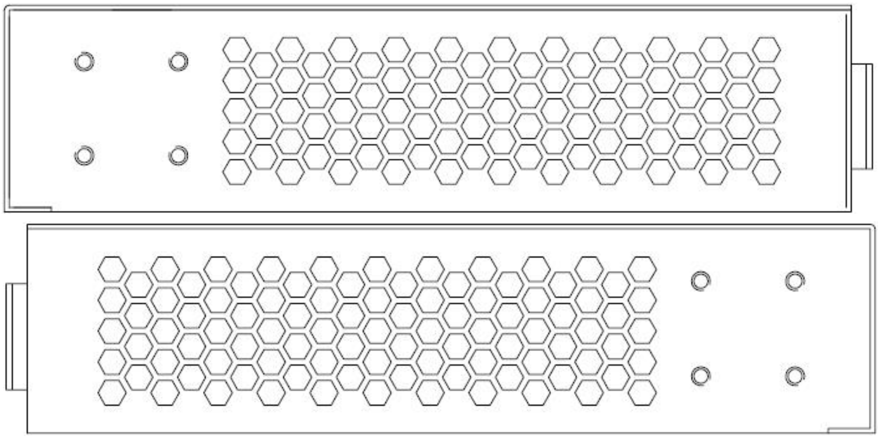


Figure 0-10. Side panels of the DES-1210-10/ME

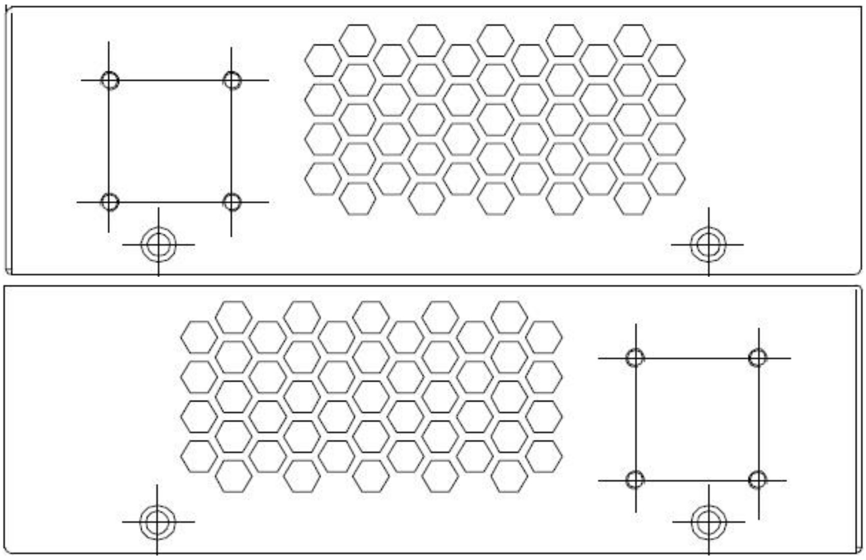


Figure 0-11. Side panels of the DES-1210-26/M

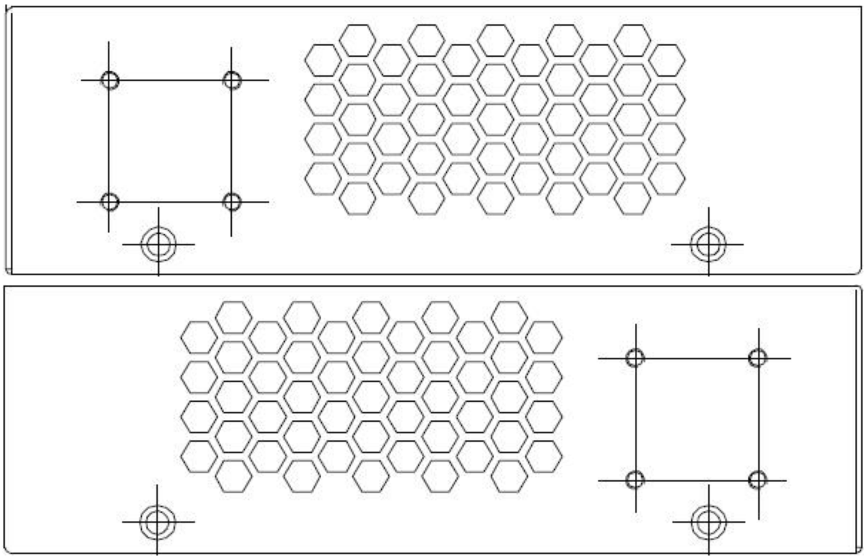


Figure 0-12. Side panels of the DES-1210-28/ME

Gigabit Combo Ports

The DES-1210 Series features either two or four Gigabit Ethernet Combo ports. These ports are 1000BASE-T copper ports (optional) and Small Form Factor Portable (SFP) ports (optional). See the diagram below to view the two SFP port modules being plugged into the Switch. Please note that although these two front panel modules can be used simultaneously, the ports must be different. The SFP port will always have the highest priority.

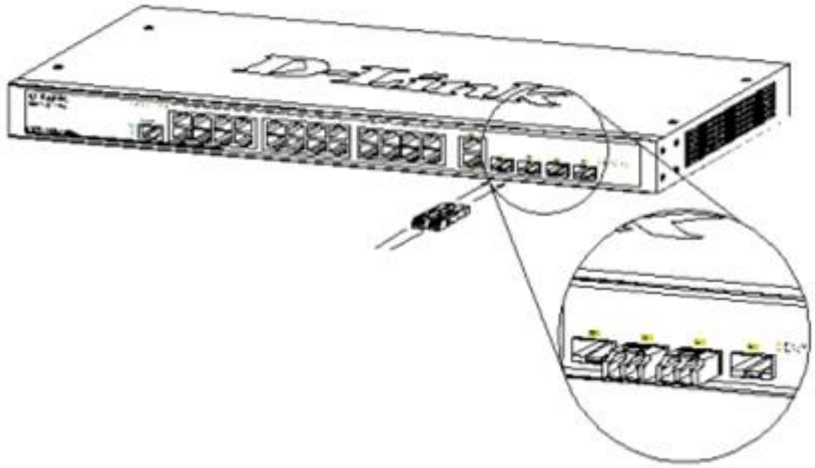


Figure 0-11. Inserting the SFP modules into the Switch

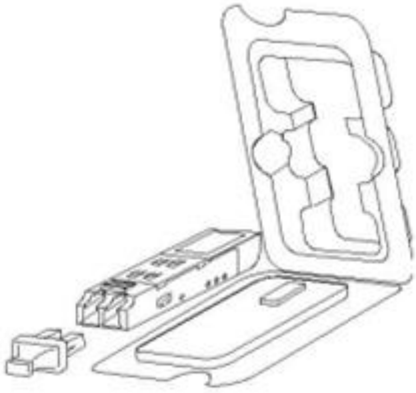


Figure 1-12. Installing the SFP Module

The Switch is equipped with SFP ports, which are to be used with fiber-optical transceiver cabling in order to uplink various other networking devices for a gigabit link that may span great distances. For a full list of supported SFP transceivers, for this switch series, refer to the Appendix-E.

2 Hardware Installation

This chapter provides unpacking and installation information for the D-Link Metro Ethernet Switch.

Step 1: Unpacking

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

- One D-Link Metro Ethernet Switch
- One AC power cord
- Four rubber feet
- Screws and two mounting brackets
- One Multi-lingual Getting Started Guide
- One CD with User Manual and D-View Module
- One RJ-45 cable for console port

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

Step 2: Switch Installation

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

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

Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.

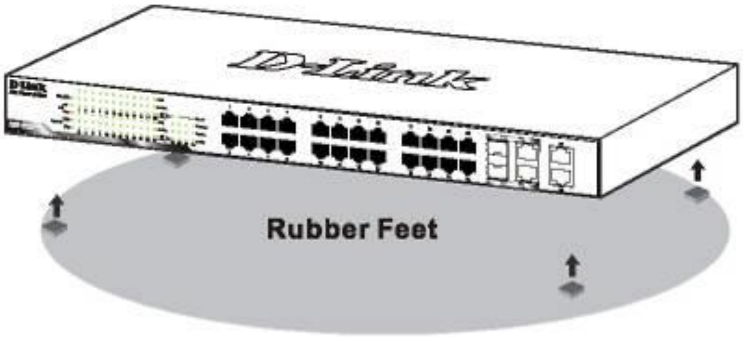


Figure 2.1 – Attach the adhesive rubber pads to the bottom

Rack Installation

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

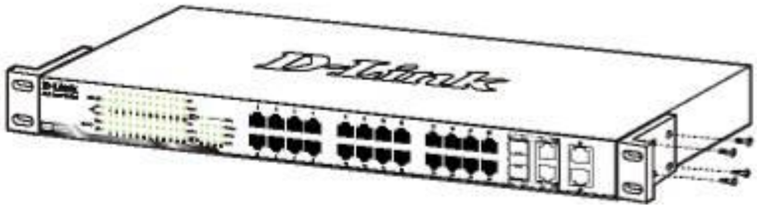


Figure 2.2 – Attach the mounting brackets to the Switch

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

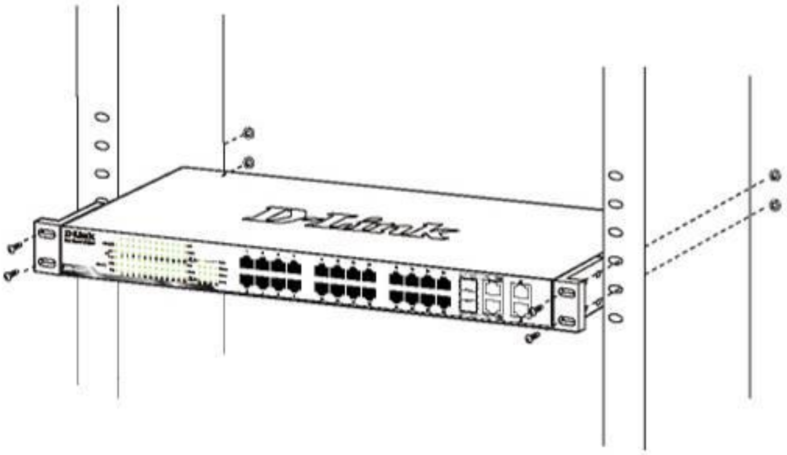


Figure 2.3 – Mount the Switch in the rack or chassis

Please be aware of following safety Instructions when installing:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Step 3 – Plugging in the AC Power Cord

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

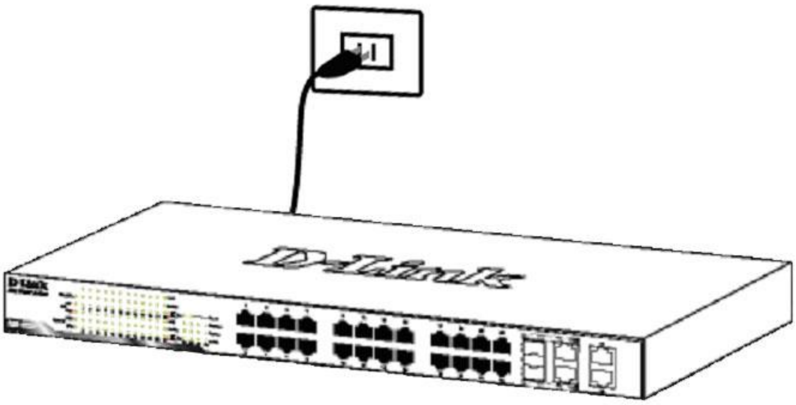


Figure 2.4 – Plugging the switch into an outlet

Power Failure

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

3 Getting Started

This chapter introduces the management interface of D-Link Metro Ethernet Switch.

Management Options

The D-Link Metro Ethernet Switch can be managed through any port on the device by using the Web-based Management.

Each switch must be assigned its own IP Address, which is used for communication with the Web-Based Management or a SNMP network manager. The PC should have an IP address in the same range as the switch. Each switch can allow up to four users to access the Web-Based Management concurrently.

Please refer to the following installation instructions for the Web-based Management.

Using Web-based Management

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

Supported Web Browsers

The embedded Web-based Management currently supports the following web browsers:

- Internet Explorer 6 or higher
- Netscape 8 or higher
- Mozilla
- Firefox 1.5/2.0 or higher

Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

1. A PC with a RJ-45 Ethernet connection
2. A standard Ethernet cable

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

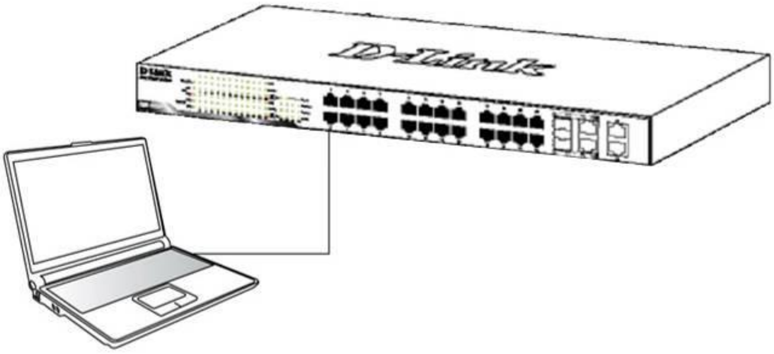


Figure 3.1 – Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. Enter 10.90.90.90 (the factory default IP address) in the address bar of your web browser and press <Enter>.

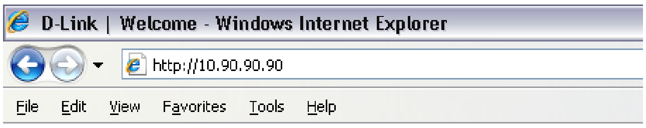


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser

NOTE: The switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

When the following logon dialog box appears, enter the password and choose the language of the Web-based Management interface then click **OK**.

By default, the Username and Password are empty.

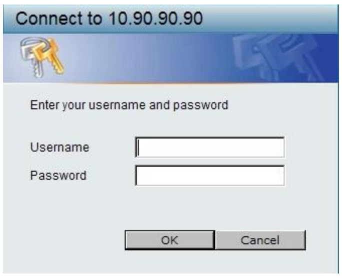


Figure 3.3 – Logon Dialog Box

Web-based Management

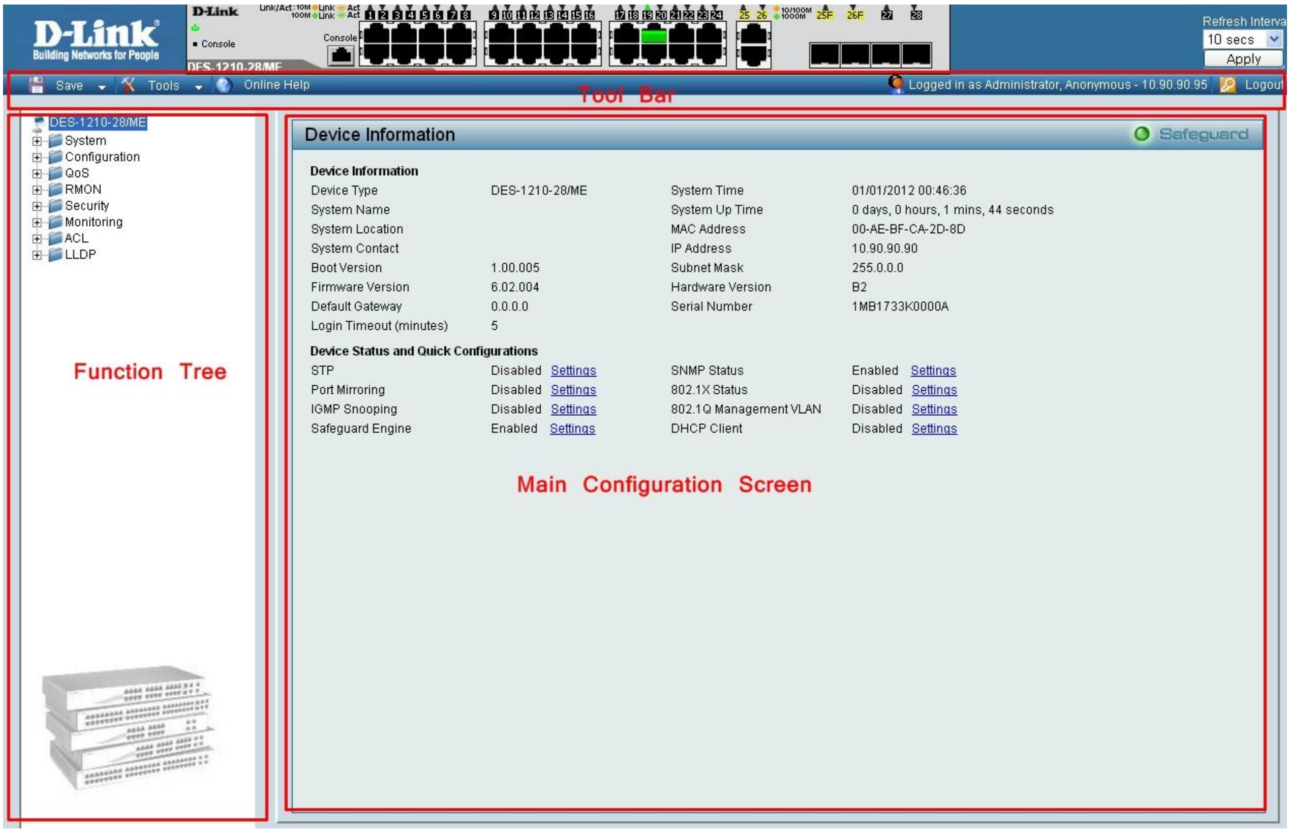
By clicking the **OK** button in Logon Dialog Box, you will enter the Web-based Management interface. Please refer to Chapter 4 Configuration for detailed instructions.

4 Configuration

The features and functions of the D-Link Metro Ethernet Managed Switch can be configured for optimum use through the Web-based user interface.

Web-based Management

After press the **OK** button in Logon Dialog Box, you will see the screen below:



Device Information

Device Type	DES-1210-28/ME	System Time	01/01/2012 00:46:36
System Name		System Up Time	0 days, 0 hours, 1 mins, 44 seconds
System Location		MAC Address	00-AE-BF-CA-2D-8D
System Contact		IP Address	10.90.90.90
Boot Version	1.00.005	Subnet Mask	255.0.0.0
Firmware Version	6.02.004	Hardware Version	B2
Default Gateway	0.0.0.0	Serial Number	1MB1733K0000A
Login Timeout (minutes)	5		

Device Status and Quick Configurations

STP	Disabled Settings	SNMP Status	Enabled Settings
Port Mirroring	Disabled Settings	802.1X Status	Disabled Settings
IGMP Snooping	Disabled Settings	802.1Q Management VLAN	Disabled Settings
Safeguard Engine	Enabled Settings	DHCP Client	Disabled Settings

Figure 4.1 – Web-based Management

The above image is the Web-based Management screen. The three main areas are the **Tool Bar** on top, the **Function Tree**, and the **Main Configuration Screen**.

The **Tool Bar** provides a quick and convenient way for essential utility functions like firmware and configuration management.

By choosing different functions in the **Function Tree**, you can change all the settings in the **Main Configuration Screen**. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree.

At the upper right corner of the screen the username and current IP address will be displayed.

Under the username is the **Logout** button. Click this to end this session.

NOTE: If you close the web browser without clicking the **Logout** button first, then it will be seen as an abnormal exit and the login session will still be occupied.

Finally, by clicking on the D-Link logo at the upper-left corner of the screen you will be redirected to the local D-Link website.

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

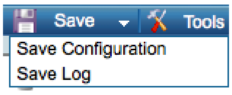
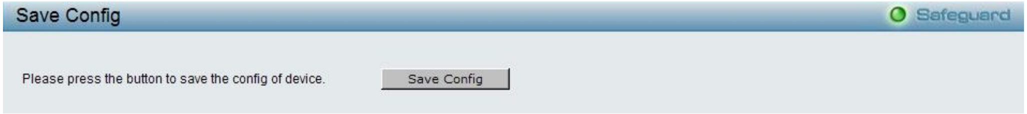


Figure 4.2 – Save Menu

Save Configuration

Select to save the entire configuration changes you have made to the device to switch's non-volatile RAM.

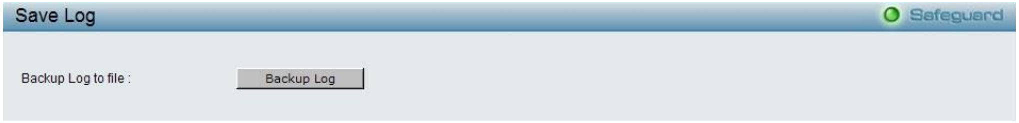


Please press the button to save the config of device.

Figure 4.3 – Save Configuration

Save Log

Save the log entries to your local drive and a pop-up message will prompt you for the file path. You can view or edit the log file by using text editor (e.g. Notepad).



Backup Log to file :

Figure 4.4 – Save Log

Tool Bar > Tool Menu

The Tool Menu offers global function controls such as Reset, Reset System, Reboot Device, Configuration Backup and Restore, Firmware Backup and Upgrade.

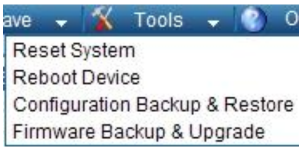
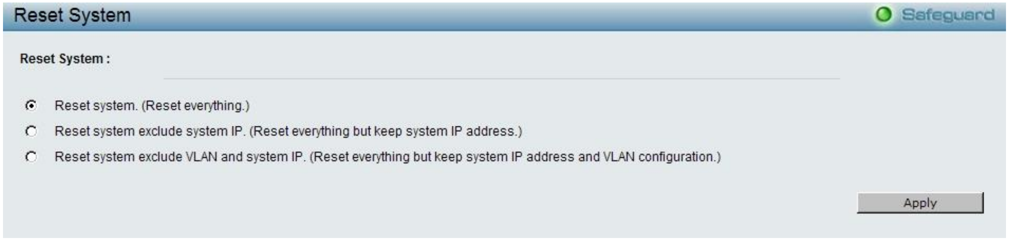


Figure 4.5 – Tool Menu

Reset System

Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot.



Reset System :

● Reset system. (Reset everything.)

○ Reset system exclude system IP. (Reset everything but keep system IP address.)

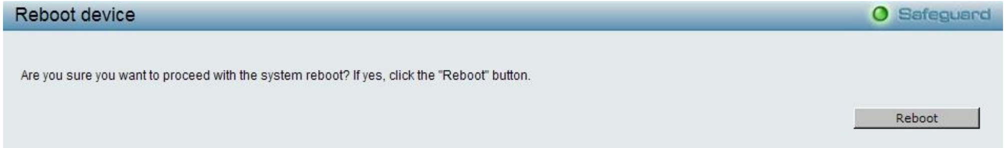
○ Reset system exclude VLAN and system IP. (Reset everything but keep system IP address and VLAN configuration.)

Figure 4.6 – Tool Menu > Reset System

Select the different reset method then click **Apply** to reset the system.

Reboot Device

Provide a safe way to reboot the system. Click **Reboot** to restart the switch.



Reboot device
Safeguard

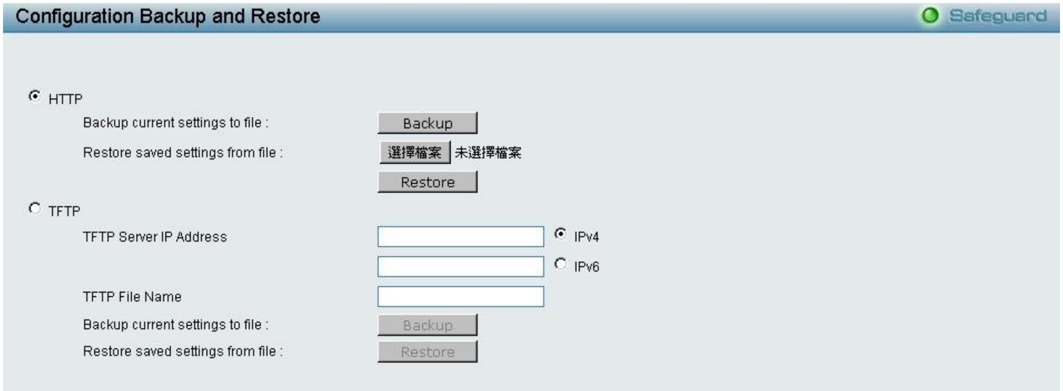
Are you sure you want to proceed with the system reboot? If yes, click the "Reboot" button.

Reboot

Figure 4.7 – Tool Menu > Reboot Device

Configuration Backup & Restore

Allow the current configuration settings to be saved to a file (not including the password), and if necessary, you can restore configuration settings from this file. Two methods can be selected: **HTTP** or **TFTP**.



Configuration Backup and Restore
Safeguard

● HTTP
Backup current settings to file : Backup
Restore saved settings from file : 選擇檔案 未選擇檔案
Restore

○ TFTP
TFTP Server IP Address ● IPv4
○ IPv6
TFTP File Name
Backup current settings to file : Backup
Restore saved settings from file : Restore

Figure 4.8 – Tool Menu > Configure Backup and Restore

HTTP: Backup or restore the configuration file to or from your local drive.

Click **Backup** to save the current settings to your disk.

Click **Browse** to browse your inventories for a saved backup settings file.

Click **Restore** after selecting the backup settings file you want to restore.

TFTP: TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows you to transfer files to a remote TFTP server. Specify **TFTP Server IPv4 or IPv6 Address** and **TFTP File Name** for the configuration file you want to save to / restore from. The maximum Telnet Server connection is 4.

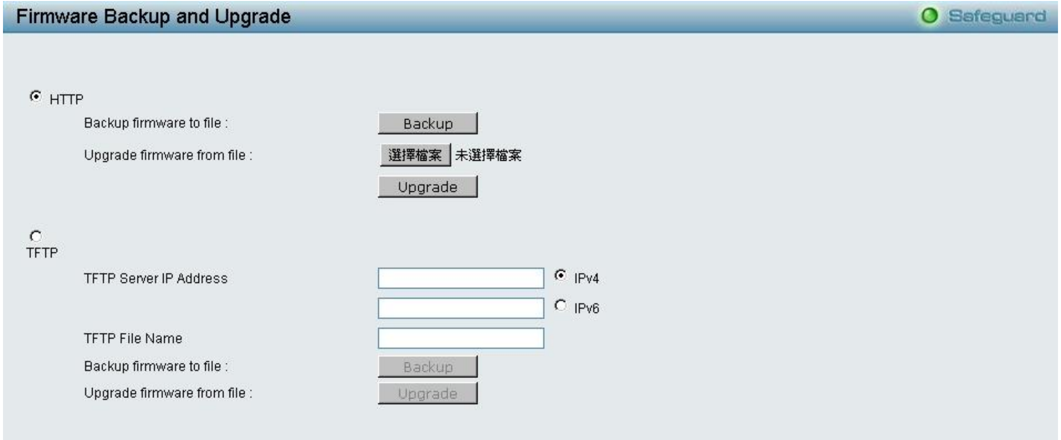
Click **Backup** to save the current settings to the TFTP server.

Click **Restore** after selecting the backup settings file you want to restore.

Note: Switch will reboot after restore, and all current configurations will be lost.

Firmware Backup & Upgrade

Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. Two methods can be selected: **HTTP** or **TFTP**.



Firmware Backup and Upgrade
Safeguard

● HTTP
Backup firmware to file : Backup
Upgrade firmware from file : 選擇檔案 未選擇檔案
Upgrade

○
TFTP
TFTP Server IP Address ● IPv4
○ IPv6
TFTP File Name
Backup firmware to file : Backup
Upgrade firmware from file : Upgrade

Figure 4.9 – Tool Menu > Firmware Backup and Upgrade

HTTP: Backup or upgrade the firmware to or from your local PC drive.

Click **Backup** to save the firmware to your disk.

Click **Browse** to browse your inventories for a saved firmware file.

Click **Upgrade** after selecting the firmware file you want to restore.

TFTP: Backup or upgrade the firmware to or from a remote TFTP server. Specify **TFTP Server IPv4 or IPv6 Address** and **File Name** for the configuration file you want to save to / restore from. The maximum Telnet Server connection is 4.

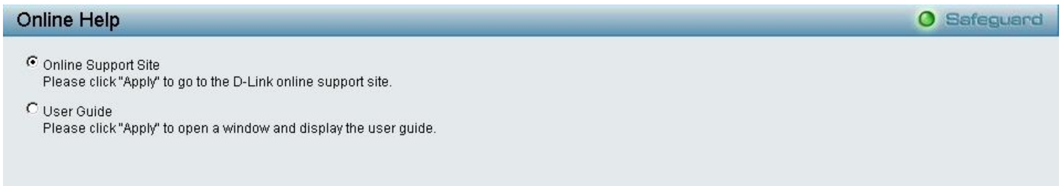
Click **Backup** to save the firmware to the TFTP server.

Click **Upgrade** after selecting the firmware file you want to restore.

⚠ **CAUTION:** Do not disconnect the PC or remove the power cord from device until the upgrade completes. The Switch may crash if the Firmware upgrade is incomplete.

Tool Bar > Online Help

The Online Help provides two ways of online support:



Online Help

● Online Support Site
Please click "Apply" to go to the D-Link online support site.

○ User Guide
Please click "Apply" to open a window and display the user guide.

Figure 4.10 – Online Help

D-Link Support Site: This will lead you to the D-Link website where you can find online resources such as updated firmware images.

User Guide: This can offer an immediate reference for the feature definition or configuration guide.

Click **Apply** to make configuration effected.

Function Tree

All configuration options on the switch are accessed through the Setup menu on the left side of the screen. Click on the setup item that you want to configure. The following sections provide more detailed description of each feature and function.

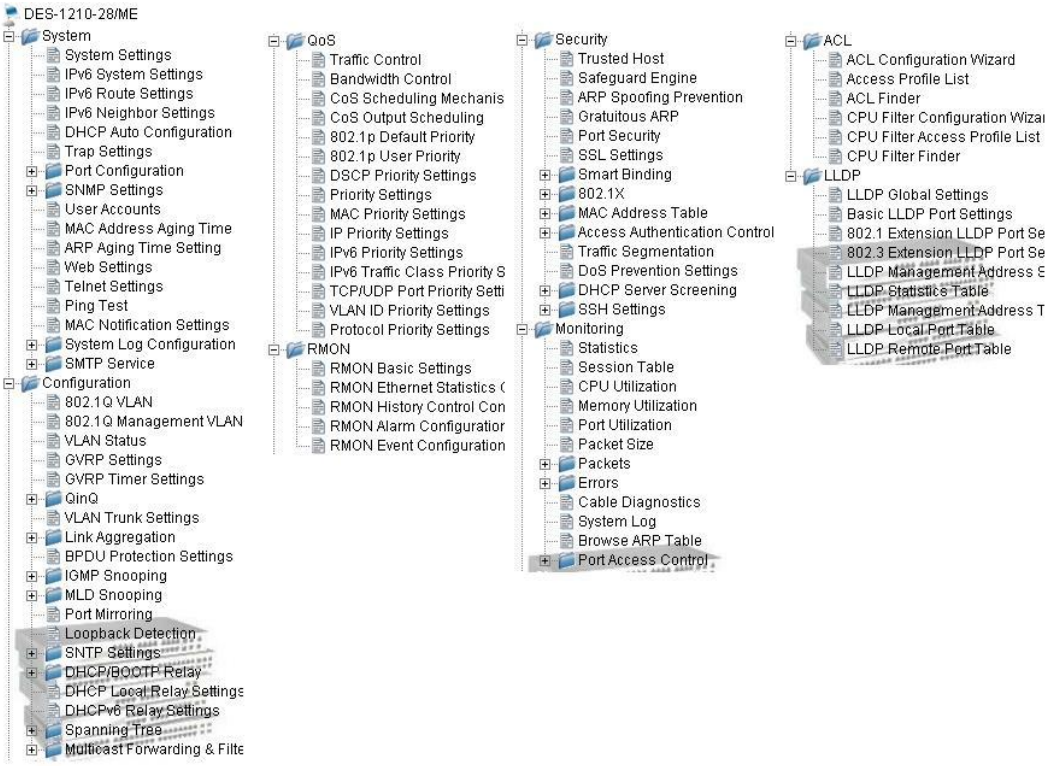


Figure 4.11 –Function Tree

Device Information

The Device Information provides an overview of the switch, including essential information such as firmware & hardware information, and IP address.

It also offers an overall status of common software features:

STP: Click **Settings** to link to Configuration > Spanning Tree > STP Bridge Global Settings. Default is disabled.

Port Mirroring: Click **Settings** to link to Configuration > Port Mirroring. Default is disabled.

IGMP Snooping: Click **Settings** to link to Configuration > IGMP Snooping > IGMP Snooping. Default is disabled.

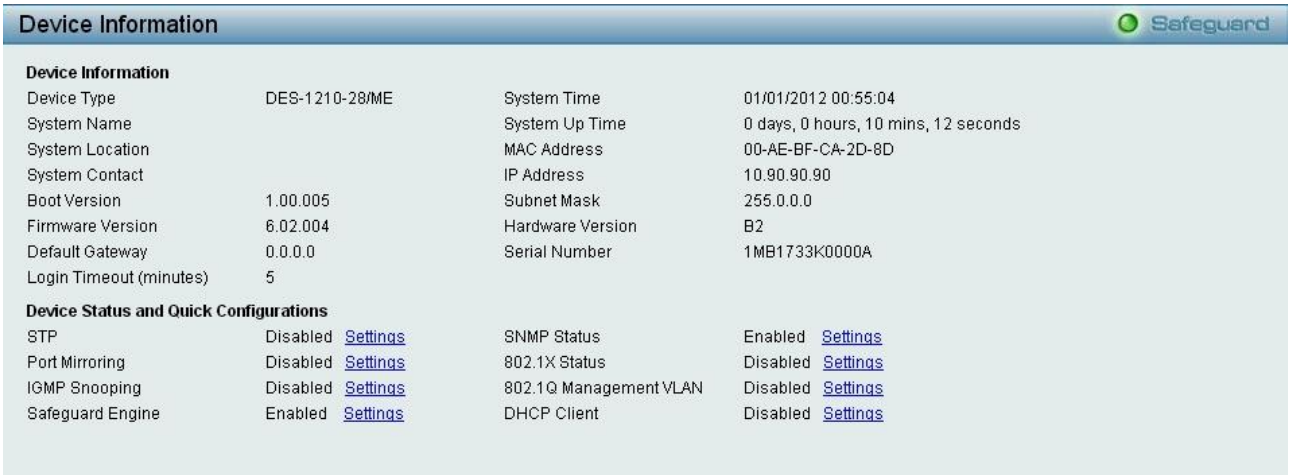
Safeguard Engine: Click **Settings** to link to Security > Safeguard Engine. Default is enabled.

SNMP Status: Click **Settings** to link to System > SNMP Settings > SNMP Global State. Default is enabled.

802.1X Status: Click **Settings** to link to Security > 802.1X > 802.1X Settings. Default is disabled.

802.1Q Management VLAN: Click **Settings** to link to Configuration > 802.1Q Management VLAN. Default is disabled.

DHCP Client: Click **Settings** to link to System > System Settings. Default is disabled.



Device Information

Device Information			
Device Type	DES-1210-28/ME	System Time	01/01/2012 00:55:04
System Name		System Up Time	0 days, 0 hours, 10 mins, 12 seconds
System Location		MAC Address	00-AE-BF-CA-2D-8D
System Contact		IP Address	10.90.90.90
Boot Version	1.00.005	Subnet Mask	255.0.0.0
Firmware Version	6.02.004	Hardware Version	B2
Default Gateway	0.0.0.0	Serial Number	1MB1733K0000A
Login Timeout (minutes)	5		
Device Status and Quick Configurations			
STP	Disabled Settings	SNMP Status	Enabled Settings
Port Mirroring	Disabled Settings	802.1X Status	Disabled Settings
IGMP Snooping	Disabled Settings	802.1Q Management VLAN	Disabled Settings
Safeguard Engine	Enabled Settings	DHCP Client	Disabled Settings

Figure 4.12 – Device Information

System > System Settings

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

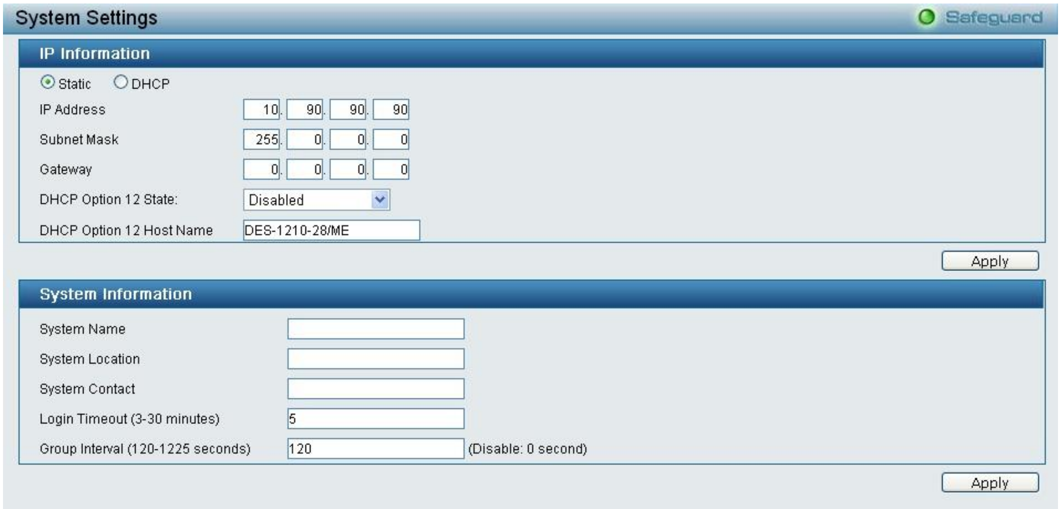
IP Information: There are two ways for the switch to obtain an IP address: Static and DHCP (Dynamic Host Configuration Protocol).

When using static mode, the **IP Address**, **Subnet Mask, Gateway** and **DHCP Option 12 State** can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is **10.90.90.90** and subnet mask is **255.0.0.0**.

System Information: By entering a **System Name** and **System Location**, the device can more easily be recognized.

Login Timeout: The Login Timeout controls the idle time-out period for security purposes, and when there is no action for a specific time span in the Web-based Management. If the current session times out (expires), the user is required a re-login before using the Web-based Management again. Selective range is from 3 to 30 minutes, and the default setting is 5 minutes.

Group Interval: The user can adjust the **Group Interval** to optimal frequency. Selective range is from 120 to 1225 seconds, and 0 means disabling the reporting function.



IP Information

● Static ○ DHCP

IP Address 10 . 90 . 90 . 90

Subnet Mask 255 . 0 . 0 . 0

Gateway 0 . 0 . 0 . 0

DHCP Option 12 State: Disabled

DHCP Option 12 Host Name DES-1210-28/ME

System Information

System Name

System Location

System Contact

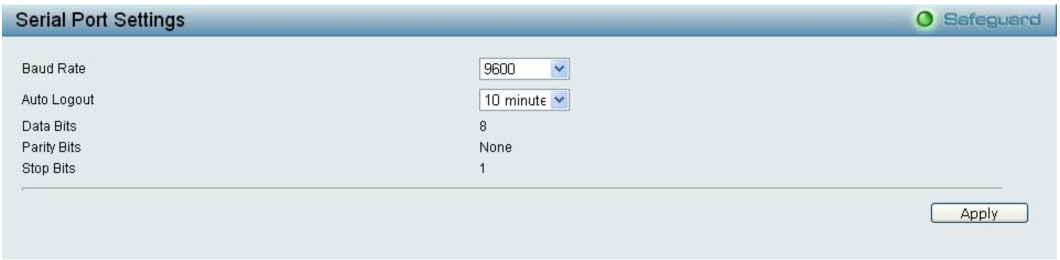
Login Timeout (3-30 minutes) 5

Group Interval (120-1225 seconds) 120 (Disable: 0 second)

Figure 4.13 – System > System Settings

System > Serial Port Settings

The Serial Port Settings page allow user to configure the Serial Port information.



Baud Rate 9600

Auto Logout 10 minute

Data Bits 8

Parity Bits None

Stop Bits 1

.

Figure 4.14 – System > Serial Port Settings

Baud Rate: Specifies the Baud rate for serial port. The values are 9600, 19200, 38400 and 115200 data bits.

Auto Logout: Specifies the auto logout time. The values are 2 mins, 5 mins, 10 mins, 15 mins and Never

Data Bits: Displays the data bits is 8.

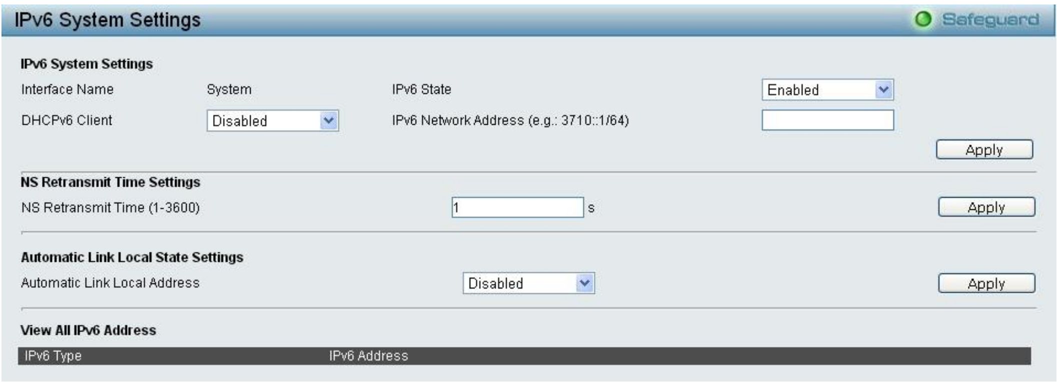
Parity Bits: Displays the parity bits is none.

Stop Bits: Displays the stop bits is 1.

Click **Apply** for the settings to take effect.

System > IPv6 System Settings

The IPv6 System Settings page allow user to configure the IPv6 system information.



IPv6 System Settings

Safeguard

IPv6 System Settings

Interface Name: System

IPv6 State: Enabled

DHCPv6 Client: Disabled

IPv6 Network Address (e.g.: 3710::1/64):

Apply

NS Retransmit Time Settings

NS Retransmit Time (1-3600): 1 s

Apply

Automatic Link Local State Settings

Automatic Link Local Address: Disabled

Apply

View All IPv6 Address

IPv6 Type	IPv6 Address

.

Figure 4.15 – System > IPv6 System Settings

IPv6 System Settings:

Interface Name: Displays the interface name of IPv6.

IPv6 State: Specifies the IPv6 to be enabled or disabled.

DHCPv6 Client: Specifies the DHCPv6 client to be enabled or disabled.

IPv6 Network Address: Specifies the IPv6 Network Address.

NS Retransmit Time Settings:

NS Retransmit Time (1-3600): Enter the Neighbor solicitation's retransmit timer in second here. Specifies the NS retransmit time for IPv6. The field range is 1-3600, and default is 1 second.

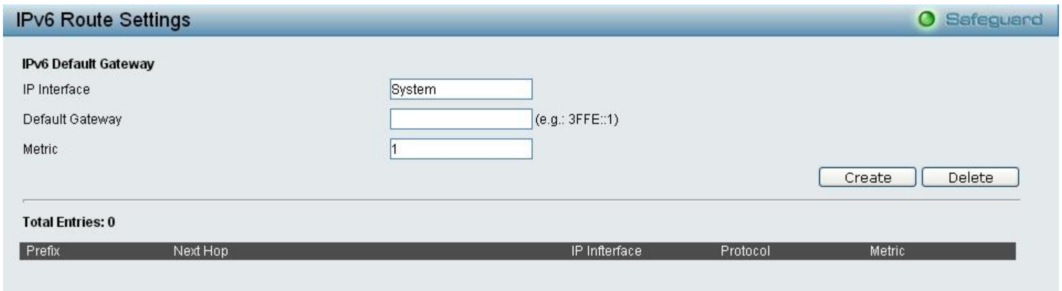
Automatic Link Local State Settings:

Automatic Link Local Address: Specifies the automatic link is enabled or disabled.

Click **Apply** for the settings to take effect.

System > IPv6 Route Settings

The IPv6 Route Settings page allows user to configure the IPv6 route settings.



IPv6 Route Settings

Safeguard

IPv6 Default Gateway

IP Interface: System

Default Gateway: (e.g.: 3FFE::1)

Metric: 1

Create Delete

Total Entries: 0

Prefix	Next Hop	IP Interface	Protocol	Metric

Figure 4.16 – System > IPv6 Route Settings

IP Interface: Specify the IP interface which to be created.

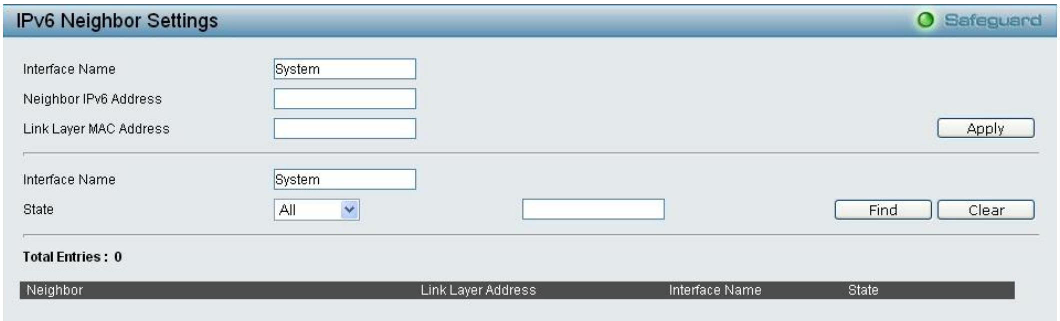
Default Gateway: The corresponding IPv6 address for the next hop Gateway address in IPv6 format..

Metric: Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.

Click **Create** to accept the changes made, and click the **Delete** button to remove the entry.

System > IPv6 Neighbor Settings

The user can configure the Switch’s IPv6 neighbor settings. The Switch’s current IPv6 neighbor settings will be displayed in the table at the bottom of this window.



Interface Name: System
Neighbor IPv6 Address:
Link Layer MAC Address:

Interface Name: System
State: All

Total Entries : 0

Neighbor	Link Layer Address	Interface Name	State

Figure 4.17 – System > IPv6 Neighbor Settings

Interface Name: Enter the interface name of the IPv6 neighbor.

Neighbor IPv6 Address: Specifies the neighbor IPv6 address.

Link Layer MAC Address: Specifies the link layer MAC address.

Click **Apply** for the settings to take effect.

Interface Name: Specifies the interface name of the IPv6 neighbor. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window, tick the All check box. Tick the Hardware option to display all the neighbor cache entries which were written into the hardware table.

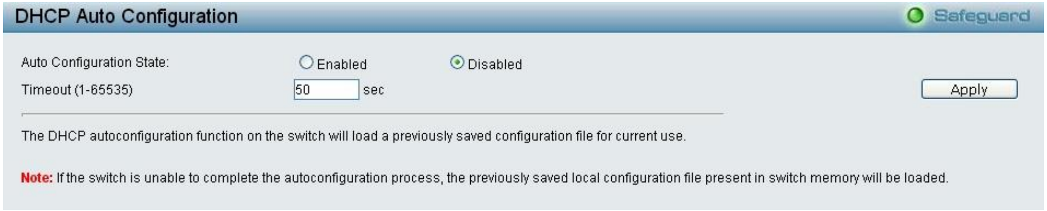
State: Use the drop-down menu to select All, Address, Static or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

Click **Find** to locate a specific entry based on the information entered.

Click **Clear** to clear all the information entered in the fields.

System > DHCP Auto Configuration

This page allows you to enable the DHCP Auto Configuration feature on the Switch. When enabled, the Switch becomes a DHCP client and gets the configuration file from a TFTP server automatically on next boot up. To accomplish this, the DHCP server must deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and store the necessary configuration file in its base directory when the request is received from the Switch.



Auto Configuration State: ○ Enabled ● Disabled
Timeout (1-65535) 50 sec

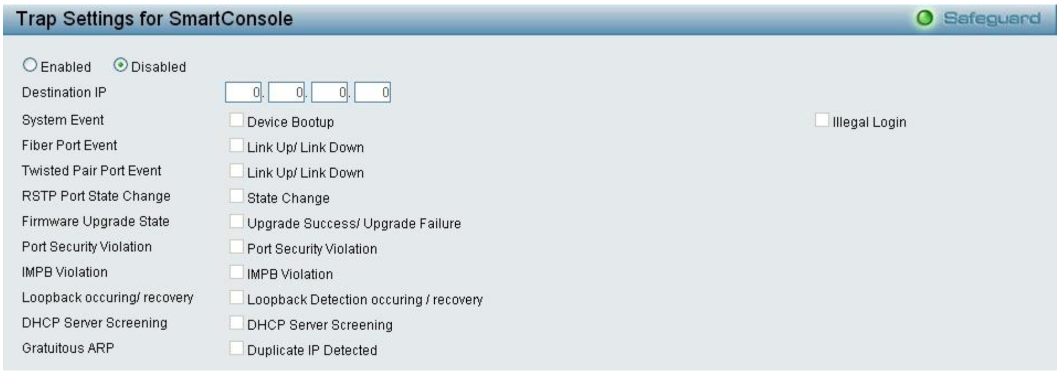
The DHCP autoconfiguration function on the switch will load a previously saved configuration file for current use.

Note: If the switch is unable to complete the autoconfiguration process, the previously saved local configuration file present in switch memory will be loaded.

Figure 4.18 – System > DHCP Auto Configuration

System > Trap Settings

The Trap Settings page allows user the set the difference status of SNMP notifications trapped to the Smartconsole. By default, Trap Setting is disabled.



Trap Settings for SmartConsole

○ Enabled ● Disabled

Destination IP	0 . 0 . 0 . 0	
System Event	□ Device Bootup	□ Illegal Login
Fiber Port Event	□ Link Up/ Link Down	
Twisted Pair Port Event	□ Link Up/ Link Down	
RSTP Port State Change	□ State Change	
Firmware Upgrade State	□ Upgrade Success/ Upgrade Failure	
Port Security Violation	□ Port Security Violation	
IMPB Violation	□ IMPB Violation	
Loopback occuring/ recovery	□ Loopback Detection occuring / recovery	
DHCP Server Screening	□ DHCP Server Screening	
Gratuitous ARP	□ Duplicate IP Detected	

Figure 4.19 – System > Trap Settings

You can select which event message(s) to be sent to the managing station.

Destination IP: Specifies the destination IP.

System Event: Specifies the device to send bootup notifications.

Fiber Port Event: Events when fiber port connection port link up / link down.

Twisted Pair Port Event: Events when pair port connection port link up / link down.

RSTP Port State Change: Events of a RSTP port state changes.

Firmware Upgrade State: Information of firmware upgrade - success or failure.

Port Security Violation: Events of port security violation.

IMPB Violation: Specifies the device to send notifications when IMPB violation detected.

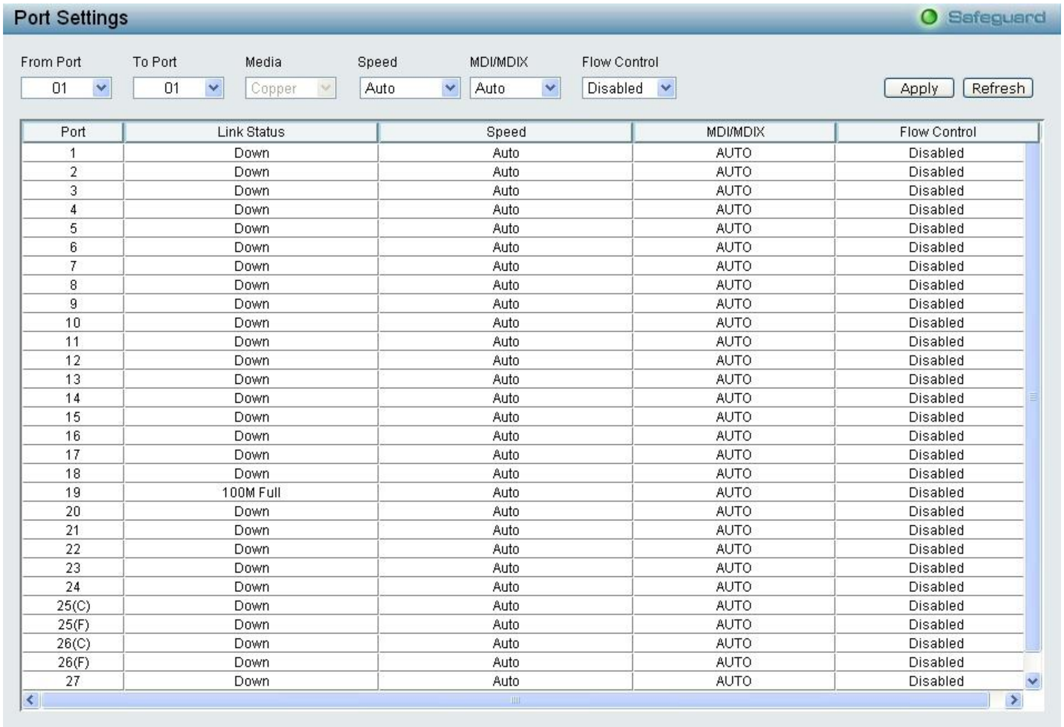
Loopback occurring/recovery: Specifies the device to send notifications when loopback occurring / recovery.

DHCP Server Screening: Specifies the device to send notifications when DHCP server screening.

Gratuitious ARP: Specifies the device to send notifications when duplicate IP were detected.

System > Port Configuration > Port Settings

In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports (**From Port** and **To Port**), the **Speed** can be set for all selected ports by clicking **Apply**. Press the **Refresh** button to view the latest information.



Port Settings

From Port	To Port	Media	Speed	MDI/MDIX	Flow Control
01	01	Copper	Auto	Auto	Disabled

Port	Link Status	Speed	MDI/MDIX	Flow Control
1	Down	Auto	AUTO	Disabled
2	Down	Auto	AUTO	Disabled
3	Down	Auto	AUTO	Disabled
4	Down	Auto	AUTO	Disabled
5	Down	Auto	AUTO	Disabled
6	Down	Auto	AUTO	Disabled
7	Down	Auto	AUTO	Disabled
8	Down	Auto	AUTO	Disabled
9	Down	Auto	AUTO	Disabled
10	Down	Auto	AUTO	Disabled
11	Down	Auto	AUTO	Disabled
12	Down	Auto	AUTO	Disabled
13	Down	Auto	AUTO	Disabled
14	Down	Auto	AUTO	Disabled
15	Down	Auto	AUTO	Disabled
16	Down	Auto	AUTO	Disabled
17	Down	Auto	AUTO	Disabled
18	Down	Auto	AUTO	Disabled
19	100M Full	Auto	AUTO	Disabled
20	Down	Auto	AUTO	Disabled
21	Down	Auto	AUTO	Disabled
22	Down	Auto	AUTO	Disabled
23	Down	Auto	AUTO	Disabled
24	Down	Auto	AUTO	Disabled
25(C)	Down	Auto	AUTO	Disabled
25(F)	Down	Auto	AUTO	Disabled
26(C)	Down	Auto	AUTO	Disabled
26(F)	Down	Auto	AUTO	Disabled
27	Down	Auto	AUTO	Disabled

Figure 4.20 – System > Port Configuration > Port Settings

Media: When port number is 25 or 26. Select the Media is *Copper, Fiber_1G or Fiber_100*.

Speed: Gigabit Fiber connections can operate in 1000M Full Force Mode, Auto Mode or Disabled. Copper connections can operate in Forced Mode settings (1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto, or Disabled. 100M Fiber connections support 100M Full Force Mode, 100M Half Force Mode, or Disabled. The default setting for all ports is **Auto**.

NOTE: Be sure to adjust port speed settings appropriately after changing the connected cable media types.

MDI/MDIX:

A **medium dependent interface** (**MDI**) port is an Ethernet port connection typically used on the Network Interface Card (NIC) or Integrated NIC port on a PC. Switches and hubs usually use **Medium dependent interface crossover (MDIX)** interface. When connecting the Switch to end stations, user have to use straight through Ethernet cables to make sure the Tx/Rx pairs match up properly. When connecting the Switch to other networking devices, a crossover cable must be used.

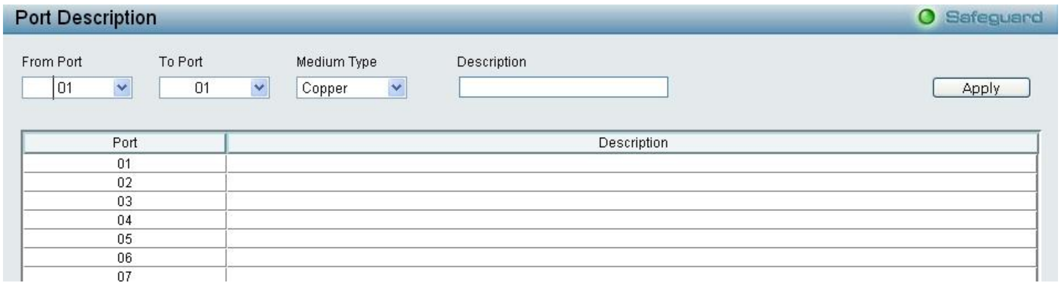
This switch provides a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

Auto is designed on the switch to detect if the connection is backwards, and automatically chooses MDI or MDIX to properly match the connection. The default setting is "**Auto" MDI/MDIX**.

Flow Control: You can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control. The default setting is Disabled.

System > Port Configuration > Port Description

In the Port Description page, the user may name various ports on the Switch.



Port Description

From Port: 01

To Port: 01

Medium Type: Copper

Description:

Port	Description
01	
02	
03	
04	
05	
06	
07	

Figure 4.21 – System > Port Configuration > Port Description

From Port / To Port: Specify the range of ports to describe.

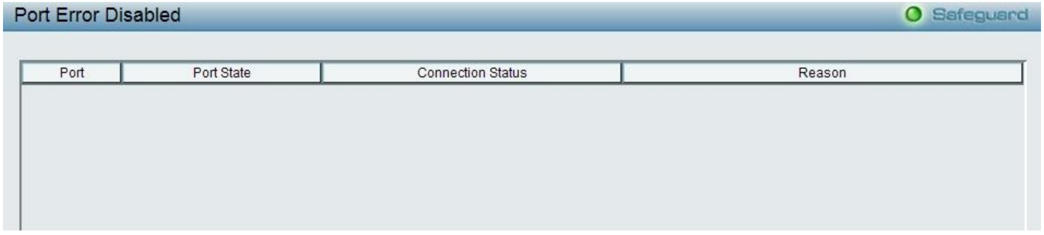
Medium Type: When port number is 25 or 26. Select the **Medium Type** is *Copper, Fiber_1G or Fiber_100*.

Description: Specify the description of ports.

Click **Apply** to set the description in the table.

System > Port Configuration > Port Error Disabled

The Port Error Disabled page displays the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status.



Port Error Disabled

Port	Port State	Connection Status	Reason

Figure 4.22 – System > Port Configuration > Port Error Disabled

Port: Displays the port that has been error disabled.

Port State: Describes the current running state of the port, whether Enabled or Disabled.

Connection Status: This field will read the uplink status of the individual ports, whether Enabled or Disabled.

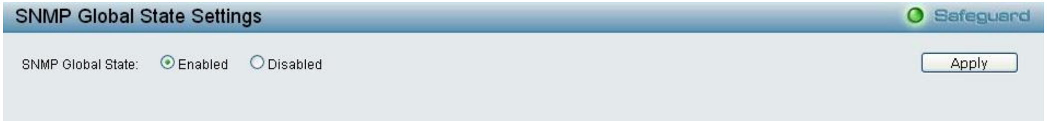
Reason: Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

System > SNMP Settings > SNMP Global State

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch or LAN.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The default SNMP global state is disabled. Select Enable and click **Apply** to enable the SNMP function.



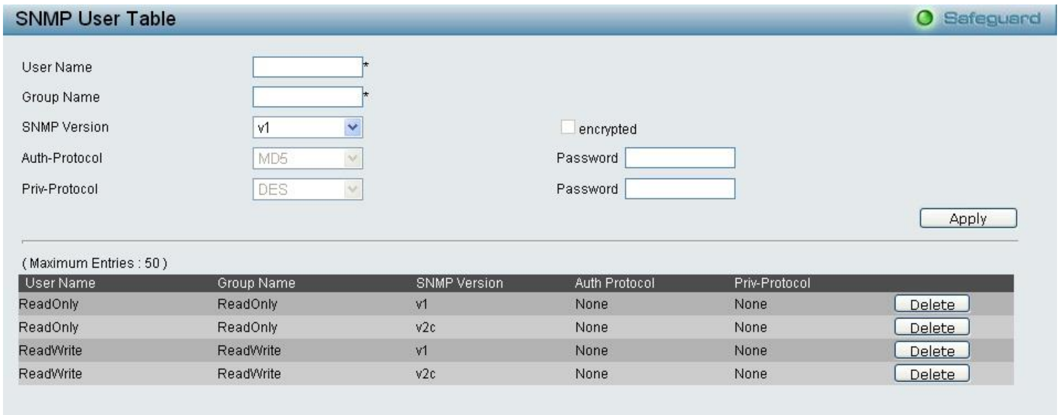
SNMP Global State Settings

SNMP Global State: ● Enabled ○ Disabled

Figure 4.23 – System > SNMP Settings > SNMP Global State

System > SNMP Settings > SNMP User Table

This page is used to maintain the SNMP user table for the use of SNMPv3. SNMPv3 allows or restricts users using the MIB OID, and also encrypts the SNMP messages sent out between users and Switch.



SNMP User Table

User Name *

Group Name *

SNMP Version: v1 □ encrypted

Auth-Protocol: MD5 Password

Priv-Protocol: DES Password

(Maximum Entries : 50)

User Name	Group Name	SNMP Version	Auth Protocol	Priv-Protocol	
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 4.24 – System > SNMP Settings > SNMP User Table

User Name: Enter a SNMP user name of up to 32 characters.

Group Name: Specify the SNMP group of the SNMP user.

SNMP Version: Specify the SNMP version of the user. Only SNMPv3 encrypts the messages.

Encrypt: Specifies the Encrypt is enabled or disabled when the SNMP Version is V3.

Auth-Protocol/Password: Specify either HMAC-MD5-96 or HMAC-SHA to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column.

Priv-Protocol/Password: Specify either **no authorization** or **DES 56-bit encryption** and then enter a password for SNMPv3 encryption in the right column.

Click **Apply** to create a new SNMP user account, and click **Delete** to remove any existing data.

System > SNMP Settings > SNMP Group Table

This page is used to maintain the SNMP Group Table associating to the users in SNMP User Table. SNMPv3 can control MIB access policy, security policy for a user group directly.

Group Name: Specify the SNMP user group of up to 32 characters.

Read View Name: Specify a SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.

Write View Name: Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.

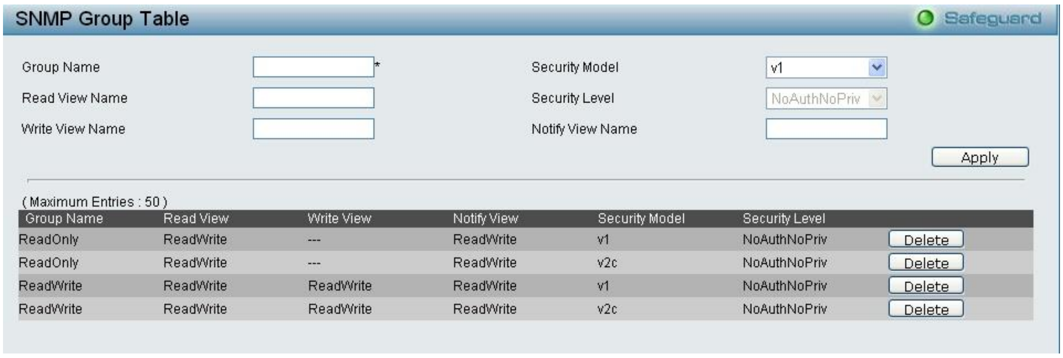
Security Model: Select the SNMP security model.

> **SNMPv1 -** SNMPv1 does not support the security features.
>
> **SNMPv2 -** SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.
>
> **SNMPv3 -** SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.

Security Level: This function is only available when you select SNMPv3 security level.

> **NoAuthNoPriv -** No authorization and no encryption for packets sent between the Switch and SNMP manager.
>
> **AuthNoPriv -** Authorization is required, but no encryption for packets sent between the Switch and SNMP manager.
>
> **AuthPriv –** Both authorization and encryption are required for packets sent between the Switch and SNMP manger.

Notify View Name: Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.



SNMP Group Table

Group Name	*	Security Model	v1
Read View Name		Security Level	NoAuthNoPriv
Write View Name		Notify View Name	

Apply

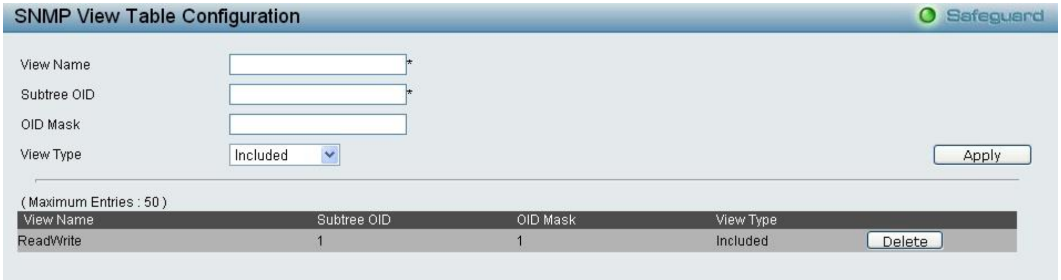
(Maximum Entries : 50)

Group Name	Read View	Write View	Notify View	Security Model	Security Level	
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	Delete

Figure 4.25– System > SNMP Settings > SNMP Group Table

System > SNMP Settings > SNMP View Table

This page allows you to maintain SNMP views to community strings that define the MIB objects which can be accessed by a remote SNMP manager.



SNMP View Table Configuration

View Name	*
Subtree OID	*
OID Mask	
View Type	Included

Apply

(Maximum Entries : 50)

View Name	Subtree OID	OID Mask	View Type	
ReadWrite	1	1	Included	Delete

Figure 4.26 – System > SNMP Settings > SNMP View Table

View Name: Name of the view, up to 32 characters.

Subtree OID: The Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.

OID Mask: The mask of the Subtree OID. 1 means this object number is concerned, 0 means do not concerned. For example 1.3.6.1.2.1.1 with mask 1.1.1.1.1.1.0 means 1.3.6.1.2.1.X.

View Type: Specify the configured OID is Included or Excluded that a SNMP manager can access.

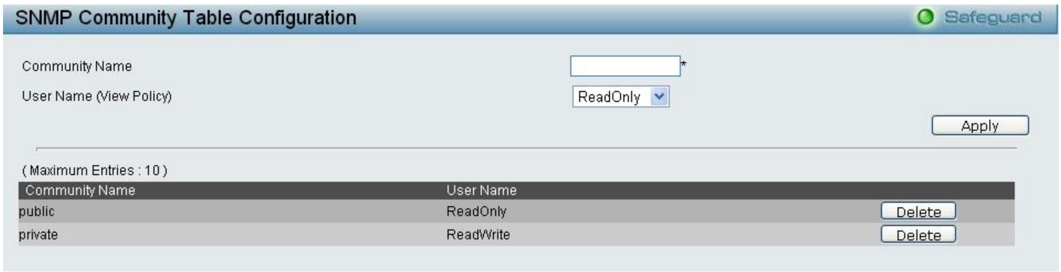
Click **Apply** to create a new view, **Delete** to remove an existing view.

System > SNMP Settings > SNMP Community Table

This page is used to maintain the SNMP community string of the. SNMP managers using the same community string are permitted to gain access to the Switch's SNMP agent.

Community Name: Name of the community string

User Name (View Policy): Specify the read/write or read-only level permission for the MIB objects accessible to the SNMP community.



SNMP Community Table Configuration

Community Name *

User Name (View Policy) ReadOnly

(Maximum Entries : 10)

Community Name	User Name	
public	ReadOnly	Delete
private	ReadWrite	Delete

Figure 4.27 – System > SNMP Settings > SNMP Community Table

Click **Apply** to create a new SNMP community, **Delete** to remove an existing community.

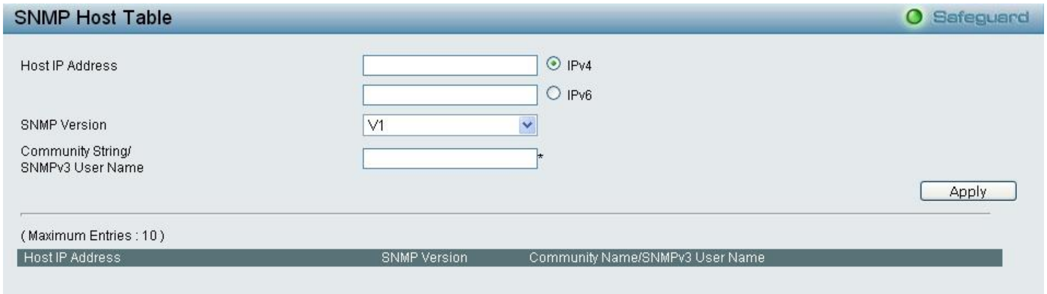
System > SNMP Settings > SNMP Host Table

This page is to configure the SNMP trap recipients.

Host IP Address: Select IPv4 or IPv6 and specify the IP address of SNMP management host.

SNMP Version: Specify the SNMP version to be used to the management host.

Community String/SNMPv3 User Name: Specify the community string or SNMPv3 user name for the management host.



SNMP Host Table

Host IP Address ● IPv4

○ IPv6

SNMP Version V1

Community String/ SNMPv3 User Name *

(Maximum Entries : 10)

Host IP Address	SNMP Version	Community Name/SNMPv3 User Name

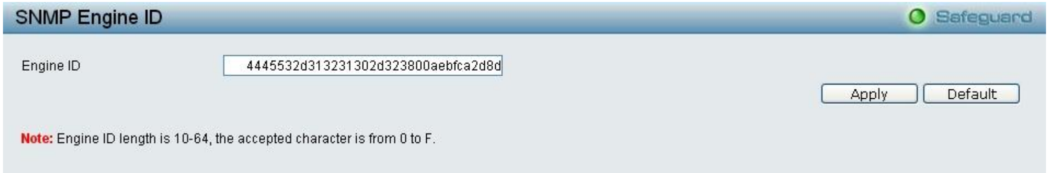
Figure 4.28– System > SNMP Settings > SNMP Host Table

Click **Apply** to create a new SNMP host, **Delete** to remove an existing host.

System > SNMP Settings > SNMP Engine ID

The Engine ID is a unique identifier used to identify the SNMPv3 engine on the Switch.

Input the Engine ID then click **Apply** to apply the changes and click **Default** resets to default value.



SNMP Engine ID

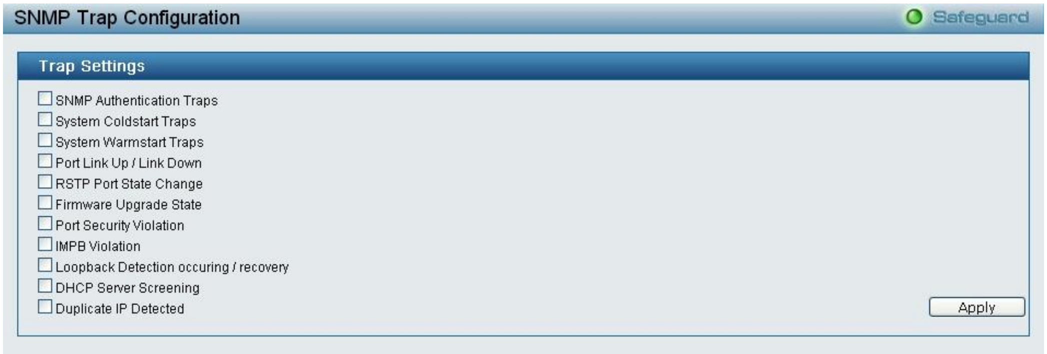
Engine ID 4445532d313231302d323800aebfca2d8d

Note: Engine ID length is 10-64, the accepted character is from 0 to F.

Figure 4.29 – System > SNMP Settings > SNMP Engine ID

System > SNMP Settings > SNMP Trap Settings

The SNMP Trap Settings page provide user to Specify whether the device can send SNMP notifications.



SNMP Trap Configuration

Trap Settings

□ SNMP Authentication Traps
□ System Coldstart Traps
□ System Warmstart Traps
□ Port Link Up / Link Down
□ RSTP Port State Change
□ Firmware Upgrade State
□ Port Security Violation
□ IMPB Violation
□ Loopback Detection occuring / recovery
□ DHCP Server Screening
□ Duplicate IP Detected

Figure 4.30 – System > SNMP Settings > SNMP Trap Settings

SNMP Authentication Traps: Specifies the device to send authentication failure notifications.

System Device Bootup: System boot-up information.

Fiber Port Link Up / Link Down: Fiber port connection information.

Twisted Pair Port Link Up / Link Down: Twisted pair port connection information.

RSTP Port State Change: Events of a RSTP port state changes.

Firmware Upgrade State: Information of firmware upgrade - success or failure.

Port Security Violation: Information of Port Security Violation.

IMPB Violation: IMPB Violation information.

Loopback Detection occurring / recovery: Specify the device to send SNMP Trap when Loopback Detection occurring and recovery.

DHCP Server Screening: Information of DHCP Server Screening.

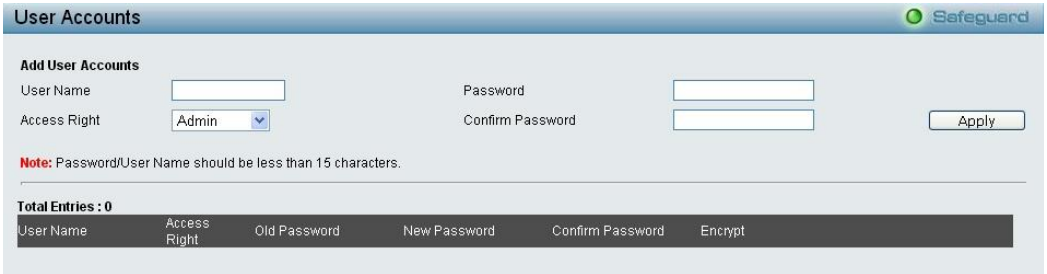
Duplicate IP Detected: Information of Duplicate IP Detected.

Click **Apply** for the changes to take effect.

System > User Accounts

The **User Accounts** page provides user to control user privileges. To add a new user by typing in a **User Name**, **Password** and retype the same password in the **Confirm Password** and choose the level of privilege(*Admin*, *Operator* or *User*) from the **Access Right** drop-down menu, then click the **Apply** button.

User can modify existing user account in the User Account Table. To change the password, type in the **Old Password**, **New Password** and retype it in the Confirm New Password entry field and select the Encrypt, then click the **Edit** button. To delete the user account, click on the **Delete** button.



User Accounts

Add User Accounts

User Name: ___ Password: ___

Access Right: Admin Confirm Password: ___

Note: Password/User Name should be less than 15 characters.

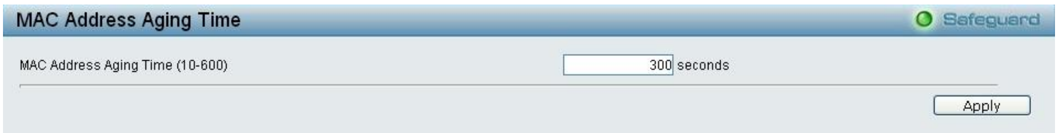
Total Entries : 0

User Name	Access Right	Old Password	New Password	Confirm Password	Encrypt

Figure 4.31– System > User Accounts

System > MAC Address Aging Time

The MAC Address Aging Time page specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC address is allowed to remain idle). To change this, type in a different value representing the MAC address age-out time in seconds.



MAC Address Aging Time

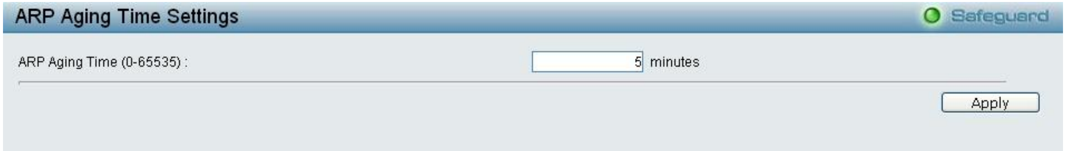
MAC Address Aging Time (10-600) 300 seconds

Figure 4.32 – System > MAC Address Aging Time

MAC Address Aging Time (10-600): Specifies the aging time of MAC address on the Switch. The range is from 10 to 600, and the default is 300 seconds.

System > ARP Aging Time Settings

The ARP Aging Time Settings page provides user to globally set the maximum amount of time, in minutes, and Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.



ARP Aging Time Settings

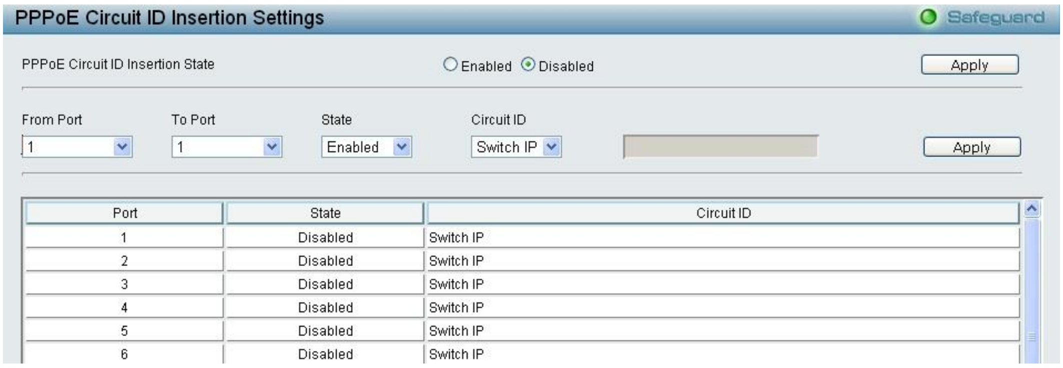
ARP Aging Time (0-65535) : 5 minutes

Figure 4.33 – System > ARP Aging Time Settings

ARP Aging Time (0-65535): Specifies the ARP aging time on the Switch. The range is from 0 to 65535 with a default setting of 5 minutes.

System > PPPoE Circuit ID Insertion Settings

The PPPoE Circuit ID Insertion Settings page specifies the configuration of settings. When enabled, the system will insert the circuit tag to the received PPPoE discover request and the request packet if the tag is absent. It will remove the circuit ID tag from the received PPPoE offer and session confirmation packet.



PPPoE Circuit ID Insertion Settings

PPPoE Circuit ID Insertion State ○ Enabled ● Disabled

From Port: 1 To Port: 1 State: Enabled Circuit ID: Switch IP

Port	State	Circuit ID
1	Disabled	Switch IP
2	Disabled	Switch IP
3	Disabled	Switch IP
4	Disabled	Switch IP
5	Disabled	Switch IP
6	Disabled	Switch IP

Figure 4.34 – System > PPPoE Circuit ID Insertion Settings

PPPoE Circuit Insertion State: Enable or disable the PPPoE circuit insertion state, and click Apply to take effect.

From Port/ To Port: Specifies the ports to be configured.

State: Enable or disable the state of specified ports.

Circuit ID: Specifies the Circuit ID is **Switch IP**, **Switch MAC** or **UDF String**.

Switch IP – The Switch's IP address will be used to encode the circuit ID option. This is the default.

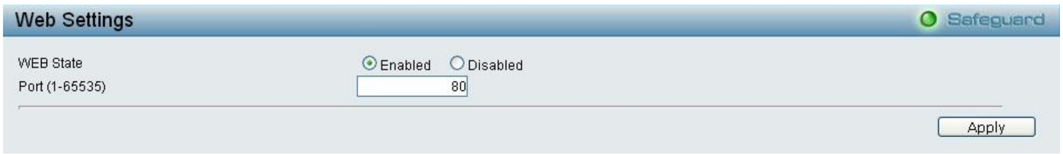
Switch MAC – The MAC address of the Switch will be used to encode the circuit ID option.

UDF String – A user specified string to be used to encode the circuit ID option. Enter a string with the maximum length of 32.

Click the **Apply** button to take effects.

System > Web Settings

The WEB State is **Enabled** by default. If user choose to disable this by selecting Disabled, user will lose the ability to configure the system through the web interface as soon as these settings are applied.



Web Settings

WEB State ● Enabled ○ Disabled

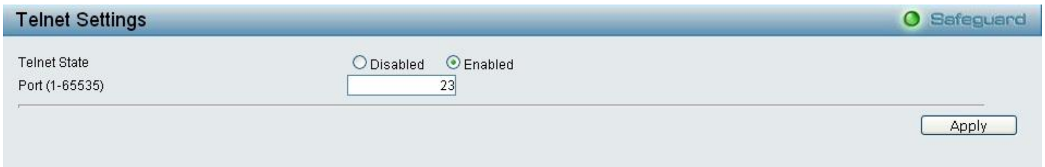
Port (1-65535) 80

Figure 4.35– System > Web Settings

Port (1-65535): Specifies the Port number. The range is between 1 and 65535 with the well-known default is 80.

System > Telnet Settings

Telnet configuration is **Enabled** by default. If user does not want to allow the Telnet configuration, they only need to disable the Telnet State.



Telnet Settings

Telnet State ○ Disabled ● Enabled

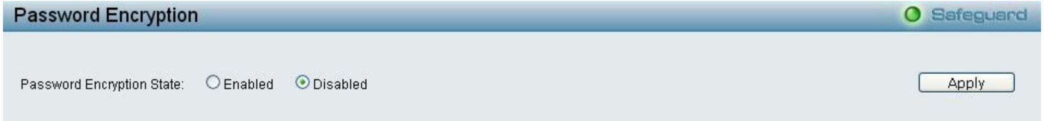
Port (1-65535) 23

Figure 4.36 – System > Telnet Settings

Port (1-65535): The TCP port number. TCP ports are numbered between 1 and 65535. The well-known TCP port for the Telnet protocol is 23.

System > Password Encryption

The Password Encryption page is used to enable or disable the password encryption state. Select **Enabled** and click **Apply** to make effect.



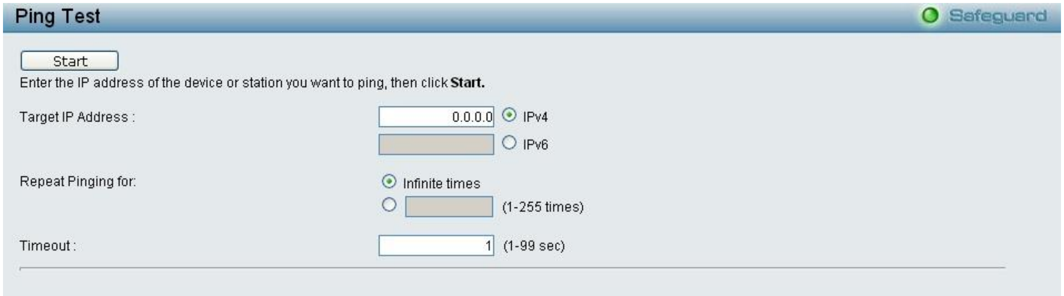
Password Encryption

Password Encryption State: ○ Enabled ● Disabled

Figure 4.37 – System > Password Encryption

System > Ping Test

The Ping Test is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.



Ping Test

Enter the IP address of the device or station you want to ping, then click **Start.**

Target IP Address : 0.0.0.0 ● IPv4 ○ IPv6

Repeat Pinging for: ● Infinite times ○ (1-255 times)

Timeout : 1 (1-99 sec)

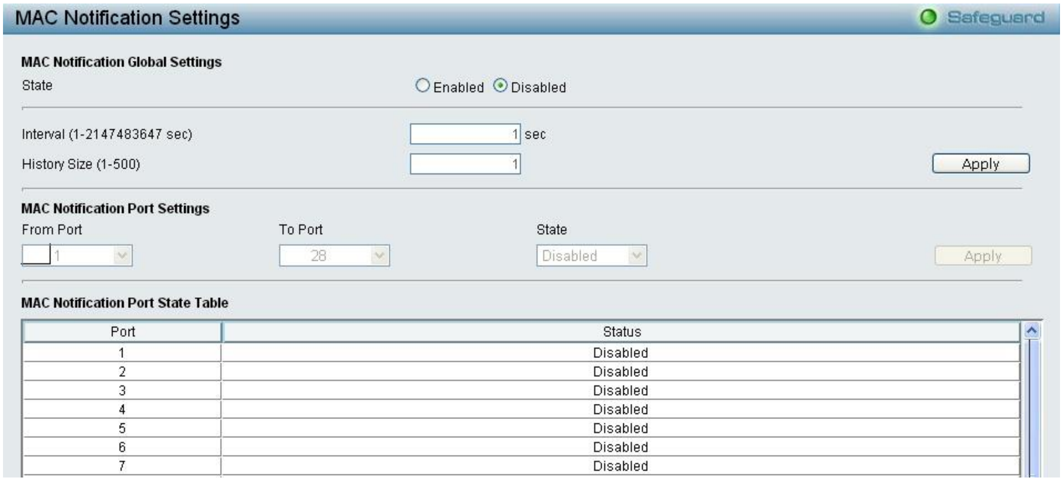
Figure 4.38 – System > Ping Test

The user may use Infinite times radio button, in the **Repeat Pinging for** field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the **Target IPv4 or IPv6 Address** by clicking its radio button and entering a number between *1* and *255*. Click **Start** to initiate the Ping Program

Timeout: Specify the timeout time of Ping test. The range is between 1 and 99 seconds.

System > MAC Notification Settings

MAC Notification page is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, user should enabled or disabled state, input the Time **Interval** between notification and **History Size** then click the **Apply** button.



MAC Notification Settings

MAC Notification Global Settings

State ○ Enabled ● Disabled

Interval (1-2147483647 sec) 1 sec

History Size (1-500) 1

MAC Notification Port Settings

From Port 1 To Port 28 State Disabled

MAC Notification Port State Table

Port	Status
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled

Figure 4.39 – System > MAC Notification Settings

State: Enabled or Disabled MAC notification globally on the Switch.

Interval (1-2147483647 sec): The time in seconds between notifications.

History Size (1-500): The maximum number of entries listed in the history log used for notification. Up to *500* entries can be specified.

Click **Apply** for the changes to take effect.

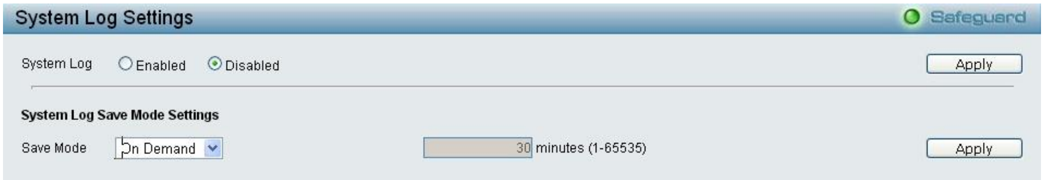
To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters. , then click the **Apply** button.

From Port / To Port: Select a port or group of ports to enable for MAC notification using the pull-down menus.

State: Enable MAC Notification for the ports selected using the pull-down menu.

System > System Log Configuration > System Log Settings

System Logs record and manage events, as well as report errors and informational messages. Message severity determines a set of event message will be sent. Click **Enable** so you can start to configure the related settings of remote system log server, then press **Apply** for the changes to take effect.



System Log Settings

System Log ○ Enabled ● Disabled

System Log Save Mode Settings

Save Mode On Demand 30 minutes (1-65535)

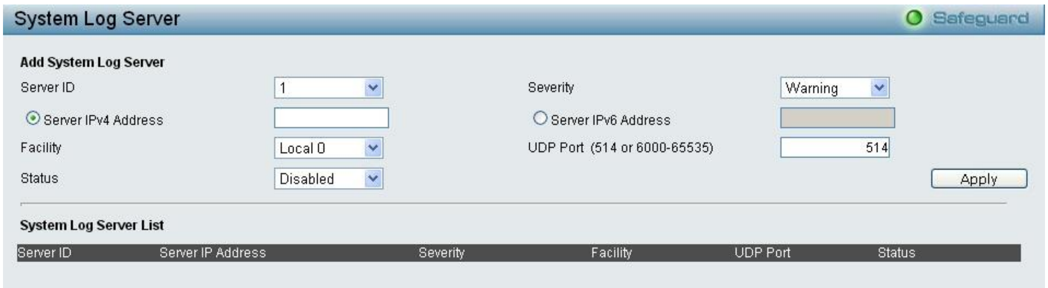
Figure 4.40 – System > System Log Configuration > System Log Settings

Save Mode: Use this drop-down menu to choose the method that will trigger a log entry. You can choose between **On Demand**, **Time Interaval** and **Log Trigger.**

Minutes: Enter a time intervel, in minutes, for which user would like a log entry to be made.

System > System Log Configuration > System Log Server

The user can send Syslog messages to up to four designated servers using the **System Log Server**. It supports maximum 500 system log entries. To set the System Log Server configuration, click **Apply**.



System Log Server — Safeguard

Add System Log Server

Server ID	1	Severity	Warning
● Server IPv4 Address		○ Server IPv6 Address	
Facility	Local 0	UDP Port (514 or 6000-65535)	514
Status	Disabled		Apply

System Log Server List

Server ID	Server IP Address	Severity	Facility	UDP Port	Status

Figure 4.41 - System > System Log Configuration > System Log Server

Server ID: Specifies the Server ID. The field range is 1-4.

Severity: Specifies the minimum severity from which warning messages are sent to the server. There are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are:

> **Warning -** The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
>
> **Informational -** Provides device information.
>
> **All -** Displays all levels of system logs.

Server IPv4 Address: Specifies the IPv4 address of the system log server.

Server IPv6 Address: Specifies the IPv6 address of the system log server.

Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7).

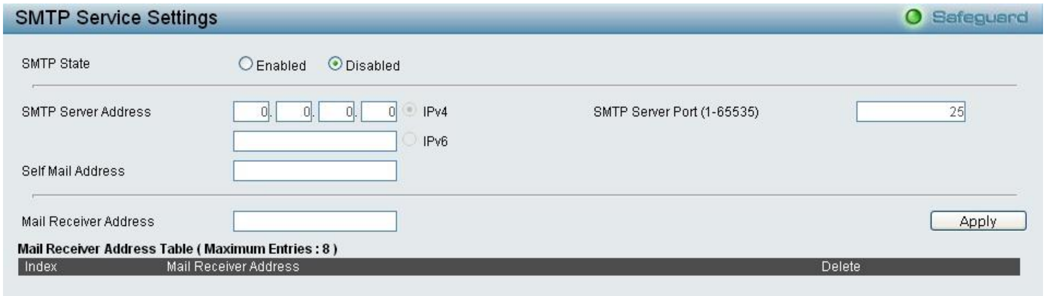
UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is *6000 – 65535*, and the default value is *514*.

Status: Specifies the status is enable or disable.

System > SMTP Service > SMTP Server Settings

The SMTP Service Settings page is used to configure the fields to set up the SMTP server for the switch, along with setting e-mail addresses to which switch log file can be sent when a problem arises on the Switch.

User can **Enabled** or **Disabled** the SMTP State, then input the **SMTP Server Address**, **SMTP Server Port**, **Self Mail Address** and **Mail Receiver Address** then click **Apply** button to configure.



SMTP Service Settings — Safeguard

SMTP State ○ Enabled ● Disabled

SMTP Server Address 0. 0. 0. 0 ● IPv4 ○ IPv6 — SMTP Server Port (1-65535) 25

Self Mail Address

Mail Receiver Address — Apply

Mail Receiver Address Table (Maximum Entries : 8)

Index	Mail Receiver Address	Delete

Figure 4.42 - System > SMTP Service > SMTP Server Settings

SMTP State: Enabled or Disabled the SMTP service on this device.

SMTP Server Address: Select IPv4 or IPv6 and enter the IP address of the SMTP server on a remote device. This will be the device that sends out the mail for user.

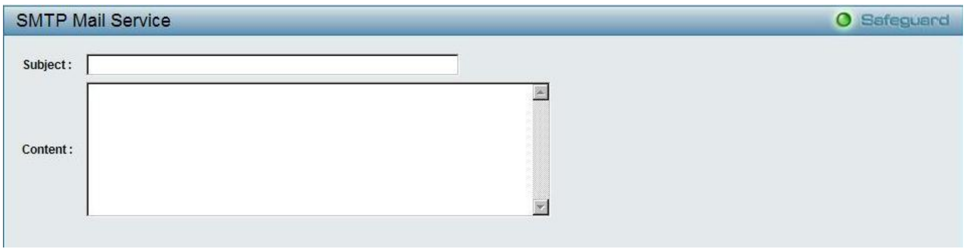
SMTP Server Port: Enter the virtual port number that the Switch will connect with on the SMTP server. The common port number for SMTP is *25*, yet a value between *1* and *65535* can be chosen.

Self Mail Address: Enter the e-mail address from which mail messages will be sent. This address will be the "from" address on the e-mail message sent to a recipient. Only one self mail address can be configured for this Switch. This string can be no more that *64* alphanumeric characters.

Mail Receiver Address: Enter a list of e-mail addresses so recipients can receive e-mail messages regarding Switch functions. Up to 8 e-mail addresses can be added per Switch. Do delete these addresses from the Switch, click **Delete** button from the Mail Receiver Address Table.

System > SMTP Service > SMTP Service

The SMTP Service is used to send test messages to all mail recipients configured on the Switch, thus testing the configurations set and the reliability of the SMTP server.



SMTP Mail Service

Subject :

Content :

Figure 4.43 - System > SMTP Service > SMTP Service

Subject: Enter the subject of the test e-mail.

Content: Enter the content of the test e-mail.

Once the message is ready, click **Send** to send this mail to all recipients configured on the Switch for SMTP.

Configuration > 802.1Q VLAN

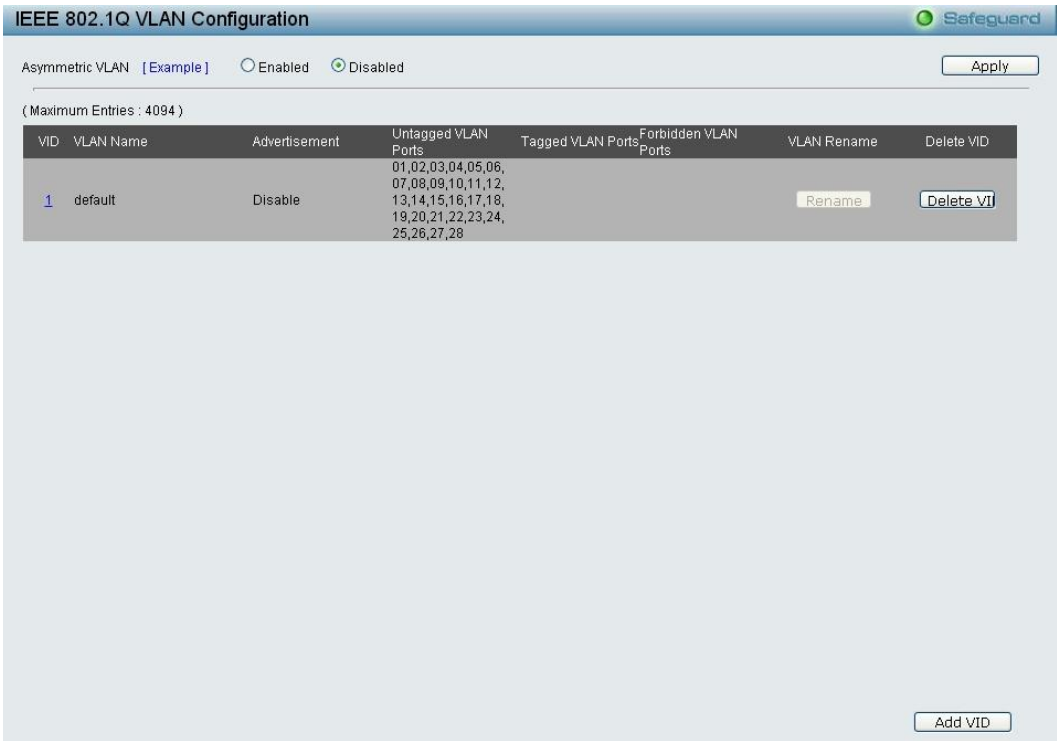
A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 1, no default name, and all ports as "Untagged"

Rename: Click to rename the VLAN group.

Delete VID: Click to delete the VLAN group.



IEEE 802.1Q VLAN Configuration

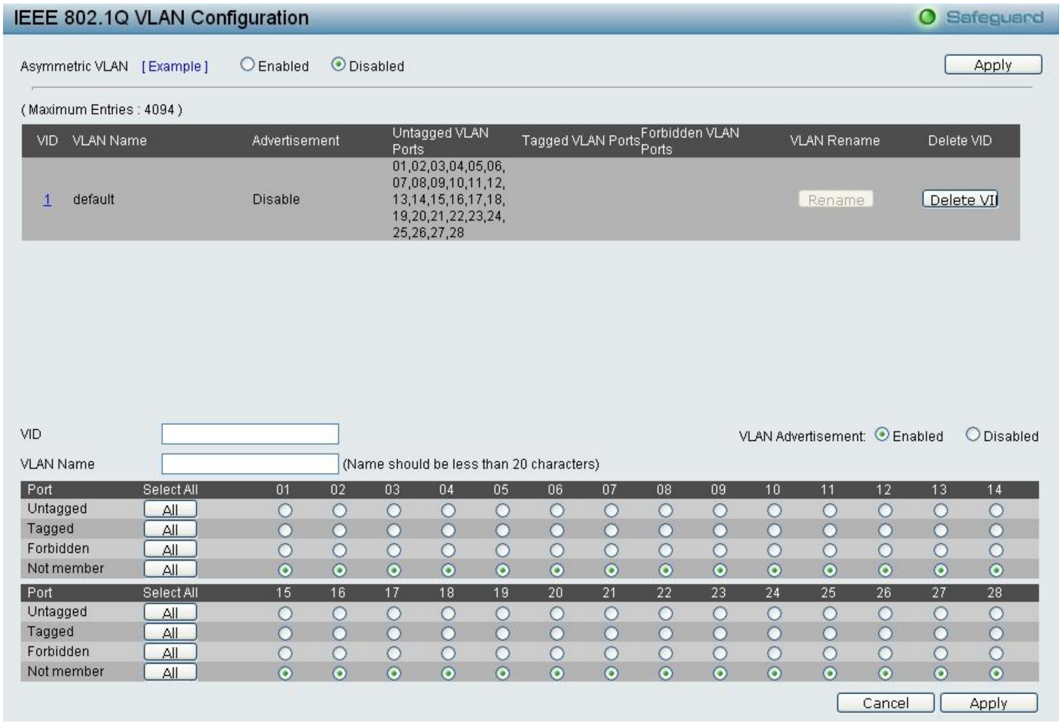
Asymmetric VLAN ○ Enabled ● Disabled

(Maximum Entries : 4094)

VID	VLAN Name	Advertisement	Untagged VLAN Ports	Tagged VLAN Ports	Forbidden VLAN Ports	VLAN Rename	Delete VID
1	default	Disable	01,02,03,04,05,06, 07,08,09,10,11,12, 13,14,15,16,17,18, 19,20,21,22,23,24, 25,26,27,28			Rename	Delete VI

Figure 4.44 – Configuration > 802.1Q VLAN

Click **Add VID** to create a new VID group, assigning ports from 01 to 10 as **Untag**, **Tag**, **Forbidden** or **Not Member**. Enable or disable the **VLAN Advertisement**. A port can be untagged in only one VID. To save the VID group, click **Apply.**



IEEE 802.1Q VLAN Configuration

Asymmetric VLAN [Example] ○ Enabled ● Disabled [Apply]

(Maximum Entries : 4094)

VID	VLAN Name	Advertisement	Untagged VLAN Ports	Tagged VLAN Ports	Forbidden VLAN Ports	VLAN Rename	Delete VID
1	default	Disable	01,02,03,04,05,06, 07,08,09,10,11,12, 13,14,15,16,17,18, 19,20,21,22,23,24, 25,26,27,28			Rename	Delete VI

VID [ ] VLAN Advertisement: ● Enabled ○ Disabled

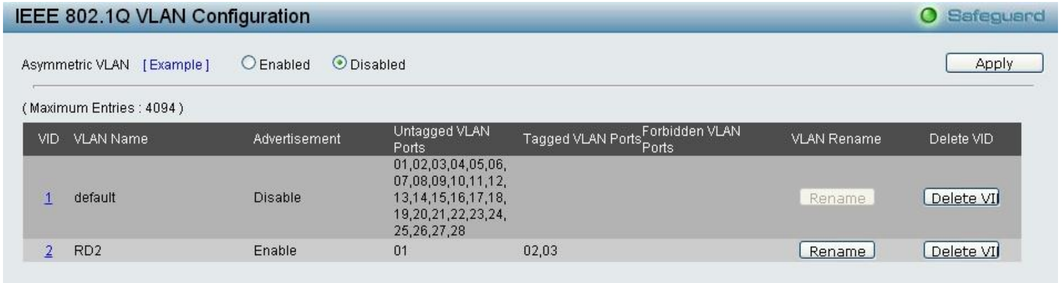
VLAN Name [ ] (Name should be less than 20 characters)

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Figure 4.45 – Configuration > 802.1Q VLAN > Add VLAN

After click **Apply**, the 802.1Q VLAN Configuration Table will displayed with updates.



IEEE 802.1Q VLAN Configuration

Asymmetric VLAN [Example] ○ Enabled ● Disabled [Apply]

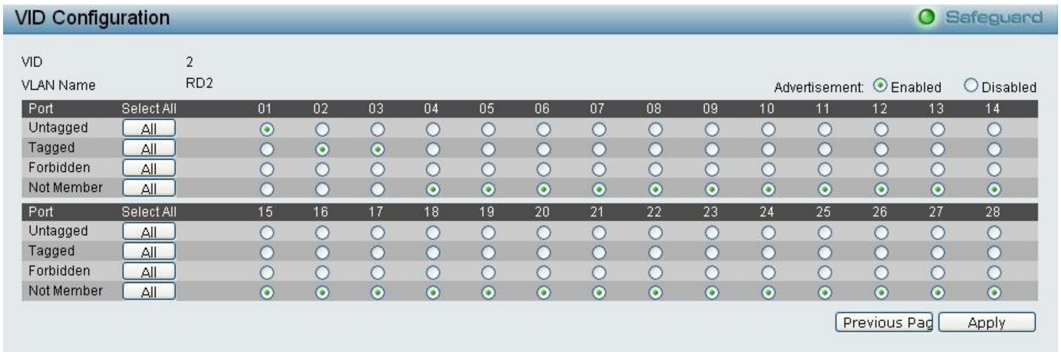
(Maximum Entries : 4094)

VID	VLAN Name	Advertisement	Untagged VLAN Ports	Tagged VLAN Ports	Forbidden VLAN Ports	VLAN Rename	Delete VID
1	default	Disable	01,02,03,04,05,06, 07,08,09,10,11,12, 13,14,15,16,17,18, 19,20,21,22,23,24, 25,26,27,28			Rename	Delete VI
2	RD2	Enable	01	02,03		Rename	Delete VI

Figure 4.46 - Configuration > 802.1Q VLAN > Example VIDs

Click the VID number, the configuration of VLAN group which selected by user will displayed.

Change the port assignment then click **Apply** to implement changes made. User can also click the **Previous Page** to the go back to the previous page.



VID Configuration

VID 2

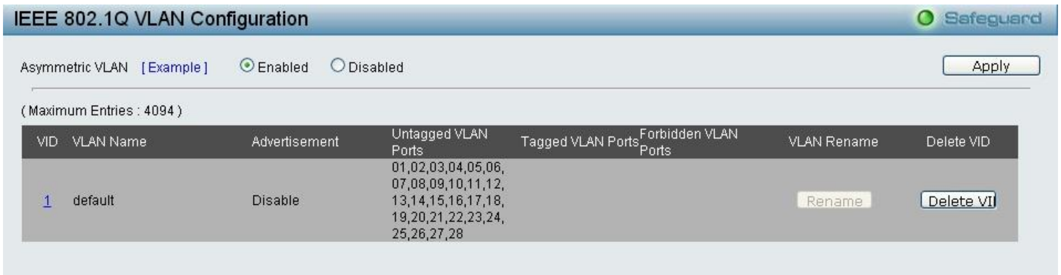
VLAN Name RD2 Advertisement: ● Enabled ○ Disabled

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	●	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	All	○	●	●	○	○	○	○	○	○	○	○	○	○	○
Forbidden	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	All	○	○	○	●	●	●	●	●	●	●	●	●	●	●

Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Figure 4.47 - Configuration > 802.1Q VLAN > VID Assignments

Select **Enabled** of Asymmetric VLAN and click **Apply** to change to Asymmetric VLAN mode:



IEEE 802.1Q VLAN Configuration

Asymmetric VLAN [Example] ● Enabled ○ Disabled

(Maximum Entries : 4094)

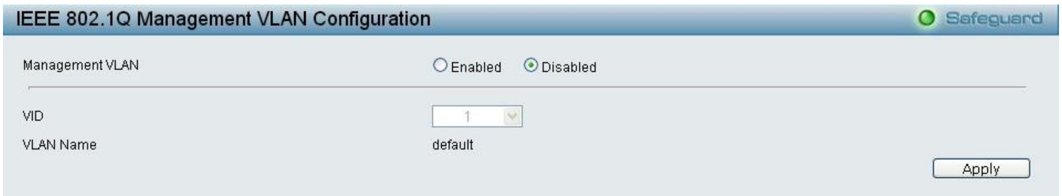
VID	VLAN Name	Advertisement	Untagged VLAN Ports	Tagged VLAN Ports	Forbidden VLAN Ports	VLAN Rename	Delete VID
1	default	Disable	01,02,03,04,05,06, 07,08,09,10,11,12, 13,14,15,16,17,18, 19,20,21,22,23,24, 25,26,27,28			Rename	Delete VI

Figure 4.48 - Configuration > 802.1Q VLAN > VID Assignments

Configuration > 802.1Q Management VLAN

The 802.1Q Management VLAN setting allows user to transfer the authority of the switch from the default VLAN to others created by users. This allows managing the whole network more flexible.

By default, the Management VLAN is disabled. You can select any existing VLAN as the management VLAN when this function is enabled. There can only be one management VLAN at a time. Click **Apply** to implement changes made.



IEEE 802.1Q Management VLAN Configuration

Management VLAN ○ Enabled ● Disabled

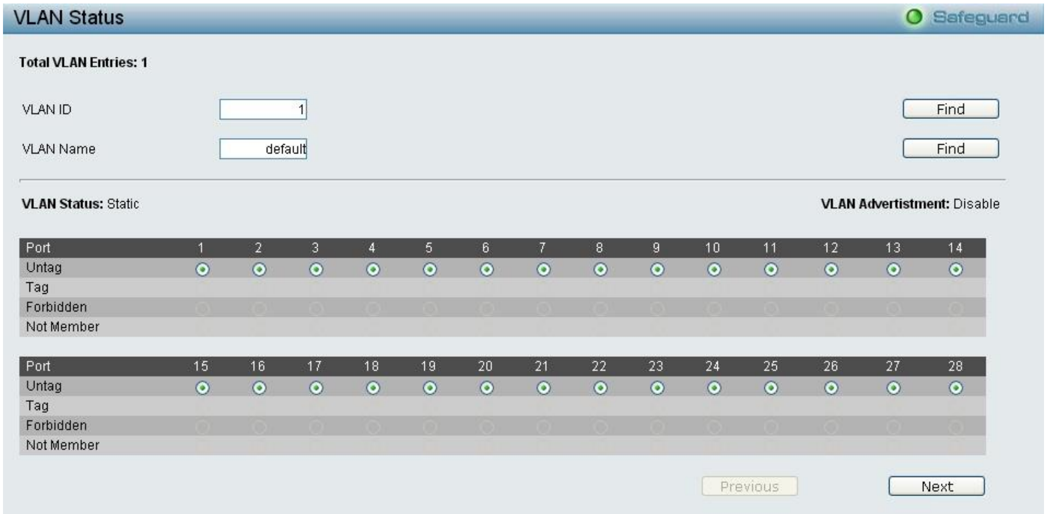
VID: 1

VLAN Name: default

Figure 4.49 – Configuration > 802.1Q Management VLAN

Configuration > VLAN Status

The VLAN Status page is for user to search the VLAN which has already existed on the Switch.



VLAN Status

Total VLAN Entries: 1

VLAN ID: 1

VLAN Name: default

VLAN Status: Static

VLAN Advertistment: Disable

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Untag	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tag	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	○	○	○	○	○	○	○	○	○

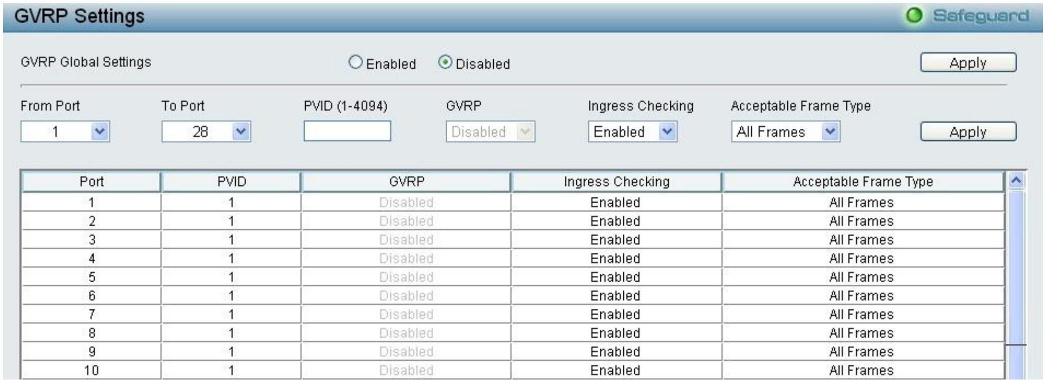
Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untag	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Tag	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Forbidden	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 4.50 - Configuration > VLAN Status

Enter the **VLAN ID** or **VLAN Name** then click **Find** to show the existed VLAN.

Configuration > GVRP Settings

The GVRP Settings page allows user to determine whether the Switch will share its VLAN configuration information with other **GARP VLAN Registration Protocol (GVRP)** enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.



GVRP Settings

GVRP Global Settings ○ Enabled ● Disabled [Apply]

From Port	To Port	PVID (1-4094)	GVRP	Ingress Checking	Acceptable Frame Type
1	28		Disabled	Enabled	All Frames

[Apply]

Port	PVID	GVRP	Ingress Checking	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
4	1	Disabled	Enabled	All Frames
5	1	Disabled	Enabled	All Frames
6	1	Disabled	Enabled	All Frames
7	1	Disabled	Enabled	All Frames
8	1	Disabled	Enabled	All Frames
9	1	Disabled	Enabled	All Frames
10	1	Disabled	Enabled	All Frames

Figure 4.51 - Configuration > GVRP Settings

From Port/To Port: These two fields allow user to specify the range of ports that will be included in the Port-based VLAN that user is creating using the 802.1Q Port Settings page.

PVID (1-4094): The read-only field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.

GVRP: The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is *Disabled* by default.

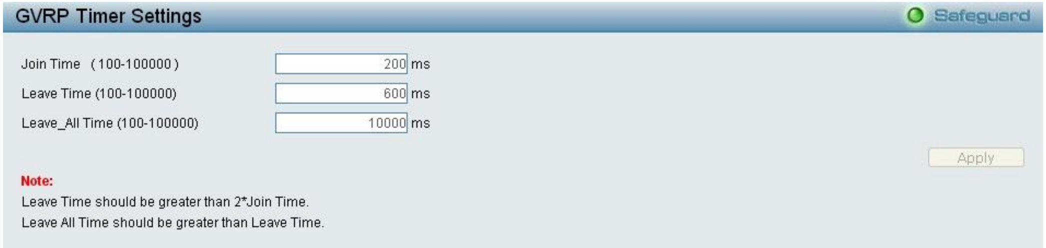
Ingress Checking: This field can be toggled using the space bar between Enabled and Disabled. Enabled enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. Disabled disables ingress filtering. Ingress Checking is *Disabled* by default.

Acceptable Frame Type: This field denotes the type of frame that will be accepted by the port. The user may choose between **Tagged Only**, which means only VLAN tagged frames will be accepted, and Admit_All, which mean both tagged and untagged frames will be accepted. **Admit_All** is enabled by default.

Click **Apply** to implement changes made.

Configuration > GVRP Timer Settings

The GVRP Timer Settings page allows user to configure the GARP timer values for application join, leave, and leave_all GARP timer values.



GVRP Timer Settings

Join Time (100-100000) 200 ms

Leave Time (100-100000) 600 ms

Leave_All Time (100-100000) 10000 ms

[Apply]

Note:
Leave Time should be greater than 2*Join Time.
Leave All Time should be greater than Leave Time.

Figure 4.52 - Configuration >GVRP Timer Settings

Join Time (100-100000): Indicates the time in milliseconds that PDUs are transmitted. The default value is *200ms*.

Leave Time (100-100000): Indicates the amount of time in milliseconds that the device waits before leaving its GARP state. The leave time is activated by a leave all time message sent/received, and cancelled by the Join message. The default value is *600ms*.

Leave_All Time (100-100000): Used to confirm the port within the VLAN. The time in milliseconds between messages sent. The default value is *10000ms*.

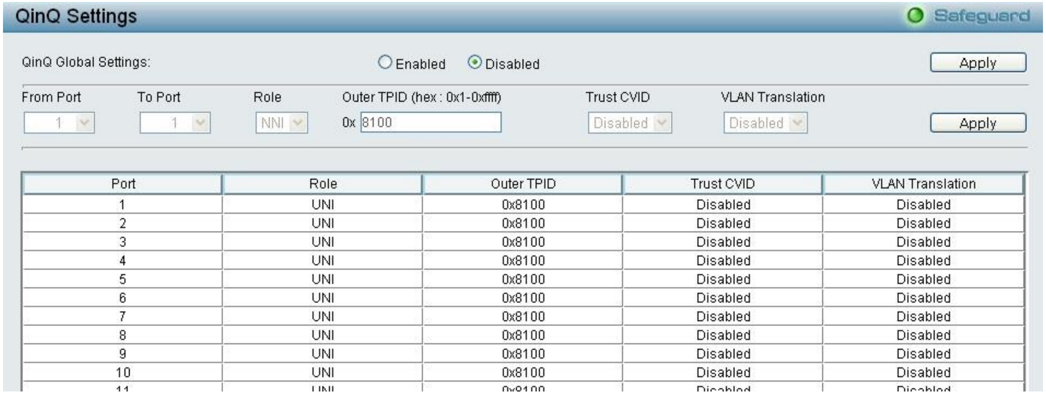
Click **Apply** to implement changes made.

Configuration > QinQ > QinQ Settings

The QinQ Settings page allows user to enable or disable the Q-in-Q function. Q-in-Q is designed for service providers to carry traffic from multiple users across a network.

Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SPVLAN tags to each new frame. Select *Enabled* or *Disabled* then click **Apply** to enable or disable the Q-in-Q Global Settings.



QinQ Settings

QinQ Global Settings: ○ Enabled ● Disabled

From Port: 1 | To Port: 1 | Role: NNI | Outer TPID (hex : 0x1-0xffff): 0x 8100 | Trust CVID: Disabled | VLAN Translation: Disabled

Port	Role	Outer TPID	Trust CVID	VLAN Translation
1	UNI	0x8100	Disabled	Disabled
2	UNI	0x8100	Disabled	Disabled
3	UNI	0x8100	Disabled	Disabled
4	UNI	0x8100	Disabled	Disabled
5	UNI	0x8100	Disabled	Disabled
6	UNI	0x8100	Disabled	Disabled
7	UNI	0x8100	Disabled	Disabled
8	UNI	0x8100	Disabled	Disabled
9	UNI	0x8100	Disabled	Disabled
10	UNI	0x8100	Disabled	Disabled
11	UNI	0x8100	Disabled	Disabled

Figure 4.53 - Configuration > QinQ > QinQ Settings

From Port / To Port: A consecutive group of ports that are part of the VLAN configuration starting with the selected port.

Role: The user can choose between *UNI* or *NNI* role.

> **UNI –** To select a user-network interface which specifies that communication between the specified user and a specified network will occur.
>
> **NNI –** To select a network-to-network interface specifies that communication between two specified networks will occur.

Outer TPID (hex: 0x1-0xffff): The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.

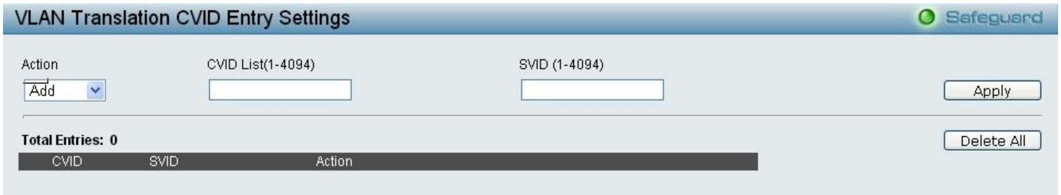
Trust CVID: Specify the Trust CVID is enabled or disabled on the ports.

VLAN Translation: Specify the VLAN Translation is enabled or disabled on the ports.

Click **Apply** to implement changes made.

Configuration > QinQ > VLAN Translation CVID Entry Settings

The VLAN Translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.



VLAN Translation CVID Entry Settings

Action: Add

CVID List(1-4094):

SVID (1-4094):

Total Entries: 0

CVID	SVID	Action

Figure 4.54 - Configuration > QinQ > VLAN Translation CVID Entry Settings

Action: Specify for SPVID packets to be added or replaced.

CVID List (1-4094): The customer VLAN ID List to which the tagged packets will be added.

SVID (1-4094): This configures the VLAN to join the Service Providers VLAN as a tagged member.

Click **Apply** to implement changes made. Click **Delete All** to remove all the CVID entries.

Q-in-Q and VLAN Translation Rules:

For Ingress untagged packets at UNI ports:

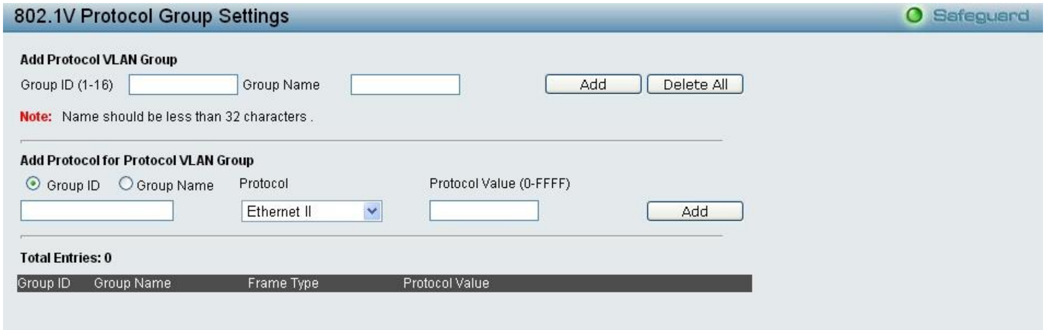
1. The Switch does not reference the VLAN translation table.
2. Check the Switch VLAN tables. The Sequence is MAC-based VLAN -> subnet-based VLAN -> protocol-based VLAN -> port-based VLAN. If matched, the matched VLAN will become this packet's SPVLAN.

For Ingress tagged packets at UNI ports:

1. The Switch looks up the VLAN translation table. If matched, the VLAN tag will be translated (replace CEVLAN with SPVLAN, or add SPVLAN).
2. Or, check the Switch VLAN tables. The sequence is the same as above. The matched VLAN becomes this packet's SPVLAN.

Configuration > 802.1v Protocol VLAN > 802.1v Protocol Group Settings

The 802.1v Protocol Group Settings page allows user to configure the untagged ports of different protocols on the same physical port.



802.1V Protocol Group Settings

Add Protocol VLAN Group

Group ID (1-16): Group Name:

Note: Name should be less than 32 characters .

Add Protocol for Protocol VLAN Group

● Group ID ○ Group Name

Protocol: Ethernet II

Protocol Value (0-FFFF):

Total Entries: 0

Group ID	Group Name	Frame Type	Protocol Value

Figure 4.55 - Configuration > 802.1v Protocol VLAN > 802.1v Protocol Group Settings

Group ID (1-16): Select an ID number for the group. The value is between 1 and 16.

Group Name: Specifies the group name for the 802.1v protocol group.

Click the **Add** button to add a new entry based on the information entered.

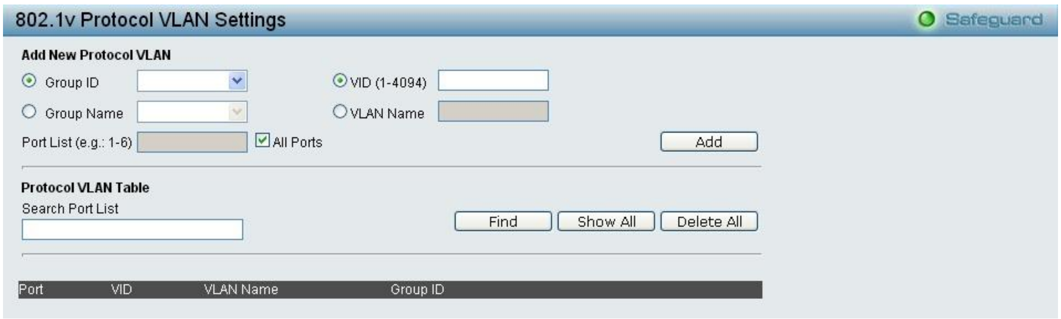
Click the **Delete All** button to remove all the entries based on the information entered.

Protocol: Specifies the packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. The types are Ethernet II, IEEE802.3 SNAP, and IEEE802.3 LLC.

Protocol Value: Enter a value for the group. The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff.

Configuration > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings

The 802.1v Protocol VLAN Settings page allows user to configure the Protocol VLAN settings.



● Group ID
○ Group Name
Port List (e.g.: 1-6) ☑ All Ports
● VID (1-4094)
○ VLAN Name

Port	VID	VLAN Name	Group ID

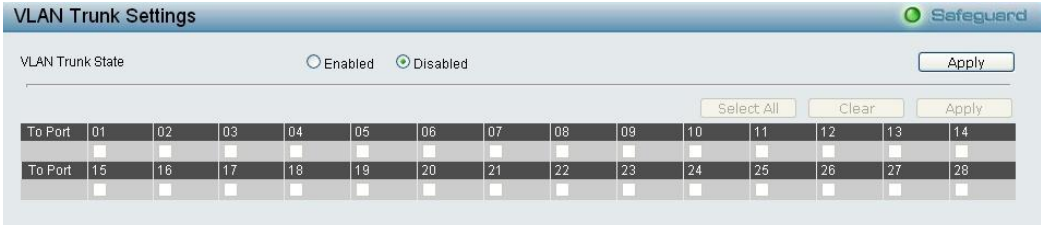
Figure 4.56 - Configuration > 802.1v Protocol VLAN > 802.1v Protocol VLAN Settings

Group ID: Select a previously configured Group ID from the drop-down menu.
VID (1-4094): Specifies the VID to be created.
Group Name: Select a previously configured Group Name from the drop-down menu.
VLAN Name: Specifies the VLAN name to be created.
Port List: Enter the specified ports to be configured or tick the **All Ports** check box.
Click the **Add** button to add a new entry based on the information entered.

Search Port List: Specifies the port to be searched.
Click the **Find** button to view the information with specified ports.
To display all previously configured port lists on the button half of the screen click the **Show All** button.
To clear all previously configured lists click the **Delete All** button.

Configuration > VLAN Trunk Settings

The VLAN Trunk Settings is used to combine a number of VLAN ports together to create VLAN trunks. To create Vlan Trunk Port settings on the Switch, enter the ports to be configured, change the state to *Enabled* and click **Apply**, the new settings will appear in the **VLAN Trunk Port Settings Table** below.



VLAN Trunk State ○ Enabled ● Disabled

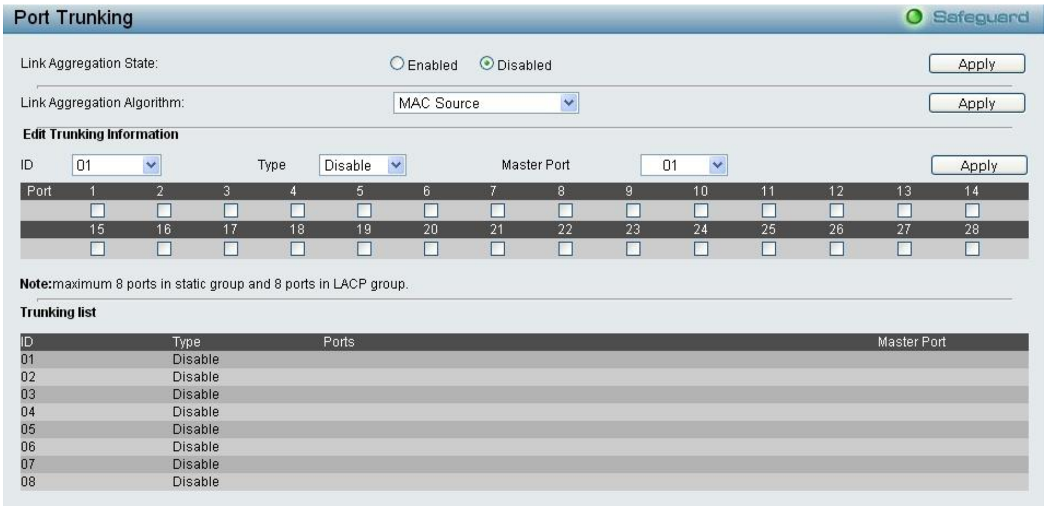
To Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
	□	□	□	□	□	□	□	□	□	□	□	□	□	□
To Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 4.57 - Configuration > VLAN Trunk Settings

Click **Select All** to check all ports or click **Clear** to remove ports then click **Apply**.
Click **Apply** to implement changes made.

Configuration > Link Aggregation > Port Trunkings

The Port Trunkings function enables the combining of two or more ports together to increase bandwidth. Up to eight Trunk groups may be created, and each group consists up to eight ports. Select **Enabled** and click **Apply** to active the Link Aggregation State.



Port Trunking

Link Aggregation State: ○ Enabled ● Disabled [Apply]

Link Aggregation Algorithm: MAC Source [Apply]

Edit Trunking Information

ID 01 Type Disable Master Port 01 [Apply]

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	□	□	□	□	□	□	□	□	□	□	□	□	□	□
	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Note:maximum 8 ports in static group and 8 ports in LACP group.

Trunking list

ID	Type	Ports	Master Port
01	Disable		
02	Disable		
03	Disable		
04	Disable		
05	Disable		
06	Disable		
07	Disable		
08	Disable		

Figure 4.58 – Configuration > Link Aggregation > Port Trunkings

Link Aggregation Algorithm: Specify the algorithm to be *MAC Source, MAC Destination, MAC Source Destination, IP Source, IP Destination or IP Source Destination*, and then click Apply to implement changes made.

Edit Trunking Information:

Specify the **ID**, **Type** and **Master Port** then select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

Static - Static link aggregation.

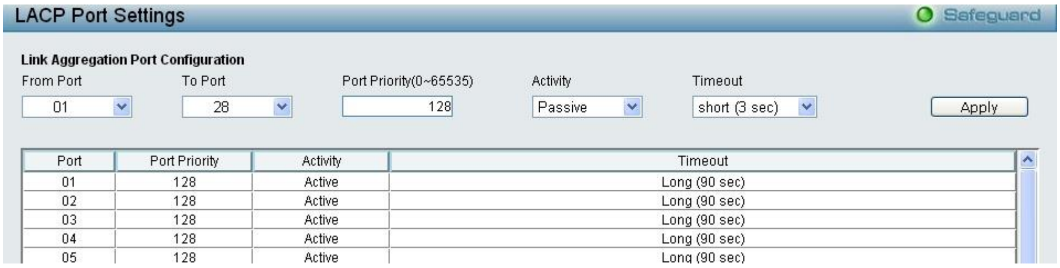
LACP - LACP (Link Aggregation Control Protocol) is enabled on the device. LACP allows for the automatic detection of links in a Port Trunking Group.

Disable - Remove all members in this trunk group.

NOTE: Each combined trunk port must be connected to devices within the same VLAN group.

Configuration > Link Aggregation > LACP Port Settings

The LACP Port Settings is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames.



LACP Port Settings

Link Aggregation Port Configuration

From Port: 01 To Port: 28 Port Priority(0~65535): 128 Activity: Passive Timeout: short (3 sec) [Apply]

Port	Port Priority	Activity	Timeout
01	128	Active	Long (90 sec)
02	128	Active	Long (90 sec)
03	128	Active	Long (90 sec)
04	128	Active	Long (90 sec)
05	128	Active	Long (90 sec)

Figure 4.59 – Configuration > Link Aggregation > LACP Port Settings

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.

To Port: The ending of a consecutive group of ports may be configured starting with the selected port.

Port Priority (0-65535): Displays the LACP priority value for the port. Default is *128*.

Activity: There are two different roles of LACP ports:

Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.

Timeout: Specify the administrative LACP timeout. The possible field values are:

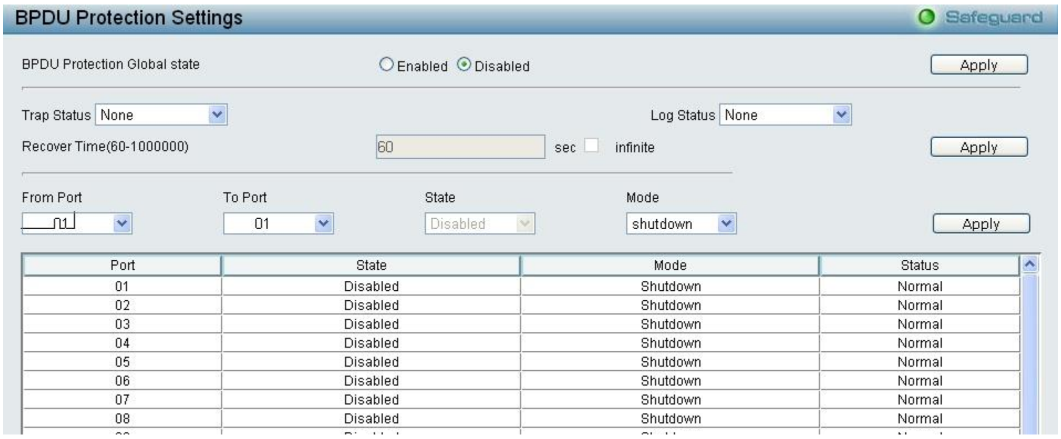
Short (3 Sec) - Defines the LACP timeout as 3 seconds.

Long (90 Sec) - Defines the LACP timeout as 90 seconds. This is the default value.

Click **Apply** to implement the changes made.

Configuration > BPDU Protection Settings

The BPDU Protection Settings page allows user to configure the BPDU protection function for the ports on the Switch. In generally, there are two states in BPDU protection function. One is normal state, and another is under attack state. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter and under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on the STP-disabled port. Select *Enabled* or *Disabled* and click **Apply** to enabled or disable the BPDU attack protection state.



BPDU Protection Global state ○ Enabled ● Disabled

Trap Status: None

Log Status: None

Recover Time(60-1000000): 60 sec □ infinite

From Port: 01

To Port: 01

State: Disabled

Mode: shutdown

Port	State	Mode	Status
01	Disabled	Shutdown	Normal
02	Disabled	Shutdown	Normal
03	Disabled	Shutdown	Normal
04	Disabled	Shutdown	Normal
05	Disabled	Shutdown	Normal
06	Disabled	Shutdown	Normal
07	Disabled	Shutdown	Normal
08	Disabled	Shutdown	Normal

Figure 4.60 – Configuration > BPDU Protection Settings

Trap Status: Specify to send trap packet when *Attack Detected, Attack Cleared, None* or *Both.*

Log Status: Specify the Log Status when *Attack Detected, Attack Cleared, None* or *Both.*

Recover Time (60-1000000): Specify the BPDU protection Auto-Recovery timer, the range is from *60* to *1000000* and default is *60* seconds. Or select *infinite*.

Click **Apply** for changes to take effect.

From Port / To Port: Specify the port ranges to be configured.

State: To enabled or disable the protection mode for a specific port.

Mode: Specify the BPDU protection mode. The default mode is shutdown.

Drop – Drop all received BPDU packets when the port enters under attack stats.

Block – Drop all packets (includes BPDU and normal packets) when the port enters under attack state.

Shutdown – Shut down the port when the port enters under attack state.

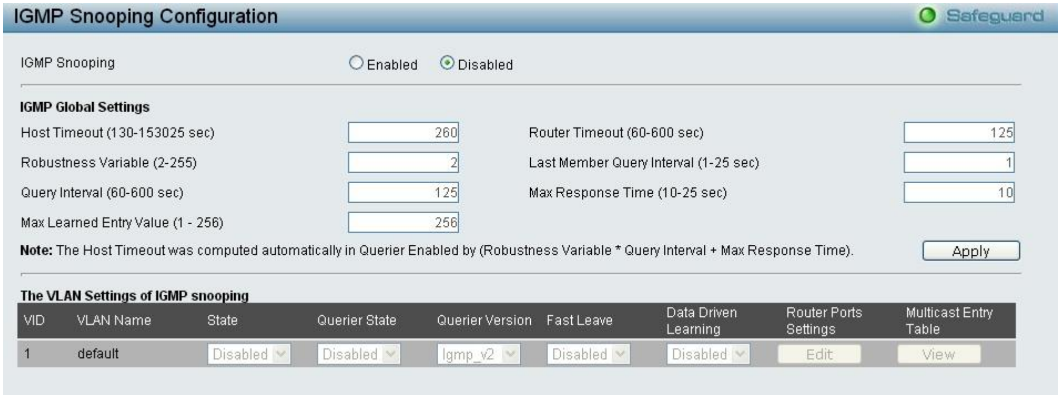
Click **Apply** for changes to take effect.

Configuration > IGMP Snooping > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the DES-1210 Metro Ethernet Managed Switch can make intelligent multicast forwarding decisions by examining the contents of each frame’s Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the DES-1210 Metro Ethernet Managed Switch will forward multicast traffic only to connections that have group members attached.

The settings of IGMP snooping is set by each VLAN individually.



IGMP Snooping Configuration

IGMP Snooping ○ Enabled ● Disabled

IGMP Global Settings

Host Timeout (130-153025 sec)	260	Router Timeout (60-600 sec)	125
Robustness Variable (2-255)	2	Last Member Query Interval (1-25 sec)	1
Query Interval (60-600 sec)	125	Max Response Time (10-25 sec)	10
Max Learned Entry Value (1 - 256)	256		

Note: The Host Timeout was computed automatically in Querier Enabled by (Robustness Variable * Query Interval + Max Response Time).

The VLAN Settings of IGMP snooping

VID	VLAN Name	State	Querier State	Querier Version	Fast Leave	Data Driven Learning	Router Ports Settings	Multicast Entry Table
1	default	Disabled	Disabled	Igmp_v2	Disabled	Disabled	Edit	View

Figure 4.61 – Configuration > IGMP Snooping > IGMP Snooping

By default, IGMP is disabled. If enabled, the IGMP Global Settings will need to be entered:

Host Timeout (130-153025 sec): This is the interval after which a learned host port entry will be purged. For each host port learned, a 'Port Purge Timer' runs for 'Host Port Purge Interval'. This timer will be restarted whenever a report message from host is received over that port. If no report messages are received for 'Host Port Purge Interval' time, the learned host entry will be purged from the multicast group. The default value is 260 seconds.

Robustness Variable (2-255 sec): The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may need to be increased. The Robustness Variable cannot be set to zero, and it SHOULD NOT be. Default is 2 seconds.

Query Interval (60-600 sec): The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of IGMP messages can be increased or decreased; larger values will cause IGMP Queries to be sent less often. Default value is 125 seconds.

Max Learned Entry Value (1-256): The Max Learned Entry Value allows adjustment for the value. Default value is 256.

Router Timeout (60-600 sec): This is the interval after which a learned router port entry will be purged. For each router port learned, a 'Router Port Purge Timer' runs for 'Router Port Purge Interval'. This timer will be restarted whenever a Query control message is received over that port. If there were no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 260 seconds.

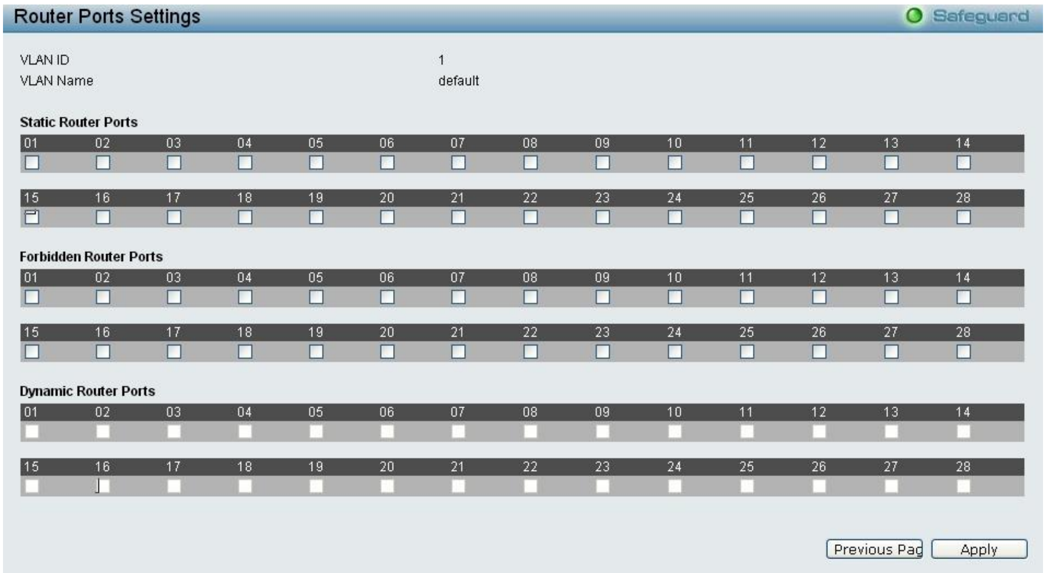
Last Member Query Interval (1-25 sec): The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.

Max Response Time (10-25 sec): The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. Default is 10 seconds.

Select the **State, Querier State, Fast Leave** and **Data Driven Learning** to be enabled or disabled then click **Apply** for changes to take effect.

Click **Edit** button to enter the Router Port Settings page, and the ports to be assigned as router ports for IGMP snooping for the VLAN.

A router port configured manually is a **Static Router Port**, a **Forbidden Router Port** and a **Dynamic Router Port** is dynamically configured by the Switch when a query control message is received. Press **Apply** for changes to take effect.



Router Ports Settings

VLAN ID 1

VLAN Name default

Static Router Ports

01	02	03	04	05	06	07	08	09	10	11	12	13	14
□	□	□	□	□	□	□	□	□	□	□	□	□	□

15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	□	□	□	□	□	□	□	□	□	□	□	□	□

Forbidden Router Ports

01	02	03	04	05	06	07	08	09	10	11	12	13	14
□	□	□	□	□	□	□	□	□	□	□	□	□	□

15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	□	□	□	□	□	□	□	□	□	□	□	□	□

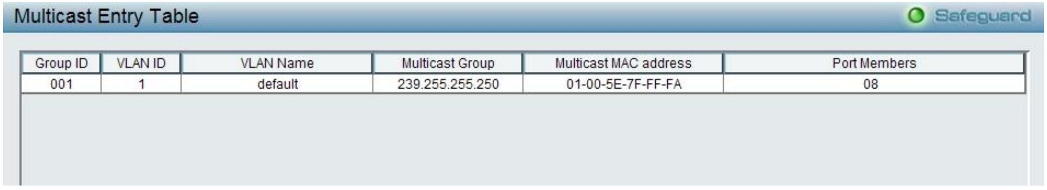
Dynamic Router Ports

01	02	03	04	05	06	07	08	09	10	11	12	13	14
□	□	□	□	□	□	□	□	□	□	□	□	□	□

15	16	17	18	19	20	21	22	23	24	25	26	27	28
□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 4.62 – Configuration > IGMP Snooping > IGMP Snooping-Router Port Settings

To view the Multicast Entry Table for a given VLAN, press the **View** button.



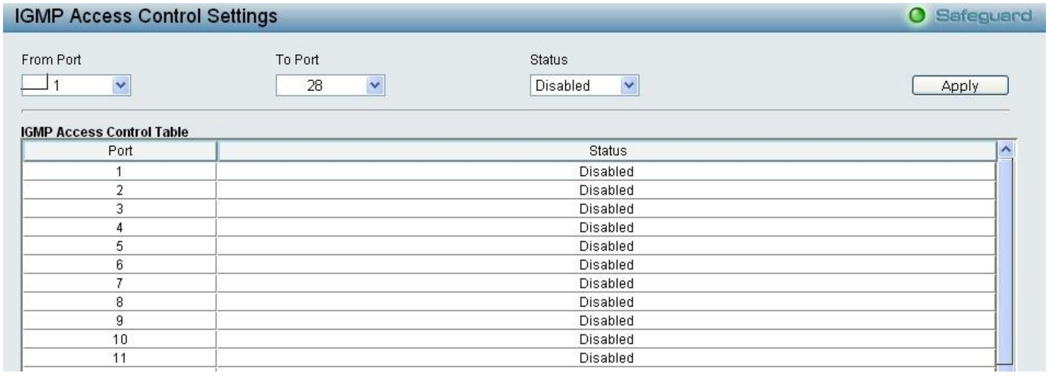
Multicast Entry Table

Group ID	VLAN ID	VLAN Name	Multicast Group	Multicast MAC address	Port Members
001	1	default	239.255.255.250	01-00-5E-7F-FF-FA	08

Figure 4.63– Configuration > IGMP Snooping > IGMP Snooping-Multicast Entry Table

Configuration > IGMP Snooping > IGMP Access Control Settings

The IGMP Access Control Settings page is used to enable or disable the IGMP access control of selected ports.



IGMP Access Control Settings

From Port: 1

To Port: 28

Status: Disabled

IGMP Access Control Table

Port	Status
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled

Figure 4.64 – Configuration > IGMP Snooping > IGMP Access Control Settings

From Port/To Port: Select the port ranges to be configured.

Status: Enable or disable the IGMP Access Control of specified ports.

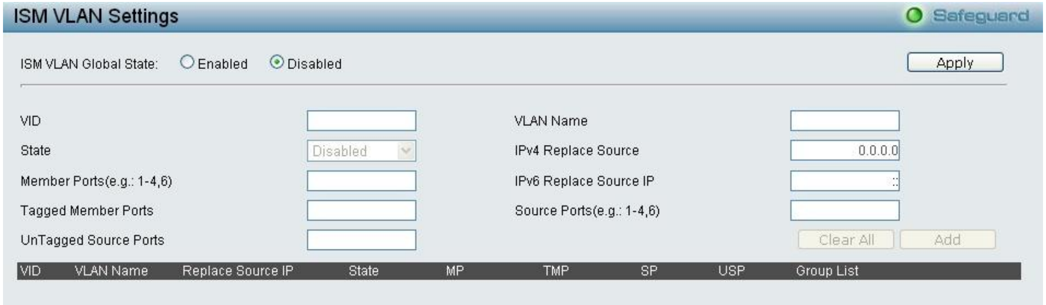
Click **Apply** to take effect.

Configuration > IGMP Snooping > ISM VLAN Settings

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

The ISM VLAN Settings page allows the user to configure the ISM VLAN.



ISM VLAN Settings

ISM VLAN Global State: ○ Enabled ● Disabled

State: Disabled

IPv4 Replace Source: 0.0.0.0

IPv6 Replace Source IP: ::

VID	VLAN Name	Replace Source IP	State	MP	TMP	SP	USP	Group List

Figure 4.65 - Configuration > IGMP Snooping > ISM VLAN Settings

ISM VLAN Global State: Enable or disable the IGMP Snooping Multicast (ISM) VLAN Global State.

Click **Apply** button to confirm the ISM VLAN Global State.

VID: Add the corresponding VLAN ID of the Multicast VLAN. Users may enter a value between *2* and *4094.*

State: Use the drop-down menu to enable or disable the selected Multicast VLAN.

Member Ports: Enter a port or list of ports to be added to the Multicast VLAN. Member ports shall be the untagged members of the multicast VLAN.

Tagged Member Ports: Enter a port or list of ports that will become tagged members of the Multicast VLAN.

UnTagged Source Ports: Enter a port or list of ports that will become unagged members of the Multicast VLAN.

VLAN Name: Enter the name of the new Multicast VLAN to be created. This name can be up to *32* characters in length.

IPv4 Replace Source: This field is used to replace the source IPv4 address of incoming packets sent by the host before being forwarded to the source port.

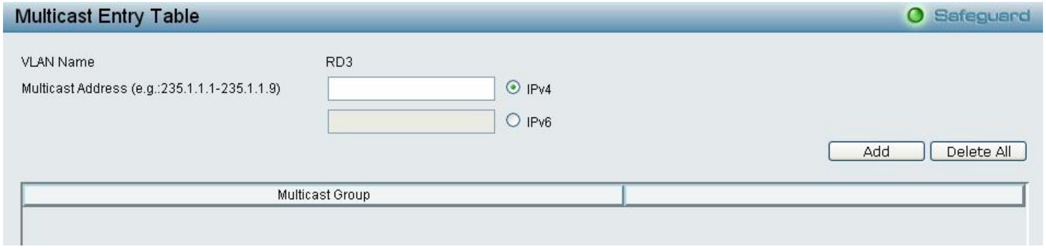
IPv6 Replace Source IP: This field is used to replace the source IPv6 address of incoming packets sent by the host before being forwarded to the source port.

Source Ports: Enter a port or list of ports to be added to the Multicast VLAN. Source ports shall be the tagged members of the multicast VLAN.

Click **Add** to add the ISM VLAN which will appear in the table, or click **Clear All** to clear all fields.

Click **Edit** button to modify the parameters and update the ISM VLAN Setting or click **Delete** to delete the ISM VLAN.

Click **View** to display the detail information of ISM VLAN.



Multicast Entry Table

VLAN Name: RD3

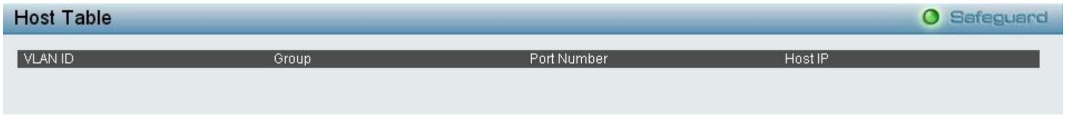
Multicast Address (e.g.:235.1.1.1-235.1.1.9): ● IPv4 ○ IPv6

Multicast Group	

Figure 4.66 - Configuration > IGMP Snooping > ISM VLAN Settings

Configuration > IGMP Snooping > Host Table

The Host Table page displays the information of Host Table. Including VLAN ID, Group, Port Number and Host IP.

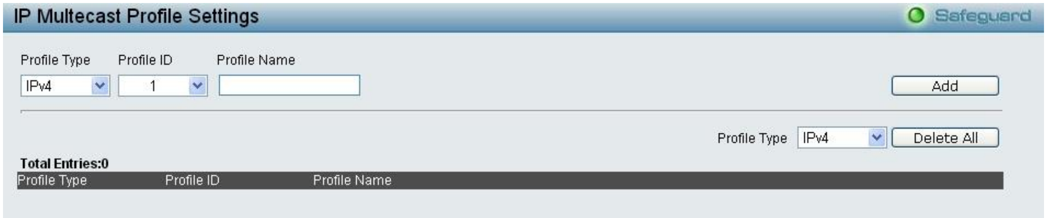


VLAN ID	Group	Port Number	Host IP

Figure 4.67 - Configuration > IGMP Snooping > Host Table

Configuration > IGMP Snooping > IP Multicast Profile Settings

The IP Multicast Profile Settings page allows user to configure the IP Multicast Profile.



Profile Type: IPv4
Profile ID: 1
Profile Name:

Profile Type: IPv4

Total Entries:0

Profile Type	Profile ID	Profile Name

Figure 4.68 - Configuration > IGMP Snooping > IP Multicast Profile Settings

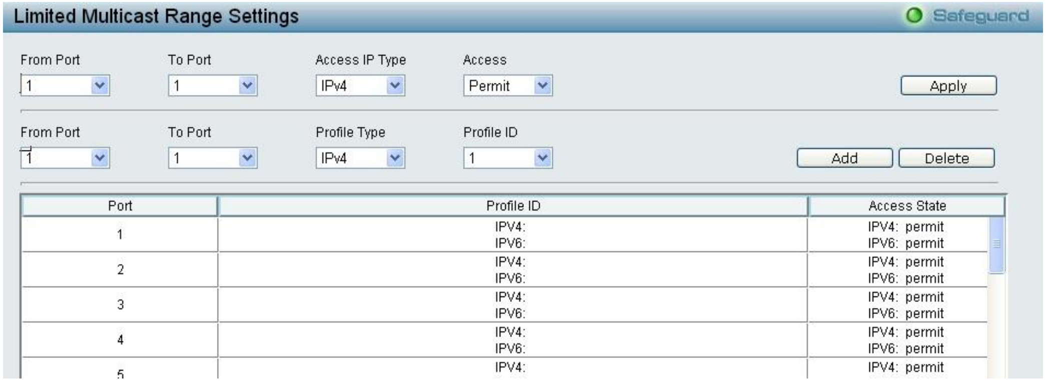
Profile ID: Specify the Profile ID.

Profile Name: Specify the Profile Name.

Click **Add** to create a new IP Multicast Profile or click **Delete All** to clear all the entries.

Configuration > IGMP Snooping > Limited Multicast Range Settings

The Limited Multicast Range Settings page allows user to configure the Limited Multicast. Specify the port range, select Access IP Type is *IPv4* or *IPv6* and select the Access is *Deny* or *Permit* then click **Apply** to implement changes made.



From Port: 1
To Port: 1
Access IP Type: IPv4
Access: Permit

From Port: 1
To Port: 1
Profile Type: IPv4
Profile ID: 1

Port	Profile ID	Access State
1	IPV4: IPV6:	IPV4: permit IPV6: permit
2	IPV4: IPV6:	IPV4: permit IPV6: permit
3	IPV4: IPV6:	IPV4: permit IPV6: permit
4	IPV4: IPV6:	IPV4: permit IPV6: permit
5	IPV4:	IPV4: permit

Figure 4.69- Configuration > IGMP Snooping > Limited Multicast Range Settings

From Port / To Port: Specify the port ranges to be configured.

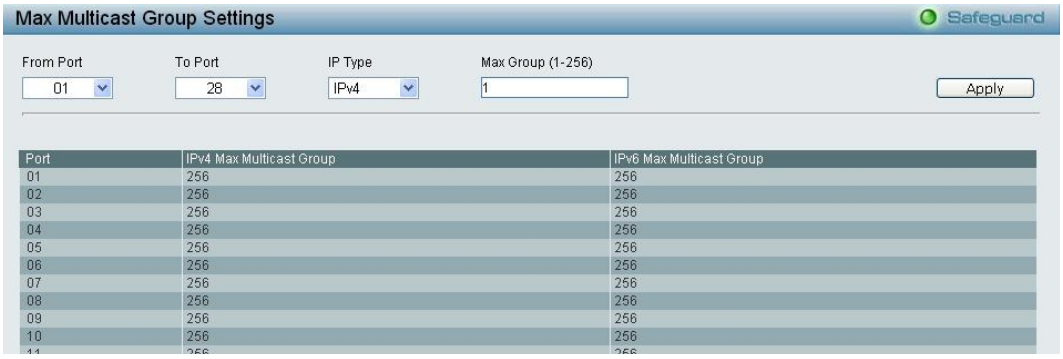
Profile Type: Specify the profile type is IPv4 or IPv6.

Profile ID: Specify the Profile ID.

Click **Add** to create the Profile ID with specified ports or click **Delete** to remove the ports.

Configuration > IGMP Snooping > Max Multicast Group Settings

The Max Multicast Group Settings page allows user to configure the max multicast group for IGMP Snooping.



Max Multicast Group Settings

From Port	To Port	IP Type	Max Group (1-256)
01	28	IPv4	1

Port	IPv4 Max Multicast Group	IPv6 Max Multicast Group
01	256	256
02	256	256
03	256	256
04	256	256
05	256	256
06	256	256
07	256	256
08	256	256
09	256	256
10	256	256
11	256	256

Figure 4.70- Configuration > IGMP Snooping > Max Multicast Group Settings

From Port / To Port: Specify the port ranges to be configured.

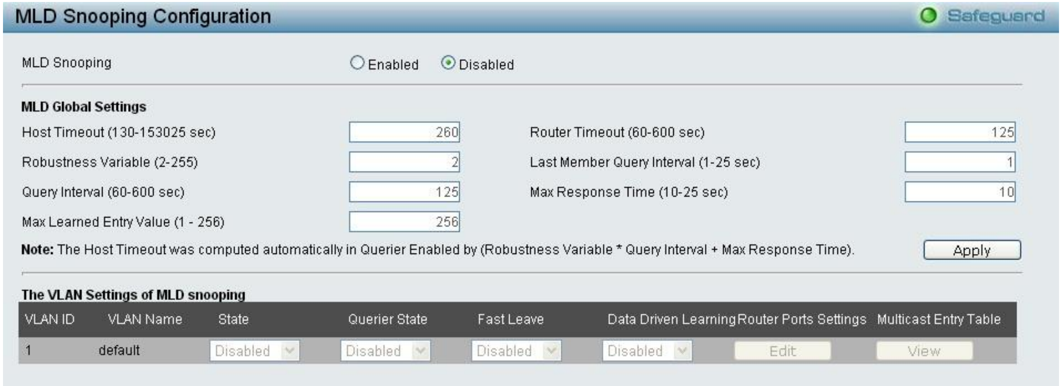
IP Type: Specify the IP type is IPv4 or IPv6.

Max Group (1-256): Specify the Max Group to be configured.

Click **Apply** to implement changes made.

Configuration > MLD Snooping > MLD Snooping Settings

The MLD Snooping Settings page allows user to configure the max multicast group for IGMP Snooping.



MLD Snooping Configuration

MLD Snooping ○ Enabled ● Disabled

MLD Global Settings

Host Timeout (130-153025 sec)	260	Router Timeout (60-600 sec)	125
Robustness Variable (2-255)	2	Last Member Query Interval (1-25 sec)	1
Query Interval (60-600 sec)	125	Max Response Time (10-25 sec)	10
Max Learned Entry Value (1 - 256)	256		

Note: The Host Timeout was computed automatically in Querier Enabled by (Robustness Variable * Query Interval + Max Response Time).

The VLAN Settings of MLD snooping

VLAN ID	VLAN Name	State	Querier State	Fast Leave	Data Driven Learning	Router Ports Settings	Multicast Entry Table
1	default	Disabled	Disabled	Disabled	Disabled	Edit	View

Figure 4.71- Configuration > MLD Snooping > MLD Snooping Settings

MLD Snooping: Enable or disable the MLD Snooping.

MLD Global Settings:

Host Timeout (130-153025 sec): Specifies the time interval in seconds after which a port is removed from a Multicast Group. Ports are removed if a Multicast group MLD report was not received from a Multicast port within the defined *Host Timeout* period. The possible field range is 130 - 153025 seconds. The default timeout is 260 seconds.

Router Timeout (60-600): Specifies the time interval in seconds the Multicast router waits to receive a message before it times out. The possible field range is 60 - 600 seconds. The default timeout is 125 seconds.

Robustness Variable (2-255): The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. The Robustness Variable can not be set zero, and SHOULD NOT be one. Default is 2 seconds.

Last Member Query Interval (1-25 sec): The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of network. A reduced value results in reduced time to detect the loss of the last member of a group. The default value is 1 second.

Query Interval (60-600 sec): The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of MLD messages can increase or decrease; larger values cause MLD Queries to be sent less often. Default is 125 seconds.

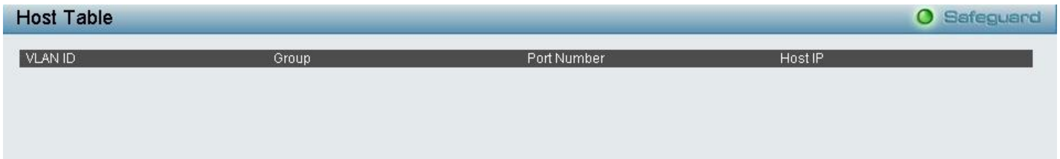
Max Response Time (10-25 sec): Specifies the time interval in seconds after which a port is removed from the Multicast membership group. Ports are removed from the Multicast membership when the port sends a Done Message, indicating the port requests to leave the Multicast group. The field range is 10-25 seconds. The default timeout is 10 seconds.

Max Learned Entry Value (1-256): Specifies the max learned entry value for MLD Snooping. The field range is 1-256. The default is 256.

Click **Apply** to implement changes made. Press the **Edit** button under **Router Port Setting**, and select the ports to be assigned for MLD snooping for the VLAN, and press **Apply** for changes to take effect.

Configuration > MLD Snooping > MLD Host Table

The MLD Host Table page displays the MLD Snooping information.



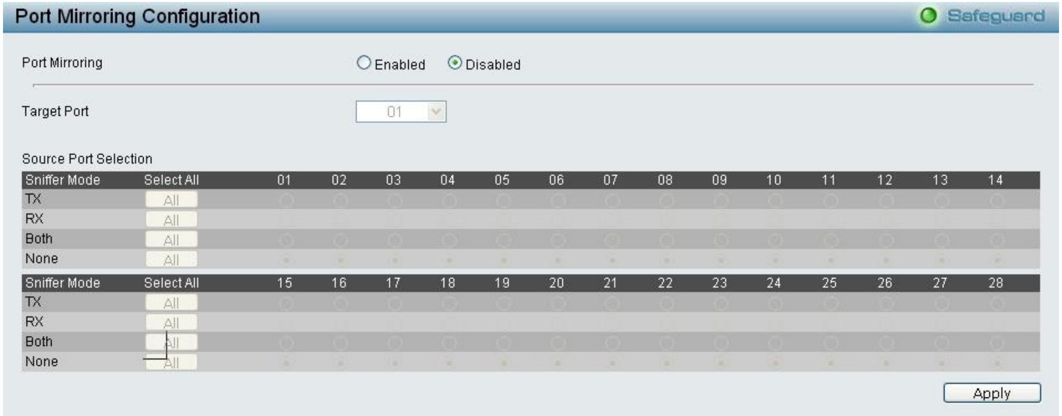
Host Table

VLAN ID	Group	Port Number	Host IP

Figure 4.72- Configuration > MLD Snooping > MLD Host Table

Configuration > Port Mirroring

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the Switch to another port, where the packet can be studied. This enables network managers to better monitor network performances.



Port Mirroring Configuration

Port Mirroring ○ Enabled ● Disabled

Target Port 01

Source Port Selection

Sniffer Mode	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
TX	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
RX	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Both	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
None	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Sniffer Mode	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
TX	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
RX	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Both	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
None	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Figure 4.73 – Configuration > Port Mirroring

Port Mirroring: Enables or Disables the port mirroring feature.

Target Port: Specifies the target port.

Selection options for the Source Ports are as follows:

TX (transmit) mode: Duplicates the data transmitted from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

RX (receive) mode: Duplicates the data that is received from the source port and forwards it to the Target Port. Click “all” to include all ports into port mirroring.

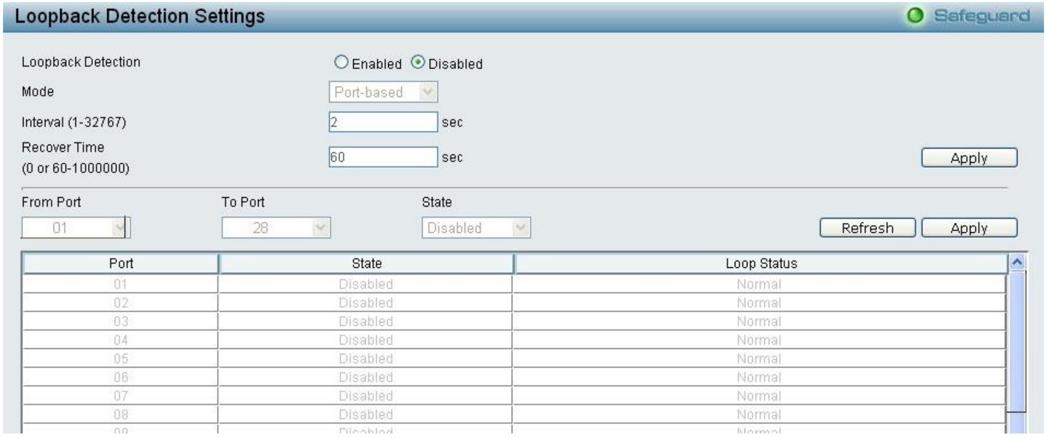
Both (TX and RX) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click “all” to include all ports into port mirroring.

None: Turns off the mirroring of the port. Click “all” to remove all ports from mirroring.

Click **Apply** to implement changes made.

Configuration > Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port while Spanning Tree Protocol (STP) is not enabled in the network, especially when the down links are hubs or unmanaged switches. The Switch will automatically shutdown the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection **Recover Time** times out. The Loopback Detection function can be implemented on a range of ports at the same time. You may enable or disable this function using the pull-down menu.



Loopback Detection ○ Enabled ● Disabled

Mode: Port-based

Interval (1-32767): 2 sec

Recover Time (0 or 60-1000000): 60 sec

From Port: 01 To Port: 28 State: Disabled

Port	State	Loop Status
01	Disabled	Normal
02	Disabled	Normal
03	Disabled	Normal
04	Disabled	Normal
05	Disabled	Normal
06	Disabled	Normal
07	Disabled	Normal
08	Disabled	Normal
09	Disabled	Normal

Figure 4.74 – Configuration > Loopback Detection

Loopback Detection State: Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*

Mode: Specify the Loopback Detection to be Port-based or VLAN-based.

Interval (1-32767): Set a Loop detection Interval between *1* and *32767* seconds. The default is 2 seconds.

Recover Time (0 or 60-1000000): Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at *0* seconds, or *60* to *1000000* seconds. Entering *0* will disable the Loop Detection Recover Time. The default is *60* seconds.

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.

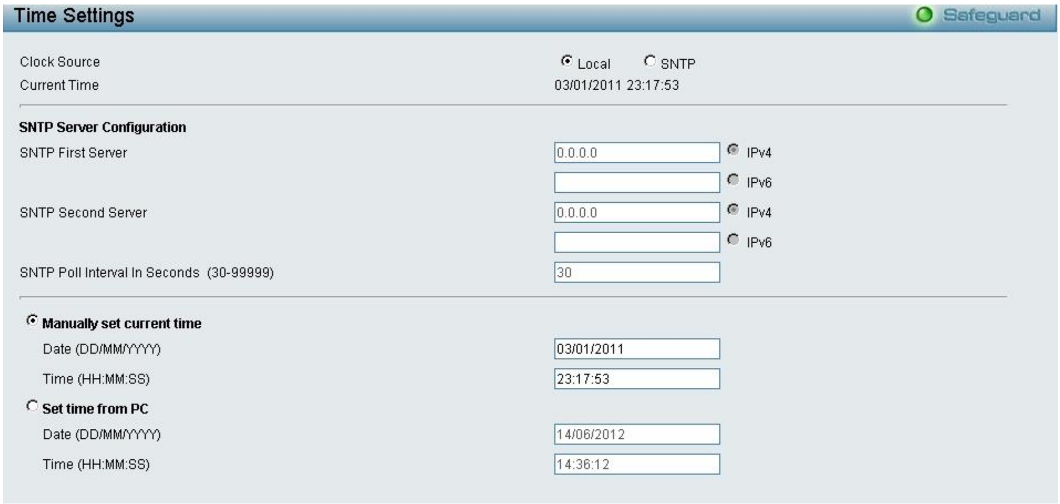
To Port: The ending of a consecutive group of ports may be configured starting with the selected port.

State: Use the drop-down menu to toggle between *Enabled* and *Disabled.* Default is *Disabled*.

Click **Apply** to implement changes made.

Configuration > SNTP Settings > Time Settings

SNTP or Simple Network Time Protocol is used by the Switch to synchronize the clock of the computer. The SNTP settings folders contain two windows: Time Settings and TimeZone Settings. Users can configure the time settings for the switch, and the following parameters can be set or are displayed in the Time Settings page.



Clock Source ● Local ○ SNTP

Current Time 03/01/2011 23:17:53

SNTP Server Configuration

SNTP First Server: 0.0.0.0 ● IPv4; ○ IPv6

SNTP Second Server: 0.0.0.0 ● IPv4; ○ IPv6

SNTP Poll Interval In Seconds (30-99999): 30

● **Manually set current time**

Date (DD/MM/YYYY): 03/01/2011

Time (HH:MM:SS): 23:17:53

○ **Set time from PC**

Date (DD/MM/YYYY): 14/06/2012

Time (HH:MM:SS): 14:36:12

Figure 4.75 – Configuration > SNTP Settings > Time Settings

Clock Source: Specify the clock source by which the system time is set. The possible options are:

Local - Indicates that the system time is set locally by the device.

SNTP - Indicates that the system time is retrieved from a SNTP server.

Current Time: Displays the current date and time for the switch.

If choosing **SNTP** for the clock source, then the following parameters will be available:

SNTP First Server: Select IPv4 or IPv6 and specify the IP address of the primary SNTP server from which the system time is retrieved.

SNTP Second Server: Select IPv4 or IPv6 and specify the IP address of the secondary SNTP server from which the system time is retrieved.

SNTP Poll Interval in Seconds (30-99999): Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 30 seconds.

Click **Apply** to implement changes made.

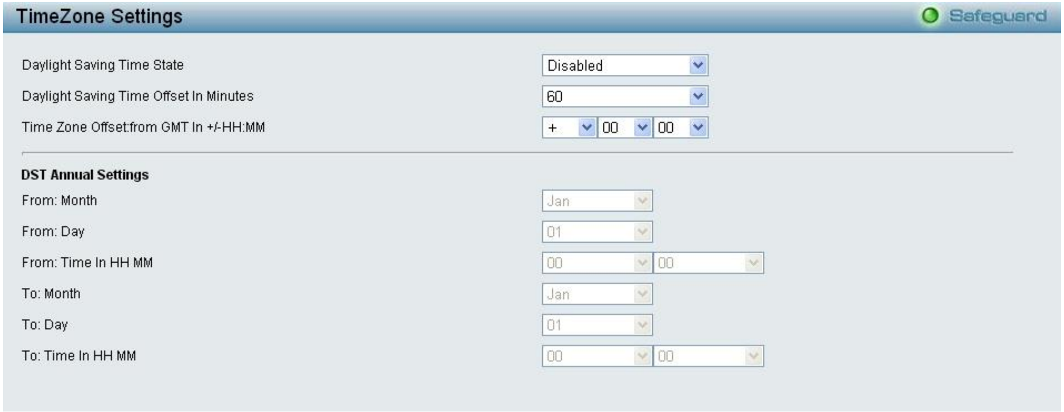
When selecting **Local** for the clock source, users can select from one of two options:

Manually set current time: Users input the system time manually.

Set time from PC: The system time will be synchronized from the local computer.

Configuration > SNTP Settings > TimeZone Settings

The TimeZone Setting Page is used to configure time zones and Daylight Savings time settings for SNTP.



Daylight Saving Time State: Disabled

Daylight Saving Time Offset In Minutes: 60

Time Zone Offset from GMT In +/-HH:MM: + 00 00

DST Annual Settings

From: Month: Jan

From: Day: 01

From: Time In HH MM: 00 00

To: Month: Jan

To: Day: 01

To: Time In HH MM: 00 00

Figure 4.76 – Configuration > SNTP > TimeZone Settings

Daylight Saving Time State: Enable or disable the DST Settings.

Daylight Saving Time Offset: Use this drop-down menu to specify the amount of time that will constitute your local DST offset - *30*, *60*, *90*, or *120* minutes.

Time Zone Offset GMT +/- HH:MM: Use these drop-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

Daylight Saving Time Settings:

From: Month / Day: Enter the month DST and date DST will start on, each year.

From: HH:MM: Enter the time of day that DST will start on, each year.

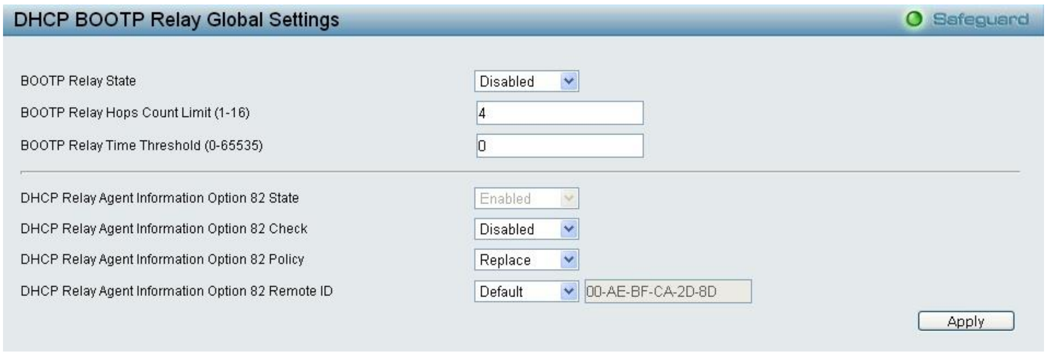
To: Month / Day: Enter the month DST and date DST will end on, each year.

To: HH:MM: Enter the time of day that DST will end on, each year.

Click **Apply** to implement changes made.

Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings

User can enable and configure DHCP/BOOTP Relay Global Settings on the Switch.



DHCP BOOTP Relay Global Settings

BOOTP Relay State: Disabled

BOOTP Relay Hops Count Limit (1-16): 4

BOOTP Relay Time Threshold (0-65535): 0

DHCP Relay Agent Information Option 82 State: Enabled

DHCP Relay Agent Information Option 82 Check: Disabled

DHCP Relay Agent Information Option 82 Policy: Replace

DHCP Relay Agent Information Option 82 Remote ID: Default 00-AE-BF-CA-2D-8D

Figure 4.77 - Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings

BOOTP Relay State: This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is *Disabled*.

BOOTP Relay Hops Count Limit (1-16): This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is 4.

BOOTP Relay Time Threshold (0-65535): Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP/BOOTP packet. If a value of 0 is entered, the Switch will not process the value in the **seconds** field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.

DHCP Relay Agent Information Option 82 State: This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is *Disabled*.

> **Enabled –** When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.
>
> **Disabled -** If the field is toggled to Disabled the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.

DHCP Relay Agent Information Option 82 Check: This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82.

> **Enabled –** When the field is toggled to Enabled, the relay agent will check the validity of the packet's option 82 fields. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.
>
> **Disabled -** When the field is toggled to Disabled, the relay agent will not check the validity of the packet's option 82 fields.

DHCP Relay Agent Information Option 82 Policy: This field can be toggled between Replace, Drop, and Keep by using the pull-down menu. It is used to set the Switches policy for handling packets when the **DHCP Agent Information Option 82 Check** is set to Disabled. The default is *Replace*.

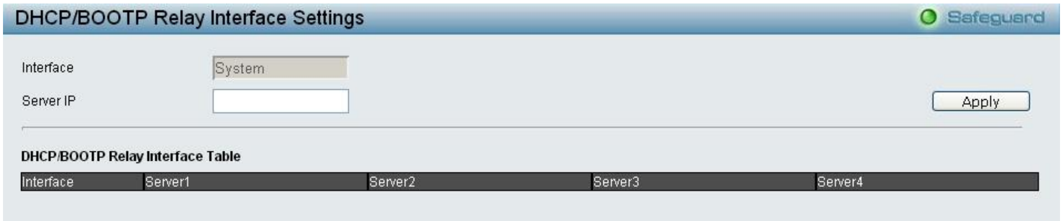
> **Replace -** The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.
>
> **Drop -** The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.
>
> **Keep -**The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.

DHCP Relay Agent Information Option 82 Remote ID: This field can be toggled between Default and User Define.

> **NOTE:** If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances, you might configure a client with the option-82 field. In this situation, you should disable the information-check feature so that the switch does not remove the option-82 field from the packet. You can configure the action that the switch takes when it receives a packet with existing option-82 information by configuring the **DHCP Agent Information Option 82 Policy**.

Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

This page allows the user to set up a server, by IP address, for relaying DHCP/BOOTP information the switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **BOOTP Relay Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking Delete button.



DHCP/BOOTP Relay Interface Settings

Interface: System

Server IP:

DHCP/BOOTP Relay Interface Table

Interface	Server1	Server2	Server3	Server4

Figure 4.78 - Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

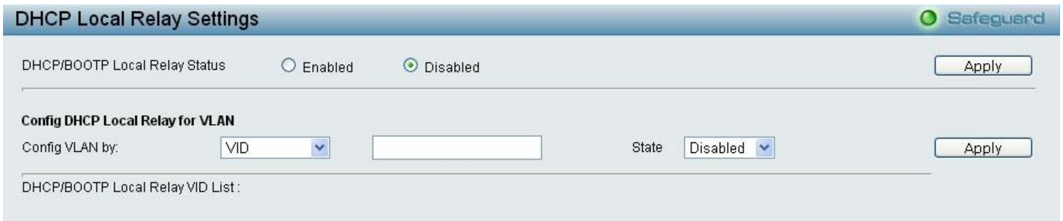
Interface: The IP interface on the Switch that will be connected directly to the Server.

Server IP: Enter the IP address of the DHCP/BOOTP server. Up to four server IPs can be configured per IP Interface.

Click **Apply** to implement changes made.

Configuration > DHCP Local Relay Settings

The DHCP Local Relay Settings page allows the user to configure DHCP Local Relay. DHCP broadcasts are trapped by the switch CPU, and replacement broadcasts are forwarded with Option 82. Replies from the DHCP servers are trapped by the switch CPU, the Option 82 is removed and the reply is sent to the DHCP Client.



DHCP Local Relay Settings

DHCP/BOOTP Local Relay Status ○ Enabled ● Disabled

Config DHCP Local Relay for VLAN

Config VLAN by: VID State: Disabled

DHCP/BOOTP Local Relay VID List :

Figure 4.79 - Configuration > DHCP Local Relay Settings

DHCP/BOOTP Local Relay Status: Specifies whether DHCP Local Relay is enabled on the device.

Enabled – Enables DHCP Local Relay on the device.

Disabled – Disables DHCP Local Relay on the device. This is the default value.

Config VLAN by: Configure the VLAN by VID or VLAN Name of drop-down menu.

State: Specifies whether DHCP Local Relay is enabled on the VLAN.

Enabled – Enables DHCP Local Relay on the VLAN.

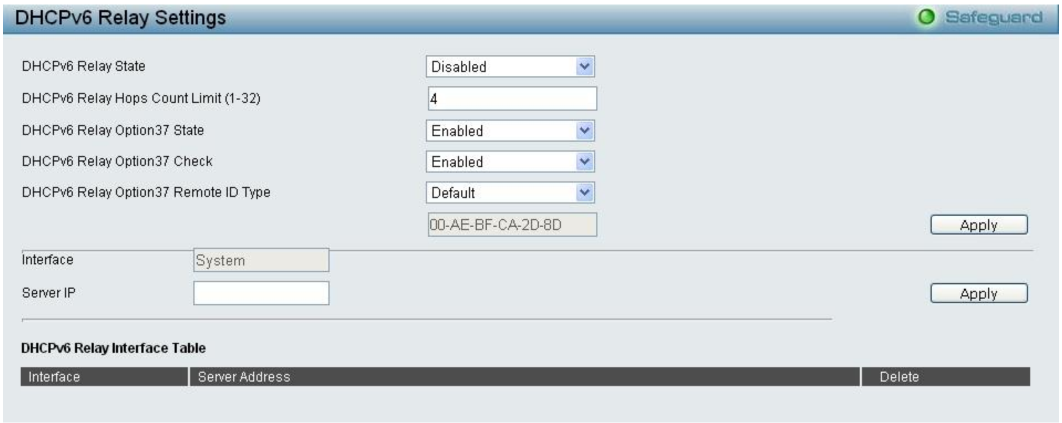
Disabled – Disables DHCP Local Relay on the VLAN.

DHCP Local Relay VID List: Displays the list of VLANs on which DHCP Local Relay has been defined.

Click **Apply** to implement changes made.

Configuration > DHCPv6 Relay Settings

The DHCPv6 Relay Settings page allows user to configure the DHCPv6 settings.



DHCPv6 Relay Settings

DHCPv6 Relay State	Disabled
DHCPv6 Relay Hops Count Limit (1-32)	4
DHCPv6 Relay Option37 State	Enabled
DHCPv6 Relay Option37 Check	Enabled
DHCPv6 Relay Option37 Remote ID Type	Default
	00-AE-BF-CA-2D-8D
Interface	System
Server IP	

DHCPv6 Relay Interface Table

Interface	Server Address	Delete

Figure 4.80 - Configuration > DHCPv6 Relay Settings

DHCPv6 Relay Status: Specifies whether DHCPv6 Relay is enabled on the device.

Enabled – Enables DHCPv6 Relay on the device.

Disabled – Disables DHCPv6 Relay on the device. This is the default value.

DHCPv6 Relay Hops Count Limit (1-32): The field allows and entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded. The default hop count is 4.

DHCPv6 Relay Option37 State: Specifies the DHCPv6 Relay Option37 State to be enabled or disabled.

DHCPv6 Relay Option37 Check: Specifies the DHCPv6 Relay Option37 Check to be enabled or disabled.

DHCPv6 Relay Option37 Remote ID Type: Specifies the DHCPv6 Relay Option37 Remote ID type is **CID with User Defined**, **User Defined** or **Default**.

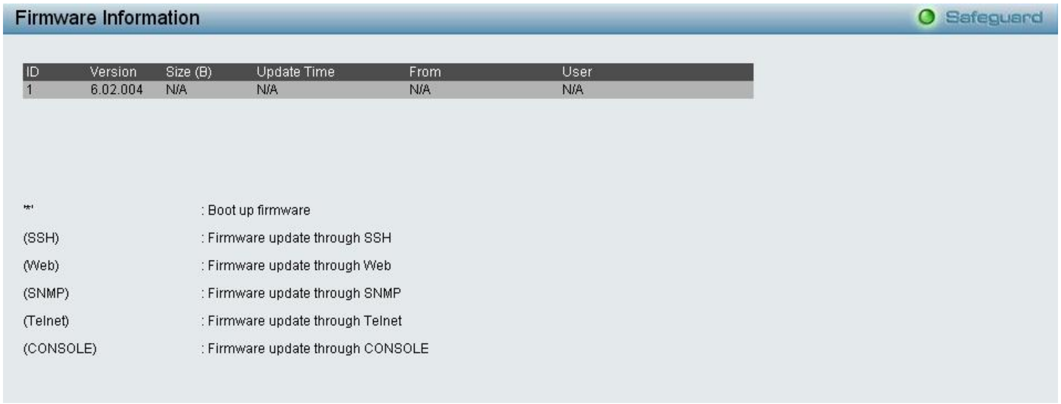
Interface: Enter a name of the interface.

Server IP: Enter the server IP address.

Click **Apply** to implement changes made.

Configuration > Firmware Information

The Firmware Information page displays the firmware detail information of device.



Firmware Information

ID	Version	Size (B)	Update Time	From	User
1	6.02.004	N/A	N/A	N/A	N/A

'*' : Boot up firmware
(SSH) : Firmware update through SSH
(Web) : Firmware update through Web
(SNMP) : Firmware update through SNMP
(Telnet) : Firmware update through Telnet
(CONSOLE) : Firmware update through CONSOLE

Figure 4.81 - Configuration > Firmware Information

Configuration > Spanning Tree > STP Bridge Global Settings

The Switch implements three versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1D STP and Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE802.1 specification. RSTP can operate with legacy equipment implementing IEEE 802.1D, however the advantages of using RSTP will be lost.

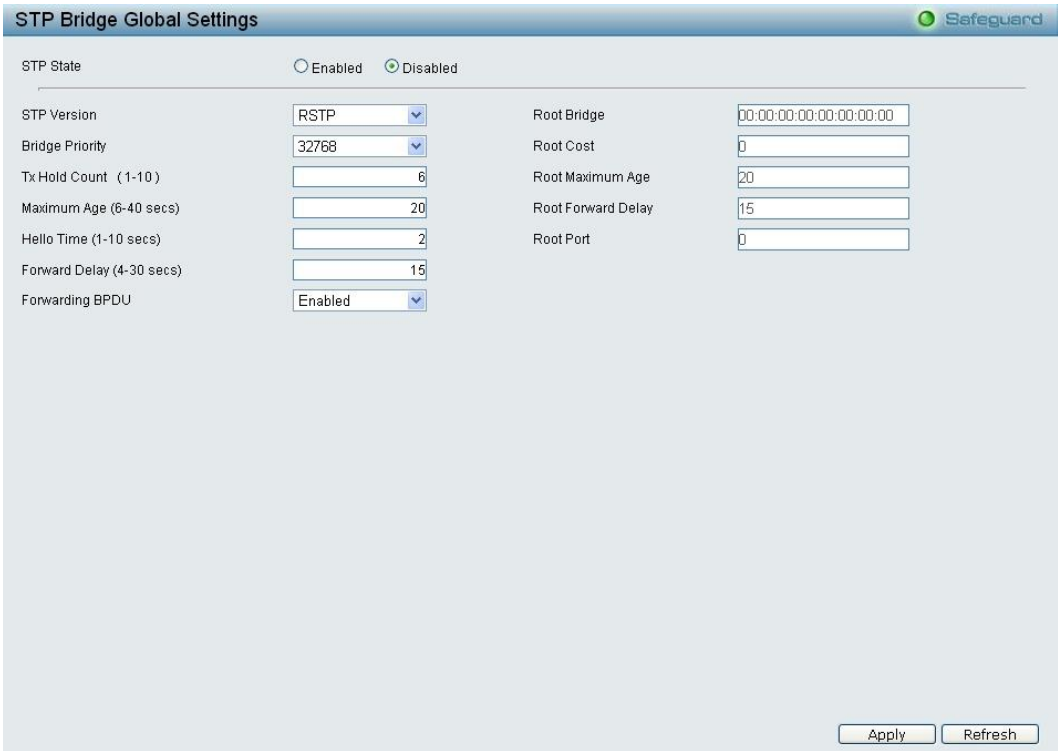
The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

The IEEE 802.1 Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment.

By default Multiple Spanning Tree is enabled. It will tag BPDU packets to receiving devices and distinguish spanning tree instances, spanning tree regions and the VLANs associated with them.

After enabling STP, setting the STP Global Setting includes the following options:



STP Bridge Global Settings

STP State ○ Enabled ● Disabled

STP Version	RSTP	Root Bridge	00:00:00:00:00:00:00:00
Bridge Priority	32768	Root Cost	0
Tx Hold Count (1-10)	6	Root Maximum Age	20
Maximum Age (6-40 secs)	20	Root Forward Delay	15
Hello Time (1-10 secs)	2	Root Port	0
Forward Delay (4-30 secs)	15		
Forwarding BPDU	Enabled		

Figure 4.82 - Configuration > Spanning Tree > STP Bridge Global Settings

Spanning Tree Protocol: Specify the Spanning Tree Protocol to be Enabled or Disabled.

STP Version: You can choose MSTP, RSTP or STP Compatible. The default setting is MSTP.

Bridge Priority: This value between 0 and 61410 specifies the priority for forwarding packets: the lower the value, the higher the priority. The default is *32768*.

TX Hold Count (1-10): Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6.*

Maximum Age (6-40 sec): This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and 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 the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between *6* and *40* seconds. The default value is *20*. (Max Age has to have a value bigger than Hello Time)

Hello Time (1-10 sec): The user may set the time interval between transmissions of configuration messages by the root device, thus stating that the Switch is still functioning. The default is *2* seconds.

Forward Delay (4-30 sec): This sets the maximum amount of time that the root device will wait before changing states. The default is *15* seconds.

Forwarding BPDU: Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface.

Enabled - BPDU filtering is enabled on the port.

Disabled - BPDU forwarding is enabled on the port (if STP is disabled).

Root Bridge: Displays the MAC address of the Root Bridge.

Root Cost: Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto).

Root Maximum Age: Displays the Maximum Age of the Root Bridge. The default is 20.

Root Forward Delay: Displays the Forward Delay of the Root Bridge. The default is 15.

Root port: Displays the root port.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

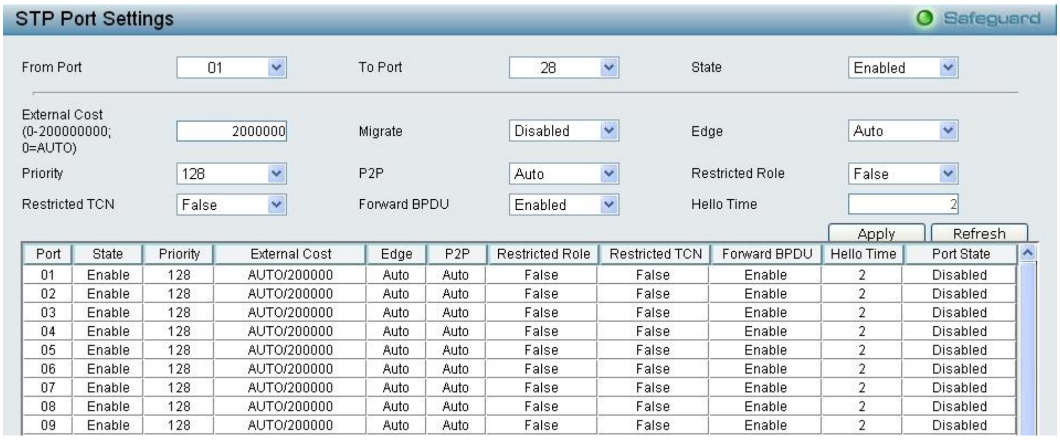
Configuration > Spanning Tree > STP Port Settings

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of the groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.



From Port	01	To Port	28	State	Enabled
External Cost (0-200000000; 0=AUTO)	2000000	Migrate	Disabled	Edge	Auto
Priority	128	P2P	Auto	Restricted Role	False
Restricted TCN	False	Forward BPDU	Enabled	Hello Time	2

Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Forward BPDU	Hello Time	Port State
01	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
02	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
03	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
04	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
05	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
06	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
07	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
08	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled
09	Enable	128	AUTO/200000	Auto	Auto	False	False	Enable	2	Disabled

Figure 4.83 – Configuration > Spanning Tree > STP Port Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

State: Use the drop-down menu to enable or disable STP by per-port based. It will be selectable after the global STP is enabled.

External Cost: This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Thedefault value is *0* (auto).

> **0 (auto) -** Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.
>
> **Value 1-200000000 -** Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

Migrate: Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.

Edge: Selecting the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Selecting the *False* parameter indicates that the port does not have edge port status. Selecting the *Auto* parameter indicates that the port have edge port status or not have edge port status automatically.

Priority: Specify the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port.

P2P: Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex.

Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *Auto*.

Restricted Role: Toggle between *True* and *False* to set the restricted role state of the packet. If set to *True*, the port will never be selected to be the Root port. The default value is *False*.

Restricted TCN: Toggle between *True* and *False* to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change. If set to *True*, it stops the port from propagating received TCN and to other ports. The default value is *False*.

Forwarding BPDU: Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are:

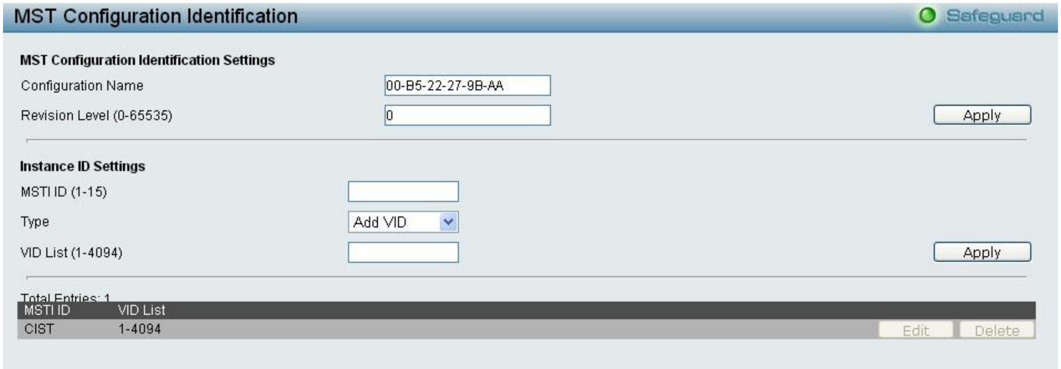
> *Disabled* – BPDU filtering is enabled on the port.
>
> *Enabled* – BPDU forwarding is enabled on the port (if STP is disabled).

Hello Time: The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. The default value is 2.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

Configuration > Spanning Tree > MST Configuration Identification

The MST Configuration Identification page allows user to configure a MSTI instance on the switch. These settings will uniquely identify a multiple spanning tree instance set on the switch. The Switch initially possesses one CIST or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.



MST Configuration Identification

MST Configuration Identification Settings

Configuration Name: 00-B5-22-27-9B-AA

Revision Level (0-65535): 0

Instance ID Settings

MSTI ID (1-15):

Type: Add VID

VID List (1-4094):

Total Entries: 1

MSTI ID	VID List		
CIST	1-4094	Edit	Delete

Figure 4.84 - Configuration > Spanning Tree > MST Configuration Identification

MST Configuration Identification Settings:

Configuration Name: A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the **STP Bridge Global Set-tings** window.

Revision Level: This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between *0* and *65535* with a default setting of *0*.

MSTI ID (1-15): Enter a number between *1* and *15* to set a new MSTI on the Switch.

Type: This field allows the user to choose a desired method for altering the MSTI settings.

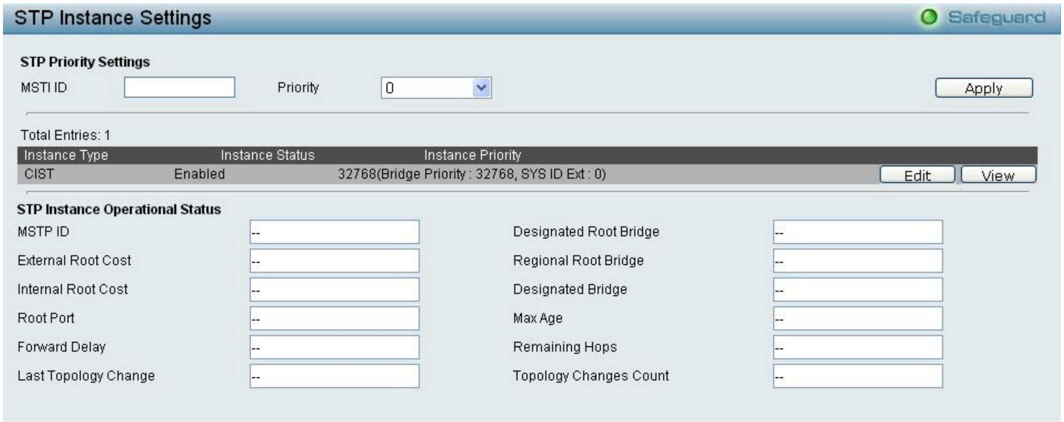
> **Add VID -** Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter.
>
> **Remote VID –** Select this parameter to remove VIDs from the MSTI ID, in con-junction with the VID List parameter.

VID List (1-4094): This field displays the VLAN IDs associated with the specific MSTI.

Click **Apply** to implement changes made.

Configuration > Spanning Tree > STP Instance Settings

The STP Instance Settings page display MSTIs currently set on the Switch and allows users to change the Priority of the MSTPs.



STP Instance Settings

STP Priority Settings

MSTI ID: Priority: 0

Total Entries: 1

Instance Type	Instance Status	Instance Priority		
CIST	Enabled	32768(Bridge Priority : 32768, SYS ID Ext : 0)	Edit	View

STP Instance Operational Status

MSTP ID	--	Designated Root Bridge	--
External Root Cost	--	Regional Root Bridge	--
Internal Root Cost	--	Designated Bridge	--
Root Port	--	Max Age	--
Forward Delay	--	Remaining Hops	--
Last Topology Change	--	Topology Changes Count	--

Figure 4.85 - Configuration > Spanning Tree > STP Instance Settings

To modify an entry on the table, click the **Edit** button. To view more information about and entry on the table at the top of the window, click the **view** button.

The window above contains the following information:

MSTI ID: Enter the MSTI ID in this field. An entry of *0* denotes the CIST (default MSTI).

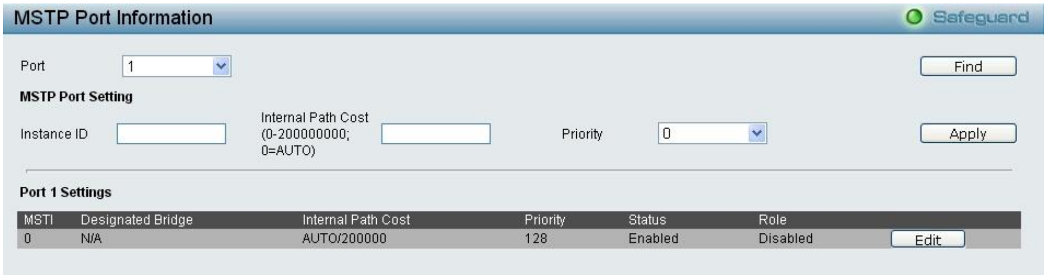
Priority: Enter the new priority in the Priority field. The user may set a priority value between *0-61440*.

Click **Apply** to implement the new priority setting.

Configuration > Spanning Tree > MSTP Port Information

The MSTP Port Information page can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked.

To View the MSTI settings for a particular port, select the Port number and click **Find** button. To modify the settings for a particular MSTI Instance, click **Edit** button, then modify the MSTP Port Setting and click **Apply**.



MSTP Port Information

Port: 1

MSTP Port Setting

Instance ID:

Internal Path Cost (0-200000000; 0=AUTO):

Priority: 0

Port 1 Settings

MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role	
0	N/A	AUTO/200000	128	Enabled	Disabled	Edit

Figure 4.86 - Configuration > Spanning Tree > MST Port Information

Instance ID: Displays the MSTI ID of the instance being configured. An entry of *0* in this field denotes the CIST (default MSTI).

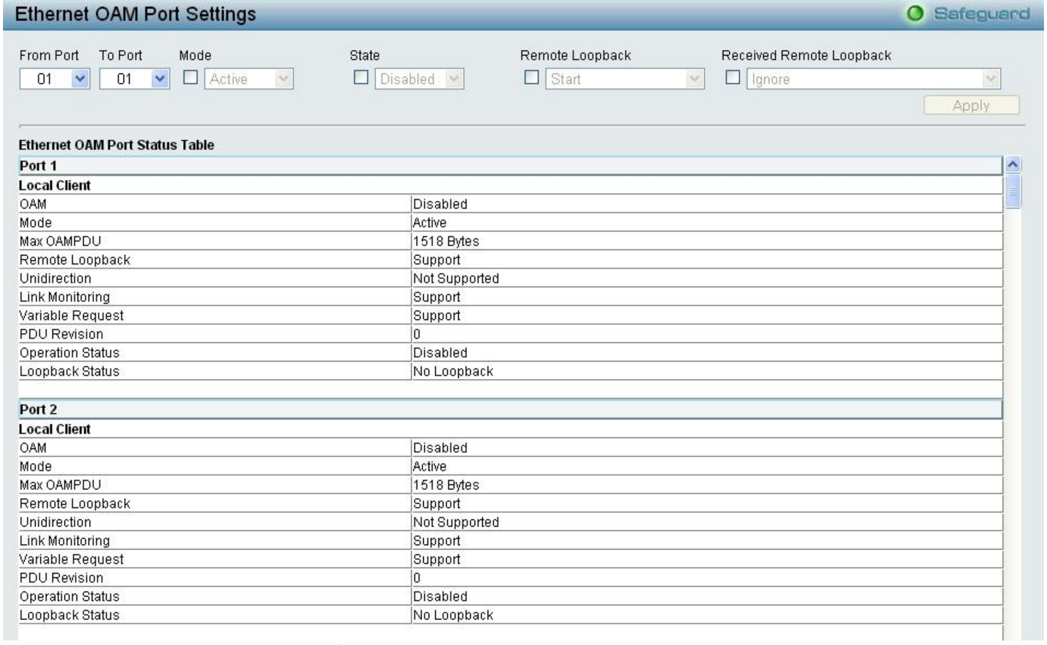
Internal Path Cost (0=Auto): This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *0* (auto).

> **0 (Auto) -** Selecting this parameter for the internal Cost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.
>
> **Value 0-2000000 -** Selecting this parameter with a value in the range of *0* to *2000000* will set the quickest route then a loop occurs. A lower Internal cost represents a quicker transmission.

Priority: Enter a value between *0* and *240* to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Configuration > Ethernet OAM > Ethernet OAM Port Settings

The Ethernet OAM Port Settings page allows user to configure the Ethernet OAM settings.



Ethernet OAM Port Settings

From Port	To Port	Mode	State	Remote Loopback	Received Remote Loopback
01	01	□ Active	□ Disabled	□ Start	□ Ignore

Ethernet OAM Port Status Table

Port 1	
Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Support
Unidirection	Not Supported
Link Monitoring	Support
Variable Request	Support
PDU Revision	0
Operation Status	Disabled
Loopback Status	No Loopback

Port 2	
Local Client	
OAM	Disabled
Mode	Active
Max OAMPDU	1518 Bytes
Remote Loopback	Support
Unidirection	Not Supported
Link Monitoring	Support
Variable Request	Support
PDU Revision	0
Operation Status	Disabled
Loopback Status	No Loopback

Figure 4.87 - Configuration > Ethernet OAM > Ethernet OAM Port Settings

From Port/To Port: Select a range of ports to be configured.

Mode: Use the drop-down menu to select to operate in either **Active** or **Passive**. The default mode is **Active**.

State: Use the drop-down menu to enable or disable the OAM function.

Remote Loopback: Specifies the Ethernet OAM remote loopback is None or Start.

None – Select to disable the remote loopback.

Start – Select to request the peer to change to the remote loopback mode.

Received Remote Loopback: To configure the client to process or to ignore the received Ethernet OAM remote loopback command.

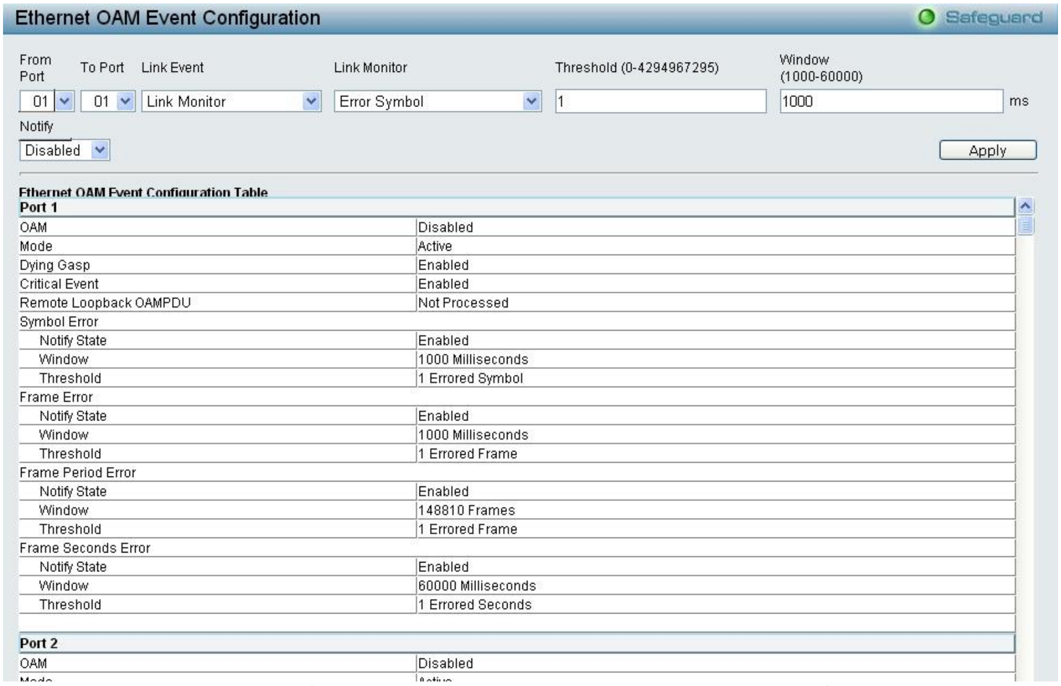
Process – Select to process the received Ethernet OAM remote loopback command.

Ignore – Select to ignore the received Ethernet OAM remote loopback command.

Click **Apply** to take effect.

Configuration > Ethernet OAM > Ethernet OAM Event Configuration

The Ethernet OAM Event Configuration page allows user to configure the Ethernet OAM configuration settings.



Ethernet OAM Event Configuration

From Port	To Port	Link Event	Link Monitor	Threshold (0-4294967295)	Window (1000-60000)
01	01	Link Monitor	Error Symbol	1	1000 ms

Notify: Disabled

Ethernet OAM Event Configuration Table

Port 1	
OAM	Disabled
Mode	Active
Dying Gasp	Enabled
Critical Event	Enabled
Remote Loopback OAMPDU	Not Processed
Symbol Error	
Notify State	Enabled
Window	1000 Milliseconds
Threshold	1 Errored Symbol
Frame Error	
Notify State	Enabled
Window	1000 Milliseconds
Threshold	1 Errored Frame
Frame Period Error	
Notify State	Enabled
Window	148810 Frames
Threshold	1 Errored Frame
Frame Seconds Error	
Notify State	Enabled
Window	60000 Milliseconds
Threshold	1 Errored Seconds
Port 2	
OAM	Disabled

Figure 4.88 - Configuration > Ethernet OAM > Ethernet OAM Event Configuration

From Port / To Port: Select a range of ports to be configured.

Link Event: Select the link event, **Link Monitor** or **Critical Link Event.**

Link Monitor: Select the link monitor. Avaliable options are **Error Symbol, Error Frame, Error Frame Period,** and **Error Frame Seconds.**

Threshold (0-4294967295): Enter the number of error frame or symbol in the period is required to be equal to or greater than in order for the event to be generated.

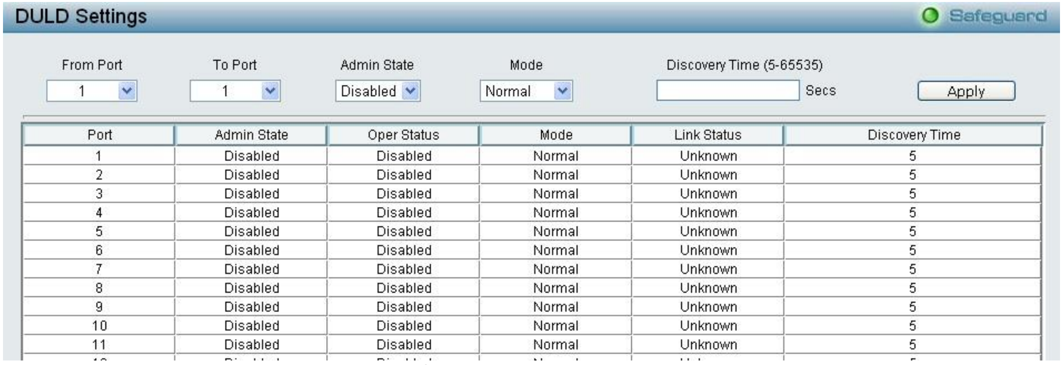
Window (1000-60000): Enter the period of error frame or symbol in milliseconds summary event.

Notify: Select the notification to be enabled or disabled.

Click the **Apply** button to accept the changes made.

Configuration > DULD > DULD Port Settings

The DULD Port Settings page allows user to configure the unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.



DULD Settings

From Port	To Port	Admin State	Mode	Discovery Time (5-65535)	
1	1	Disabled	Normal	Secs	Apply

Port	Admin State	Oper Status	Mode	Link Status	Discovery Time
1	Disabled	Disabled	Normal	Unknown	5
2	Disabled	Disabled	Normal	Unknown	5
3	Disabled	Disabled	Normal	Unknown	5
4	Disabled	Disabled	Normal	Unknown	5
5	Disabled	Disabled	Normal	Unknown	5
6	Disabled	Disabled	Normal	Unknown	5
7	Disabled	Disabled	Normal	Unknown	5
8	Disabled	Disabled	Normal	Unknown	5
9	Disabled	Disabled	Normal	Unknown	5
10	Disabled	Disabled	Normal	Unknown	5
11	Disabled	Disabled	Normal	Unknown	5

Figure 4.89 - Configuration > DULD > DULD Port Settings

From Port / To Port: Specifies a range of ports to be configured.

Admin State: Enable or disable the port unidirectional link detection status. The default is disabled.

Mode: Specifies the mode of DULD.

Normal – Only log and event when a unidirectional link is detected.

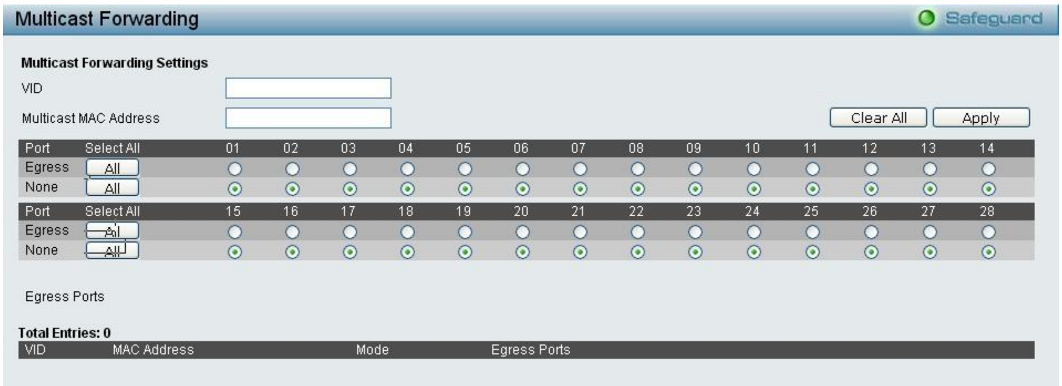
Shutdown – If any unidirectional link is detected, disable the port and log an event.

Discovery Time (5-65535): Specifies these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start. The default discovery time is **5** seconds.

Click the **Apply** button to take effect.

Configuration > Multicast Forwarding & Filtering > Multicast Forwarding

The Multicast Forwarding page displays all of the entries made into the Switch's static multicast forwarding table.



Multicast Forwarding

Multicast Forwarding Settings

VID

Multicast MAC Address

Clear All Apply

Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Egress	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
None	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Egress	All	○	○	○	○	○	○	○	○	○	○	○	○	○	○
None	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Egress Ports

Total Entries: 0

VID	MAC Address	Mode	Egress Ports

Figure 4.90 - Configuration > Multicast Forwarding & Filtering > Multicast Forwarding

VID: The VLAN ID of the VLAN to which the corresponding MAC address belongs.

Multicast MAC Address: The MAC address of the static source of multicast packets. This must be a multicast MAC address.

Port Settings: Allows the selection of ports that will be members of the static multicast group and ports either that are forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP.

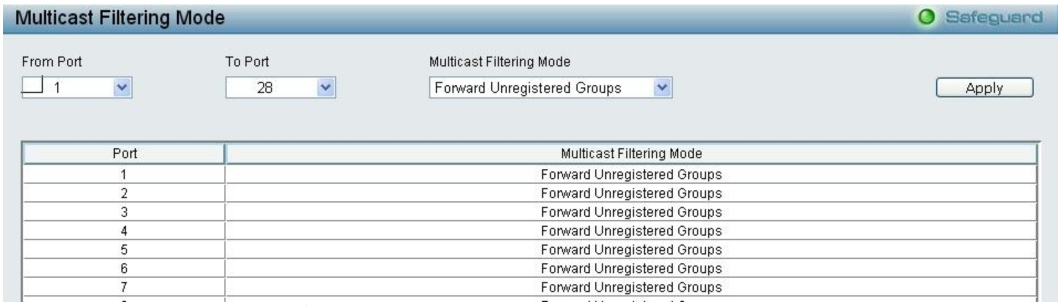
Egress - The port is a static member of the multicast group.

None - No restrictions on the port dynamically joining the multicast group. When **None** is chosen, the port will not be a member of the Static Multicast Group.

Click **Apply** or **Clear All** to implement changes made.

Configuration > Multicast Forwarding & Filtering > Multicast Filtering

The Multicast Filtering Mode page allows user to set up the filtering mode.



Multicast Filtering Mode

From Port: 1

To Port: 28

Multicast Filtering Mode: Forward Unregistered Groups

Port	Multicast Filtering Mode
1	Forward Unregistered Groups
2	Forward Unregistered Groups
3	Forward Unregistered Groups
4	Forward Unregistered Groups
5	Forward Unregistered Groups
6	Forward Unregistered Groups
7	Forward Unregistered Groups

Figure 4.91 - Configuration > Multicast Forwarding & Filtering > Multicast Filtering

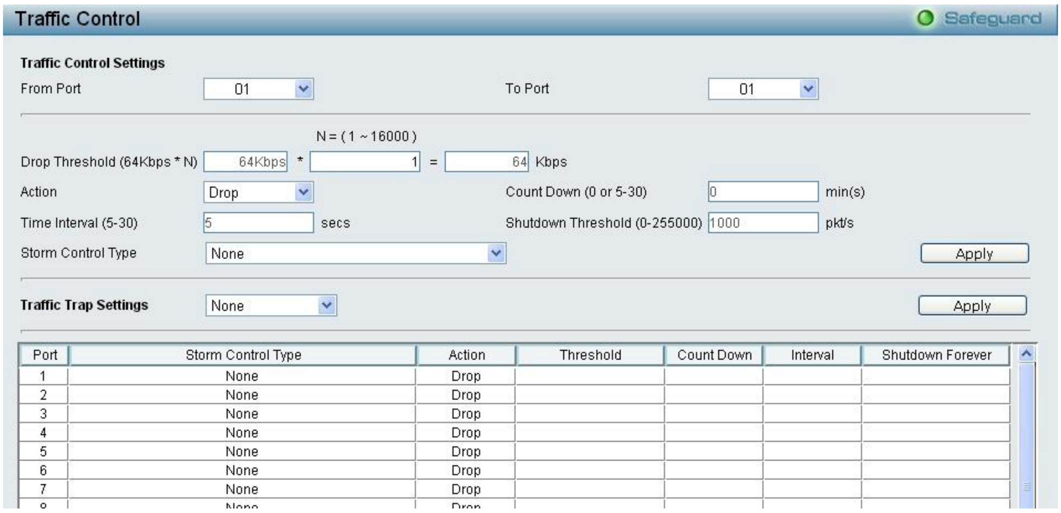
From Port / To Port: Specify the ports of the VLAN on which the corresponding MAC address belongs to.

Multicast Filtering Mode: This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.

> **Forward Unregistered Groups -** This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.
>
> **Filter Unregistered Groups -** This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above.

QoS > Traffic Control

The Traffic Control feature provides the ability to control the receive rate of broadcast, multicast, and unknown unicast packets. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.



Traffic Control

Traffic Control Settings

From Port: 01

To Port: 01

N = (1 ~ 16000)

Drop Threshold (64Kbps * N): 64Kbps * 1 = 64 Kbps

Action: Drop

Count Down (0 or 5-30): 0 min(s)

Time Interval (5-30): 5 secs

Shutdown Threshold (0-255000): 1000 pkt/s

Storm Control Type: None

Traffic Trap Settings: None

Port	Storm Control Type	Action	Threshold	Count Down	Interval	Shutdown Forever
1	None	Drop				
2	None	Drop				
3	None	Drop				
4	None	Drop				
5	None	Drop				
6	None	Drop				
7	None	Drop				

Figure 4.92 – QoS > Traffic Control

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

Drop Threshold (64Kbps * N): If storm control is enabled (default is disabled), the threshold is from of 64 ~ 1,024,000 Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000.

Action: Select the method of traffic control from the pull down menu. The choices are:

> Drop – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.
>
> Shutdown – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in rest mode and if no action is taken will enter auto-recovery mode after a five minute period. Choosing this option obligates the user to configure the interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.

Count Down (0 or 5-30): The count down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are 0, 5-30 minutes. 0 denotes that the port will never shutdown.

Time Interval (5-30): The interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The interval may be set between 5 and 30 seconds with the default setting of 5 seconds.

Shutdown Threshold (0-255000): Specify the shutdown threshold for traffic threshold.

Storm Control Type: User can select the different Storm type from Broadcast, Multicast, Broadcast + Multicast, Unknown Unicast, Broadcast + Unknown Unicast, Multicast + Unknown Unicast, and Broadcast + Multicast + Unknown Unicast.

Click **Apply** for the settings to take effect.

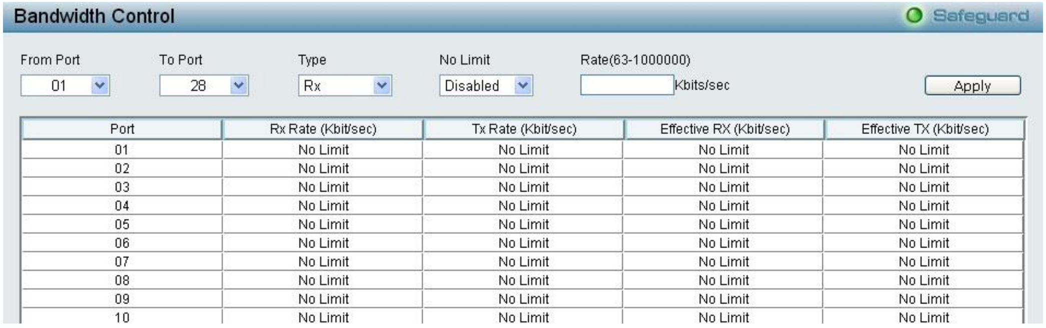
NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation.

NOTE: Ports that are in the rest mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.

NOTE: Ports that are in rest mode will be seen as link down in all windows and screens until it enters the auto-recovery mode or the user recovers these ports by configuring the port state.

QoS > Bandwidth Control

The Bandwidth Control page allows network managers to define the bandwidth settings for a specified port's transmitting and receiving data rates.



Bandwidth Control

From Port	To Port	Type	No Limit	Rate(63-1000000)	
01	28	Rx	Disabled	Kbits/sec	Apply

Port	Rx Rate (Kbit/sec)	Tx Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
01	No Limit	No Limit	No Limit	No Limit
02	No Limit	No Limit	No Limit	No Limit
03	No Limit	No Limit	No Limit	No Limit
04	No Limit	No Limit	No Limit	No Limit
05	No Limit	No Limit	No Limit	No Limit
06	No Limit	No Limit	No Limit	No Limit
07	No Limit	No Limit	No Limit	No Limit
08	No Limit	No Limit	No Limit	No Limit
09	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit

Figure 4.93 – QoS > Bandwidth Control

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

Type: This drop-down menu allows you to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit: This drop-down menu allows you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.

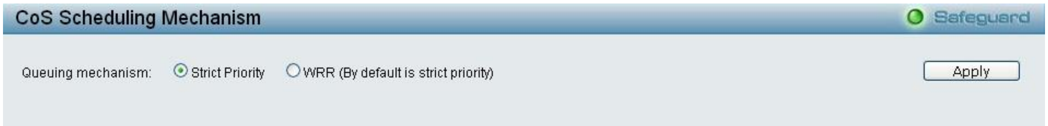
Rate (63-1024000): This field allows you to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 63 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports.

NOTE: The TX rate for Gigabit ports can only be configured in multiples of 1850kbps. If any other value is used, the system automatically rounds it down to the lower multiple of 1850.

QoS > CoS Scheduling Mechanism

The CoS Scheduling Mechanism page allows user to select between a **WRR** and a **Strict** mechanism for emptying the priority classes.



CoS Scheduling Mechanism

Queuing mechanism: ● Strict Priority ○ WRR (By default is strict priority)

Figure 4.94 - QoS > CoS Scheduling Mechanism

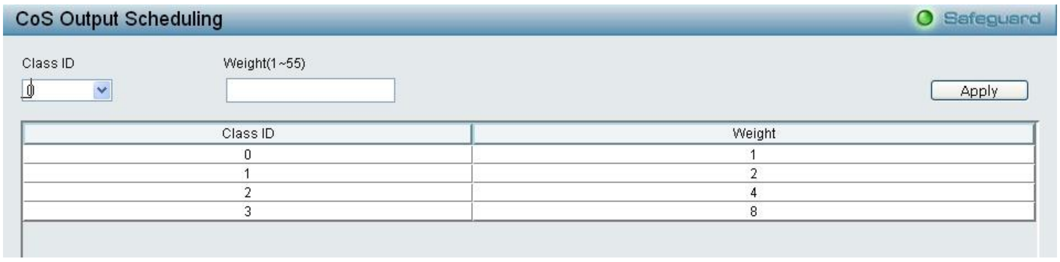
Strict Priority: Denoting a Strict scheduling will set the highest queue to be emptied first while the other queues will follow the weighted round-robin scheduling scheme

WRR: Use the weighted round-robin (WRR) algorithm to handle packets in an even distribution in priority classes of service.

Click **Apply** to let your changes take effect.

QoS > CoS Output Scheduling

CoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to CoS implementation, careful consideration should be given to how network traffic in lower priority classes of service is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the CoS settings are not suitable.



CoS Output Scheduling

Class ID: 0

Weight(1~55):

Class ID	Weight
0	1
1	2
2	4
3	8

Figure 4.95 - QoS > CoS Output Scheduling

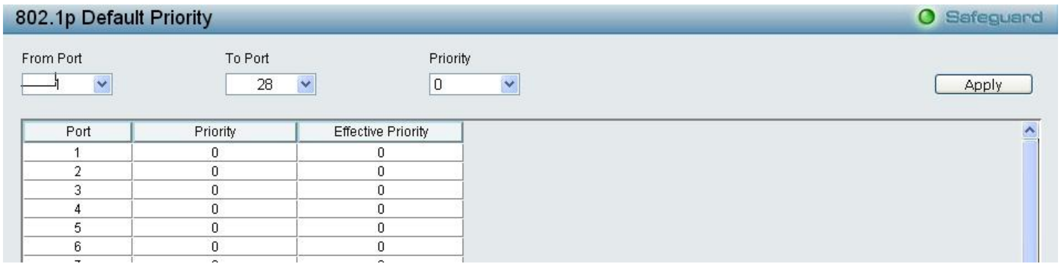
Class ID: Specify the priority queue for the switch. The value is from *0* to *3*.

Weight (1-55): Specify the weight for a CoS. The value is from *1* to *55*.

Click **Apply** to let your changes take effect.

QoS > 802.1p Default Priority

QoS is an implementation of the IEEE 802.1p standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Thus with larger bandwidth, less critical traffic is limited, and therefore excessive bandwidth can be saved.



802.1p Default Priority

From Port: 1

To Port: 28

Priority: 0

Port	Priority	Effective Priority
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0

Figure 4.96 - QoS > 802.1p Default Priority

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

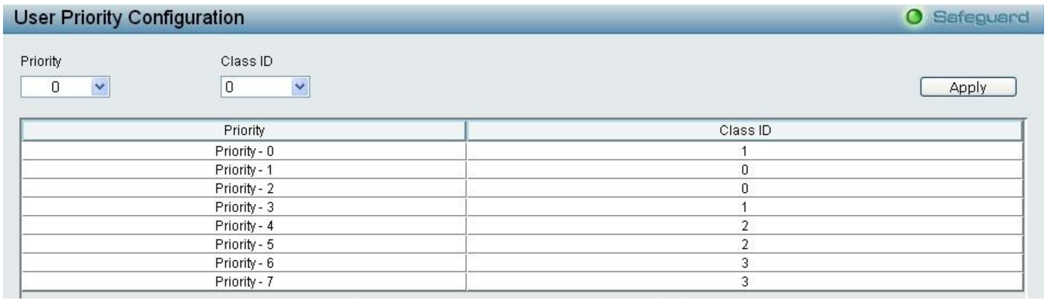
Priority: Defines the priority assigned to the port. The priority are 0~7.

Click **Apply** to implement changes made.

QoS > 802.1p User Priority

When using 802.1p priority mechanism, the packet is examined for the presence of a valid 802.1p priority tag. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues.

The Switch allows the assignment of a class of service to each of the 802.1p priorities.



User Priority Configuration

Priority: 0

Class ID: 0

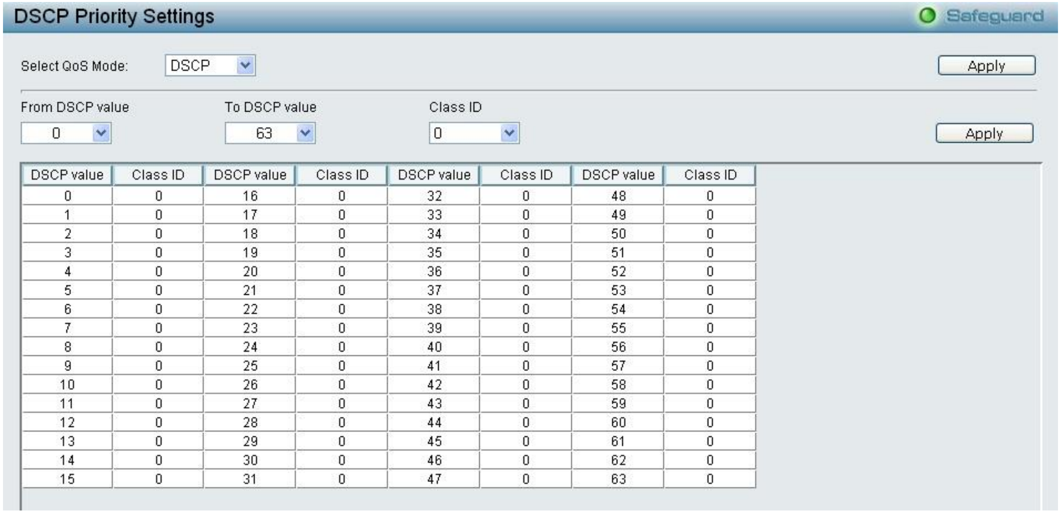
Priority	Class ID
Priority - 0	1
Priority - 1	0
Priority - 2	0
Priority - 3	1
Priority - 4	2
Priority - 5	2
Priority - 6	3
Priority - 7	3

Figure 4.97 - QoS > 802.1p User Priority

Once the user had assigned a priority to the port groups on the Switch, you can then assign this Class to each of the four levels of 802.1p priorities. Click **Apply** to set your changes.

QoS > DSCP Priority Settings

When using the DSCP priority mechanism, the packet is classified based on the DSCP field in the IP header. If the tag is present, the packet is assigned to a programmable egress queue based on the value of the tagged priority. The tagged priority can be designated to any of the available queues. When a packet is received containing this DSCP tag, it will be mapped to the CoS queue configured here. These settings will only take effect if at least one of the priority settings per port is configured for DSCP.When DSCP is set to enable, TOS cannot be used, and when TOS is set to enable, DSCP cannot be used.



DSCP Priority Settings

Select QoS Mode: DSCP

From DSCP value: 0

To DSCP value: 63

Class ID: 0

DSCP value	Class ID	DSCP value	Class ID	DSCP value	Class ID	DSCP value	Class ID
0	0	16	0	32	0	48	0
1	0	17	0	33	0	49	0
2	0	18	0	34	0	50	0
3	0	19	0	35	0	51	0
4	0	20	0	36	0	52	0
5	0	21	0	37	0	53	0
6	0	22	0	38	0	54	0
7	0	23	0	39	0	55	0
8	0	24	0	40	0	56	0
9	0	25	0	41	0	57	0
10	0	26	0	42	0	58	0
11	0	27	0	43	0	59	0
12	0	28	0	44	0	60	0
13	0	29	0	45	0	61	0
14	0	30	0	46	0	62	0
15	0	31	0	47	0	63	0

Figure 4.98 - QoS > DSCP Priority Settings

Select QoS Mode: Specify the mode to be DASP or TOS.

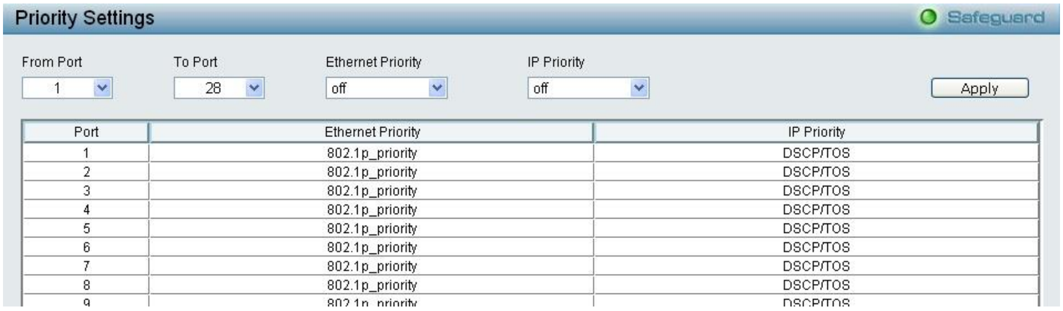
From DSCP value / To DSCP value: Specify the range of DSCP values.

Class ID: Specify the priority queue for the switch. The value is from *0* to *3*.

Click **Apply** to implement changes made.

QoS > Priority Settings

The Priority Setting page allow users to configure the CoS priority settings on a port or ports. When CoS tagged packets arrive on the switch, they are mapped to the settings configured here. For example, if a port has been assigned a MAC priority, the packet that has the CoS priority assigned to a MAC address will be sent to the CoS queue configured for that MAC address. Once the configuration has been completed, users may see the results in the Priority Settings Table seen here. After configuring the port priorities, users may adjust the individual CoS settings on the other windows located in the CoS folder of the Switch.



Priority Settings

From Port	To Port	Ethernet Priority	IP Priority
1	28	off	off

Port	Ethernet Priority	IP Priority
1	802.1p_priority	DSCP/TOS
2	802.1p_priority	DSCP/TOS
3	802.1p_priority	DSCP/TOS
4	802.1p_priority	DSCP/TOS
5	802.1p_priority	DSCP/TOS
6	802.1p_priority	DSCP/TOS
7	802.1p_priority	DSCP/TOS
8	802.1p_priority	DSCP/TOS
9	802.1p_priority	DSCP/TOS

Figure 4.99 - QoS > Priority Settings

From Port/To Port: Users may select a port or group of ports to assign the priority settings.

Port Priority: Specify the Port Priority is *Off* or *On* on the port.

Ethernet Priority: Specify the Ethernet Priority is Off or 802.1p on the port.

IP Priority: Specify the IP Priority is Off or DSCP on the port.

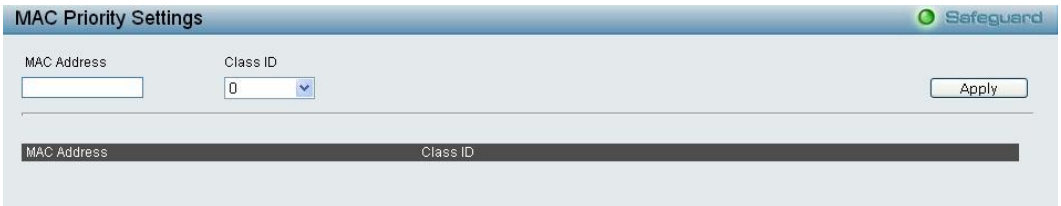
Click **Apply** to implement changes made.

QoS > MAC Priority Settings

When using the MAC Priority mechanism, the packet is classified based on the MAC address field priority in the MAC priority table entries.

To configure a destination MAC address for a CoS queue, users must adhere to the following steps:

1. Once a destination MAC has been added to the FDB, users must then configure the appropriate queue to be mapped to this destination MAC address, using the following window.
2. Once the previous parameters are set, users should go to the **Priority Settings** window located in this folder and set the egress ports on the switch to **MAC Priority**. These ports must only be set for MAC Priority and not for any other priority choice. Please be advised that the default priority setting is for 802.1p and users must change the priority to MAC Priority for this function to work properly. Be sure that the device with this destination MAC address is connected to the port for which this priority is configured.



MAC Priority Settings

MAC Address	Class ID
	0

MAC Address	Class ID

Figure 4.100 - QoS > MAC Priority Settings

Enter the destination **MAC Address** and select a **Class ID** where packets containing this destination MAC address will be sent. Click **Apply** to implement changes made.

QoS > IP Priority Settings

When using the IP Priority mechanism, the packet is classified based on the IP address field priority in the IP priority table entries.

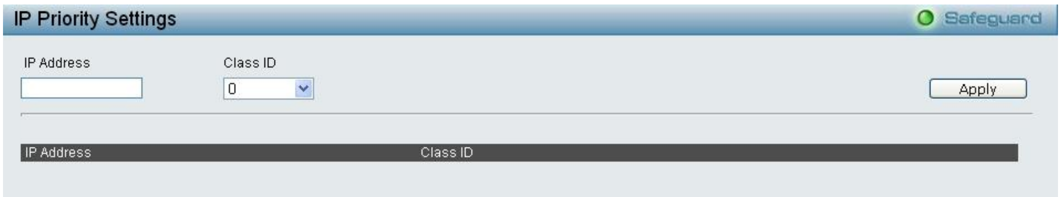


Figure 4.101 - QoS > IP Priority Settings

Enter the IP **Address** and select a Class ID where packets containing this destination IP address will be sent. Click **Apply** to implement changes made.

QoS > IPv6 Priority Settings

When using the IPv6 Priority mechanism, the packet is classified based on the IP address field priority in the IP priority table entries.

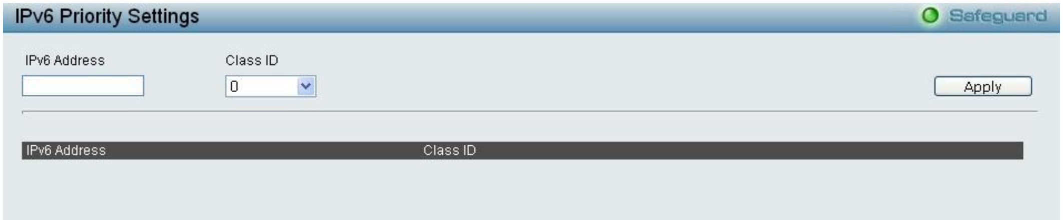


Figure 4.102 - QoS > IPv6 Priority Settings

Enter the **IP Address** and select a Class ID where packets containing this destination IP address will be sent. Click **Apply** to implement changes made.

QoS > IPv6 Traffic Class Priority Settings

The IPv6 Traffic Class Priority Settings page allows user to configure the priority of traffic class.

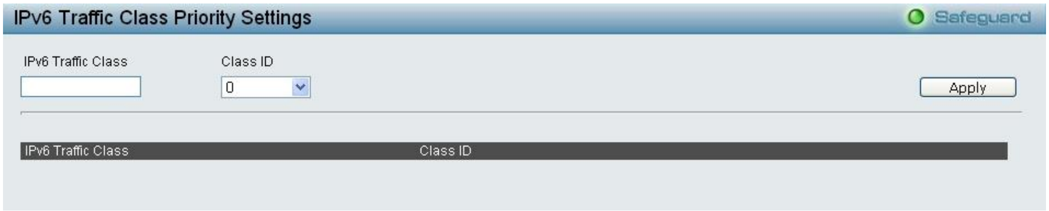


Figure 4.103 - QoS > IPv6 Traffic Class Priority Settings

Enter the **IPv6 Traffic Class** and select a Class ID where packets containing this traffic class address will be sent.

Click **Apply** to implement changes made.

QoS > TCP/UDP Port Priority Settings

When using the TCP/UDP Port Priority mechanism, the packet is classified based on the TCP/UDP field priority in the TCP/UDP priority table entries. The TCP/UDP port number now supports with IPv0034.

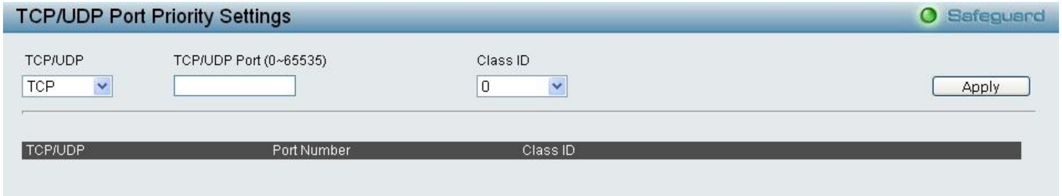


Figure 4.104 - QoS > TCP/UDP Port Priority Settings

TCP/UDP: Specify the port priority to be TCP or UDP.

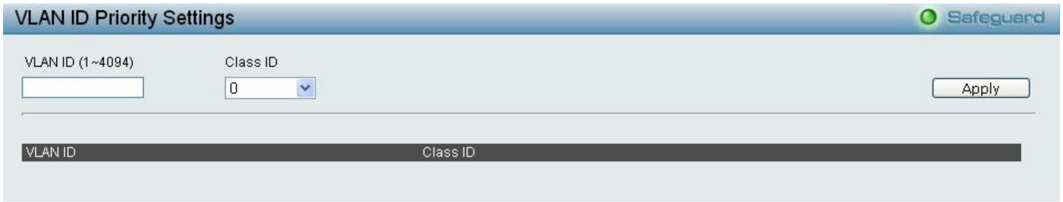
TCP/UDP Port (0-65535): Specify the TCP/UDP port number.

Class ID: Defines the Class ID assigned to the port. The priority Class ID fields are 0-3.

Click **Apply** to implement changes made.

QoS > VLAN ID Priority Settings

When using the VLAN ID Priority mechanism, the packet is classified based on the VLAN ID field priority in the VLAN ID priority table entries.



VLAN ID (1~4094):

Class ID: 0

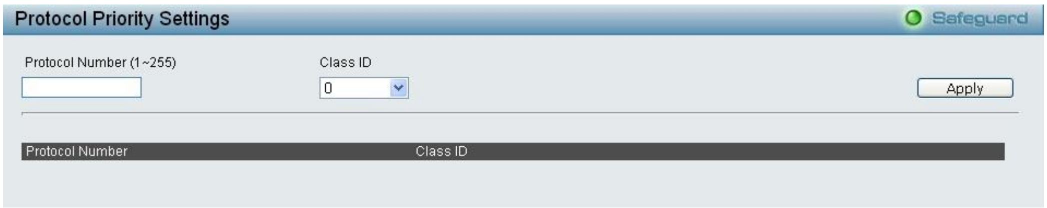
VLAN ID	Class ID

Figure 4.105 - QoS > VLAN ID Priority Settings

Enter **VLAN ID** and select a **Class ID** where packets containing this VLAN ID will be sent. Click **Apply** to implement changes made.

QoS > Protocol Priority Settings

When using the Protocol Priority mechanism, the packet is classified based on the Protocol Number field priority in the Protocol priority table entries.



Protocol Number (1~255):

Class ID: 0

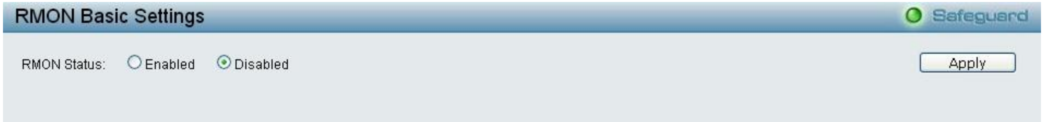
Protocol Number	Class ID

Figure 4.106 - QoS > Protocol Priority Settings

Enter **Protocol Number** and select a **Class ID** where packets containing this Protocol will be sent. Click **Apply** to implement changes made.

RMON > RMON Basic Settings

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch. In addition, RMON Rising and Falling Alarm Traps can be enabled and disabled. Click **Apply** to make effects.

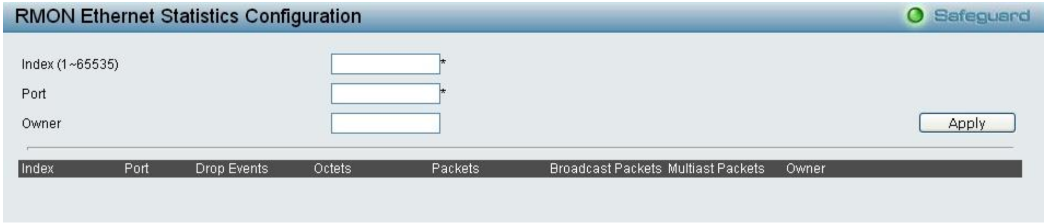


RMON Status: ○ Enabled ● Disabled

Figure 4.107 - RMON > RMON Basic Settings

RMON > RMON Ethernet Statistics Configuration

The RMON Statistics Configuration page displays the information of RMON Ethernet Statistics and allows the user to configure the settings.



Index (1~65535) *

Port *

Owner

Index	Port	Drop Events	Octets	Packets	Broadcast Packets	Multiast Packets	Owner

Figure 4.108 - RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:

Index (1 - 65535): Indicates the RMON Ethernet Statistics entry number.

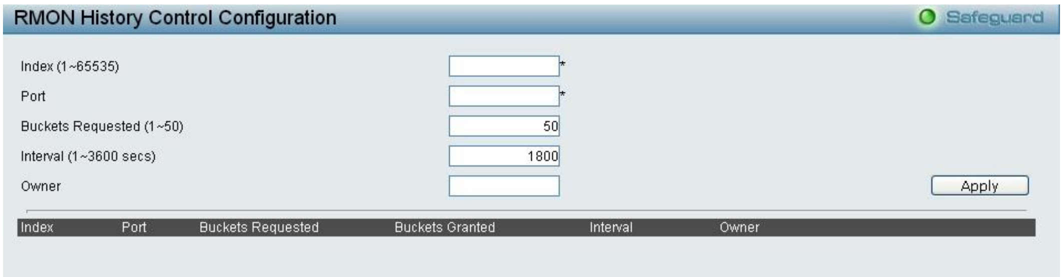
Port: Specifies the port from which the RMON information was taken.

Owner: Displays the RMON station or user that requested the RMON information.

Click **Apply** to make the configurations take effects.

RMON > RMON History Control Configuration

The RMON History Control Configuration page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.



Index (1~65535) *

Port *

Buckets Requested (1~50) 50

Interval (1~3600 secs) 1800

Owner

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner

Figure 4.109 - RMON > RMON History Control Configuration

The History Control Configuration contains the following fields:

Index (1 - 65535): Indicates the history control entry number.

Port: Specifies the port from which the RMON information was taken.

Buckets Requested (1 ~ 50): Specifies the number of buckets that the device saves.

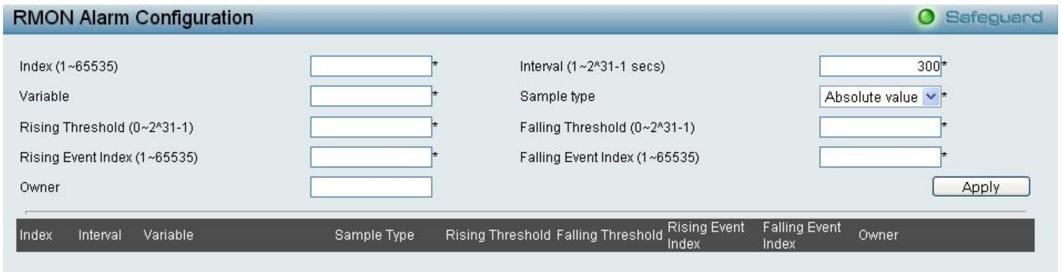
Interval (1 ~ 3600): Indicates in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes).

Owner: Displays the RMON station or user that requested the RMON information.

Click **Apply** to make the configurations take effects.

RMON > RMON Alarm Configuration

The RMON Alarm Configuration page allows the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.



Index (1~65535) *

Variable *

Rising Threshold (0~2^31-1) *

Rising Event Index (1~65535) *

Owner

Interval (1~2^31-1 secs) 300*

Sample type Absolute value *

Falling Threshold (0~2^31-1) *

Falling Event Index (1~65535) *

Index	Interval	Variable	Sample Type	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner

Figure 4.110 - RMON > RMON Alarm Settings

The configuration contains the following fields:

Index (1 - 65535): Indicates a specific alarm.

Variable: Specify the selected MIB variable value.

Rising Threshold (0 ~ 2^31-1): Displays the rising counter value that triggers the rising threshold alarm.

Rising Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Owner: Displays the device or user that defined the alarm.

Interval (1 ~ 2^31-1): Defines the alarm interval time in seconds.

Sample type: Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

> **Delta value –** Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
>
> **Absolute value –** Compares the values directly with the thresholds at the end of the sampling interval.

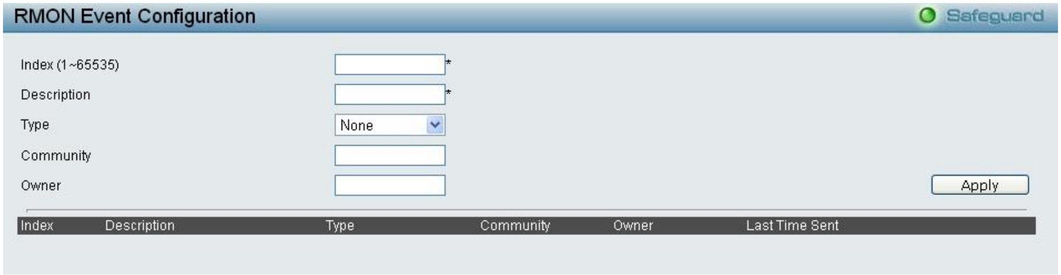
Falling Threshold (0 ~ 2^31-1): Displays the falling counter value that triggers the falling threshold alarm.

Falling Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Click **Apply** to make the configurations take effects.

RMON > RMON Event Configuration

The RMON Event page contains fields for defining, modifying and viewing RMON events statistics.



RMON Event Configuration

Index (1~65535) *

Description *

Type: None

Community

Owner

Index	Description	Type	Community	Owner	Last Time Sent

Figure 4.111 - RMON > RMON Event Configuration

The RMON Events Page contains the following fields:

Index (1~ 65535): Displays the event.

Description: Specifies the user-defined event description.

Type: Specifies the event type. The possible values are:

None – Indicates that no event occurred.

Log – Indicates that the event is a log entry.

SNMP Trap – Indicates that the event is a trap.

Log and Trap – Indicates that the event is both a log entry and a trap.

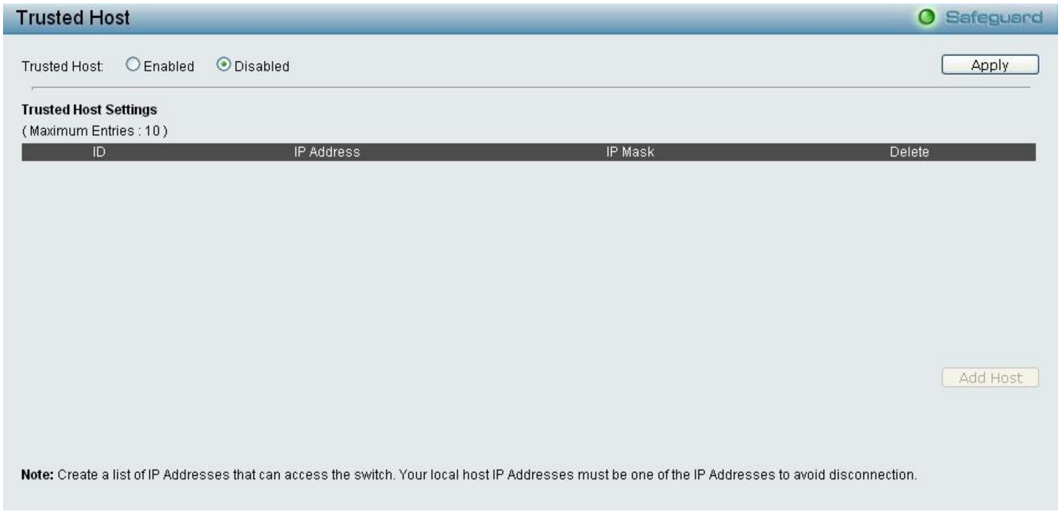
Community: Specifies the community to which the event belongs.

Owner: Specifies the time that the event occurred.

Click **Apply** to add a new RMON event.

Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. You can enter up to ten designated management stations networks by defining the IP address/Subnet Mask as seen in the figure below.



Trusted Host

Trusted Host: ○ Enabled ● Disabled

Trusted Host Settings

(Maximum Entries : 10)

ID	IP Address	IP Mask	Delete

Note: Create a list of IP Addresses that can access the switch. Your local host IP Addresses must be one of the IP Addresses to avoid disconnection.

Figure 4.112 - Security > Trusted Host

To define a management station IP setting, click the **Add Host** button and type in the IP address and Subnet mask. Click the **Apply** button to save your settings. You may permit only single or a range of IP addresses by different IP mask settings, the format can either be 192.168.1.1/255.255.255.0 or 192.168.0.1/24. Please see the example below for permitting the IP range

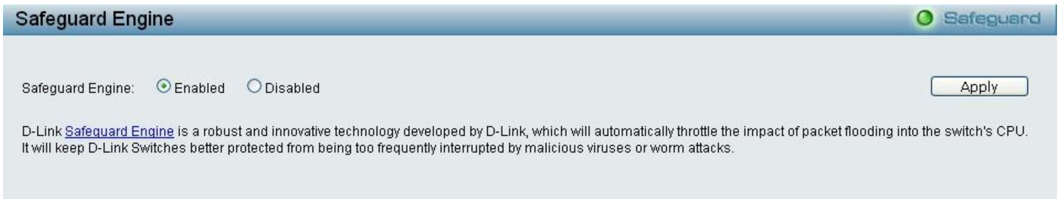
IP Address	Subnet Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255

172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

To delete the IP address, simply click the **Delete** button. Check the unwanted address, and then click **Apply**.

Security > Safeguard Engine

D-Link's **Safeguard Engine** is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps protect the Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.



Safeguard Engine: ● Enabled ○ Disabled

D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU. It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

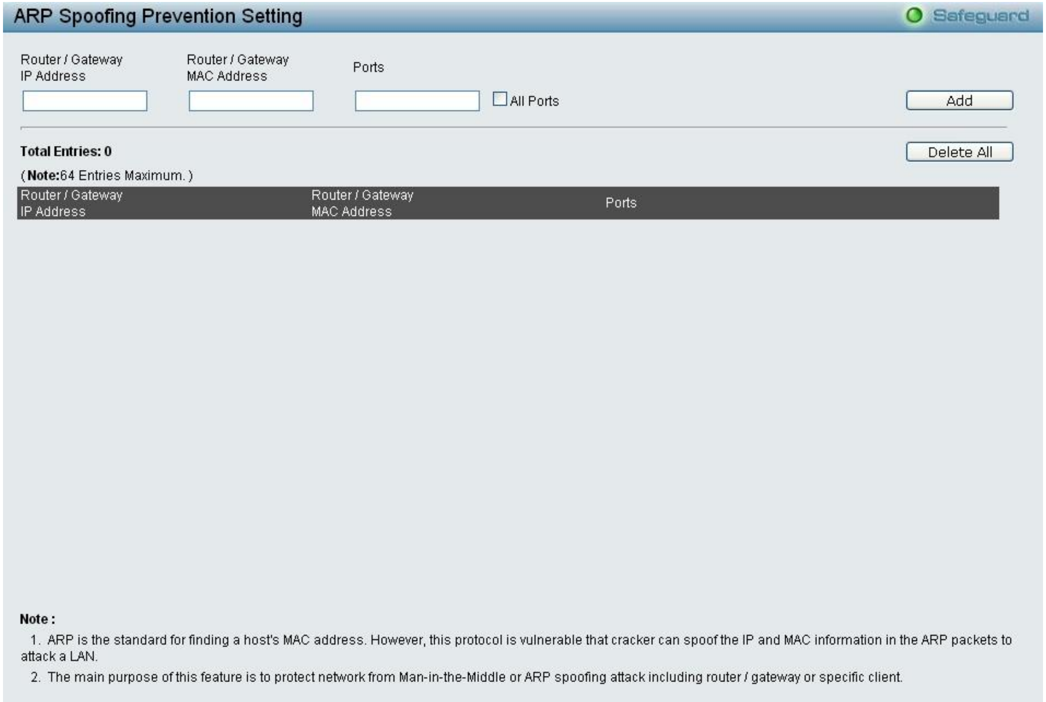
Figure 4.113 – Security > Safeguard Engine

Security > ARP Spoofing Prevention

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network by allowing an attacker to sniff data frames on a LAN, modifying the traffic, or stopping the traffic (known as a Denial of Service – DoS attack). The main idea of ARP spoofing is to send fake or spoofed ARP messages to an Ethernet network. It associates the attacker's or random MAC address with the IP address of another node such as the default gateway. Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one gratuitous ARP to the network claiming to be the gateway, so that the whole network operation is turned down as all packets to the Internet will be directed to the wrong node.

The ARP Spoofing Prevention function can discard the ARP Spoofing Attack in the network by checking the gratuitous ARP packets and filtering those with illegal IP or MAC addresses.


ARP Spoofing Prevention Setting
Safeguard
Router / Gateway IP Address
Router / Gateway MAC Address
Ports
□ All Ports
Add
Delete All

Total Entries: 0

(Note:64 Entries Maximum.)

Router / Gateway IP Address	Router / Gateway MAC Address	Ports

Note :

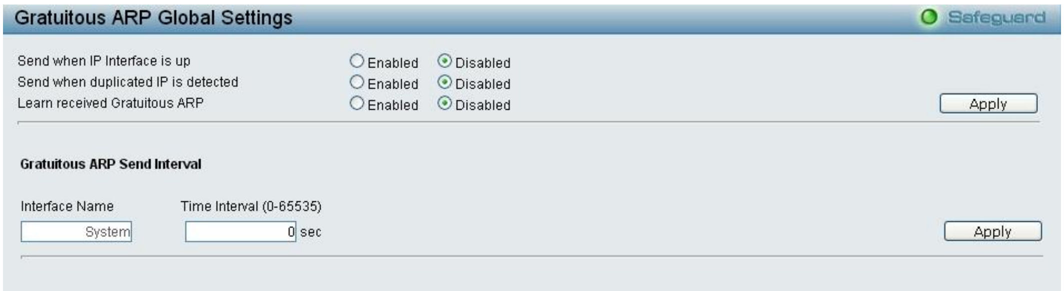
1. ARP is the standard for finding a host's MAC address. However, this protocol is vulnerable that cracker can spoof the IP and MAC information in the ARP packets to attack a LAN.
2. The main purpose of this feature is to protect network from Man-in-the-Middle or ARP spoofing attack including router / gateway or specific client.

Figure 4.114 – Security > ARP Spoofing Prevention Setting

Enter the **IP Address**, **MAC Address**, **Ports** and then click **Add** to create a checking/filtering rule. Click **Delete** to remove an existing rule and **Delete All** to clear all the entries.

Security > Gratuitous ARP

The Gratuitous ARP page shows the settings on the Switch. An ARP announcement (also known as Gratuitous ARP) is a packet (usually an ARP Request) containing a valid SHA (Sender Hardware Address) and SPA (Sender Protocol Address) for the host which sent it, with TPA (Target Protocol Address) equal to SPA. Such a request is not intended to solicit a reply, but merely update the ARP caches of other hosts which receive the packet and determine if there are any IP conflicts.



Gratuitous ARP Global Settings

Send when IP Interface is up ○ Enabled ● Disabled
Send when duplicated IP is detected ○ Enabled ● Disabled
Learn received Gratuitous ARP ○ Enabled ● Disabled

Gratuitous ARP Send Interval

Interface Name: System
Time Interval (0-65535): 0 sec

Figure 4.115 – Security > Gratuitous ARP

Send when IP Interface is up: This is used to enable/disable the sending of gratuitous ARP request packets while an IP interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is *Disabled*, and only one ARP packet will be broadcast.
Send when duplicated IP is detected: This is used to enable/disable the sending of gratuitous ARP request packets while a duplicate IP is detected. By default, the state is *Disabled*. Duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address.
Learn received Gratuitous ARP: This is used to enable/disable updating ARP cache based on the received gratuitous ARP packet. If a switch receives a gratuitous ARP packet and the sender's IP address in its ARP table, it should update the ARP entry. This is D*isabled* by default.

Gratuitous ARP Send Interval: Specify the interval value.

Interface Name: Specify the Interface Name.

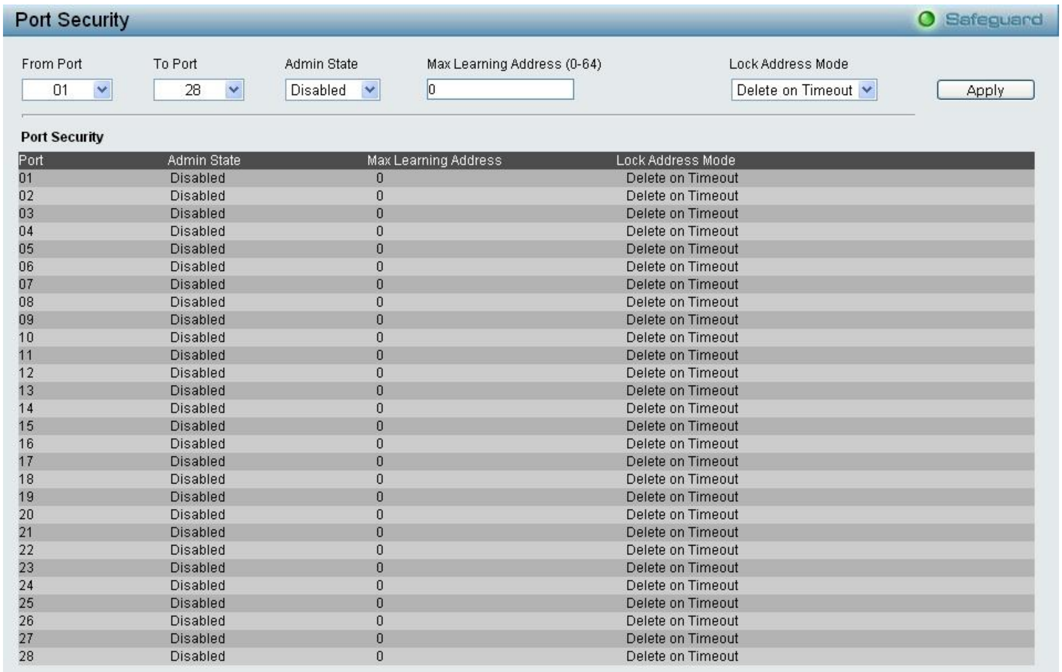
Time Interval (0-65535): Specify the time interval, the range is from 0 to 65535, and the default is 0 seconds.

Click **Apply** to make configurations make effects.

Security > Port Security

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port is enabled.



Port Security

From Port	To Port	Admin State	Max Learning Address (0-64)	Lock Address Mode
01	28	Disabled	0	Delete on Timeout

Port Security

Port	Admin State	Max Learning Address	Lock Address Mode
01	Disabled	0	Delete on Timeout
02	Disabled	0	Delete on Timeout
03	Disabled	0	Delete on Timeout
04	Disabled	0	Delete on Timeout
05	Disabled	0	Delete on Timeout
06	Disabled	0	Delete on Timeout
07	Disabled	0	Delete on Timeout
08	Disabled	0	Delete on Timeout
09	Disabled	0	Delete on Timeout
10	Disabled	0	Delete on Timeout
11	Disabled	0	Delete on Timeout
12	Disabled	0	Delete on Timeout
13	Disabled	0	Delete on Timeout
14	Disabled	0	Delete on Timeout
15	Disabled	0	Delete on Timeout
16	Disabled	0	Delete on Timeout
17	Disabled	0	Delete on Timeout
18	Disabled	0	Delete on Timeout
19	Disabled	0	Delete on Timeout
20	Disabled	0	Delete on Timeout
21	Disabled	0	Delete on Timeout
22	Disabled	0	Delete on Timeout
23	Disabled	0	Delete on Timeout
24	Disabled	0	Delete on Timeout
25	Disabled	0	Delete on Timeout
26	Disabled	0	Delete on Timeout
27	Disabled	0	Delete on Timeout
28	Disabled	0	Delete on Timeout

Figure 4.116 - Security > Port Security

The Port Security page contains the following fields:

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

Admin State: This pull-down menu allows users to enable or disable Port Security (locked MAC address table for the selected ports).

Max. Learning Address (0-64): The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.

Lock Address Mode: This pull-down menu allows you to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are:

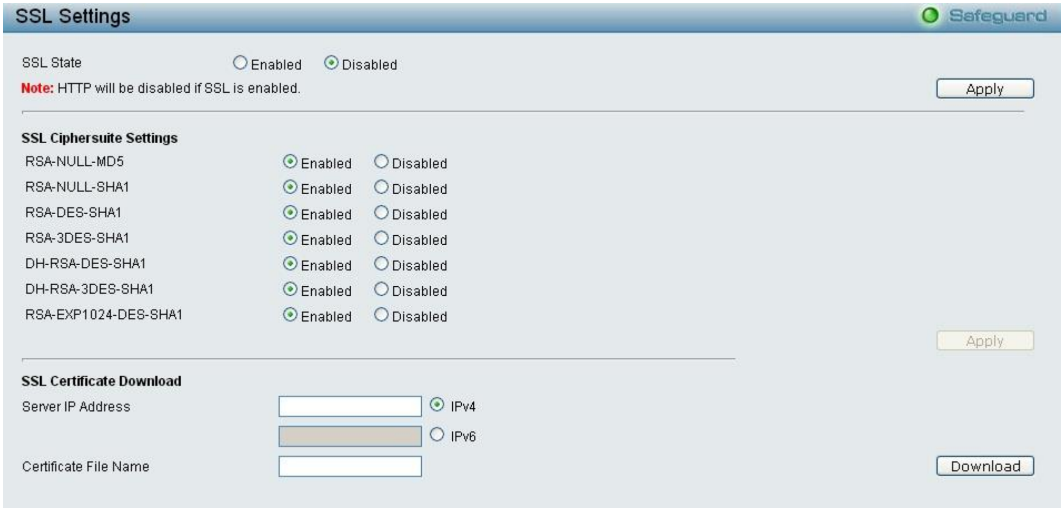
> **Delete On Reset –** The locked addresses will not age out until the Switch has been reset.
>
> **Delete On Timeout –** The locked addresses will age out after the aging timer expires.
>
> **Permanent –** The locked addresses will not age out after the aging timer expires.

Click **Apply** to make configurations make effects.

Security > SSL Settings

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between a Web Management host and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes.

This page allows you to configure the SSL global state and the Ciphersuite settings. Select **Enable** or **Disable** and then click **Apply** to change the SSL state or the Ciphersuite settings of the Switch. By default, SSL is **Disabled** and all Ciphersuites are **Enabled**.



SSL Settings

SSL State ○ Enabled ● Disabled

Note: HTTP will be disabled if SSL is enabled.

SSL Ciphersuite Settings

RSA-NULL-MD5	● Enabled	○ Disabled
RSA-NULL-SHA1	● Enabled	○ Disabled
RSA-DES-SHA1	● Enabled	○ Disabled
RSA-3DES-SHA1	● Enabled	○ Disabled
DH-RSA-DES-SHA1	● Enabled	○ Disabled
DH-RSA-3DES-SHA1	● Enabled	○ Disabled
RSA-EXP1024-DES-SHA1	● Enabled	○ Disabled

SSL Certificate Download

Server IP Address ● IPv4 ○ IPv6

Certificate File Name

Figure 4.117 - Security > SSL Settings

The SSL Settings page allows users to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. The Switch is shipped with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

Server IP Address: Select IPv4 or IPv6 and enter the IP address of the TFTP server where the certificate files are located.

Certificate File Name: Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)

Click **Download** to download the certificate file.

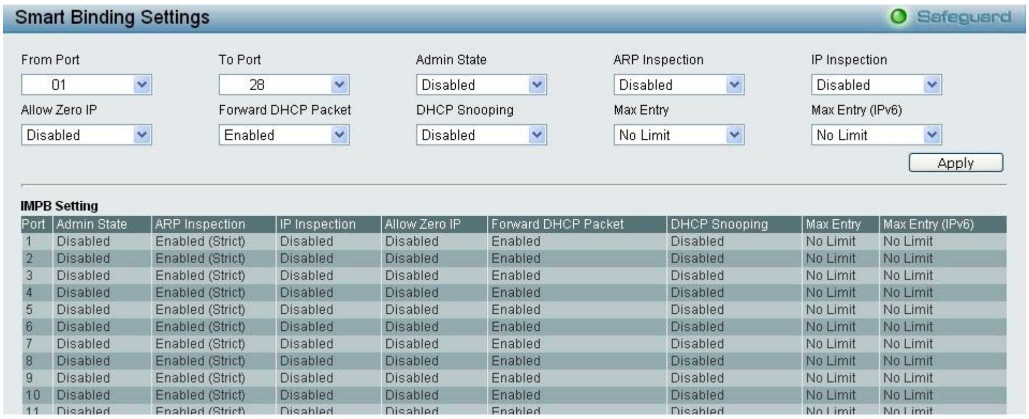
NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

Security > Smart Binding > Smart Binding Settings

The primary purpose of Smart Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

The Smart Binding function is port-based, meaning that a user can enable or disable the function on any individual port. Once Smart Binding is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the “IMPB white list”.

Users can enable or disable the **Packet Inspection** and **DHCP Snooping** on the Switch.



From Port	To Port	Admin State	ARP Inspection	IP Inspection
01	28	Disabled	Disabled	Disabled

Allow Zero IP	Forward DHCP Packet	DHCP Snooping	Max Entry	Max Entry (IPv6)
Disabled	Enabled	Disabled	No Limit	No Limit

IMPB Setting

Port	Admin State	ARP Inspection	IP Inspection	Allow Zero IP	Forward DHCP Packet	DHCP Snooping	Max Entry	Max Entry (IPv6)
1	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
2	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
3	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
4	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
5	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
6	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
7	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
8	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
9	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
10	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit
11	Disabled	Enabled (Strict)	Disabled	Disabled	Enabled	Disabled	No Limit	No Limit

Figure 4.118 – Security > Smart Binding > Smart Binding Settings

The Smart Binding Settings page contains the following fields:

From Port/ To Port: Select a range of ports to set for IP-MAC-port binding.

Admin State: Use the drop-down menu to enable or disable these ports for Smart Binding.

Enabled –Enable Smart Binding with related configurations to the ports

Disabled –Disable Smart Binding.

ARP Inspection: If ARP inspection is enabled, the Switch will inspect incoming ARP packets and compare them with the Switch's Smart Binding white list entries. If the IP-MAC pair of an ARP packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources. However, it cannot block malicious users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets.

IP Inspection: When IP Inspection is enabled, and ARP Inspection is disabled, all non-IP packets are forwarded by default. If **ARP Inspection** and **IP Inspection** mode are enabled, the Switch will inspect all incoming ARP and IP packets and compare them to the IMPB white list. If the IP-MAC pair find a match in the white list, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the mode examines every ingress ARP and IP packet, it enforces better security.

Allow Zero IP: Enable or disable to allow zero IP to configure the state which allows ARP packets with 0.0.0.0 source IP to bypass.

Forward DHCP Packet: Enable or disable to forward DHCP packet.

DHCP Snooping: By enable DHCP Snooping, the switch will snoop the packets sent from DHCP Server and clients, and update information to the White List.

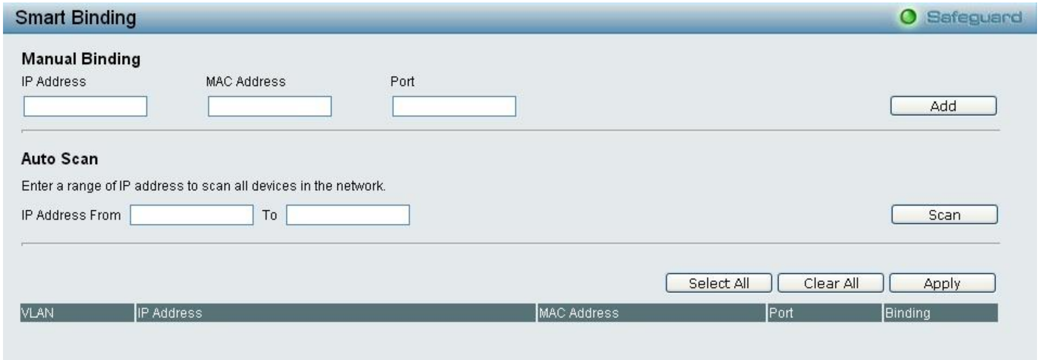
Max Entry: Specifies the max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Max Entry(IPv6): Specifies the IPv6 max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Click **Apply** to make configurations make effects.

Security > Smart Binding > Smart Binding

The Smart Binding Settings page allows the user to create Static IP-MAC-Port Binding entries on the Switch.



Manual Binding

IP Address MAC Address Port

Auto Scan

Enter a range of IP address to scan all devices in the network.

IP Address From To

VLAN	IP Address	MAC Address	Port	Binding

Figure 4.119 – Security > Smart Binding > Smart Binding

The Manual Binding Settings contains the following fields:

IP Address: Specifies the IP address to bind to the MAC address set below.

MAC Address: Specifies the MAC address to bind to the IP address set above.

Port: Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click **Add** to add a new entry.

Auto Scan: Specifies to scan connected devices in a range of IP address.

IP Address From/To: Specifies the range of IP Address to scan all devices in the network.

Click **Scan** and the search results will be listed in below table.

Binding: check the box to select desired binding devices.

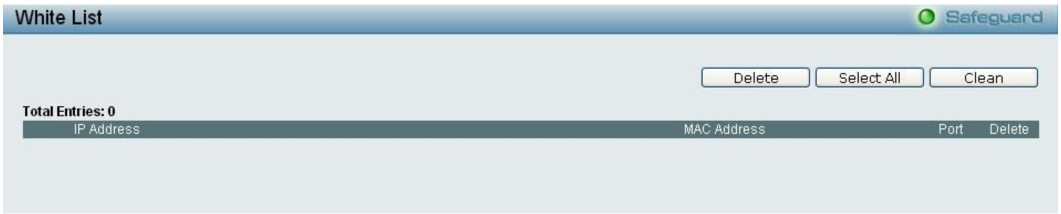
Apply: click **Apply** to set IP-MAC-Port Binding entries.”

Select All: to check the boxes of Binding for all found devices.

Clear All: to cancel the box of Binding.

Security > Smart Binding > White List

When IP+ARP Inspection Mode were selected, the White List page displays finished IP-MAC-Port Binding entries from page Smart Binding. Only IP packets or ARP packets carrying matched IP-MAC-Port information can access to the switch. You can cancel a device’s authorization by deleting it from the table.



White List

Total Entries: 0

IP Address	MAC Address	Port	Delete

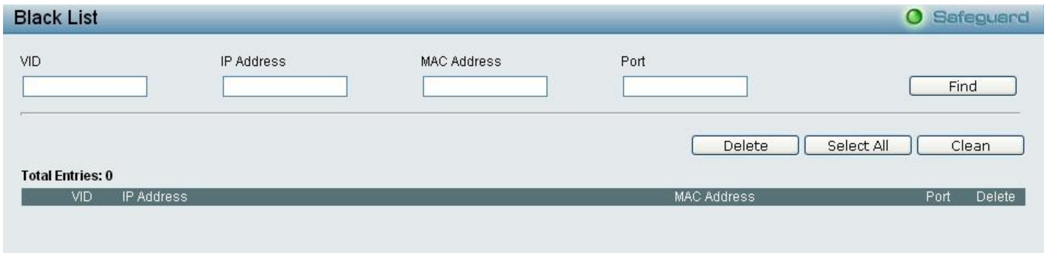
Figure 4.120 – Security > Smart Binding > White List

Select the check box of entry then click **Delete** to remove it.

Click **Select All** to select all entries of the table or click **Clean** to select none entries. Please keep at least one management host in the White List.

Security > Smart Binding > Black List

The Black List page shows unauthorized accesses. When ARP Inspection is selected and a device sends out an ARP packet containing unmatched IP-MAC-Port information, the device will be forbidden and listed here.



Black List

Total Entries: 0

VID	IP Address	MAC Address	Port	Delete

Figure 4.121 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below then click **Find** to search for a list of the entry:

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

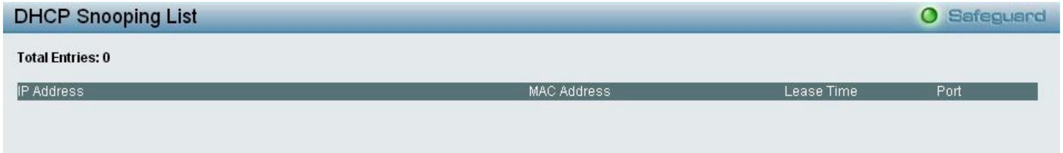
Port: Enter the port number which the device connects.

Check a box of **Delete** column to release an entry from the forbidden list then click **Apply** to delete an entry from the list.

Click **Select All** to select all entries, or click **Clean** to select none of the entries.

Security > Smart Binding > DHCP Snooping List

The DHCP Snooping List page shows the DHCP Snooping list.



DHCP Snooping List

Total Entries: 0

IP Address	MAC Address	Lease Time	Port

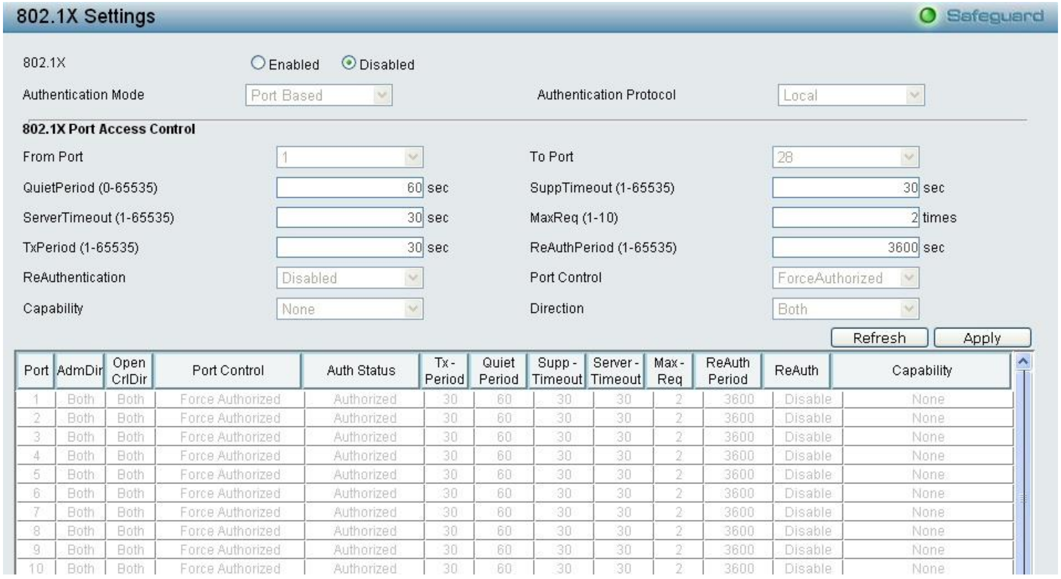
Figure 4.122 – Security > Smart Binding > DHCP Snooping List

Security > 802.1X > 802.1X Settings

Network switches provide easy and open access to resources by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.



802.1X Settings

802.1X ○ Enabled ● Disabled

Authentication Mode: Port Based

Authentication Protocol: Local

802.1X Port Access Control

From Port: 1

To Port: 28

QuietPeriod (0-65535): 60 sec

SuppTimeout (1-65535): 30 sec

ServerTimeout (1-65535): 30 sec

MaxReq (1-10): 2 times

TxPeriod (1-65535): 30 sec

ReAuthPeriod (1-65535): 3600 sec

ReAuthentication: Disabled

Port Control: ForceAuthorized

Capability: None

Direction: Both

Port	AdmDir	Open CrlDir	Port Control	Auth Status	Tx - Period	Quiet Period	Supp - Timeout	Server - Timeout	Max - Req	ReAuth Period	ReAuth	Capability
1	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
2	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
3	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
4	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
5	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
6	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
7	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
8	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
9	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None
10	Both	Both	Force Authorized	Authorized	30	60	30	30	2	3600	Disable	None

Figure 4.123 - Security > 802.1X > 802.1X Settings

By default, 802.1X is disabled. To use EAP for security, select enabled and set the **Authentication Mode** and **Authentication Protocol** then click **Apply**.

Authentication Mode: Indicates the 802.1X mode enabled on the device. The possible field values are:

Port Based – Enables 802.1X on ports. This is the default value.

MAC Based – Enables 802.1X on MAC addresses.

Authentication Protocol: Indicates the 802.1X Protocol on the device. The possible field values are *Local* and *RADIUS EAP*.

From Port/To Port: Enter the port or ports to be set.

QuietPeriod (0 – 65535 sec): Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is *60* seconds.

ServerTimeout (1 – 65535 sec): Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is *30* seconds.

TxPeriod (1 – 65535 sec): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. Default is *30* seconds.

ReAuthentication: Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.

Capability: Indicates the capability of the 802.1X. The possible field values are:

> **Authenticator –** Specify the Authenticator settings to be applied on a per-port basis.
>
> **None –** Disable 802.1X functions on the port.

SuppTimeout (1 – 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is *30* seconds.

MaxReq (1 – 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. Default is *2* times.

ReAuthPeriod (1 – 65535 sec): A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.

Port Control: This allows user to control the port authorization state.

> Select **ForceAuthorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.
>
> If **ForceUnauthorized** is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.
>
> If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.
>
> The default setting is *Auto***.**

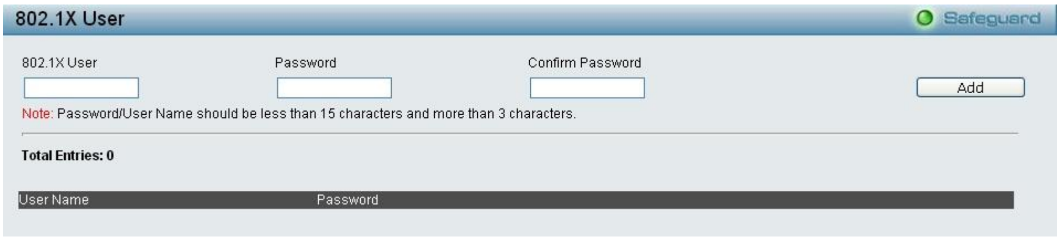
Direction: Sets the administrative-controlled direction on the port. The possible field values are:

> **Both –** Specify the control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
>
> **In –** Disables the support in the present firmware release.

Click **Apply** to implement configuration changes.

Security > 802.1X > 802.1X User

The **802.1X User** page allows user to set different local users on the Switch. Enter a **802.1X User** name, **Password** and **Confirm Password**. Properly configured local users will be displayed in the table.



Note: Password/User Name should be less than 15 characters and more than 3 characters.

Total Entries: 0

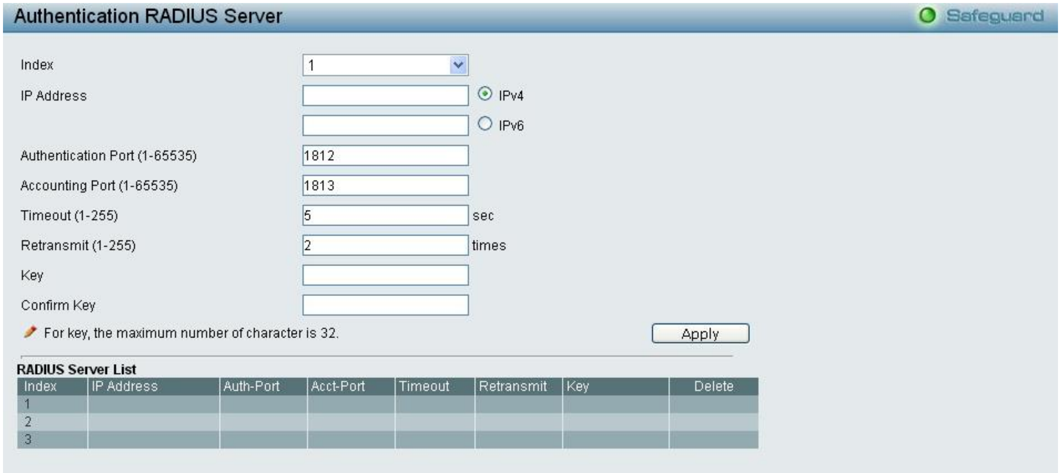
User Name	Password

Figure 4.124 - Security > 802.1X > 802.1X User

Click **Add** to add a new 802.1X user.

Security > 802.1X > 802.1X Authentication RADIUS

The 802.1X Authentication RUAIUS of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.



Authentication RADIUS Server

Index	1
IP Address	● IPv4
	○ IPv6
Authentication Port (1-65535)	1812
Accounting Port (1-65535)	1813
Timeout (1-255)	5 sec
Retransmit (1-255)	2 times
Key	
Confirm Key	

For key, the maximum number of character is 32.

RADIUS Server List

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key	Delete
1							
2							
3							

Figure 4.125 - Security > 802.1X > 802.1X Authentication RUDIUS

Index: Choose the desired RADIUS server to configure: 1, 2 or 3.

IP Address: Select IPv4 or IPv6 and enter the IP address.

Authentication Port (1 - 65535): Set the RADIUS authentic server(s) UDP port. The default port is 1812.

Accounting Port (1 - 65535): Set the RADIUS account server(s) UDP port. The default port is 1813.

Timeout (1 – 255 sec): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *1* and *255* seconds. The default setting is *5* seconds.

Retransmit (1 – 255 times): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *2*.

Key: Set the key the same as that of the RADIUS server.

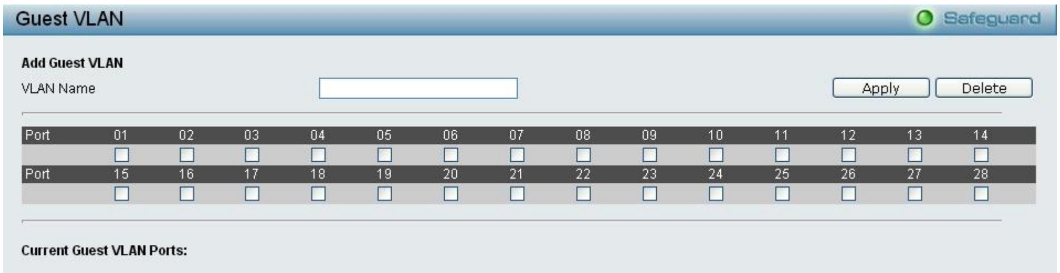
Confirm Key: Confirm the shared key is the same as that of the RADIUS server.

Click **Apply** to implement configuration changes.

Security > 802.1X > 802.1X Guest VLAN

The 802.1X Guest VLAN page allows user to set a Guest VLAN, and the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

Enter the pre-configured VLAN name to create as a Guest 802.1X VLAN and select the port or ports. Click **Apply** to implement the settings.



Guest VLAN

Add Guest VLAN

VLAN Name

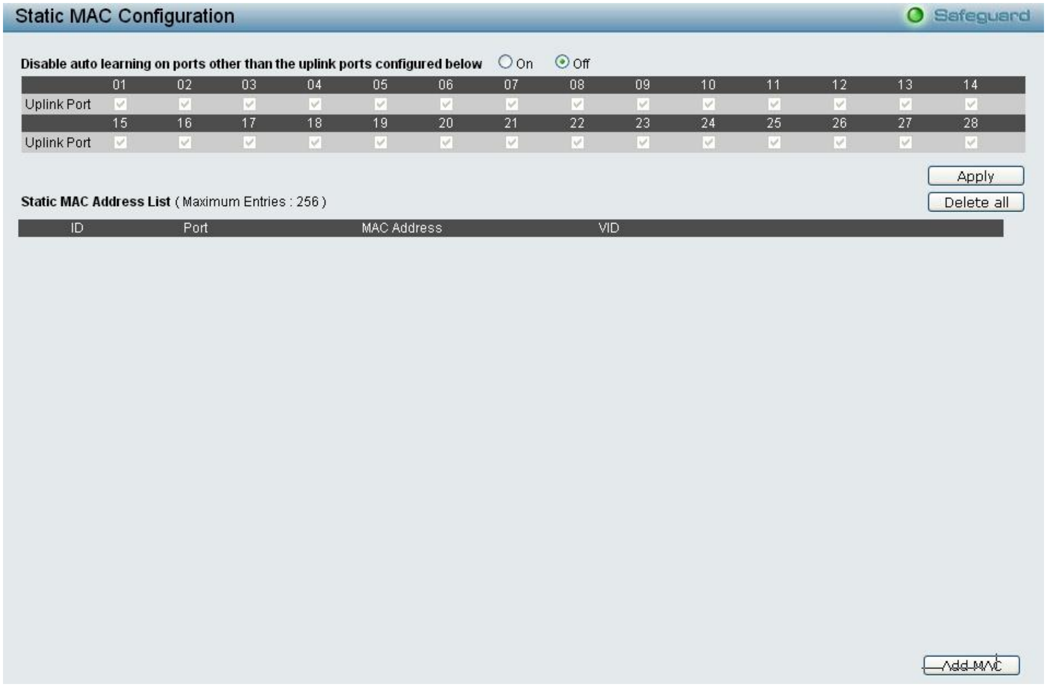
Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Current Guest VLAN Ports:

Figure 4.126 - Security > 802.1X > 802.1X Guest VLAN

Security > MAC Address Table > Static MAC

This feature provides two distinct functions. The **Disable Auto Learning** table allows turning off the function of learning MAC address automatically, if a port isn't specified as an uplink port (for example, connects to a DHCP Server or Gateway). By default, this feature is Off (disabled).



Disable auto learning on ports other than the uplink ports configured below ○ On ● Off

	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Uplink Port	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Uplink Port	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Static MAC Address List (Maximum Entries : 256)

ID	Port	MAC Address	VID

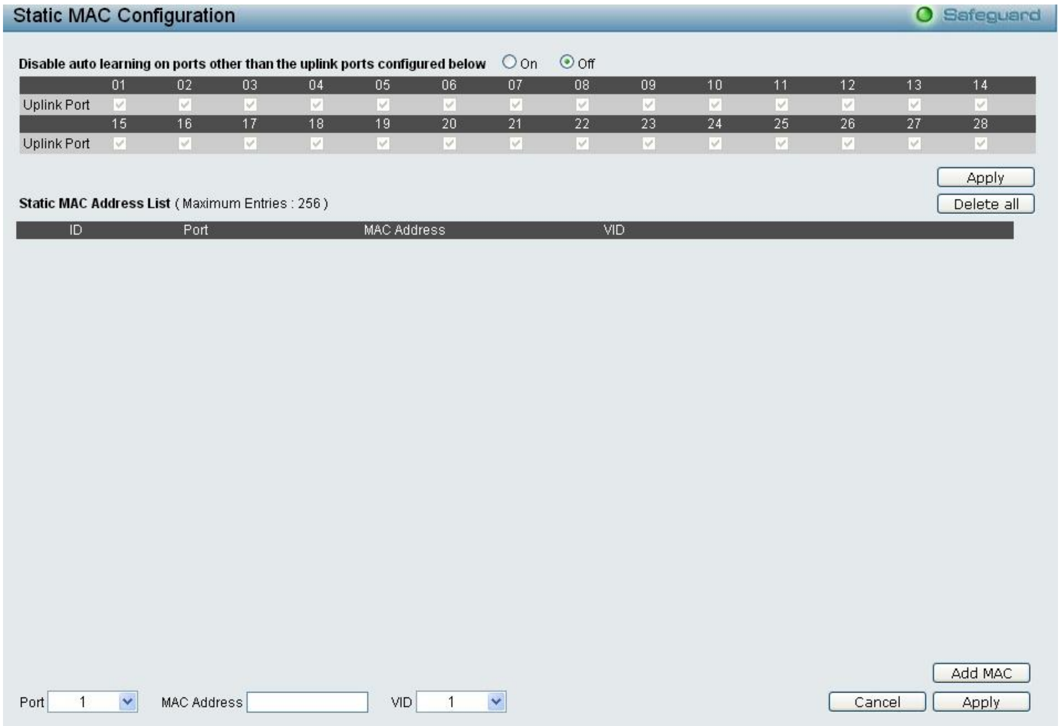
Figure 4.127 - Security > MAC Address Table > Static Mac Address

To initiate the removal of auto-learning for any of the uplink ports, click **On** to enable this feature, and then select the port(s) for auto learning to be disabled.

The **Static MAC Address List** table displays the static MAC addresses connected, as well as the VID. Click **Add Mac** to add a new MAC address, you also need to select the assigned Port number, enter both the Mac Address and VID and Click **Apply**. Click **Delete** to remove one entry or click **Delete all** to clear the list. You can also copy a learned MAC address from **Dynamic Forwarding Table** (please refer to **Security > MAC Address Table > Dynamic Forwarding Table** for details).

By disabling Auto Learning capability and specify the static MAC addresses, the network is protected from potential threats like hackers because traffic from illegal MAC addresses will not be forwarded by the Switch.

Click **Add MAC** button, select the **Port, VID** and enter the **MAC address** then click **Apply** to add a new MAC address.



Static MAC Configuration

Disable auto learning on ports other than the uplink ports configured below ○ On ● Off

	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Uplink Port	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Uplink Port	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Static MAC Address List (Maximum Entries : 256)

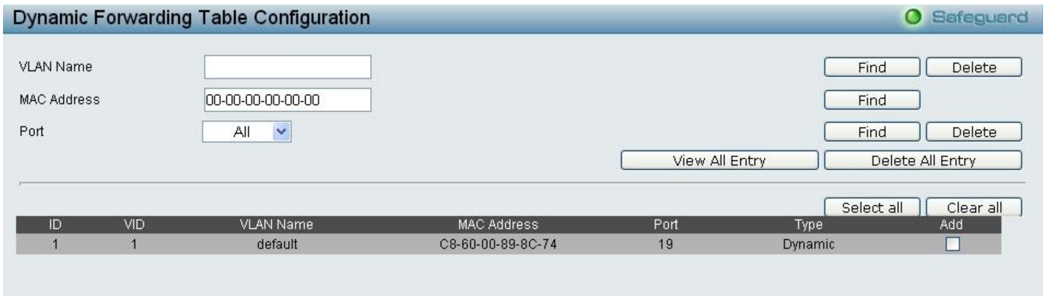
ID	Port	MAC Address	VID

Port 1 MAC Address VID 1

Figure 4.128 - Security > MAC Address Table > Static Mac Address-add MAC

Security > MAC Address Table > Dynamic Forwarding Table

This allows the Switch’s dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.



Dynamic Forwarding Table Configuration

VLAN Name

MAC Address 00-00-00-00-00-00

Port All

ID	VID	VLAN Name	MAC Address	Port	Type	Add
1	1	default	C8-60-00-89-8C-74	19	Dynamic	□

Figure 4.129 - Security > MAC Address Table > Dynamic Forwarding Table

VLAN Name: Enter a VLAN Name by which to browse the forwarding table.

MAC Address: Enter a MAC address by which to browse the forwarding table.

Port: Select the port or all ports by using the corresponding pull-down menu.

Find: Allows the user to move to a sector of the database corresponding to a user defined port, VLAN or MAC address.

VID: The VLAN ID of the VLAN of which the port is a member.

MAC Address: The MAC address entered into the address table.

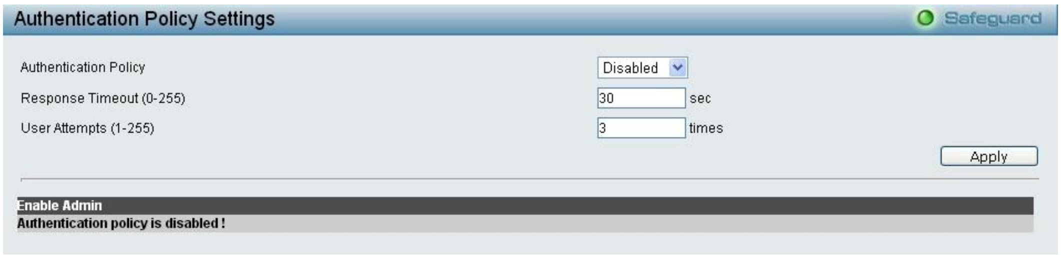
Port: The port to which the MAC address above corresponds.

Type: Describes the method which the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.

View All Entry: Clicking this button will allow the user to view all entries of the address table.

Security > Access Authentication Control > Authentication Policy Settings

This feature will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.



Authentication Policy Settings

Authentication Policy	Disabled
Response Timeout (0-255)	30 sec
User Attempts (1-255)	3 times

Enable Admin

Authentication policy is disabled !

Figure 4.130 – Security > Access Authentication control > Authentication Policy Settings

Authentication Policy: Use the pull-down menu to enable or disable the Authentication Policy on the Switch.

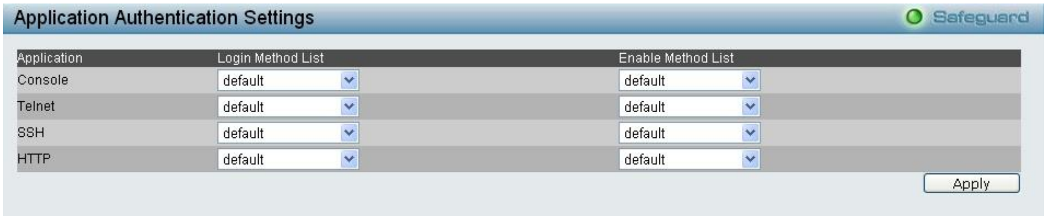
Response Timeout (0 - 255): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.

User attempts (1 - 255): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

Click **Apply** to implement configuration changes.

Security > Access Authentication Control > Application Authentication Settings

The Application Authentication Settings page allows user to configure switch configuration applications (Console, Telnet, SSH, HTTP) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list.



Application Authentication Settings

Application	Login Method List	Enable Method List
Console	default	default
Telnet	default	default
SSH	default	default
HTTP	default	default

Figure 4.131 – Security > Access Authentication control > Application Authentication Settings

Application: Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for Console, Telnet application, SSH and the WEB (HTTP) application.

Login Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

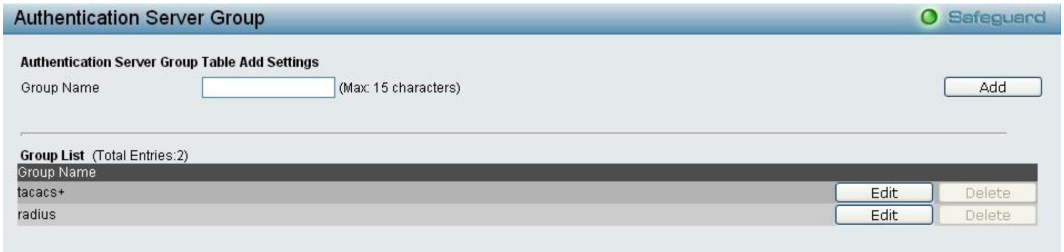
Enable Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

Click **Apply** to implement configuration changes.

Security > Access Authentication Control > Authentication Server Group

A server group is a technique used to group TACACS+ and RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified.

To add a user-defined group to the list, click the **Add** button in the **Authentication Server Group** page.

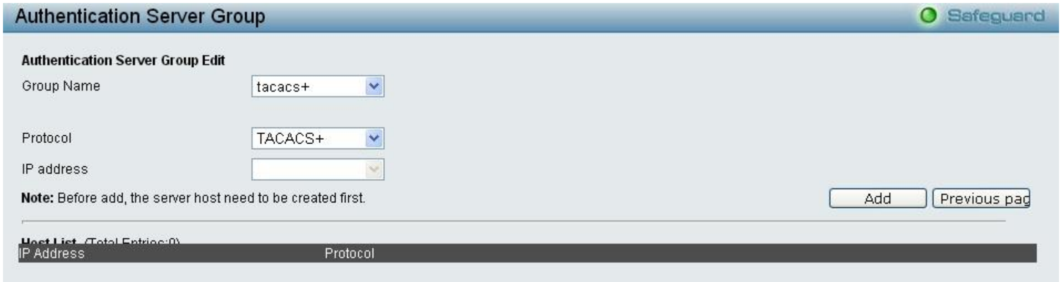

Authentication Server Group
Safeguard
Authentication Server Group Table Add Settings
Group Name
(Max: 15 characters)
Add
Group List (Total Entries:2)

Group Name		
tacacs+	Edit	Delete
radius	Edit	Delete

Figure 4.132 – Security > Access Authentication control > Authentication Server Group

Simply enter a group name of no more than 15 alphanumeric characters to define the user group to add. After clicking **Apply**, the new user-defined group will be displayed in the **Server Group** table. Here, it can be configured as the user desires.

The Switch has two built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click **Edit** button, which will then display the following window.


Authentication Server Group
Safeguard
Authentication Server Group Edit
Add
Previous pag
Host List (Total Entries:0)
IP Address
Protocol

Group Name: tacacs+

Protocol: TACACS+

IP address:

Note: Before add, the server host need to be created first.

Figure 4.133 – Security > Access Authentication control > Authentication Server Group-Edit

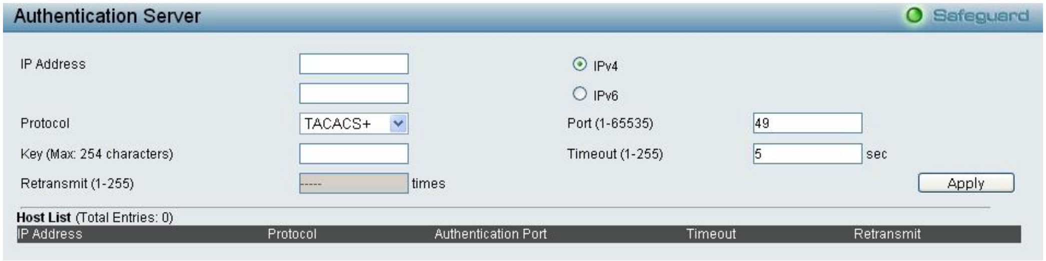
Select **Group Name**, **Protocol** and **IP address** then click **Add** to implement the changes.

NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts page before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

NOTE: The two built in server groups can only have server hosts running the same TACACS daemon. The TACACS+ and RADIUS protocols are separate entities and are not compatible with each other.

Security > Access Authentication Control > Authentication Server

This Authentication Server page will set user-defined **Authentication Server Hosts** for the TACACS+ and RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS+ or RADIUS server host on a remote host. The TACACS+ or RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+ and RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is *16*.



IP Address		● IPv4	
		○ IPv6	
Protocol	TACACS+	Port (1-65535)	49
Key (Max: 254 characters)		Timeout (1-255)	5 sec
Retransmit (1-255)	----- times		

Host List (Total Entries: 0)

IP Address	Protocol	Authentication Port	Timeout	Retransmit

Figure 4.134 – Security > Access Authentication control > Authentication Server

To add an Authentication Server Host:

IP Address: Select IPv4 or IPv6 and enter the IP address.

Protocol: The protocol used by the server host. The user may choose one of the following:

TACACS+ – Enter this parameter if the server host utilizes the TACACS+ protocol.

RADIUS – Enter this parameter if the server host utilizes the RADIUS protocol.

Key: Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to *254* characters.

Port (1 - 65535): Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS+ server and *1813* for RADIUS servers but the user may set a unique port number for higher security.

Timeout (1 - 255): Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds.

Retransmit (1 - 255): Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.

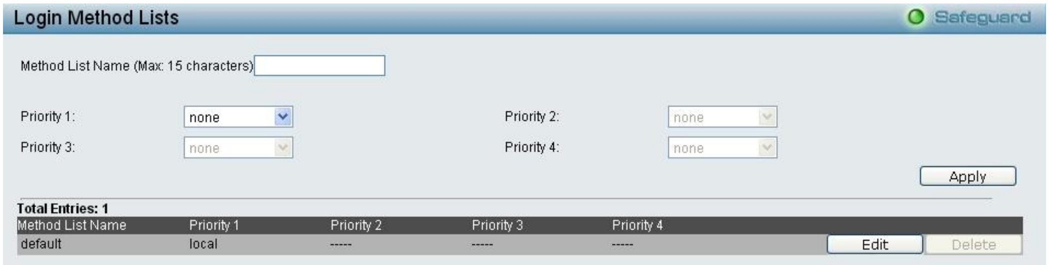
Click **Apply** to add a new Authentication Server Host.

NOTE: More than one authentication protocol can be run on the same physical server host.

Security > Access Authentication Control > Login Method Lists

This feature will configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. Successful login using any of these techniques will give the user a "**User**" privilege only. To upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator.

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click **Delete** button. To modify the Login Method List, click **Edit** button.



Method List Name (Max: 15 characters)

Priority 1:	none	Priority 2:	none
Priority 3:	none	Priority 4:	none

Total Entries: 1

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4		
default	local	-----	-----	-----	Edit	Delete

Figure 4.135 – Security > Access Authentication control > Login Method Lists

To define a Login Method List, set the following parameters and click **Apply**:

Method List Name: Enter a method list name defined by the user of up to *15* characters.

Priority 1, 2, 3, 4: The user may add one, or a combination of up to four of the following authentication methods to this method list:

none – Adding this parameter will require an authentication to access the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

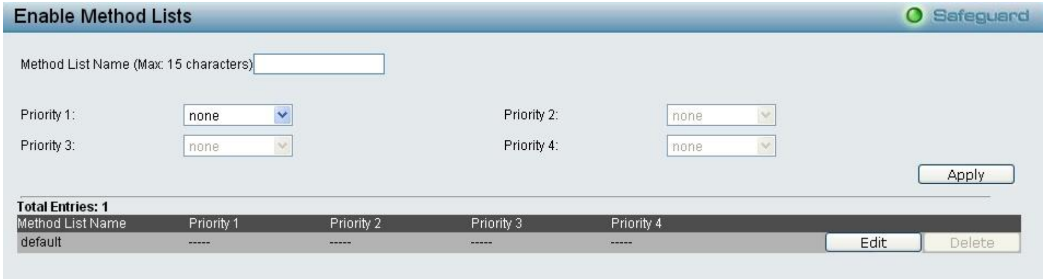
tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

Security > Access Authentication Control > Enable Method Lists

The Enable Method Lists page is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

To delete an Enable Method List defined by the use, click Delete button to the entry desired to be deleted. To modify and Enable Method List, click **Edit** button to make the changes and click **Apply**.



Enable Method Lists

Method List Name (Max: 15 characters)

Priority 1: none

Priority 2: none

Priority 3: none

Priority 4: none

Total Entries: 1

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4		
default	-----	-----	-----	-----	Edit	Delete

Figure 4.136 – Security > Access Authentication control > Enable Method Lists

To define an Enable Login Method List, set the following parameter and click **Apply**:

Method List Name: Enter a method list name defined by the user of up to *15* characters.

Priority 1, 2, 3, 4: The user may add one, or a combination of up to four of the following authentication methods to this method list:

none – Adding this parameter will require an authentication to access the Switch.

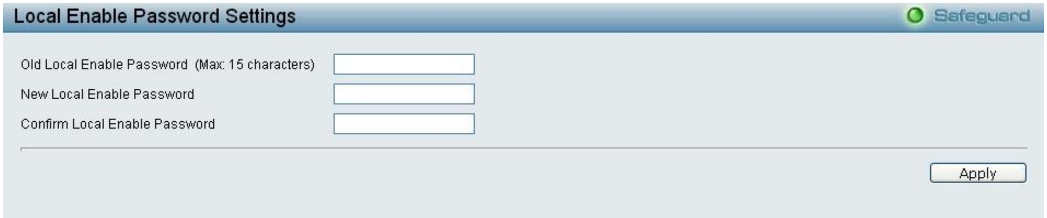
local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

Security > Access Authentication Control > Local Enable Password Settings

The Local Enable Password Settings page allows user to configure the locally enabled password. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.



Local Enable Password Settings

Old Local Enable Password (Max: 15 characters)

New Local Enable Password

Confirm Local Enable Password

Figure 4.137 – Security > Access Authentication control > Local Enable Password Settings

To set the Local Enable Password, set the following parameters and click **Apply**:

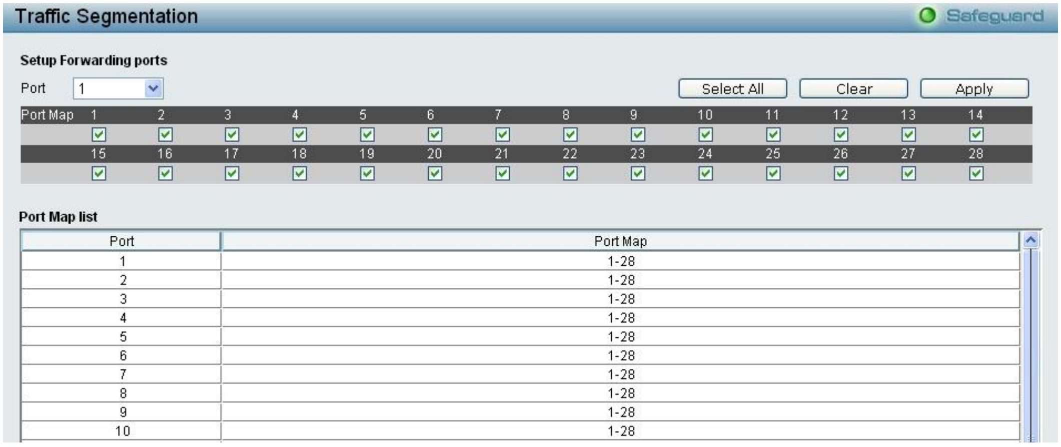
Old Local Enable Password: If a password was previously configured for this entry, enter it here in order to change it to a new password.

New Local Enable Password: Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.

Confirm Local Enable Password: Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Security > Traffic Segmentation

This feature provides administrators to limit traffic flow from a single port to a group of ports on a single Switch. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive.



Traffic Segmentation

Setup Forwarding ports

Port 1

Select All Clear Apply

Port Map	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Port Map list

Port	Port Map
1	1-28
2	1-28
3	1-28
4	1-28
5	1-28
6	1-28
7	1-28
8	1-28
9	1-28
10	1-28

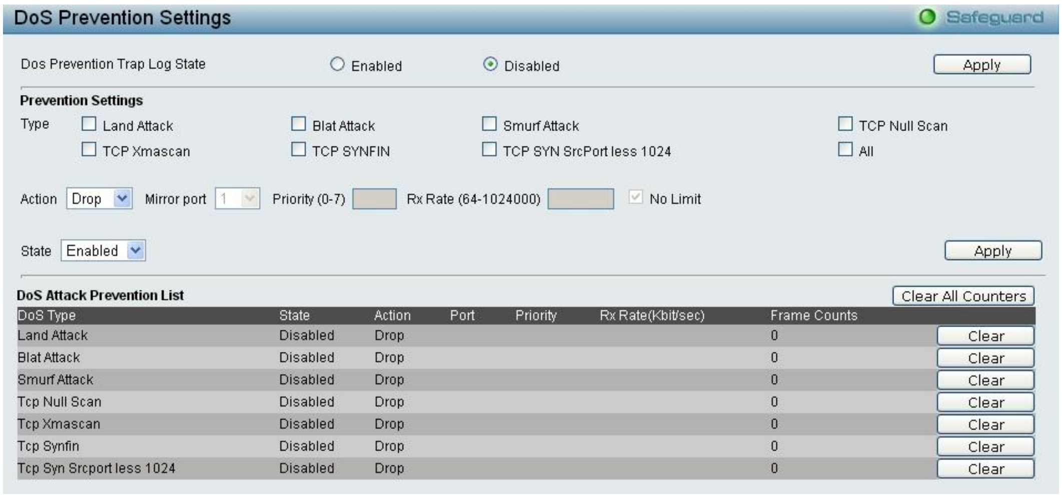
Figure 4.138 – Security > Traffic Segmentation

To configure traffic segmentation specify a port or All ports from the switch, using the **Port** pull-down menu and select **Port Map** then click **Apply** to enter the settings into the Switch's **Traffic Segmentation** table.

Click **Select All** to select all port maps or click **Clear** button to uncheck port maps.

Security > DoS Prevention Settings

The DoS is a malicious attack against a network. This attack is designed to stop a network from functioning by flooding it with useless traffic. Symptoms of a malicious attack include the inability to access any web site or a particular web site being unavailable and network performance slowing down.



DoS Prevention Settings

Dos Prevention Trap Log State ○ Enabled ● Disabled Apply

Prevention Settings

Type □ Land Attack □ Blat Attack □ Smurf Attack □ TCP Null Scan
□ TCP Xmascan □ TCP SYNFIN □ TCP SYN SrcPort less 1024 □ All

Action Drop Mirror port 1 Priority (0-7) Rx Rate (64-1024000) ☑ No Limit

State Enabled Apply

DoS Attack Prevention List Clear All Counters

DoS Type	State	Action	Port	Priority	Rx Rate(Kbit/sec)	Frame Counts	
Land Attack	Disabled	Drop				0	Clear
Blat Attack	Disabled	Drop				0	Clear
Smurf Attack	Disabled	Drop				0	Clear
Tcp Null Scan	Disabled	Drop				0	Clear
Tcp Xmascan	Disabled	Drop				0	Clear
Tcp Synfin	Disabled	Drop				0	Clear
Tcp Syn Srcport less 1024	Disabled	Drop				0	Clear

Figure 4.139 – Security > DoS Prevention Settings

Prevention Settings:

Type: Select the attack types to be prevented. The types are *Land Attack, Blat Attack, Smurf Attack, TCP Null Scan, TCP Xmascan, TCP SYNFIN, TCP SYN SrcPortless 1024* or *All*.

Action: Set action to Drop or Mirror the selected types of attacks. When Mirror was selected, also specifies the *mirror port.*

Mirror Port: Specifies the mirror port to be active.

Priority (0-7): Specifies the priority. The priority range is between 0 and 7.

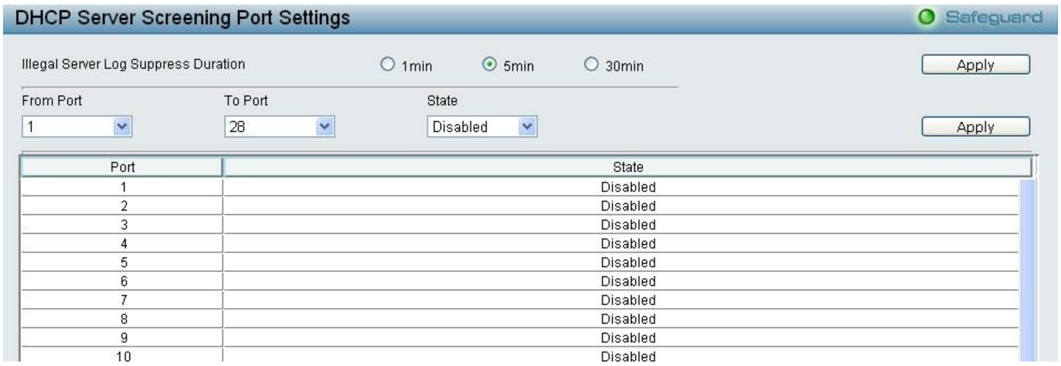
Rx Rate (64-1024000): Specifies the RX rate. The range is between 64 and 1024000.

State: Specify the state to be enabled or disabled.

Click **Apply** to implement changes made.

Security > DHCP Server Screening > DHCP Server Screening Port Settings

DHCP Server Screening function allows user to restrict the illegal DHCP server by discarding the DHCP service from distrusted ports. This page allows you to configure the DHCP Server Screening state for each port and designed trusted DHCP server IP address.



Illegal Server Log Suppress Duration ○ 1min ● 5min ○ 30min

From Port: 1 To Port: 28 State: Disabled

Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Figure 4.140 – Security > DHCP Server Screening > DHCP Server Screening Port Settings

Illegal Server Log Suppress Duration: Specifies the illegal server log suppress duration for DHCP server screening port.

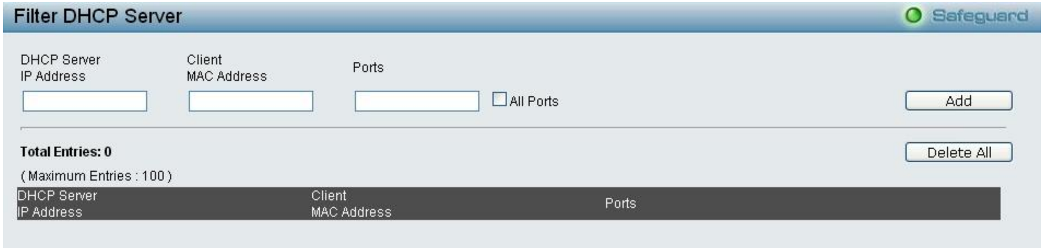
From Port/ To Port: Specifies a range of ports to be DHCP server screening port.

State: Specifies the DHCP server screening port to be enabled or disabled.

Click **Apply** to makes effects.

Security > DHCP Server Screening > Filter DHCP Server

This page allows you to designed trusted DHCP Server IP address and Client MAC Address.



Total Entries: 0

(Maximum Entries : 100)

DHCP Server IP Address	Client MAC Address	Ports

Figure 4.141 – Security > DHCP Server Screening > Filter DHCP Server

To add the DHCP Trusted DHCP Server, set the following fields and click **Add**. Or click **Delete All** to remove all DHCP Server IP Address.

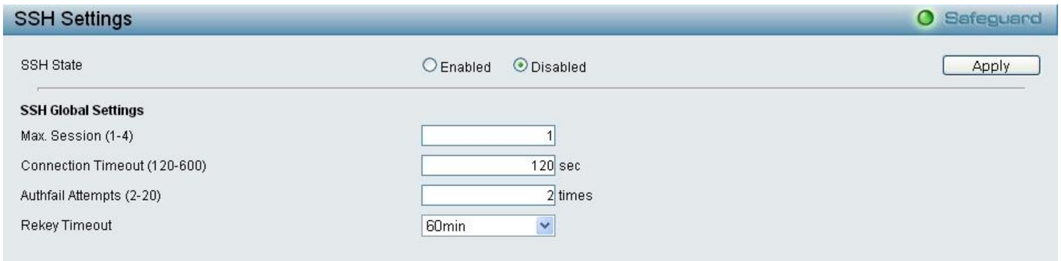
DHCP Server IP Address: Specifies the IP address of the DHCP server to be trusted.

Client MAC Address: Specifies the MAC address of the Client to be trusted.

Ports: Specifies the ports, or select **All Ports**.

Security > SSH Settings > SSH Settings

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.



SSH Settings

SSH State ○ Enabled ● Disabled [Apply]

SSH Global Settings

Max. Session (1-4): 1

Connection Timeout (120-600): 120 sec

Authfail Attempts (2-20): 2 times

Rekey Timeout: 60min

Figure 4.142 – Security > SSH Settings > SSH Settings

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

SSH State: Enabled or Disabled SSH on the Switch. The default is *Disabled*.

Max Session (1 - 4): Enter a value between *1* and 4 to set the number of users that may simultaneously access the Switch. The default setting is *1*.

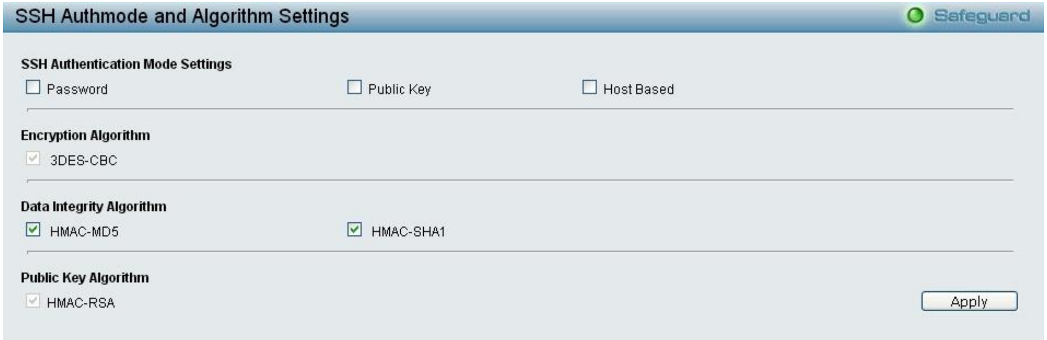
Connection Timeout (120 - 600): Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *120* seconds.

Authfail Attempts (2 - 20): Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.

Rekey Timeout: Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min.* The default setting is *60 min.*

Security > SSH Settings > SSH Authmode and Algorithm Settings

The SSH Authentication and Algorithm Settings page allows user to configure the desired types of SSH algorithms used for authentication encryption.



SSH Authmode and Algorithm Settings

SSH Authentication Mode Settings

□ Password □ Public Key □ Host Based

Encryption Algorithm

☑ 3DES-CBC

Data Integrity Algorithm

☑ HMAC-MD5 ☑ HMAC-SHA1

Public Key Algorithm

☑ HMAC-RSA [Apply]

Figure 4.143 – Security > SSH Settings > SSH Authmode and Algorithm Settings

SSH Authentication Mode Settings:

Password: Allows user to use a locally configured password for authentication on the Switch.

Public Key: This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch.

Host Based: This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed.

Encryption Algorithm:

3DES-CBC: Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.

Data Integrity Algorithm:

HMAC-MD5: Use the check box to enable the supports of hash for message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism.

HMAC-SHA1: Use the check box to enable the supports of hash for message Authentication Code (HMAC) Secure Hash Algorithm (SHA) mechanism.

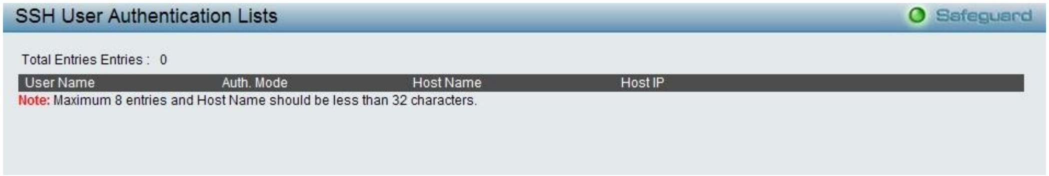
Public Key Algorithm:

HMAC-RSA: Use the check box to enable the supports of Hash for Message Authentication Code (HMAC) mechanism utilizing the RSA encryption algorithm.

Click **Apply** to implement changes made.

Security > SSH Settings > SSH User Authentication Lists

The SSH User Authentication Lists page is used to configure parameters for users attempting to access the Switch through SSH.



SSH User Authentication Lists

Total Entries Entries : 0

User Name	Auth. Mode	Host Name	Host IP

Note: Maximum 8 entries and Host Name should be less than 32 characters.

Figure 4.144 – Security > SSH Settings > SSH User Authentication Lists

The user may view the following parameters:

User Name: A name of no more than *15* characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.

Auth. Mode: The administrator may choose one of the following to set the authorization for users attempting to access the Switch.

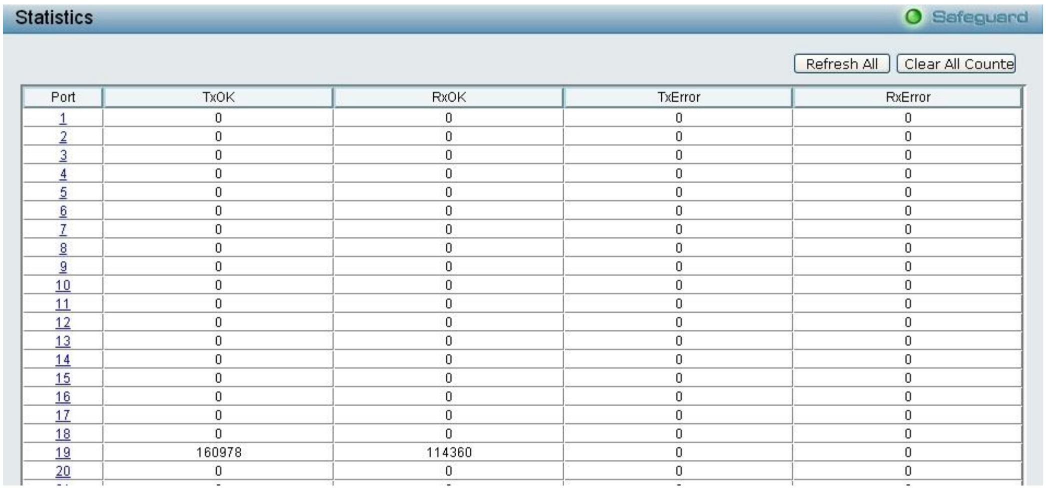
> **Host Based –** This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes.
>
> **Password –** This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.
>
> **Public Key –** This parameter should be chosen if the administrator wishes to use the public key on an SSH server for authentication.

Host Name: Enter an alphanumeric string of no more than *32* characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Host IP: Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Monitoring > Statistics

The Statistics screen displays the status of each port packet count.

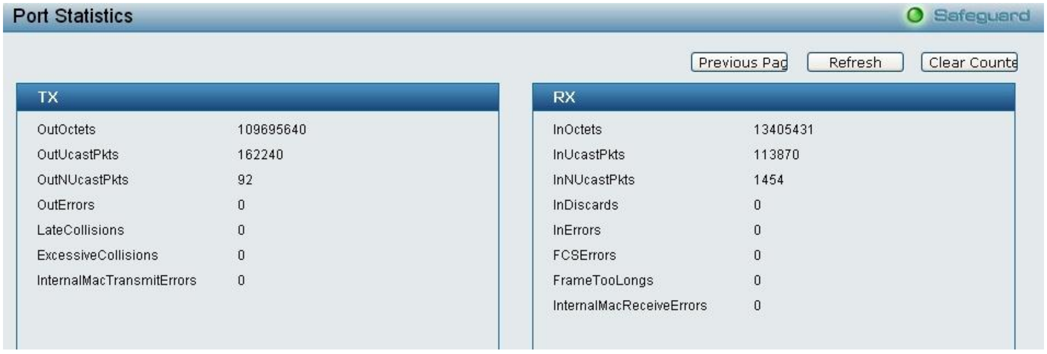


Port	TxOK	RxOK	TxError	RxError
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	160978	114360	0	0
20	0	0	0	0

Figure 4.145 – Monitoring > Statistics

Refresh All: Renews the details collected and displayed.
Clear All: To reset the details displayed.
TxOK: Number of packets transmitted successfully.
RxOK: Number of packets received successfully.
TxError: Number of transmitted packets resulting in error.
RxError: Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked port numbers for details.



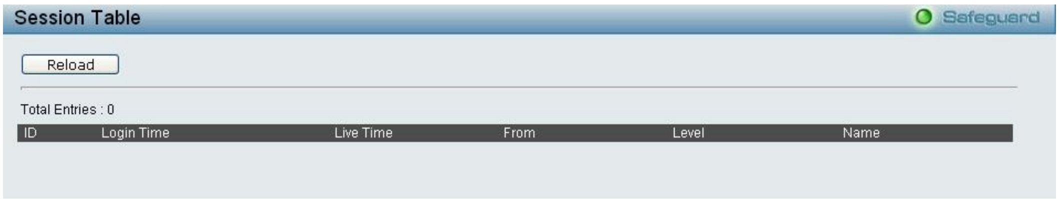
TX		RX	
OutOctets	109695640	InOctets	13405431
OutUcastPkts	162240	InUcastPkts	113870
OutNUcastPkts	92	InNUcastPkts	1454
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

Figure 4.146 – Monitoring > Port Statistics

Previous Page: Go back to the Statistics main page.
Refresh: To renew the details collected and displayed.
Clear Counter: To reset the details displayed.

Monitoring > Session Table

The Session Table allows the user to view detailed information on the current configuration session of the Switch. Information such as the Session **ID** of the user, initial **Login Time**, **Live Time**, configuration connection **From** the Switch, **Level** and **Name** of the user are displayed. Click **Reload** to refresh this window.



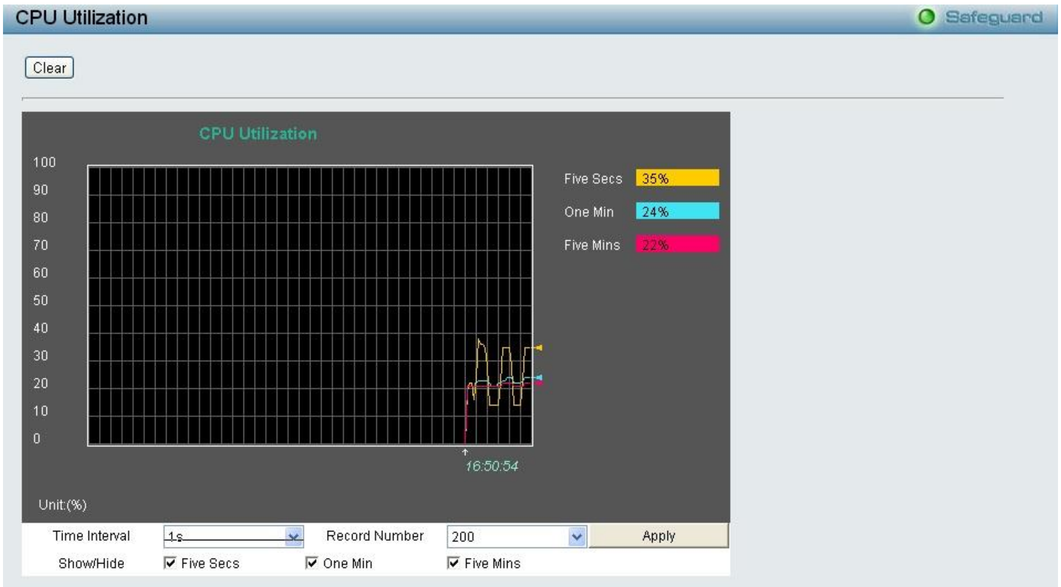
Total Entries : 0

ID	Login Time	Live Time	From	Level	Name

Figure 4.147 – Monitoring > Session Table

Monitoring > CPU Utilization

The **CPU Utilization** displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.



Time Interval 1s
Record Number 200
Show/Hide ☑ Five Secs ☑ One Min ☑ Five Mins

Figure 4.148 – Monitoring > CPU Utilization

The information is described as follows:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

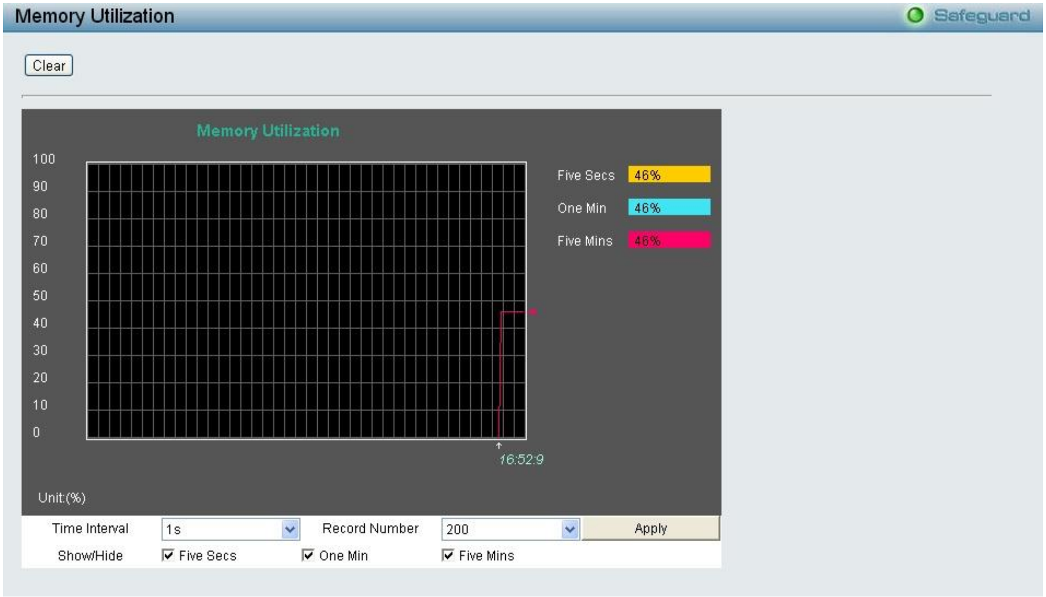
Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Show/Hide: Check whether to display *Five Secs*, *One Min*, and/or *Five Mins*.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Memory Utilization

The Memory Utilization displays the percentage of the memory being used, expressed as an integer percentage and calculated as a simple average by time interval. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.



Time Interval 1s
Record Number 200
Show/Hide ☑ Five Secs ☑ One Min ☑ Five Mins

Figure 4.149 – Monitoring > Memory Utilization

The information is described as follows:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

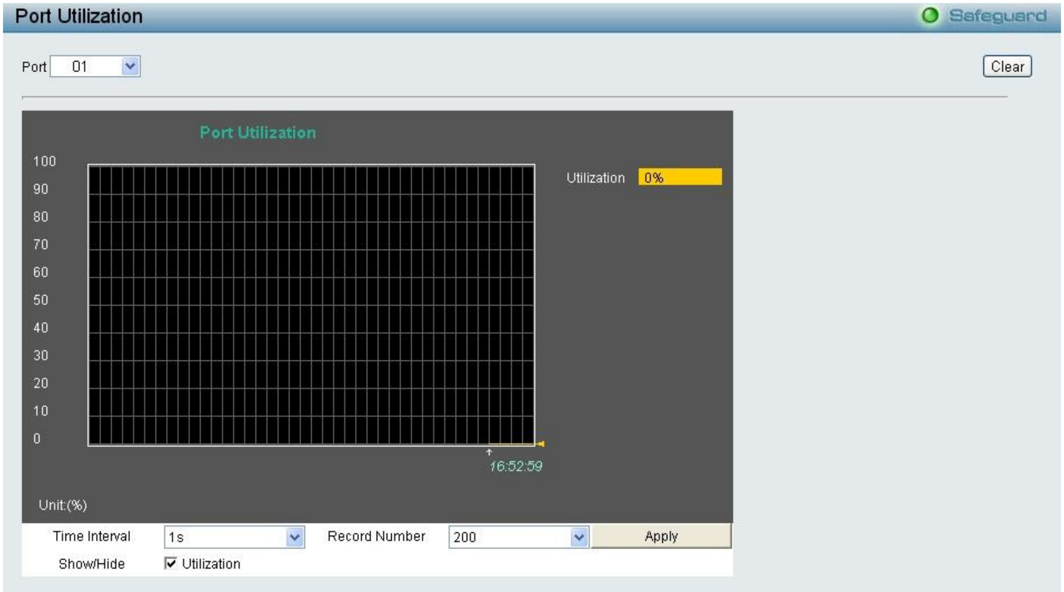
Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Show/Hide: Check whether to display *Five Secs*, *One Min*, and/or *Five Mins*.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Port Utilization

The Port Utilization page displays the percentage of the total available bandwidth being used on the port.



Port Utilization

Port: 01

Time Interval: 1s

Record Number: 200

Show/Hide: ☑ Utilization

Figure 4.150 – Monitoring > Port Utilization

The user may use the real-time graphic of the Switch at the top of the web page to view utilization statistics per port by clicking on a port. Click **Apply** to implement changes made. The following field can be set:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

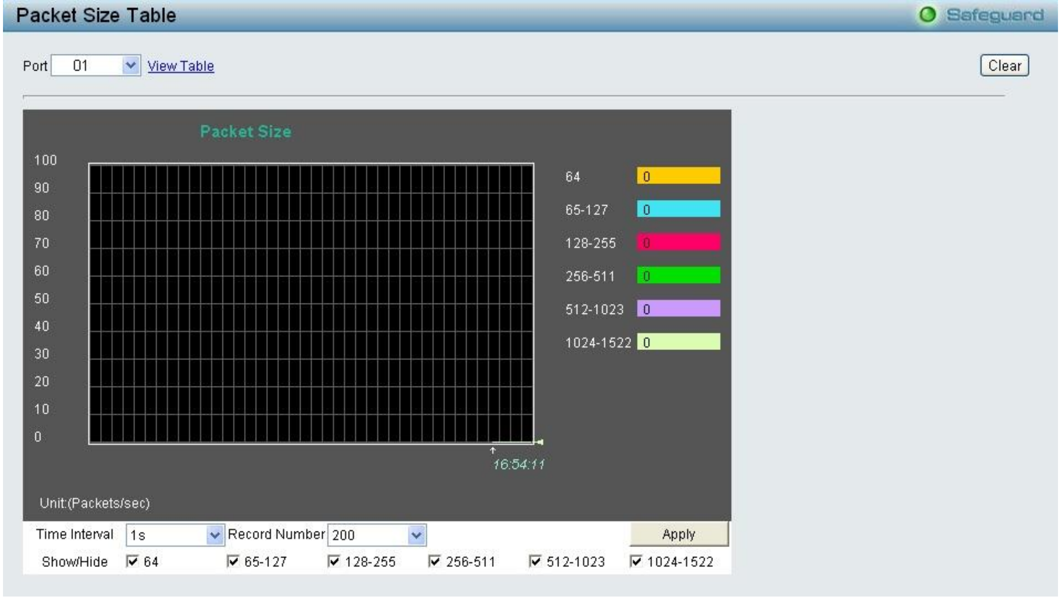
Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Show/Hide: Check whether to display Utilization.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Port 01

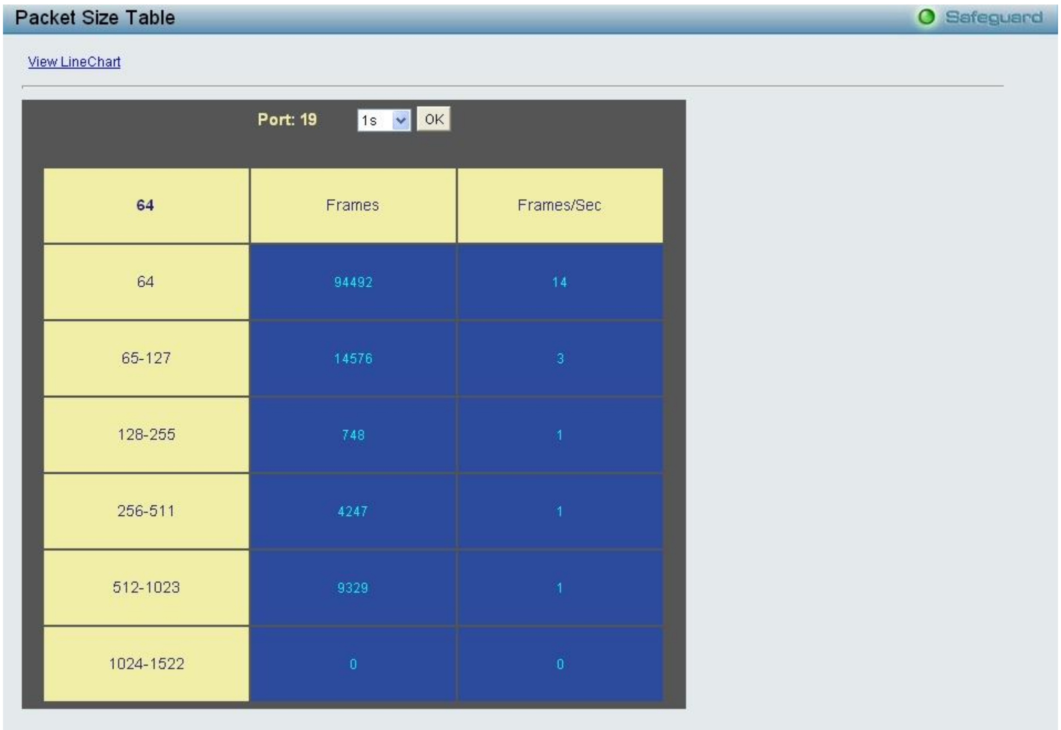
64	0
65-127	0
128-255	0
256-511	0
512-1023	0
1024-1522	0

Time Interval 1s Record Number 200

Show/Hide ☑ 64 ☑ 65-127 ☑ 128-255 ☑ 256-511 ☑ 512-1023 ☑ 1024-1522

Figure 4.151 – Monitoring > Packet Size

To view the **Packet Size Analysis Table**, click the link View Table, which will show the following table:



Port: 19 1s

64	Frames	Frames/Sec
64	94492	14
65-127	14576	3
128-255	748	1
256-511	4247	1
512-1023	9329	1
1024-1522	0	0

Figure 4.152 – Monitoring > Packet Size Table

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

64: The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

65-127: The total number of packets (including bad packets) received that were between *65* and *127* octets in length inclusive (excluding framing bits but including FCS octets).

128-255: The total number of packets (including bad packets) received that were between *128* and *255* octets in length inclusive (excluding framing bits but including FCS octets).

256-511: The total number of packets (including bad packets) received that were between *256* and *511* octets in length inclusive (excluding framing bits but including FCS octets).

512-1023: The total number of packets (including bad packets) received that were between *512* and *1023* octets in length inclusive (excluding framing bits but including FCS octets).

1024-1518: The total number of packets (including bad packets) received that were between *1024* and *1518* octets in length inclusive (excluding framing bits but including FCS octets).

Show/Hide: Check whether or not to display *64*, *65-127*, *128-255*, *256-511*, *512-1023*, and *1024-1518* packets received.

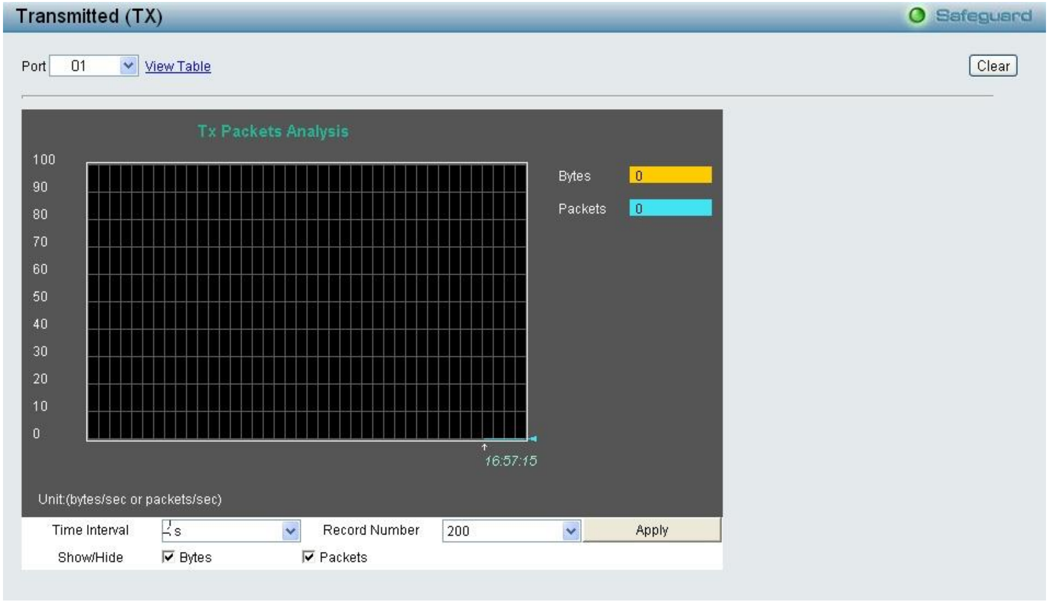
Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > Transmitted (TX)

The Transmitted (TX) page displays the following graph of packets transmitted from the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.


Transmitted (TX)

Port 01 View Table

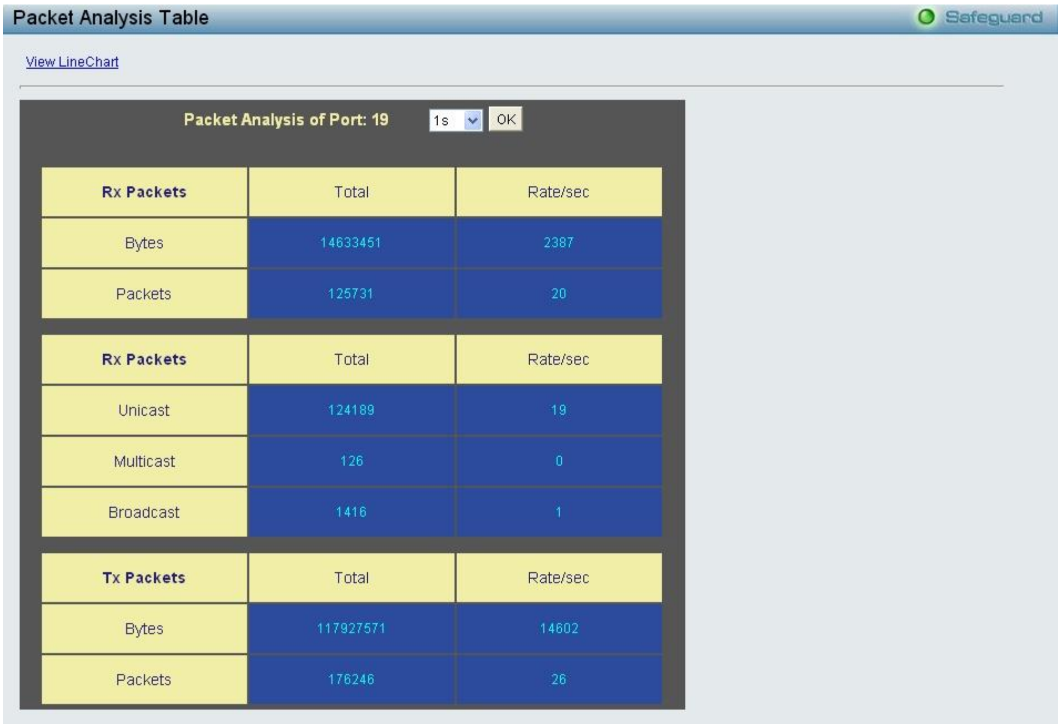
Bytes 0
Packets 0

Unit:(bytes/sec or packets/sec)

Time Interval 1s
Record Number 200
Show/Hide ☑ Bytes ☑ Packets

Figure 4.153 - Monitoring > Packets > Transmitted (TX) (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link View Table, which will show the following table:



Packet Analysis Table

Packet Analysis of Port: 19 1s OK

Rx Packets	Total	Rate/sec
Bytes	14633451	2387
Packets	125731	20

Rx Packets	Total	Rate/sec
Unicast	124189	19
Multicast	126	0
Broadcast	1416	1

Tx Packets	Total	Rate/sec
Bytes	117927571	14602
Packets	176246	26

Figure 4.154 - Monitoring > Packet s > Transmitted (TX) (table for Bytes and Packets)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Bytes: Counts the number of bytes successfully sent from the port.

Packets: Counts the number of packets successfully sent on the port.

Unicast: Counts the total number of good packets that were transmitted by a unicast address.

Multicast: Counts the total number of good packets that were transmitted by a multicast address.

Broadcast: Counts the total number of good packets that were transmitted by a broadcast address.

Show/Hide: Check whether or not to display Bytes and Packets.

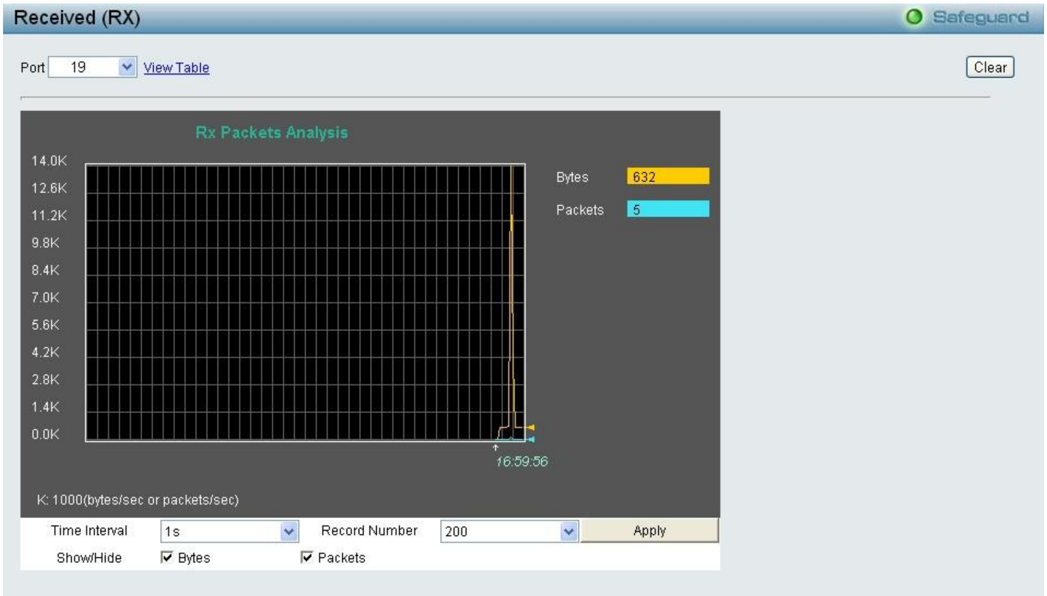
Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > Received (RX)

The Received (RX) page displays the following graph of packets received on the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Received (RX)

Port 19 View Table

Bytes 632

Packets 5

K: 1000(bytes/sec or packets/sec)

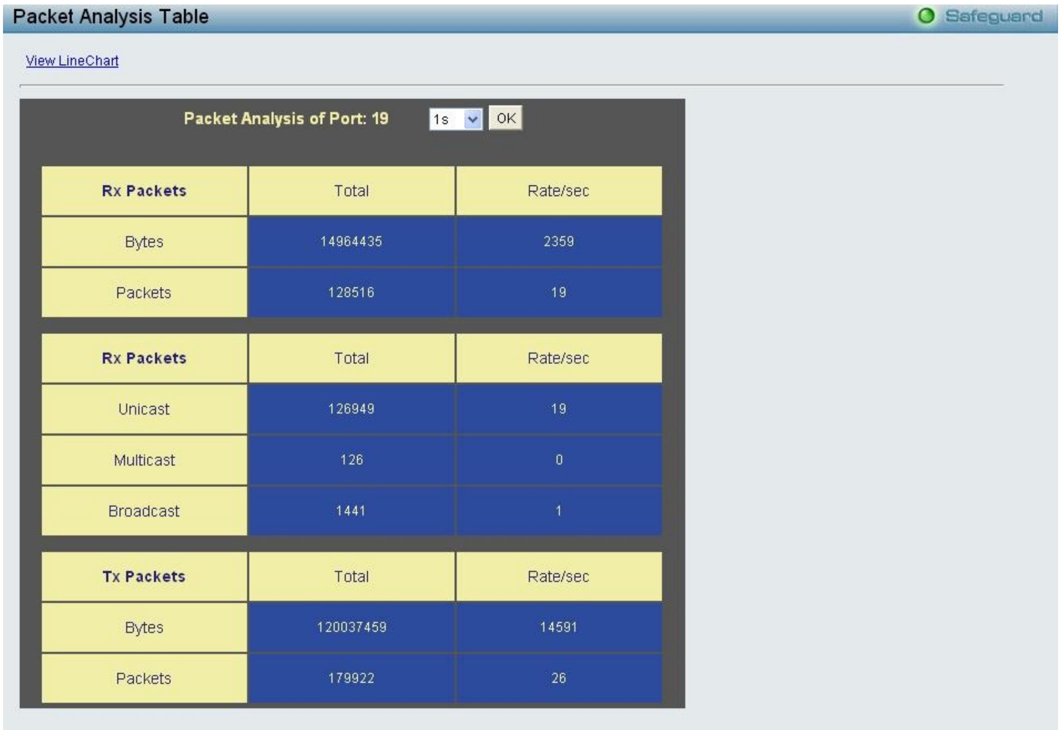
Time Interval 1s

Record Number 200

Show/Hide ☑ Bytes ☑ Packets

Figure 4.155 - Monitoring > Packets > Received (RX) (line graph for Bytes and Packets)

To view the **Received Packets Table**, click the link View Table, which will show the following table:



Packet Analysis Table

View LineChart

Packet Analysis of Port: 19 1s OK

Rx Packets	Total	Rate/sec
Bytes	14964435	2359
Packets	128516	19

Rx Packets	Total	Rate/sec
Unicast	126949	19
Multicast	126	0
Broadcast	1441	1

Tx Packets	Total	Rate/sec
Bytes	120037459	14591
Packets	179922	26

Figure 4.156 - Monitoring > Packet s > Received (RX) (table for Bytes and Packets)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Bytes: Counts the number of bytes received on the port.

Packets: Counts the number of packets received on the port.

Unicast: Counts the total number of good packets that were received by a unicast address.

Multicast: Counts the total number of good packets that were received by a multicast address.

Broadcast: Counts the total number of good packets that were received by a broadcast address.

Show/Hide: Check whether or not to display Bytes and Packets.

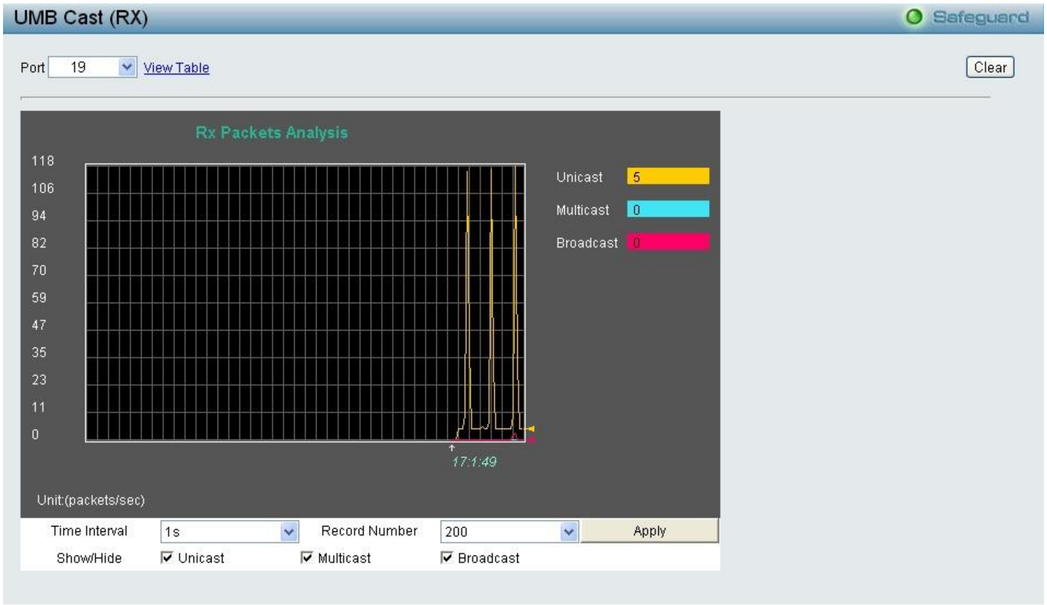
Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > UMB Cast (RX)

The **UMB Cast (RX)** page displays the following graph of UMB cast packets received on the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



UMB Cast (RX)

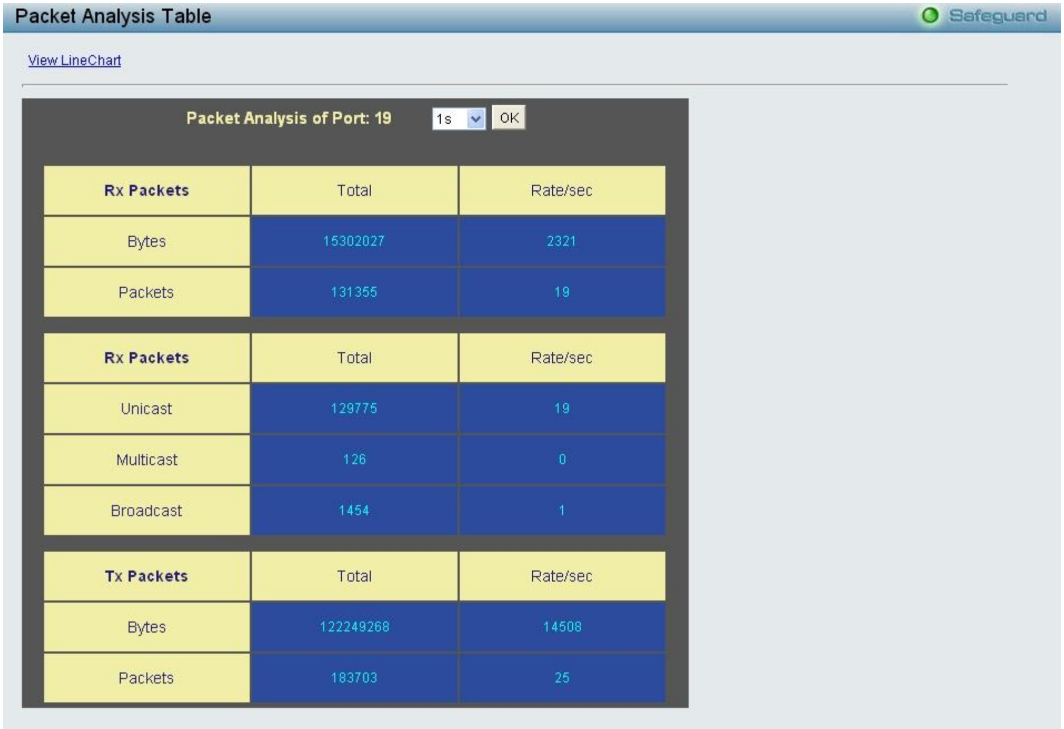
Port 19 View Table

Time Interval 1s Record Number 200

Show/Hide ☑ Unicast ☑ Multicast ☑ Broadcast

Figure 4.157 - Monitoring > Packets > UMB Cast (RX) (line graph for Unicast, Multicast and Broadcast Packets)

To view the **UMB Cast Table**, click the View Table link, which will show the following table:



Packet Analysis Table

View LineChart

Packet Analysis of Port: 19 1s OK

Rx Packets	Total	Rate/sec
Bytes	15302027	2321
Packets	131355	19
Rx Packets	**Total**	**Rate/sec**
Unicast	129775	19
Multicast	126	0
Broadcast	1454	1
Tx Packets	**Total**	**Rate/sec**
Bytes	122249268	14508
Packets	183703	25

Figure 4.158 - Monitoring > Packets > UMB Cast (RX) (table for Unicast, Multicast and Broadcast Packets)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

Unicast: Counts the total number of good packets that were received by a unicast address.

Multicast: Counts the total number of good packets that were received by a multicast address.

Broadcast: Counts the total number of good packets that were received by a broadcast address.

Show/Hide: Check whether or not to display Multicast, Broadcast and Unicast packets.

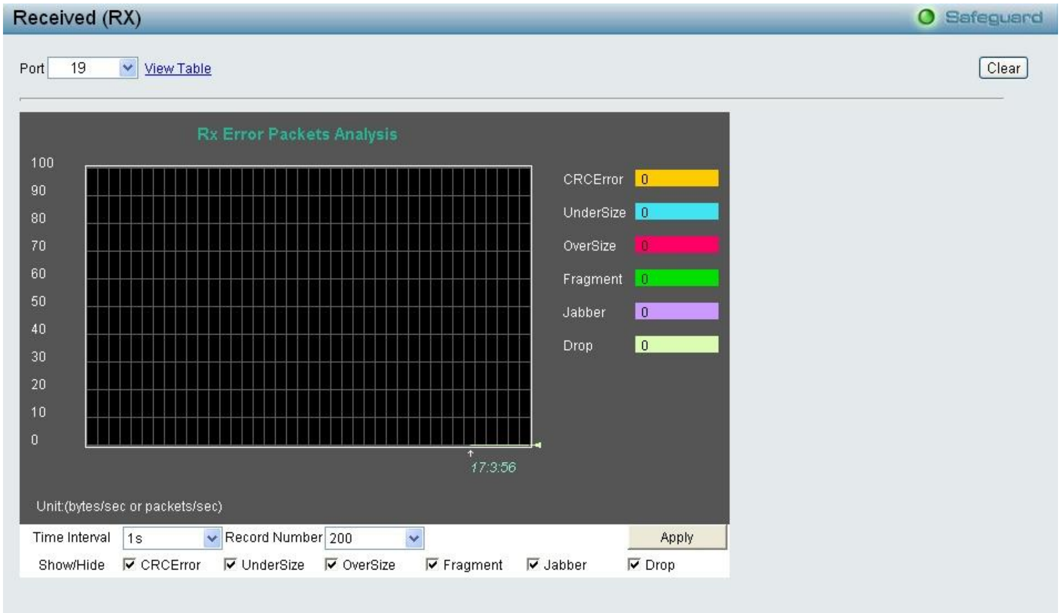
Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Errors > Received (RX)

This page displays the following graph of error packets received on the Switch. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Received (RX)

Port 19 View Table

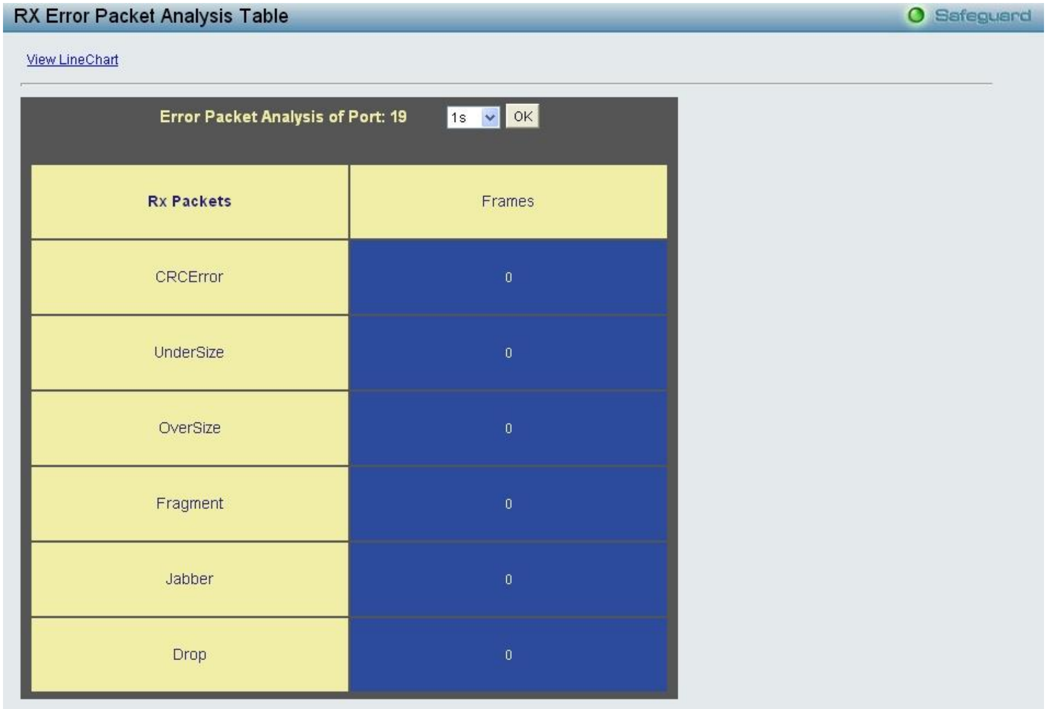
Clear

Time Interval 1s Record Number 200 Apply

Show/Hide ☑ CRCError ☑ UnderSize ☑ OverSize ☑ Fragment ☑ Jabber ☑ Drop

Figure 4.159 - Monitoring > Errors > Received (RX) (line graph)

To view the **Received Error Packets Table**, click the link **View Table**, which will show the following table:



RX Error Packet Analysis Table
Safeguard
View LineChart
Error Packet Analysis of Port: 19
1s
OK

Rx Packets	Frames
CRCError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0
Drop	0

Figure 4.160 - Monitoring > Errors > Received (RX) (table)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where “s” stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

CRC Error: Counts otherwise valid packets that did not end on a byte (octet) boundary.

UnderSize: The number of packets detected that are less that the minimum permitted packets size of *64* bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.

OverSize: Counts packets received that were longer that *1518* octets, or if a VLAN frame is *1522* octets, and less that the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to *1522*.

Fragment: The number of packets less than *64* bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

Jabber: The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to *1522*.

Drop: The number of packets that are dropped by this port since the last Switch reboot.

Show/Hide: Check whether or not to display CRC Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.

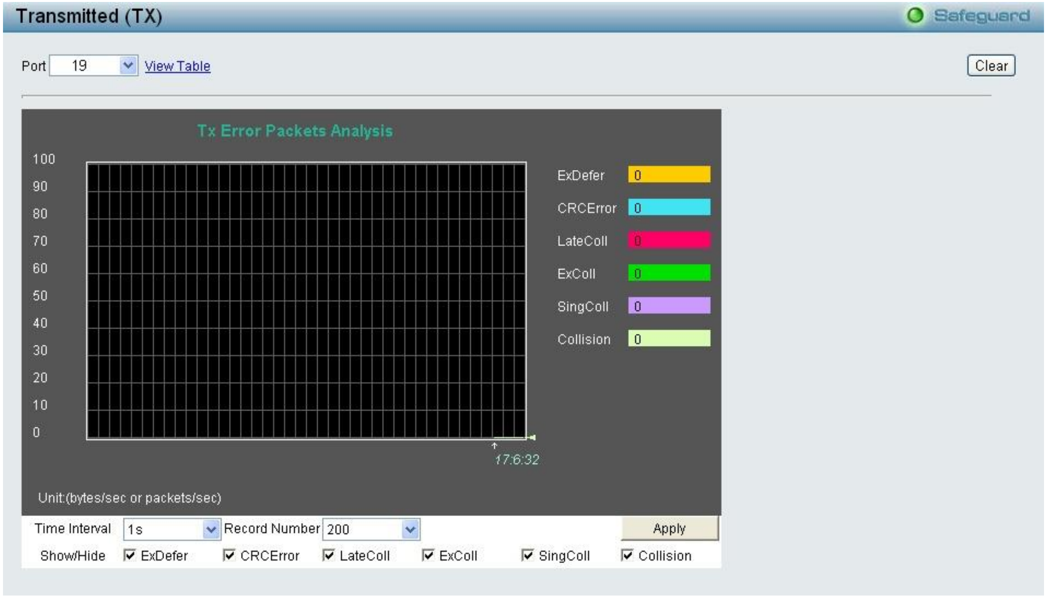
Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Errors > Transmitted (TX)

This page displays the following graph of error packets transmitted on the Switch. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Port 19

ExDefer 0
CRCError 0
LateColl 0
ExColl 0
SingColl 0
Collision 0

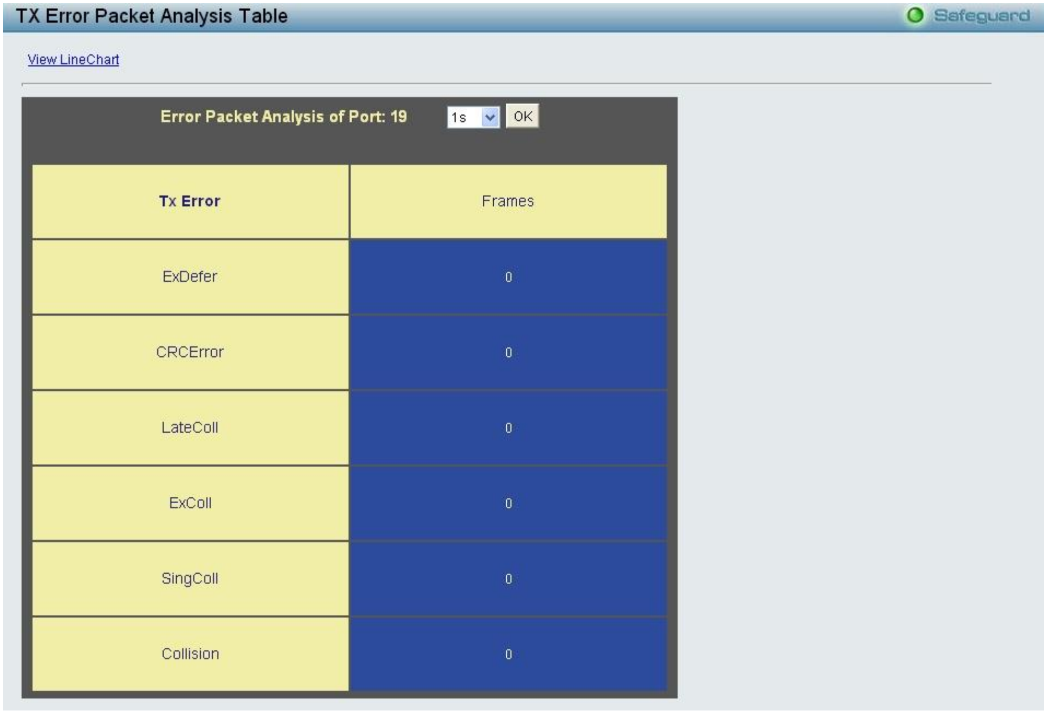
Unit:(bytes/sec or packets/sec)

Time Interval 1s Record Number 200

Show/Hide ☑ ExDefer ☑ CRCError ☑ LateColl ☑ ExColl ☑ SingColl ☑ Collision

Figure 4.161 - Monitoring > Errors > Transmitted (TX) (line graph)

To view the **Transmitted Error Packets Table**, click the link View Table, which will show the following table:



Error Packet Analysis of Port: 19 1s

Tx Error	Frames
ExDefer	0
CRCError	0
LateColl	0
ExColl	0
SingColl	0
Collision	0

Figure 4.162 - Monitoring > Errors > Transmitted (TX) (table)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

ExDefet: Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.

CRC Error: Counts otherwise valid packets that did not end on a byte (octet) boundary.

LateColl: Counts the number of times that a collision is detected later than *512* bit-times into the transmission of a packet.

ExColl: Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.

SingColl: Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.

Coll: An estimate of the total number of collisions on this network segment.

Show/Hide: Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.

Clear: Clicking this button clears all statistics counters on this window.

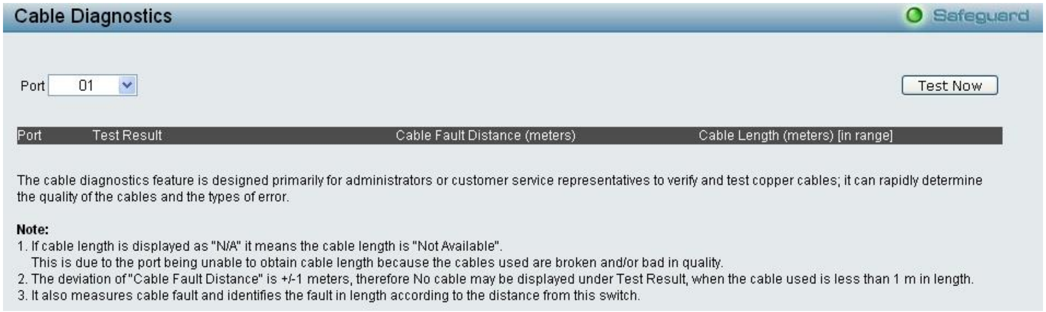
View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine of the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.



Port 01

Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters) [in range]

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

Note:

1. If cable length is displayed as "N/A" it means the cable length is "Not Available".
   This is due to the port being unable to obtain cable length because the cables used are broken and/or bad in quality.
2. The deviation of "Cable Fault Distance" is +/-1 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 1 m in length.
3. It also measures cable fault and identifies the fault in length according to the distance from this switch.

Figure 4.163 - Monitoring > Cable Diagnostics

Test Result: The description of the cable diagnostic results.

- **OK** means the cable is good for the connection.
- **Short in Cable** means the wires of the RJ45 cable may be in contact somewhere.
- **Open in Cable** means the wires of RJ45 cable may be broken or the other end of the cable is simply disconnected.
- **Test Failed** means some other errors occurred during cable diagnostics. Please select the same port and test again.

Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show “No Cable”, whether the fiber is connected to the port or not.

Cable Length (meter): If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and >100 meters. Deviation is +/-2 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 2 m in length. This test can only be performed when the port is up and operating at 1 Gbps.

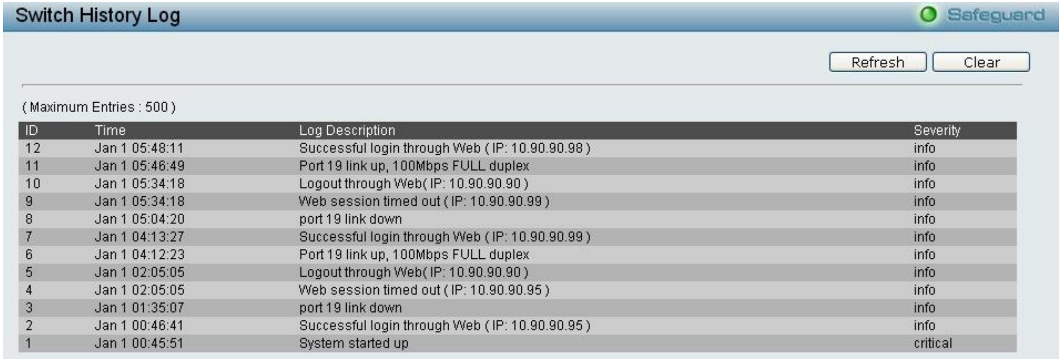
NOTE: Cable length detection is effective on Gigabit ports only.

The definition of cable pair is listed below:

Pair1: PIN4, PIN5
Pair2: PIN1, PIN2
Pair3: PIN3, PIN6
Pair4: PIN7, PIN8

Monitoring > System Log

The System Log page provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.



(Maximum Entries : 500)

ID	Time	Log Description	Severity
12	Jan 1 05:48:11	Successful login through Web (IP: 10.90.90.98)	info
11	Jan 1 05:46:49	Port 19 link up, 100Mbps FULL duplex	info
10	Jan 1 05:34:18	Logout through Web(IP: 10.90.90.90)	info
9	Jan 1 05:34:18	Web session timed out (IP: 10.90.90.99)	info
8	Jan 1 05:04:20	port 19 link down	info
7	Jan 1 04:13:27	Successful login through Web (IP: 10.90.90.99)	info
6	Jan 1 04:12:23	Port 19 link up, 100Mbps FULL duplex	info
5	Jan 1 02:05:05	Logout through Web(IP: 10.90.90.90)	info
4	Jan 1 02:05:05	Web session timed out (IP: 10.90.90.95)	info
3	Jan 1 01:35:07	port 19 link down	info
2	Jan 1 00:46:41	Successful login through Web (IP: 10.90.90.95)	info
1	Jan 1 00:45:51	System started up	critical

Figure 4.164 - Monitoring > System Log

ID: Displays an incremented counter of the System Log entry. The Maximum entries are 500.

Time: Displays the time in days, hours, and minutes the log was entered.

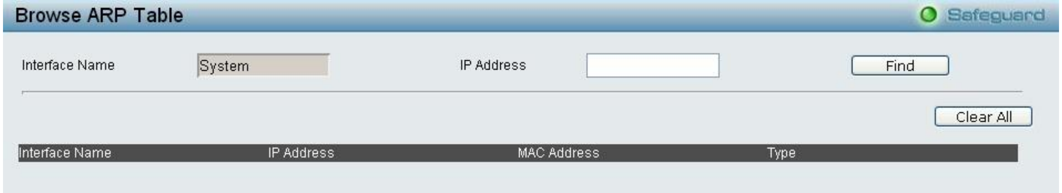
Log Description: Displays the description of event recorded.

Severity: Displays a severity level of the event recorded.

Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.

Monitoring > Browse ARP Table

The Browse ARP Table page provides information regarding ARP VLANs, including which IP address was mapped to what MAC address. To clear the ARP Table, click **Clear All.**



Interface Name: System
IP Address:

Interface Name	IP Address	MAC Address	Type

Figure 4.165 - Monitoring > Browse ARP Table

Click **Find**, The table updates and displays the values required.

Interface Name: Defines the name of ARP mappings.

IP Address: Defines the station IP address, which is associated with the MAC address.

MAC Address: Displays the MAC address associated with the IP address.

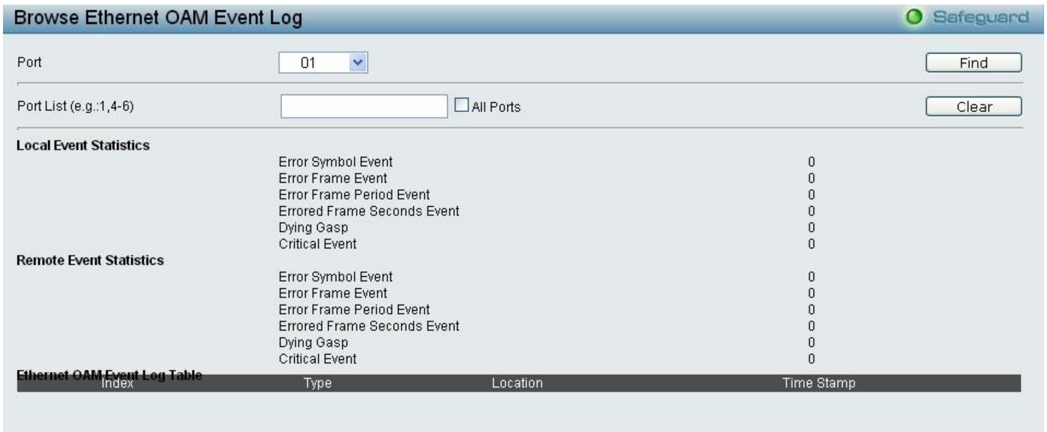
Type: Indicates how the MAC was assigned. The possible values are:

> **Dynamic** – Indicates that the MAC address is dynamically created.
>
> **Static –** Indicates the MAC address is a static IP address.

Port: Defines the ARP mapping ports.

Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

The Browse Ethernet OAM Event Log page displays the ports Ethernet OAM event log information.



Browse Ethernet OAM Event Log

Port: 01 | Find

Port List (e.g.:1,4-6) □ All Ports | Clear

Local Event Statistics

Error Symbol Event	0
Error Frame Event	0
Error Frame Period Event	0
Errored Frame Seconds Event	0
Dying Gasp	0
Critical Event	0

Remote Event Statistics

Error Symbol Event	0
Error Frame Event	0
Error Frame Period Event	0
Errored Frame Seconds Event	0
Dying Gasp	0
Critical Event	0

Ethernet OAM Event Log Table

Index	Type	Location	Time Stamp

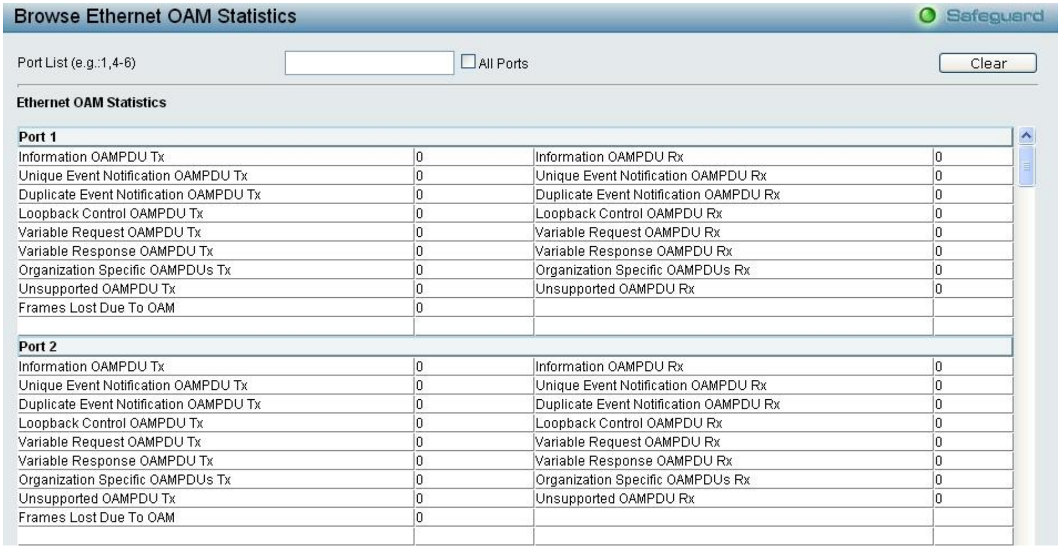
Figure 4.166 - Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

Port: Select the port to be viewed.
Port List: Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click **Find** to locate a specific entry based on the information entered.
Click **Clear** to clear all the information entered in the fields.

Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

The Browse Ethernet OAM Statistics page displays the ports Ethernet OAM statistics information.



Browse Ethernet OAM Statistics

Port List (e.g.:1,4-6) □ All Ports | Clear

Ethernet OAM Statistics

Port 1			
Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDUs Tx	0	Organization Specific OAMPDUs Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		
Port 2			
Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDUs Tx	0	Organization Specific OAMPDUs Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		

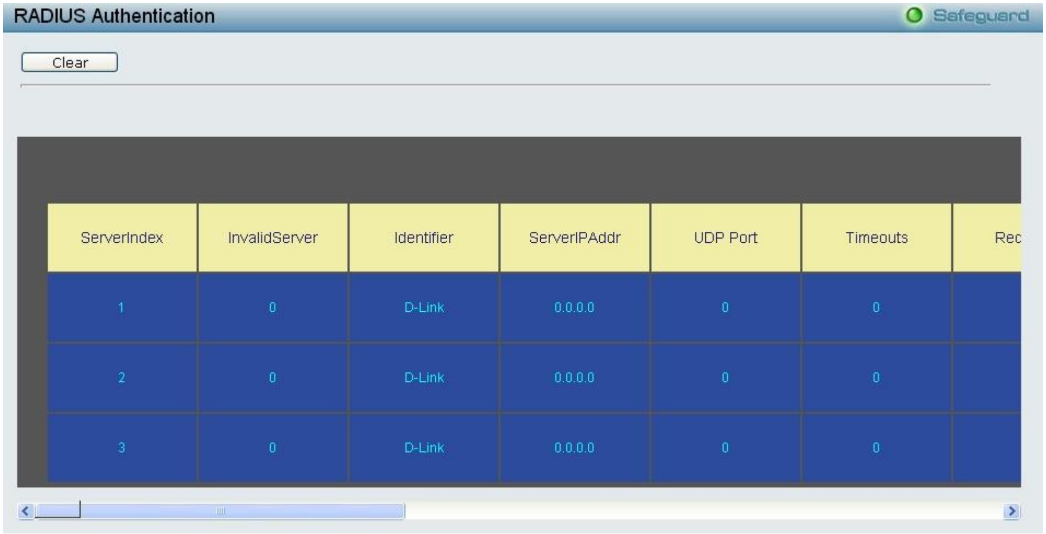
Figure 4.167 - Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

Port List: Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click **Clear** to clear all the information entered in the fields.

Monitoring > Port Access Control > RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. It has one row for each RADIUS authentication server that the client shares a secret with.



RADIUS Authentication

ServerIndex	InvalidServer	Identifier	ServerIPAddr	UDP Port	Timeouts	Rec
1	0	D-Link	0.0.0.0	0	0	
2	0	D-Link	0.0.0.0	0	0	
3	0	D-Link	0.0.0.0	0	0	

Figure 4.168 - Monitoring > Port Access Control > RADIUS Authentication

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the **Clear** button in the top left hand corner.

The following fields can be viewed:

Server Index: The identification number assigned to each RADIUS Authentication server that the client shares a secret with.

UDP Port: The UDP port the client is using to send requests to this server.

Timeouts: The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Requests: The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.

Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.

Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from this server.

Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from this server.

RoundTripTime: The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.

AccessRetrans: The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

PendingRequests: The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.

AccessResponses: The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.

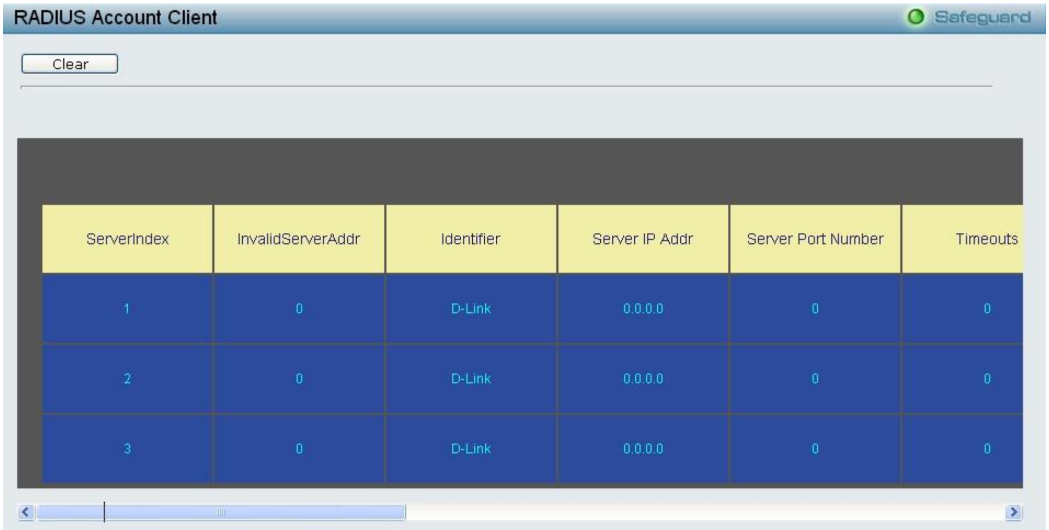
BadAuthenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.

UnknownTypes: The number of RADIUS packets of unknown type which were received from this server on the authentication port.

PacketsDropped: The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Monitoring > Port Access Control > RADIUS Account Client

This RADIUS Account Client page shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. It has one row for each RADIUS authentication server that the client shares a secret with.



ServerIndex	InvalidServerAddr	Identifier	Server IP Addr	Server Port Number	Timeouts
1	0	D-Link	0.0.0.0	0	0
2	0	D-Link	0.0.0.0	0	0
3	0	D-Link	0.0.0.0	0	0

Figure 4.169 - Monitoring > Port Access Control > RADIUS Account Client

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second. To clear the current statistics shown, click the Clear button in the top left hand corner.

The following fields can be viewed:

Server IP Addr: The IP address assigned to each RADIUS Accounting server that the client shares a secret with.

Server Port Number: The UDP port the client is using to send requests to this server.

Timeouts: The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.

Requests: The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.

Responses: The number of RADIUS packets received on the accounting port from this server.

RoundTripTime: The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.

AccessRetrans: The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

PendindRequests: The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.

MalformedResponses: The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

BadAuthenticators: The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.

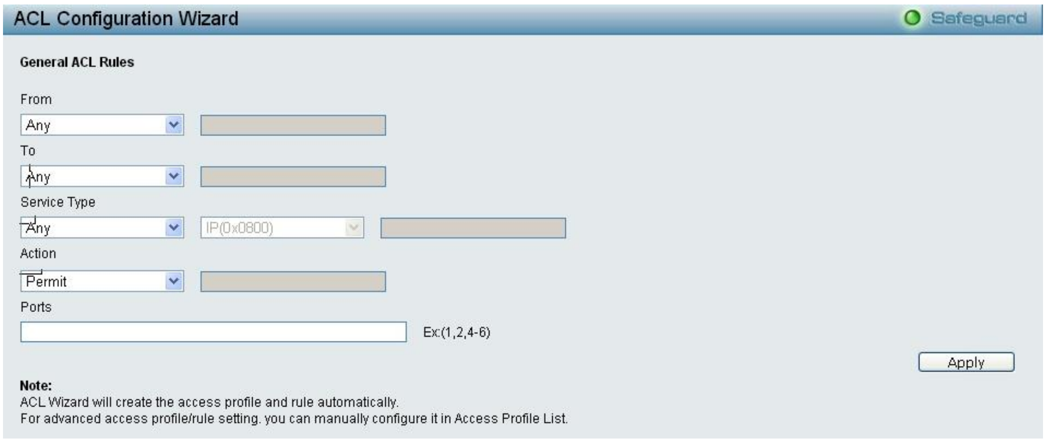
UnknownTypes: The number of RADIUS packets of unknown type which were received from this server on the accounting port.

PacketsDropped: The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

ACL > ACL Configuration Wizard

Access Control List (ACL) allows you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of MAC address, or IP address.

The **ACL Configuration Wizard** will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 240 Rules in total for the switch.



ACL Configuration Wizard

General ACL Rules

From: Any

To: Any

Service Type: Any, IP(0x0800)

Action: Permit

Ports: Ex:(1,2,4-6)

Apply

Note:
ACL Wizard will create the access profile and rule automatically.
For advanced access profile/rule setting, you can manually configure it in Access Profile List.

Figure 4.170 - ACL > ACL Configuration Wizard

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address. The field of format is xx-xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates ACL action will be on packets from any service type.

Ether type - Specifies an Ethernet type for filtering packets.

ICMP All - Indicates ACL action will be on packets from ICMP packets.

IGMP - IGMP packets can be filtered by IGMP message type.

TCP All - Indicates ACL action will be on packets from TCP Packets.

TCP Source Port - Matches the packet to the TCP Source Port.

TCP Destination Port - Matches the packet to the TCP Destination Port.

UDP All - Indicates ACL action will be on packets from UDP Packets.

UDP Source Port - Matches the packet to the UDP Source Port.

UDP Destination Port - Matches the packet to the UDP Destination Port.

Action: Specify the ACL forwarding action matching the rule criteria.

Permit - Forwards packets if all other ACL criteria are met.

Deny - Drops packets if all other ACL criteria is met.

Mirror - Mirrors packets if all other ACL criteria is met.

Rate Limit - Rate limiting is activated if all other ACL criteria is met.

Replace DSCP - Reassigns a new DSCP value to the packet if all other ACL criteria are met.

Port: Enter a range of ports to be configured.

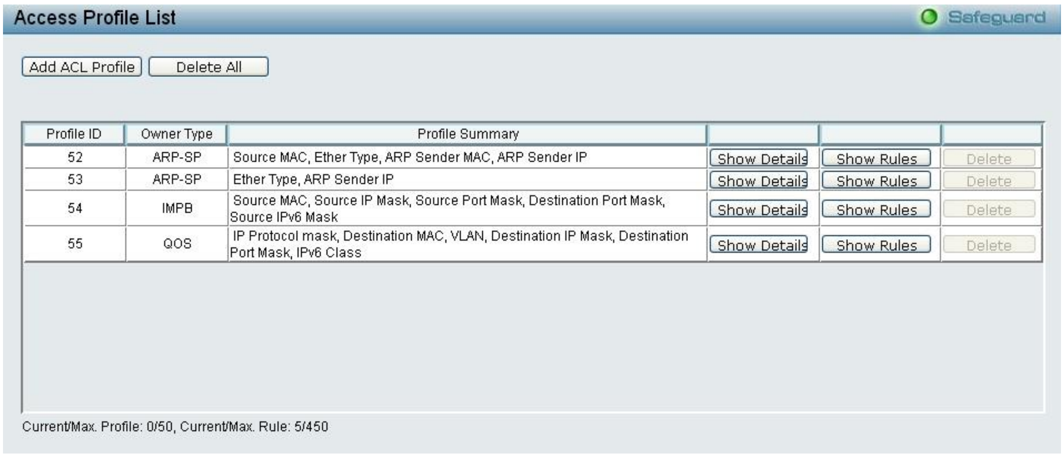
Press **Apply** for the settings to take effect.

NOTE: Once the ACL rules conflict, rules with smaller rule ID will take higher priority.

NOTE: Be careful when configuring ACL rules, an inappropriate may cause management access failed.

ACL > Access Profile List

The Access Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.



Access Profile List

Profile ID	Owner Type	Profile Summary			
52	ARP-SP	Source MAC, Ether Type, ARP Sender MAC, ARP Sender IP	Show Details	Show Rules	Delete
53	ARP-SP	Ether Type, ARP Sender IP	Show Details	Show Rules	Delete
54	IMPB	Source MAC, Source IP Mask, Source Port Mask, Destination Port Mask, Source IPv6 Mask	Show Details	Show Rules	Delete
55	QOS	IP Protocol mask, Destination MAC, VLAN, Destination IP Mask, Destination Port Mask, IPv6 Class	Show Details	Show Rules	Delete

Current/Max. Profile: 0/50, Current/Max. Rule: 5/450

Figure 4.171 - ACL > Access Profile List

The contents of Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are *1~50*, and profile ID 51~55 are reserved for the pre-defined features.

Owner Type: The owner type of ACL profile; it can be normal ACL, Voice VLAN, Surveillance VLAN or ARP Spoofing Protection.

Profile Summary: Displays the profile summary.

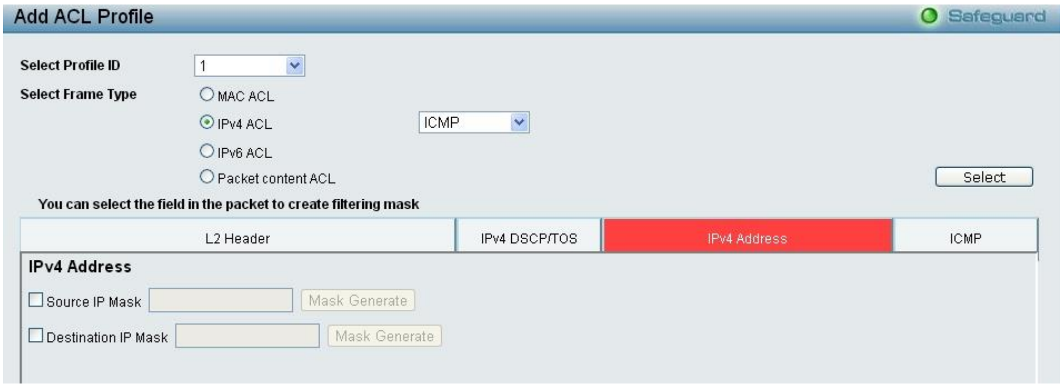
Show Details: To display an ACL's profile details. The ACL profile details are displayed below the ACL table.

Show Rules: To show the access rule in this profile.

To add a new rule, please see **Access Rule List** in the next section.

Delete: To delete an access profile.

To manually add a profile, click **Add ACL Profile**:



Add ACL Profile

Select Profile ID: 1

Select Frame Type:
○ MAC ACL
● IPv4 ACL ICMP
○ IPv6 ACL
○ Packet content ACL

You can select the field in the packet to create filtering mask

IPv4 Address

□ Source IP Mask

□ Destination IP Mask

Figure 4.172 - Add ACL Profile

The steps of adding an access profile is like below:

1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4, IPv6 or Packet content ACL), specify attributes like Untagged/Tagged (for MAC), ICMP/IGMP/TCP/UDP/Protocol ID (for IPv4), or ICMPv6/TCP/UDP (for IPv6), then click **Select** and a simplified frame diagram will be displayed.

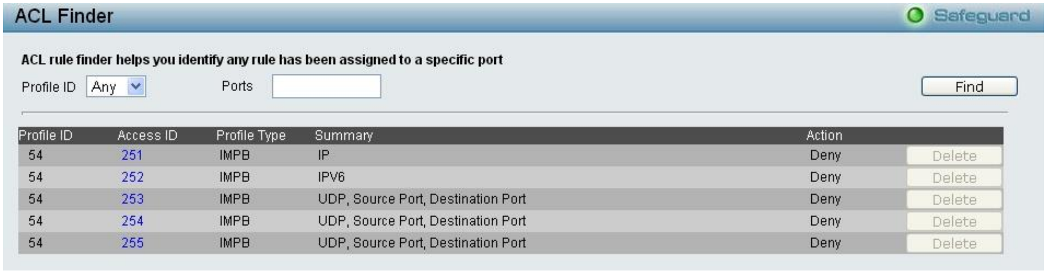
2) Select the field of interest and related columns will be displayed in lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that you want to check. For example, if you want to check a network of 192.168.1.0/24, then you should enter the IP mask as 255.255.255.0.

NOTE: You cannot select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, it will go back to the main Access Profile List page.

ACL > ACL Finder

The ACL Finder page is used to help user to find a previously configured ACL entry. To search for an entry, enter the Profile ID from the drop-down menu, select a port that you wish to view and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.



ACL Finder

ACL rule finder helps you identify any rule has been assigned to a specific port

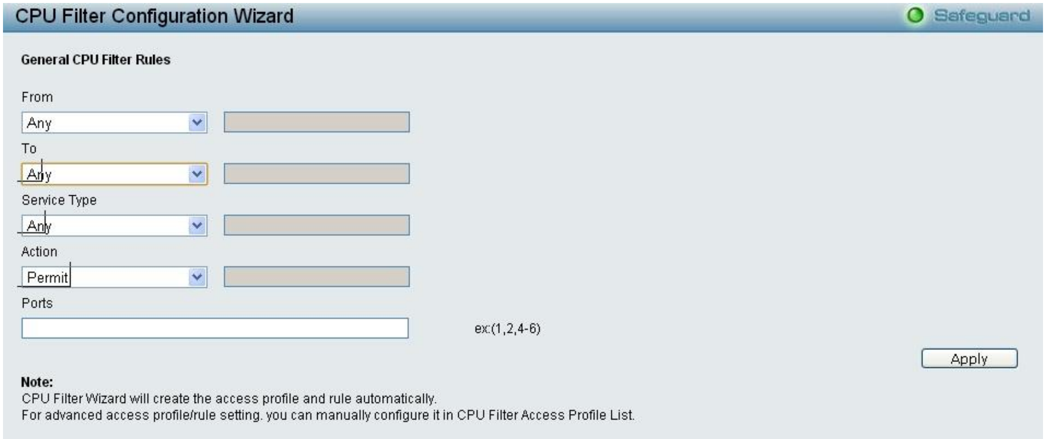
Profile ID: Any Ports:

Profile ID	Access ID	Profile Type	Summary	Action	
54	251	IMPB	IP	Deny	Delete
54	252	IMPB	IPV6	Deny	Delete
54	253	IMPB	UDP, Source Port, Destination Port	Deny	Delete
54	254	IMPB	UDP, Source Port, Destination Port	Deny	Delete
54	255	IMPB	UDP, Source Port, Destination Port	Deny	Delete

Figure 4.173 - ACL > ACL Finder

ACL > CPU Filter Configuration Wizard

The CPU Filter Configuration Wizard will aid with the creation of CPU Filter Rules.



CPU Filter Configuration Wizard

General CPU Filter Rules

From: Any

To: Any

Service Type: Any

Action: Permit

Ports: ex:(1,2,4-6)

Note:
CPU Filter Wizard will create the access profile and rule automatically.
For advanced access profile/rule setting. you can manually configure it in CPU Filter Access Profile List.

Figure 4.174 - ACL > CPU Filter Configuration Wizard

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates CPU Filter action will be on packets from any source.

MAC Address - Indicates CPU Filter action will be on packets from this MAC address.

IPv4 Addresses - Indicates CPU Filter action will be on packets from this IPv4 source address.

IPv6 - Indicates CPU Filter action will be on packets from this IPv6 source address.

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates CPU Filter action will be on packets to any source.

MAC Address - Indicates CPU Filter action will be on packets to this MAC address. The field of format is xx-xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates CPU Filter action will be on packets to this IPv4 source address.

IPv6 - Indicates CPU Filter action will be on packets to this IPv6 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates CPU Filter action will be on packets of any service type.

Ether type - Specifies an Ethernet type for filtering packets.

ICMP All - Indicates CPU Filter action will be on all ICMP packets.

IGMP - IGMP packets can be filtered by IGMP message type.

TCP All - Indicates CPU Filter action will be on all TCP Packets.

TCP Source Port - Take effect if TCP Source Port matches.

TCP Destination Port - Take effect if TCP Destination Port matches.

UDP All - Indicates CPU Filter action will be on all UDP Packets.

UDP Source Port - Take effect if UDP Source Port matches.

UDP Destination Port - Take effect if UDP Destination Port matches.

Action: Specify the CPU Filter forwarding action matching the rule criteria.

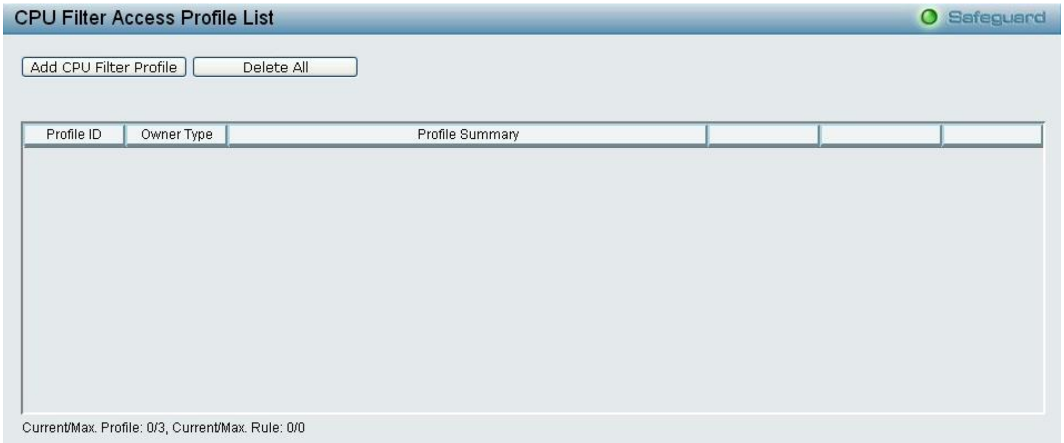
Permit - Forwards packets if all other CPU Filter criteria are met.

Deny - Drops packets if all other CPU Filter criteria is met.

Press **Apply** for the settings to take effect.

ACL > CPU Filter Access Profile List

The CPU Filter Access Profile List provides information for configuring CPU Profiles manually. CPU Filter Access profiles are attached to interfaces, and define how packets are forwarded if they match the CPU Filter criteria.



Profile ID	Owner Type	Profile Summary			

Current/Max. Profile: 0/3, Current/Max. Rule: 0/0

Figure 4.175 - ACL > CPU Filter Access Profile List

The contents of CPU Filter Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are *1~50*, and profile ID *51* is reserved for Voice VLAN.

Owner Type: The owner type of CPU Filter profile, it can be normal CPU Filter, Voice VLAN, Surveillance VLAN or ARP Spoofing Protection.

Profile Summary: Displays the profile summary.

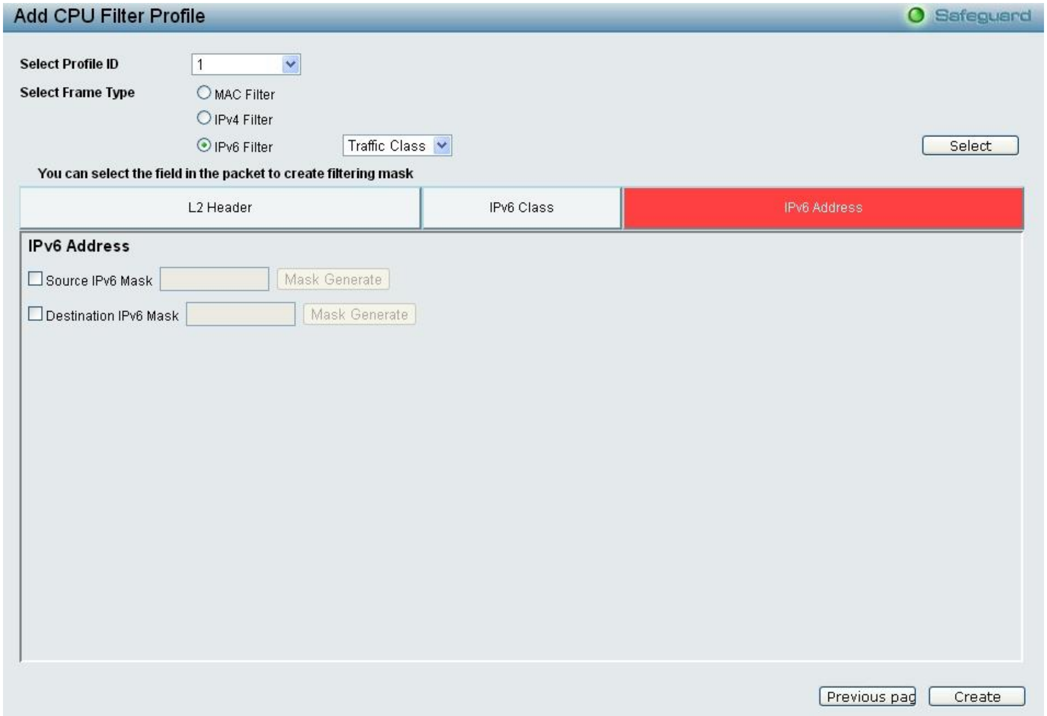
Show Details: To display a CPU Filter's profile details. The CPU Filter profile details are displayed below the CPU Filter table.

Edit/New Rules: To configure or add the CPU access rule in this profile.

To add a new rule, please see **Add CPU Filter Profile** in the next section.

Delete All: To delete all access profile.

To manually add a profile, click **Add CPU Filter Profile**.



Add CPU Filter Profile

Select Profile ID: 1

Select Frame Type: ○ MAC Filter ○ IPv4 Filter ● IPv6 Filter — Traffic Class

You can select the field in the packet to create filtering mask

IPv6 Address

□ Source IPv6 Mask

□ Destination IPv6 Mask

Figure 4.176 - ACL > CPU Filter Access Profile List -Add CPU Filter Profile

The steps of adding a CPU Filter profile is like below:

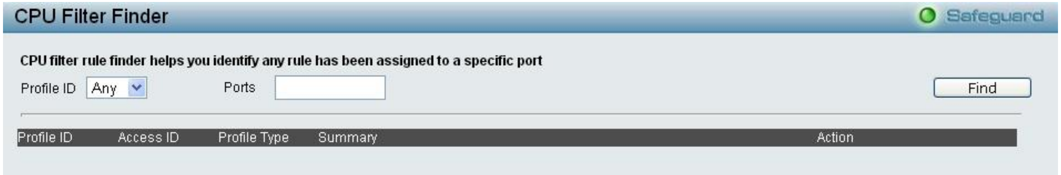
1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4 or IPv6), specify attributes like Untagged/Tagged (for MAC), or ICMP/IGMP/TCP/UDP/Protocol ID (for IPv4), or Traffic Class (for IPv6), then click **Select** and a simplified frame diagram will be displayed.

2) Select the field of interest and related columns will be displayed in lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that you want to check. For example, if you want to check a network of 192.168.1.0/24, then you should enter the IP mask as 255.255.255.0.

3) After the **Profile ID** has been created, it will go back to the main **CPU Filter Access Profile** List page.

ACL > CPU Filter Finder

The CPU Filter Finder page is used to help user to find a previously configured CPU entry. To search for an entry, enter the Profile ID from the drop-down menu, select a port that you wish to view and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.



CPU Filter Finder

CPU filter rule finder helps you identify any rule has been assigned to a specific port

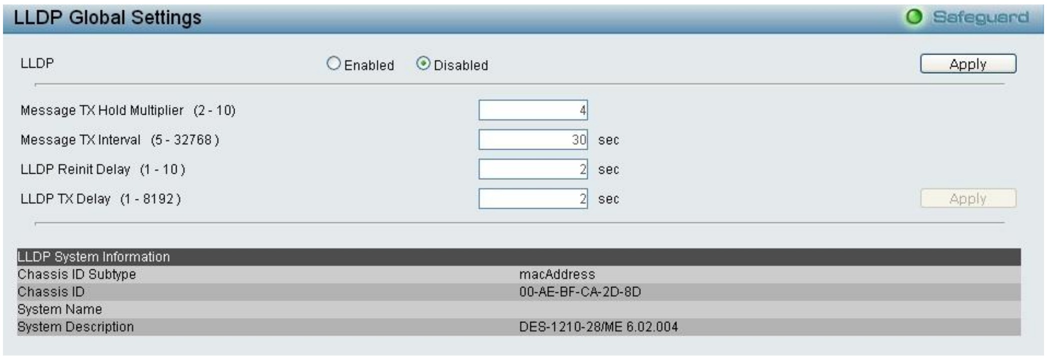
Profile ID: Any Ports:

Profile ID	Access ID	Profile Type	Summary	Action

Figure 4.177 - ACL > CPU Filter Finder

LLDP > LLDP Global Settings

LLDP (Link Layer Discovery Protocol) provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices. The switch will keep the information in the Management Information Base (MIB). SNMP utilities can learn the network topology by obtaining the MIB information in each LLDP device. The LLDP function is enabled by default.



LLDP Global Settings

LLDP ○ Enabled ● Disabled Apply

Message TX Hold Multiplier (2 - 10): 4

Message TX Interval (5 - 32768): 30 sec

LLDP Reinit Delay (1 - 10): 2 sec

LLDP TX Delay (1 - 8192): 2 sec

Apply

LLDP System Information	
Chassis ID Subtype	macAddress
Chassis ID	00-AE-BF-CA-2D-8D
System Name	
System Description	DES-1210-28/ME 6.02.004

Figure 4.178 – LLDP > LLDP Global Settings

LLDP: When this function is *Enabled*, the switch can start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

Message TX Hold Multiplier (2-10): This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is **4**.

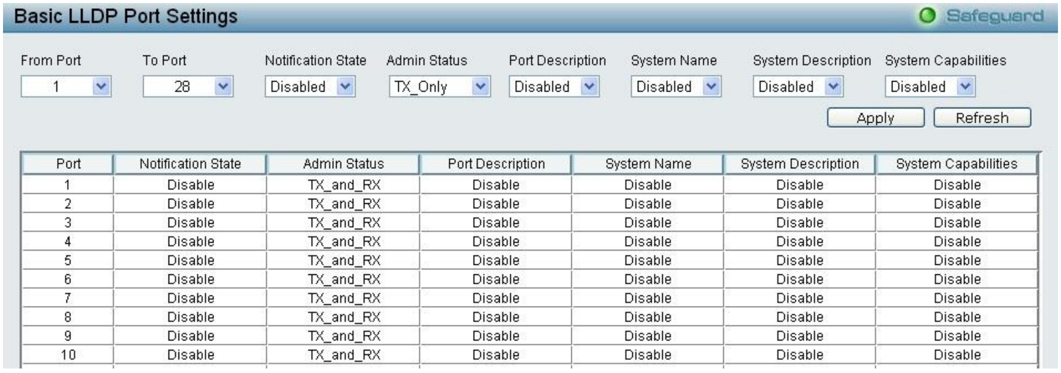
Message TX Interval (5-32768): This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is **30** seconds.

LLDP ReInit Delay (1-10): This parameter indicates the amount of delay from the time adminStatus becomes "disabled" until re-initialization is attempted. The default value is **2** seconds.

LLDP TX Delay (1-8192): This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: 1 < txDelay < (0.25 °— msgTxInterval). The default value is **2** seconds.

LLDP > Basic LLDP Port Settings

The Basic LLDP Port Settings page displays LLDP port information and contains parameters for configuring LLDP port settings.



Basic LLDP Port Settings

From Port	To Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	28	Disabled	TX_Only	Disabled	Disabled	Disabled	Disabled

Apply Refresh

Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	Disable	TX_and_RX	Disable	Disable	Disable	Disable
2	Disable	TX_and_RX	Disable	Disable	Disable	Disable
3	Disable	TX_and_RX	Disable	Disable	Disable	Disable
4	Disable	TX_and_RX	Disable	Disable	Disable	Disable
5	Disable	TX_and_RX	Disable	Disable	Disable	Disable
6	Disable	TX_and_RX	Disable	Disable	Disable	Disable
7	Disable	TX_and_RX	Disable	Disable	Disable	Disable
8	Disable	TX_and_RX	Disable	Disable	Disable	Disable
9	Disable	TX_and_RX	Disable	Disable	Disable	Disable
10	Disable	TX_and_RX	Disable	Disable	Disable	Disable

Figure 4.179– LLDP > Basic LLDP Port Settings

From Port/ To Port: A consecutive group of ports may be configured starting with the selected port.

Notification State: Specifies whether notification is sent when an LLDP topology change occurs on the port. The possible field values are:

Enabled – Enables LLDP notification on the port.

Disabled – Disables LLDP notification on the port. This is the default value.

Admin Status: Specifies the LLDP transmission mode on the port. The possible field values are:

TX_Only – Enables transmitting LLDP packets only.

RX_Only – Enables receiving LLDP packets only.

TX_and_RX – Enables transmitting and receiving LLDP packets. This is the default.

Disabled – Disables LLDP on the port.

Port Description: Specifies whether the Port Description TLV is enabled on the port. The possible field values are:

Enabled – Enables the Port Description TLV on the port.

Disabled – Disables the Port Description TLV on the port.

System Name: Specifies whether the System Name TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Name TLV on the port.

Disabled – Disables the System Name TLV on the port.

System Description: Specifies whether the System Description TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Description TLV on the port.

Disabled – Disables the System Description TLV on the port.

System Capabilities: Specifies whether the System Capabilities TLV is enabled on the port. The possible field values are:

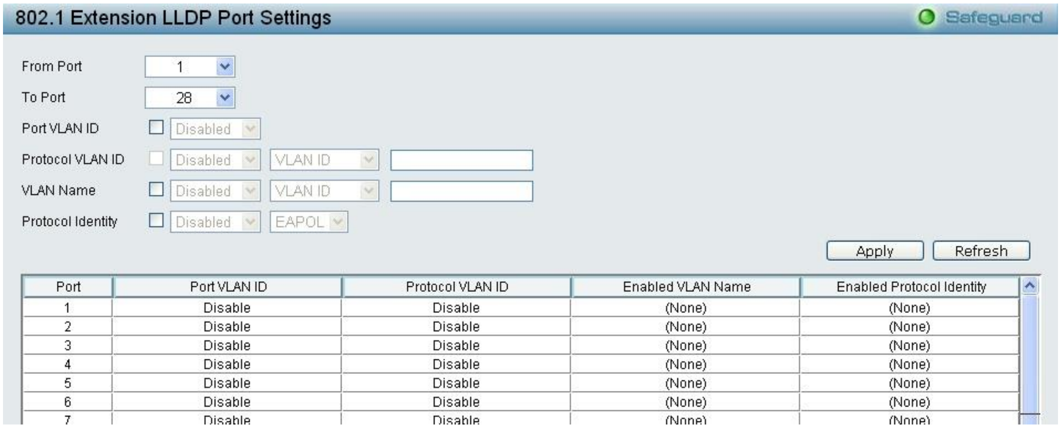
Enabled – Enables the System Capabilities TLV on the port.

Disabled – Disables the System Capabilities TLV on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > 802.1 Extension LLDP Port Settings

This 802.1 Extension LLDP Port Settings page is used to configure the LLDP Port settings.



802.1 Extension LLDP Port Settings

From Port	1		
To Port	28		
Port VLAN ID	□ Disabled		
Protocol VLAN ID	□ Disabled	VLAN ID	
VLAN Name	□ Disabled	VLAN ID	
Protocol Identity	□ Disabled	EAPOL	

Port	Port VLAN ID	Protocol VLAN ID	Enabled VLAN Name	Enabled Protocol Identity
1	Disable	Disable	(None)	(None)
2	Disable	Disable	(None)	(None)
3	Disable	Disable	(None)	(None)
4	Disable	Disable	(None)	(None)
5	Disable	Disable	(None)	(None)
6	Disable	Disable	(None)	(None)
7	Disable	Disable	(None)	(None)

Figure 4.180 – LLDP > 802.1 Extension LLDP Port Settings

From Port / To Port : A consecutive group of ports may be configured starting with the selected port.

Port VLAN ID : Specifies the Port VLAN ID to be enabled or disabled.

Protocol VLAN ID : Specifies the VLAN ID to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN ID.

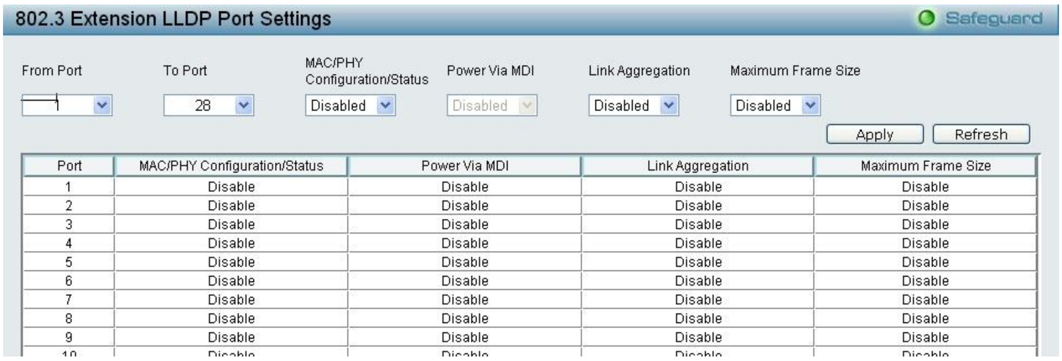
VLAN Name : Specifies the VLAN name to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN Name.

Protocol Identity : Specifies the Protocol Identity to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the EAPOL, LACP, GVRP, STP or ALL.

Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > 802.3 Extension LLDP Port Settings

The 802.3 Extension LLDP Port Settings page displays 802.3 Extension LLDP port information and contains parameters for configuring 802.3 Extension LLDP port settings.



802.3 Extension LLDP Port Settings

From Port	To Port	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size
1	28	Disabled	Disabled	Disabled	Disabled

Port	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size
1	Disable	Disable	Disable	Disable
2	Disable	Disable	Disable	Disable
3	Disable	Disable	Disable	Disable
4	Disable	Disable	Disable	Disable
5	Disable	Disable	Disable	Disable
6	Disable	Disable	Disable	Disable
7	Disable	Disable	Disable	Disable
8	Disable	Disable	Disable	Disable
9	Disable	Disable	Disable	Disable
10	Disable	Disable	Disable	Disable

Figure 4.181 – LLDP > 802.3 Extension LLDP Port Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

MAC/PHY Configuration/Status: Specifies whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are:

Enabled – Enables the MAC/PHY Configuration Status on the port.

Disabled – Disables the MAC/PHY Configuration Status on the port.

Power Via MDI: Advertises the Power via MDI implementations supported by the port. The possible field values are:

Enabled – Enables the Power via MDI configured on the port.

Disabled – Disables the Power via MDI configured on the port.

Link Aggregation: Specifies whether the link aggregation is enabled on the port. The possible field values are:

Enabled – Enables the link aggregation configured on the port.

Disabled – Disables the link aggregation configured on the port.

Maximum Frame Size: Specifies whether the Maximum Frame Size is enabled on the port. The possible field values are:

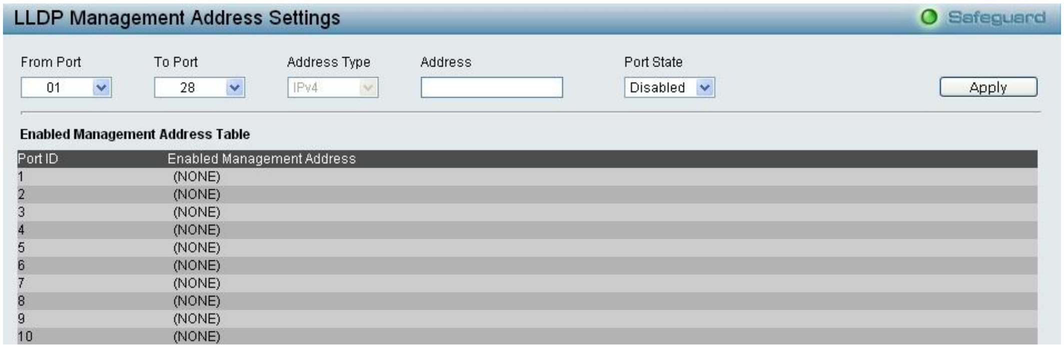
Enabled – Enables the Maximum Frame Size configured on the port.

Disabled – Disables the Maximum Frame Size configured on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > LLDP Management Address Settings

The LLDP Management Address Settings allows the user to set management address which is included in LLDP information transmitted.



LLDP Management Address Settings

From Port	To Port	Address Type	Address	Port State
01	28	IPv4		Disabled

Enabled Management Address Table

Port ID	Enabled Management Address
1	(NONE)
2	(NONE)
3	(NONE)
4	(NONE)
5	(NONE)
6	(NONE)
7	(NONE)
8	(NONE)
9	(NONE)
10	(NONE)

Figure 4.182 – LLDP > LLDP Management Address Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

Address Type: Specify the LLDP address type on the port. The value is always IPv4.

Address: Specify the address.

Port State: Specify whether the Port State is enabled n the port. The possible field values are:

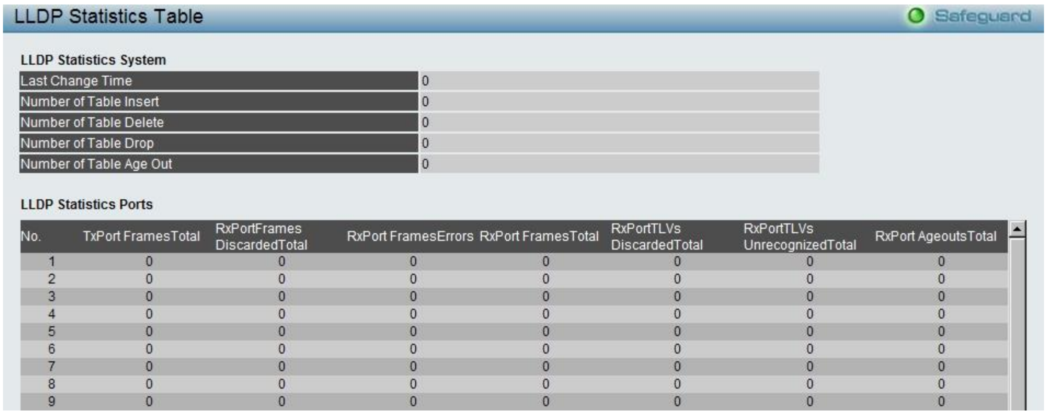
Enabled – Enables the port state configured on the port.

Disabled – Disables the port state configured on the port.

Click **Apply** to implement changes made.

LLDP > LLDP Statistics Table

The LLDP Statistics page displays an overview of all LLDP traffic.



LLDP Statistics Table

LLDP Statistics System

Last Change Time	0
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Age Out	0

LLDP Statistics Ports

No.	TxPort FramesTotal	RxPortFrames DiscardedTotal	RxPort FramesErrors	RxPort FramesTotal	RxPortTLVs DiscardedTotal	RxPortTLVs UnrecognizedTotal	RxPort AgeoutsTotal
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0

Figure 4.183 – LLDP > LLDP Statistics Table

The following information can be viewed:

LLDP Statistics System: Displays the counters that refer to the whole switch.

Last Change Time – Displays the time for when the last change entry was last deleted or added. It is also displays the time elapsed since last change was detected.

Number of Table Insert – Displays the number of new entries inserted since switch reboot.

Number of Table Delete – Displays the number of new entries deleted since switch reboot.

Number of Table Drop – Displays the number of LLDP frames dropped due to that the table was full.

Number of Table Age Out – Displays the number of entries deleted due to Time-To-Live expiring.

LLDP Port Statistics: Displays the counters that refer to the ports.

TxPort FramesTotal – Displays the total number of LLDP frames transmitted on the port.

RxPort FramesDiscarded – Displays the total discarded frame number of LLDP frames received on the port.

RxPort FramesErrors – Displays the Error frame number of LLDP frames received on the port.

RxPort Frames – Displays the total number of LLDP frames received on the port.

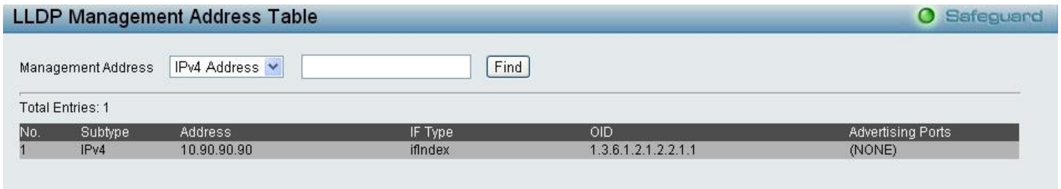
RxPortTLVsDiscarded – Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

RxPortTLVsUnrecognized – Displays the number of well-formed TLVs, but with a known type value.

RxPort Ageouts – Each LLDP frame contains information about how long time the LLDP information is valid. If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

LLDP > LLDP Management Address Table

The LLDP Management Address Table page displays the detailed management address information for the entry.



LLDP Management Address Table

Management Address: IPv4 Address

Total Entries: 1

No.	Subtype	Address	IF Type	OID	Advertising Ports
1	IPv4	10.90.90.90	ifIndex	1.3.6.1.2.1.2.2.1.1	(NONE)

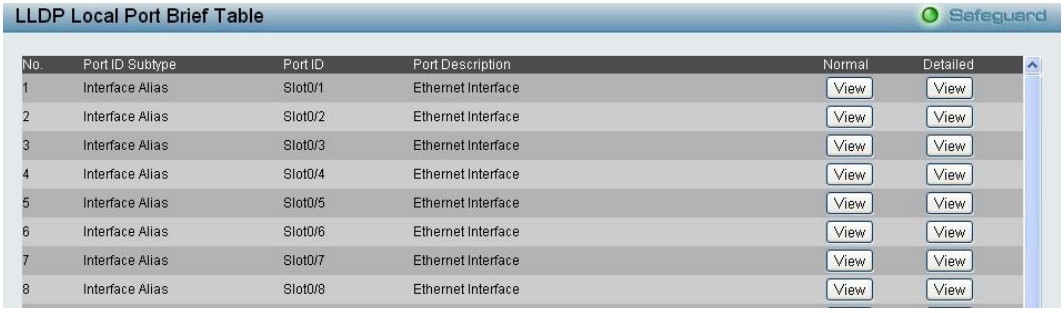
Figure 4.184 – LLDP > LLDP Management Address Table

Management Address: Specifies IPv4 or IPv6 address then enter the address. Click **Search** and the table will update and display the values required.

Subtype: Displays the managed address subtype. For example, MAC or IPv4.
Management Address: Displays the IP address.
IF Type: Displays the IF Type.
OID: Displays the SNMP OID.
Advertising Ports: Displays the advertising ports.

LLDP > LLDP Local Port Table

The LLDP Local Port Table page displays LLDP local port information.



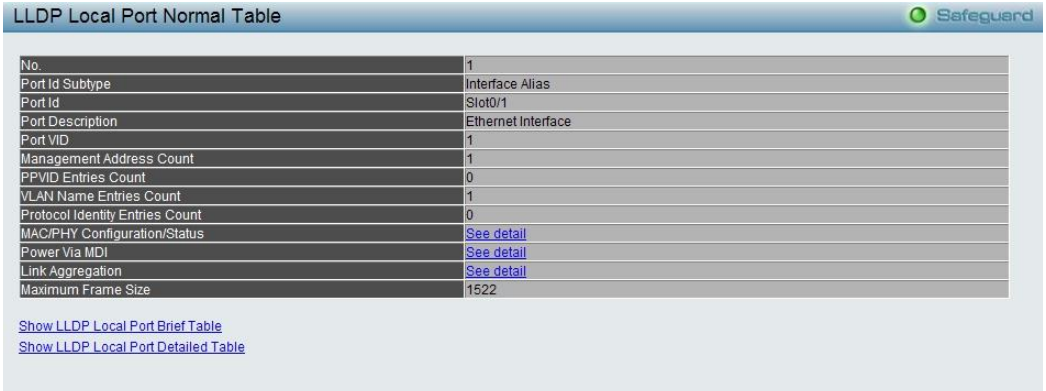
LLDP Local Port Brief Table

No.	Port ID Subtype	Port ID	Port Description	Normal	Detailed
1	Interface Alias	Slot0/1	Ethernet Interface	View	View
2	Interface Alias	Slot0/2	Ethernet Interface	View	View
3	Interface Alias	Slot0/3	Ethernet Interface	View	View
4	Interface Alias	Slot0/4	Ethernet Interface	View	View
5	Interface Alias	Slot0/5	Ethernet Interface	View	View
6	Interface Alias	Slot0/6	Ethernet Interface	View	View
7	Interface Alias	Slot0/7	Ethernet Interface	View	View
8	Interface Alias	Slot0/8	Ethernet Interface	View	View

Figure 4.185 –LLDP > LLDP Local Port Table

Port : Displays the port number.
Port ID Subtype: Displays the port ID subtype.
Port ID: Displays the port ID (Unit number/Port number).
Port Description: Displays the port description.

Click **View** of Normal column to display more information.



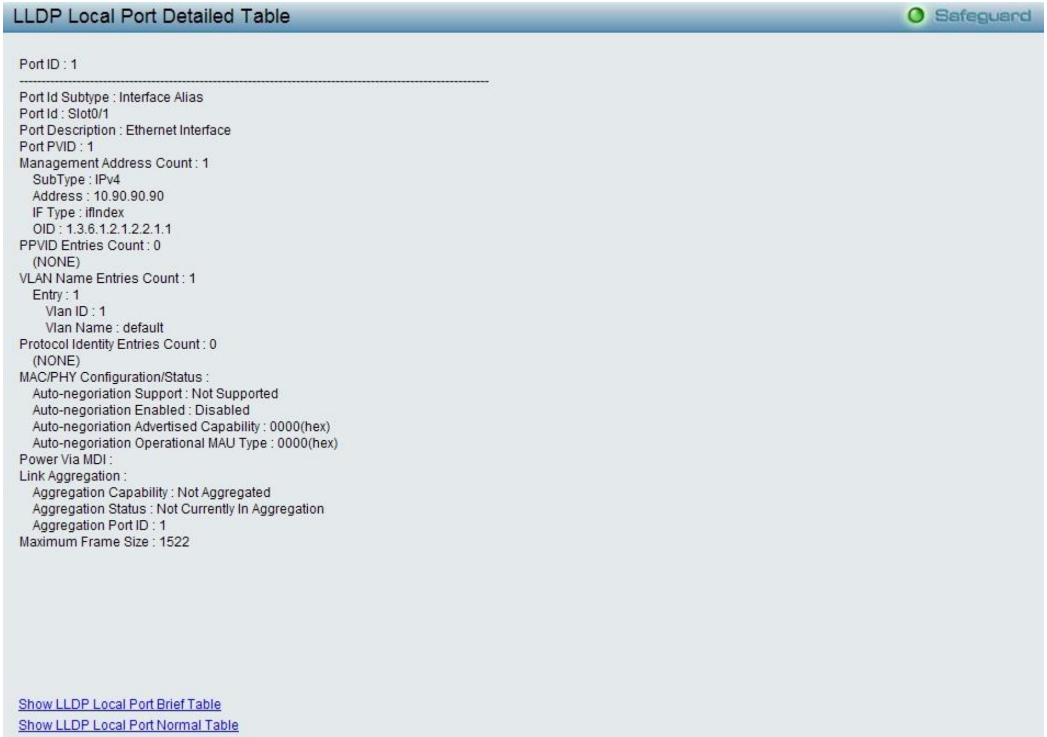
LLDP Local Port Normal Table

No.	1
Port Id Subtype	Interface Alias
Port Id	Slot0/1
Port Description	Ethernet Interface
Port VID	1
Management Address Count	1
PPVID Entries Count	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	See detail
Power Via MDI	See detail
Link Aggregation	See detail
Maximum Frame Size	1522

Show LLDP Local Port Brief Table
Show LLDP Local Port Detailed Table

Figure 4.186 – LLDP > LLDP Local Port Normal Table

Click **View** of Detailed column to display detail information.

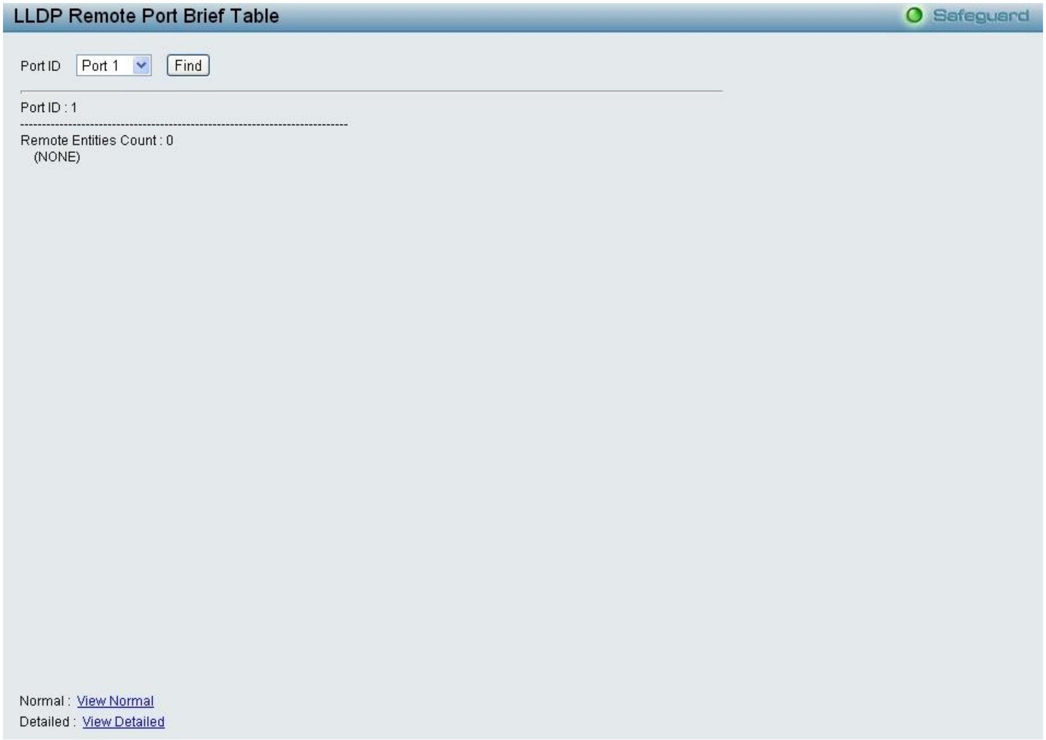

LLDP Local Port Detailed Table
Safeguard
Show LLDP Local Port Brief Table
Show LLDP Local Port Normal Table

```
Port ID : 1
----------------------------------------------------------------------------------------------------
Port Id Subtype : Interface Alias
Port Id : Slot0/1
Port Description : Ethernet Interface
Port PVID : 1
Management Address Count : 1
   SubType : IPv4
   Address : 10.90.90.90
   IF Type : ifIndex
   OID : 1.3.6.1.2.1.2.2.1.1
PPVID Entries Count : 0
   (NONE)
VLAN Name Entries Count : 1
   Entry : 1
      Vlan ID : 1
      Vlan Name : default
Protocol Identity Entries Count : 0
   (NONE)
MAC/PHY Configuration/Status :
   Auto-negoriation Support : Not Supported
   Auto-negoriation Enabled : Disabled
   Auto-negoriation Advertised Capability : 0000(hex)
   Auto-negoriation Operational MAU Type : 0000(hex)
Power Via MDI :
Link Aggregation :
   Aggregation Capability : Not Aggregated
   Aggregation Status : Not Currently In Aggregation
   Aggregation Port ID : 1
Maximum Frame Size : 1522
```

Figure 4.187 – LLDP > LLDP Local Port Detailed Table

LLDP > LLDP Remote Port Table

This LLDP Remote Port Table page is used to display the LLDP Remote Port Brief Table. Select port number and click **Search** to display additional information.

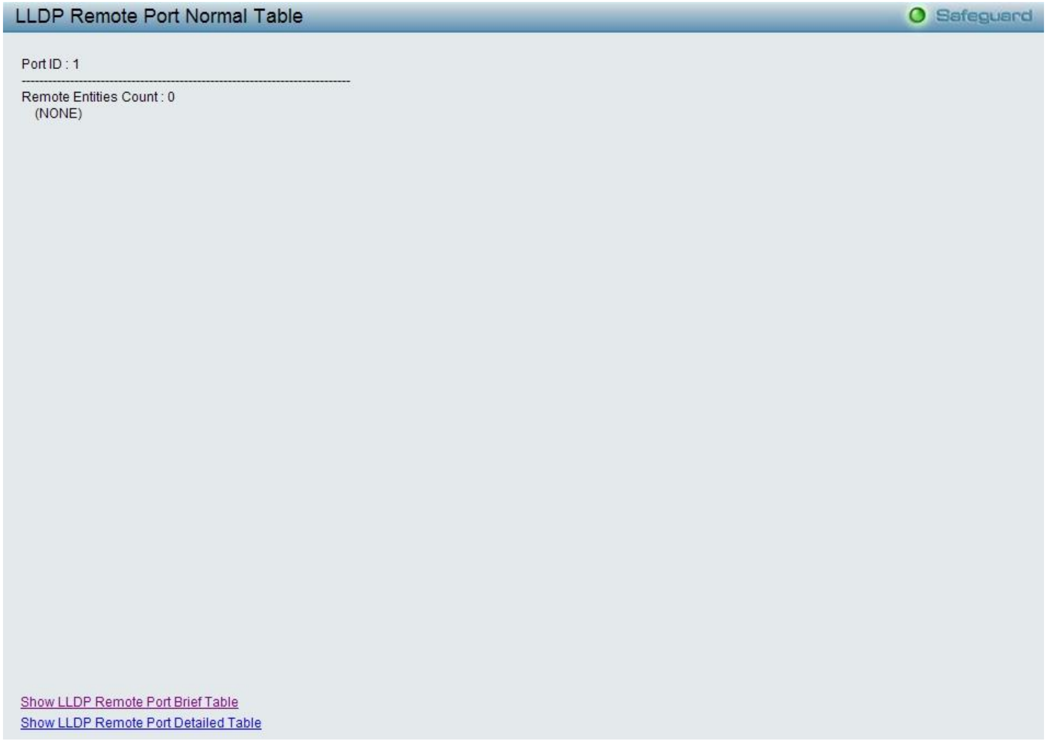


Port ID: Port 1

```
Port ID : 1
----------------------------------------------------------------------
Remote Entities Count : 0
   (NONE)
```

Figure 4.188 – LLDP > LLDP Remote Port Table

To view the settings for a remote port, click **View Normal** and the following page displays.



LLDP Remote Port Normal Table

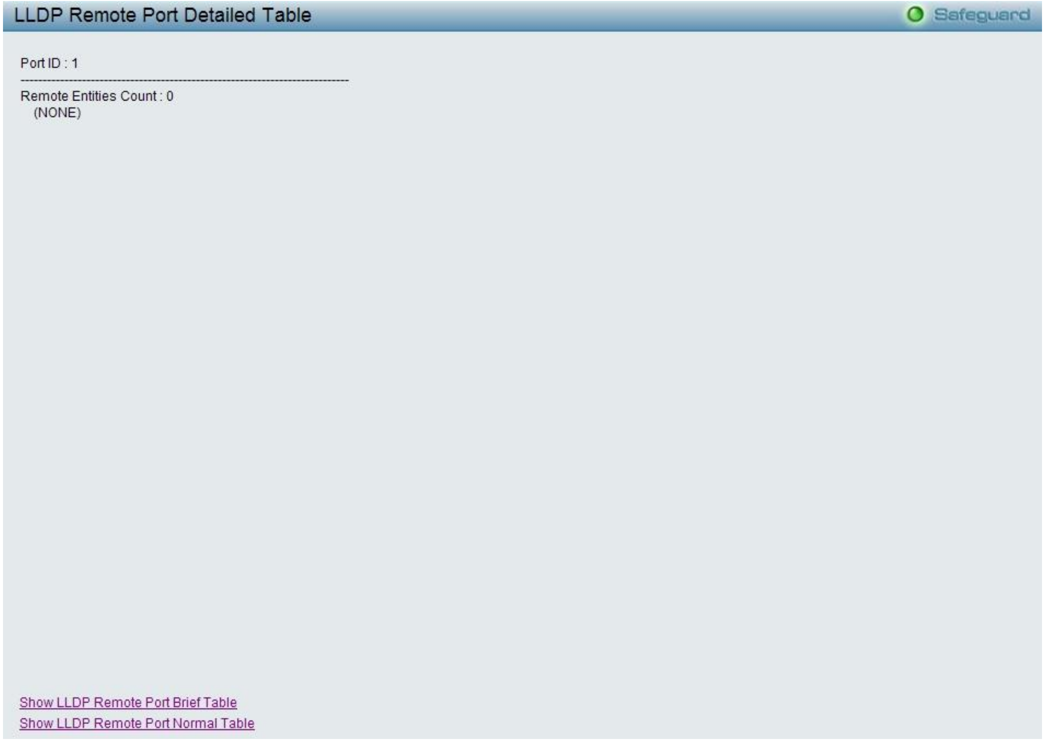
Port ID : 1

Remote Entities Count : 0
(NONE)

Show LLDP Remote Port Brief Table
Show LLDP Remote Port Detailed Table

Figure 4.189 – LLDP > LLDP Remote Port Normal Table

To view the detail settings for a remote port, click **View Detailed** and the following page displays.



LLDP Remote Port Detailed Table

Port ID : 1

Remote Entities Count : 0
(NONE)

Show LLDP Remote Port Brief Table
Show LLDP Remote Port Normal Table

Figure 4.190 – LLDP > LLDP Remote Port Detailed Table

Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential in solving network bottlenecks, which frequently develops as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology, can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. With expected advances in the coming years in silicon technology and digital signal processing, which will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, a flexible foundation for the next generation of network technology products will be created. This will outfit your network with a powerful 1000-Mbps-capable backbone/server connection.

Fast Ethernet Technology

The growing importance of LANs, and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments, which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

Appendix B - Ethernet Technology

Hardware Specifications

Key Components / Performance	
Switching Capacity	DES-1210-10/ME: 5.6Gbps DES-1210-26/ME: 12.8Gbps DES-1210-28/ME: 12.8Gbps
Max. Forwarding Rate	DES-1210-10/ME: 4.2Mpps DES-1210-26/ME: 9.5Mpps DES-1210/28/ME : 9.5Mpps
Forwarding Mode	Store and Forward
Packet Buffer memory	384K Bytes
DDRII for CPU	128M Bytes
Flash Memory	16M Bytes
Console Port	A RJ-45 console port for out-of-band configuration of the software features.
Port Functions	
10/100BASE-TX Ethernet ports	8 10/100Base-TX ports compliant with the following standards for DES1210-10/ME: - IEEE 802.3 - IEEE 802.3u - Supports Half/Full-Duplex operations - Back Pressure for Half-Duplex mode - Head-of-line blocking prevention - IEEE 802.3x Flow Control support for Full-Duplex mode - Auto MDI/MDIX - Auto-negotiation 24 10/100Base-TX ports compliant with the following standards for DES-1210-26/ME and DES-1210-28/ME: - IEEE 802.3 - IEEE 802.3u - Supports Half/Full-Duplex operations - Back Pressure for Half-Duplex mode - Head-of-line blocking prevention - IEEE 802.3x Flow Control support for Full-Duplex mode - Auto MDI/MDIX - Auto-negotiation
10/100/1000BASE-T ports	2 10/100/1000Base-T ports compliant with the following standards: - IEEE 802.3 - IEEE 802.3u - IEEE 802.3ab - IEEE 802.3z - Supports Full-Duplex operations - IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention.
Combo ports	2 combo SFP and 2 individual SFP ports supporting SFP Transceivers:

	- DEM-310GT (1000BASE-LX, 10km) - DEM-311GT (1000BASE-SX, 550m) - DEM-314GT (1000BASE-LH, 50km) - DEM-315GT (1000BASE-ZX, 80km) - DEM-312GT2 (1000BASE-SX, 2km) - DEM-210 (100BASE-FX, 15km) - DEM-211 (100BASE-FX, 2km) 2 combo SFP and 2 individual SFP ports supporting WDM Transceivers: - DEM-330T (1000Base-BX,TX-1550/RX-1310nm, 10km) - DEM-330R (1000Base-BX,TX-1310/RX-1550nm, 10km) - DEM-331T (1000Base-BX,TX-1550/RX-1310nm, 40km) - DEM-331R (1000Base-BX,TX-1310/RX-1550nm, 40km) - DEM-220T (100Base-BX, TX-1550/RX-1310nm, 20km) - DEM-220R (100Base-BX, TX-1310/RX-1550nm, 20km)
Physical & Environment	
Internal Power Supply	DES-1210-10/ME: 24W AC Input: 100 – 240 VAC, 50-60 Hz DES-1210-26/ME: 24W AC Input: 100 – 240 VAC, 50-60 Hz DES-1210-28/ME: 24W AC Input: 100 – 240 VAC, 50-60 Hz
Operation Temperature	-5~50°C
Storage Temperature	-40~70°C
Operation Humidity	10%~90% RH
Storage Humidity	5%~90% RH
EMI Certifications	FCC, CE,
Safety Certifications	cUL, LVD

Features

L2 Features

- Supports up to 8K MAC address
- Supports 256 static MAC
- IGMP snooping:
  - Supports 256 multicast groups
  - Supports at least 256 static multicast groups
- Limited IP Multicast:
  - Support up to 24 profiles and each profile can add up to 256 multicast groups
  - Able to configure the maximum multicast group number for a port, ranging from 1-256
- MLD Snooping:
  - Supports 256 MLD snooping groups
  - Supports 256 static multicast addresses
- 802.1D Spanning Tree
- 802.1w RSTP
- 802.1s MSTP: up to 8 instances
- Loopback Detection
- 802.3ad Link Aggregation: Support max 8 groups per device, 8 ports per group
- Port mirroring
- IPv6 Neighbor Discovery:
  - Supports Max 512 ND entries
  - Support up to 64 static ND entries
- SNTP
- LLDP
- L2 Multicast Filtering

VLAN

- 802.1Q VLAN standard (VLAN Tagging)
- Total 4094 VLAN groups
- Asymmetric VLAN
- Management VLAN
- ISM VLAN
- GVRP: Support 256 dynamic VLANs
- VLAN Trunking
- Supports Port-based Q-in-Q
- 802.1v

L3 Features

- ARP:
  - Max 256 ARP entries
  - Support 255 static ARP
  - Support Gratuitous ARP

QoS (Quality of Service)

- Be able to classify packets according to follow contents:
  - Switch port
  - 802.1p priority
  - VID
  - MAC address
  - IP address
  - IPv6 Traffic Class
  - TCP/UDP Port
  - DSCP
  - TOS
  - Protocol type
- - TCP/UDP port number Up to 4 queues per port
- Supports Strict / WRR mode in queue handling
- Support Port and Flow based bandwidth control

AAA

- 802.1X Local/RADIUS/TACACS+ server
- 802.1X port-based/MAC-based access control
- RADIUS Accounting: Support Network accounting (for 802.1x user)
- User Account Privilege for Mgmt Access:
  - Support 4 level user account
    - Operator (Read/Write)
    - Administrator (Read/Write)
    - Power user (for account management and service)
    - User (read only)

ACL

- Max 256 ingress ACL profile, 256 ingress ACL rules
- Each rule can be associated to a single port, multiple ports
- Support different ACL policy packet contents:
  - Switch port
  - MAC address
  - Ether type
  - IPv4 address
  - IPv6 address
  - TOS
  - 802.1p
  - DSCP
  - Protocol type
  - TCP/UDP port number
  - IPv6 traffic class

Security

- Trusted Host
- Port Security:Support 64 MACs per port
- Traffic Segmentation
- D-Link Safeguard Engine
- Broadcast Storm Control
- ARP Spoofing Prevention: Supports max 64 entries

- DHCP Server Screening: Able to configure IPv4 and IPv6 addresses for DHCP server.
- SSH: Support v2 and IPv6
- SSL: Support v3, IPv4 and IPv6
- Smart Binding

  - Supports D-Link IMPB

  - Supports ARP packet Inspection as default, ARP and IP packet Inspection as option.

  - Supports DHCP Snooping
- Dos Attack Prevention

OAM

- Cable Diagnostics: Detect and show cable length and status
- 802.3ah
  - Support 802.3ah link layer remote loopback and discovery
  - 802.3ah D-Link extension: D-link Undirectional Link Detection (DULD)

Management

- Web-based GUI
- D-Link proprietary CLI
- Telnet Server
- SNMP support
- DHCP client
- DHCP Relay: Support DHCP local relay, option 82 and 12.
- DHCPv6 Relay: Support DHCP local relay and option 37
- SNMP Trap
- System Log: Support log server with IPv4 or IPv6 address
- RMON v1/v2
- Password access control
- Password Encryption
- Web-based configuration backup / restoration
- Reset, Reboot

Appendix C – Rack mount Instructions

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Appendix D – Cables and Connectors

Ethernet Cable:

When connecting the Switch to another switch, a bridge or hub, a normal cable is necessary. Please review these products for matching cable pin assignment.

The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments.

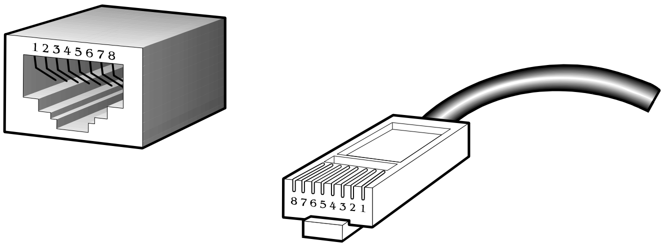


Figure D- 1. The standard RJ-45 port and connector

RJ-45 Pin Assignments		
Contact	**MDI-X Port**	**MDI-II Port**
1	RD+ (receive)	TD+ (transmit)
2	RD- (receive)	TD- (transmit)
3	TD+ (transmit)	RD+ (receive)
4	1000BASE-T	1000BASE-T
5	1000BASE-T	1000BASE-T
6	TD- (transmit)	RD- (receive)
7	1000BASE-T	1000BASE-T
8	1000BASE-T	1000BASE-T

Console Cable:

When connecting the Switch a PC, a Console cable is necessary. The following diagrams and tables show the standard Console-to-DJ-45 receptacle/connector and their pin assignments.

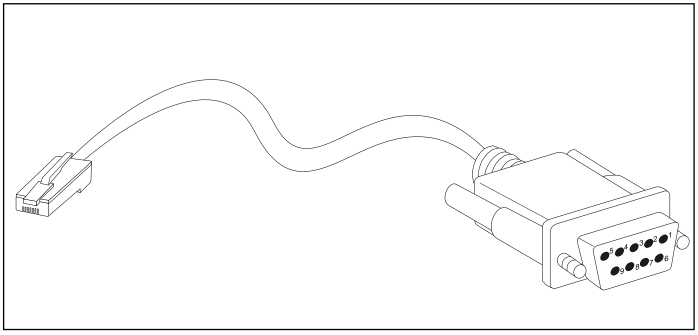


Figure B- 2. Console-to-RJ-45 Cable

Console-RJ-45 Pin Assignments		
Pin	**Console (DB9/RS232)**	**RJ-45**
1	Not Used	Not Used
2	RXD	Not Used
3	TXD	TXD
4	Not Used	GND
5	GND (shared)	GND
6	Not Used	RXD
7	Not Used	Not Used
8	Not Used	Not Used

Appendix E– Module Specs and Cable Lengths

Use the following table to as a guide for the module specs and maximum cable lengths.

Standard	Media Type	Maximum Distance
SFP	1000BASE-LX, Single-mode fiber module 1000BASE-SX, Multi-mode fiber module 1000BASE-LHX, Single-mode fiber module 1000BASE-ZX, Single-mode fiber module	10km 550m / 2km 50km 80km
1000BASE-T	Category 5e UTP Cable	100m
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3, 4 or 5 UTP Cable (10 Mbps)	100m
DEM-310GT	1000Base-LX, Single-mode	10km
DEM-311GT	1000ase-SX, Multi-mode	500m
DEM-312GT2	1000Base-SX, Multi-mode	2km
DEM-314GT	1000BASE-LHX, Single-mode	50km
DEM-315GT	1000BASE-ZX, Single-mode	80km
DEM-210	100BASE-FX, Single-mode	15km
DEM-211	100BASE-FX, Multi-mode	2km
DEM-220T	TX-1550/RX-1310nm, Single-mode	Up to 20km
DEM-220R	TX-1310/RX-1550nm, Single-mode	Up to 20km
DEM-330T	TX-1550/RX-1310nm, Single-mode	Up to 10km
DEM-330R	TX-1310/RX-1550 nm, Single-mode	Up to 10km
DEM-331T	TX-1550/RX-1310 nm, Single-Mode	Up to 40km
DEM-331R	TX-1310/RX-1550 nm, Single-Mode	Up to 40km

Network pluggable optical modules meet the following regulatory requirements:

- Class 1 Laser Product
- EN60825-1+A2:2001 or later, European laser standard
- FCC 21 CFR Chapter 1, Subchapter J in accordance with FDA & CDRH requirements

D-Link®

Building Networks for People