D-Link®
Building Networks for People

User Manual

Product Model : DGS-1100-06/ME

Metro Ethernet Managed Switch

Release 1.00

Table of Contents

About This Guide

This guide provides instructions to install the D-Link Metro Ethernet Switch DGS-1100-06/ME 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 DGS-1100-06/ME, 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

The DGS-1100-06/ME is a member of the D-Link Metro Ethernet Switches. This 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 through Telnet, and the Smart Console Utility.

DGS-1100-06/ME

Metro Ethernet Switch with 5 10/100/1000Base-T ports plus 1 dual speed SFP.

Front Panel

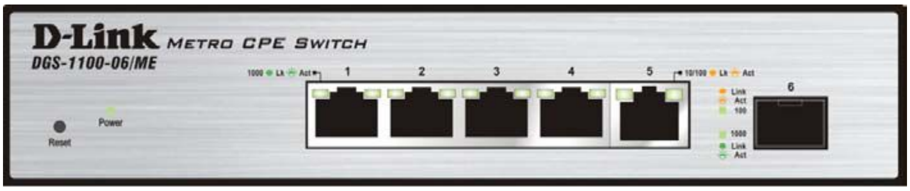


Figure 1.1 – DGS-1100-06/ME Front Panel

Power LED: The Power LED lights up when the Switch is connected to a power source.

Reset: By pressing the Reset button the Switch will change back to the default configuration and all changes will be lost.

Port Link/Act/Speed LED (1-5): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.

Port Link/Ace/Speed LED (6): The Link/Act/Speed LED flashes which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has amber light indicates that port is running on 10M or 100M.

NOTE: The MiniGBIC ports are shared with normal RJ-45 ports 5. 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.

Rear Panel

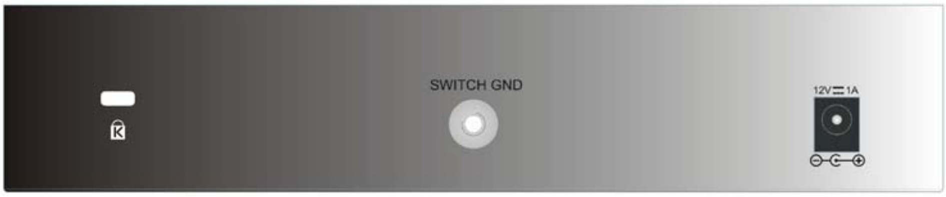


Figure 1.2 – DGS-1100-06/ME Rear Panel

Power: Connect the supplied AC power cable to this port.

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 adapter
- Four rubber feet
- Screws and two mounting brackets
- Wall-mount kit

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.

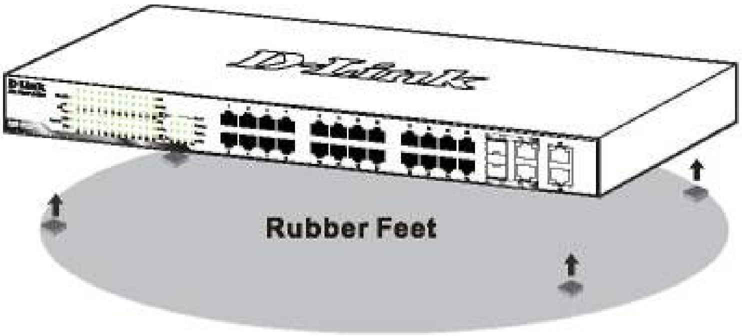


Figure 2.1 – Attach the adhesive rubber pads to the bottom

Wall-mount

The Switch can be mounted on a wall. Two mounting slots are provided on the bottom of the switch for this purpose.

Please follow the installation steps to complete wall-mount process.

- **Mounting on a cement wall**

  Step 1: Mount the nylon screw anchors ø5 x 22L mm (included in the accessory kit) into a cement wall
  Step 2: Drive the T3 x 15L screws into the nylon screw anchors.
  Step 3: Hook the mounting holes of the switch back on the screws.

- **Mounting on a wood wall**

  Step 1: Drive the T3 x 15L screws into a wood wall.
  Step 2. Hook the mounting holes of the switch back on the screws.

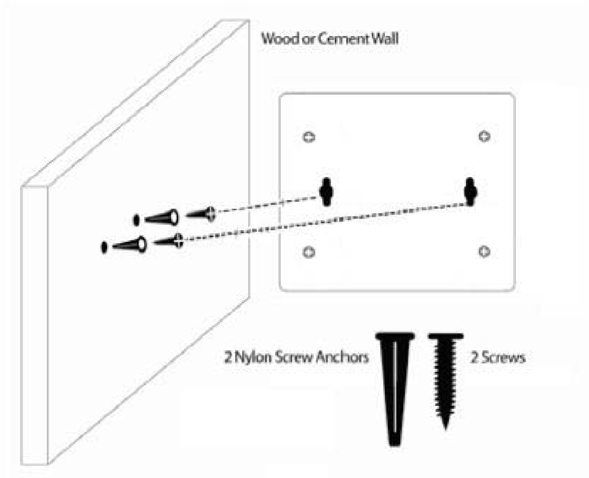


Figure 2.2 – Wall mount installation

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).

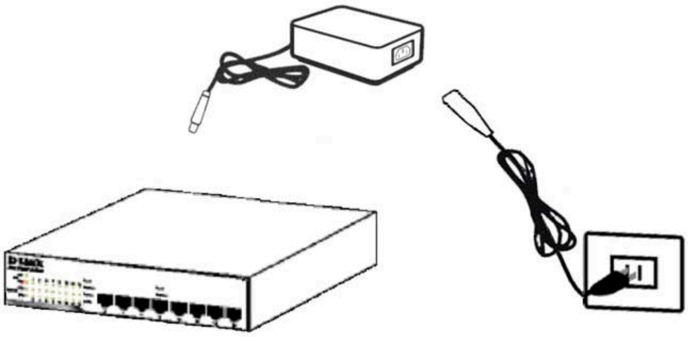


Figure 2.3 – Plugging the switch into an outlet

⚠ **CAUTION:** Do not turn on the power switch of DGS-1100-06/ME before power cables are connected. Power surge may cause damage to the Switch.

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 6/7 or later version
- Netscape 8 or later version
- Mozilla
- Firefox 1.5/2.0 or later version
- Chrome 5.0 or later version
- Safari 4.0 or later version

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.

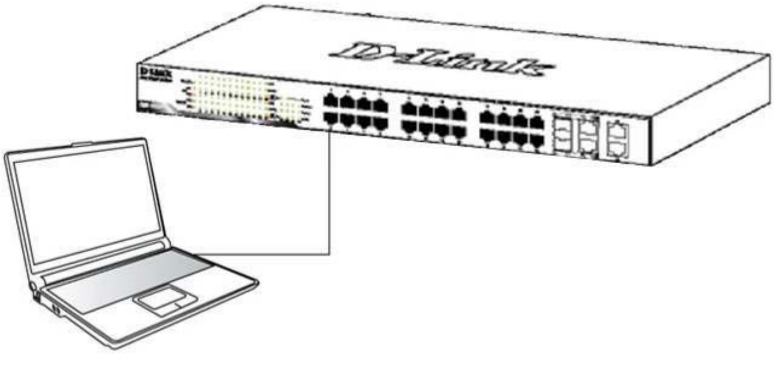


Figure 3.1 – Connected Ethernet cable

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>.

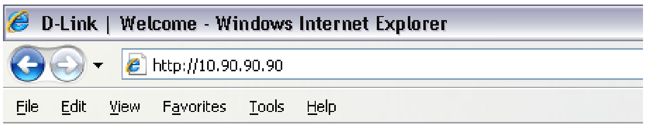


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser

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.

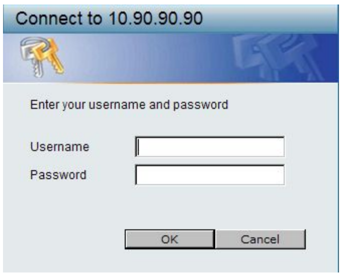


Figure 3.3 – Logon Dialog Box

Smart Wizard

After a successful login, the Smart Wizard will guide you through essential settings of the Switch. Please refer to the Smart Wizard Configuration section for details.

Web-based Management

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface. Please refer to Chapter 5 Configuration for detailed instructions.

SmartConsole Utility

The SmartConsole Utility included in the installation CD is a program for discovering D-Link Smart Switches within the same network segment connected to your PC. This tool is only for computers running Windows 2000, Windows XP, Windows 7, or Windows Vista operating systems. There are two options for the installation of the SmartConsole Utility; one is through the autorun program on the installation CD and the other is manual installation.

NOTE: Please be sure to uninstall any existing SmartConsole Utility from your PC before installing the latest SmartConsole Utility.

Option 1: Follow these steps to install the SmartConsole Utility via the autorun program on the installation CD.

1. Insert the Utility CD into your CD-Rom/DVD-Rom Drive.
2. The autorun program will appear automatically.
3. Click on the ”Install SmartConsole Utility” button and an installation wizard will guide you through the process.
4. After successfully installing the SmartConsole Utility, you can open the utility by clicking Start > Programs > D-Link SmartConsole Utility.

5. Connect the Smart Switch to the same L2 network segment of your PC and use the SmartConsole Utility to discover the Smart Switches.

Option 2: Follow these steps to install the SmartConsole Utility manually.

1. Insert the Utility CD into your CD-Rom/DVD-Rom Drive.
2. From the Start menu on the Windows desktop, click Run.
3. In the **Run** dialog box, type D:\D-Link SmartConsole Utility\D-Link_SmartConsole_Utility_v3.00.10.exe (where D:\ represents the drive letter of your CD-Rom) and click **OK**.
4. Follow the on-screen instructions to install the utility.
5. Upon completion, go to Start > Programs > D-Link SmartConsole Utility and open the SmartConsole Utility.
6. Connect the Smart Switch to the same L2 network segment of your PC and use the SmartConsole Utility to discover the Smart Switches.

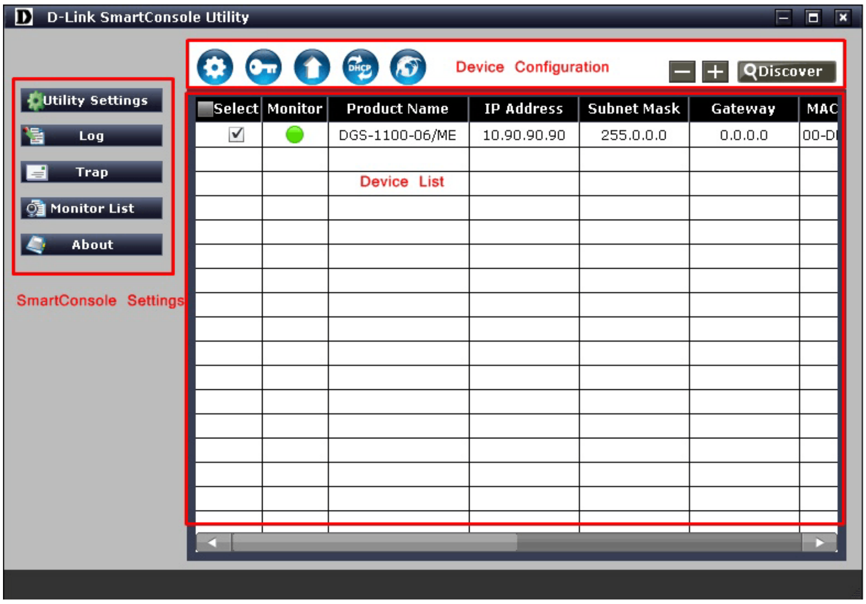
For detailed explanations of SmartConsole's functions, please refer to Chapter 4 *SmartConsole Utility*

NOTE: The current SmartConsole Utility does not support IPv6 feature. Please be sure to install the SmartConsole Utility from you PC with IPv4 address. After installed SmartConsole Utility, then it can discover the D-Link Smart switches with IPv6 address.

4 *SmartConsole Utility*

The D-Link SmartConsole Utility allows the administrator to quickly discover all D-Link smart switches and DGS-1100-06/ME, which are in the same domain of the PC, collect traps and log messages, and quick access to basic configurations of the switch.

The SmartConsole Utility consists of three parts, **Device Configurations** at the top, **Device List** as the main body, and **SmartConsole Settings** at the left.



Select	Monitor	Product Name	IP Address	Subnet Mask	Gateway	MAC
☑	●	DGS-1100-06/ME	10.90.90.90	255.0.0.0	0.0.0.0	00-D

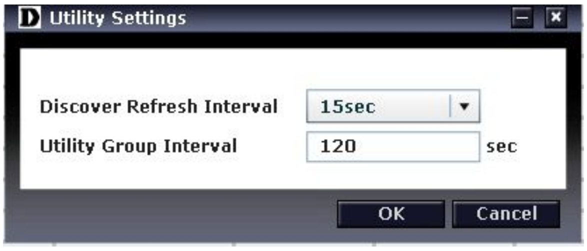
Figure 4.1 – SmartConsole Utility

SmartConsole Settings

The SmartConsole Settings at the left has five icons, **Utility Settings**, **Log**, **Trap**, **Monitor list**, and **About**.

Utility Settings

Click this icon to launch the Utility Settings window. **Refresh time** refreshes the devices, which were selected as monitored devices in the Device List. Choices include **15 secs, 30 secs, 1 mins, 2 mins,** and **5 mins** for selecting the monitoring time intervals. **Utility Group Interval** establishes the intervals (in seconds) that the Switch will be discovered in the SmartConsole Device List.



Discover Refresh Interval 15sec ▾

Utility Group Interval 120 sec

Figure 4.2 – SmartConsole Utility Settings

NOTE: If the Group Interval is set to 0, IGMP Snooping must be disabled in the Switch, or the SmartPro Switch will not be discovered.

Log

Click this icon to launch the Log window. Click **View Log** to show the events of the SmartConsole Utility and the device. **Time** indicates when the message was received, Location indicates where the message was received and **IP Address** denotes where it comes from. Click **Refresh** to redisplay all log entries, click **Clear** to clear all log entries. Click **Exit** to exit.

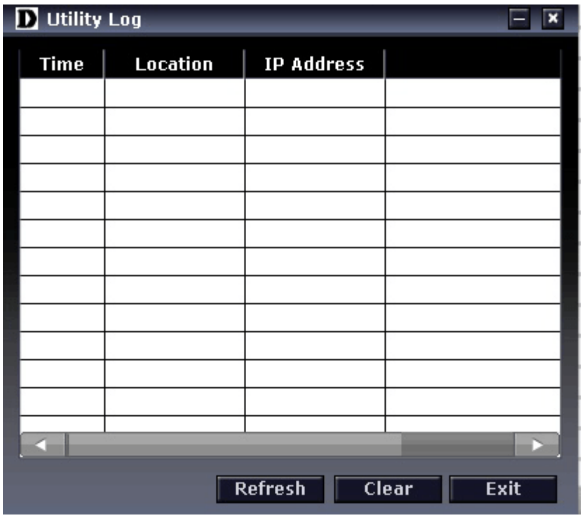


Figure 4.3 – SmartConsole Log

Trap

Click this icon to launch the Trap window. Click **View Trap** to show the events of the SmartConsole Utility and the device. **Time** indicates when the trap message was received, **Location** indicates where the trap message was received, **IP** denotes where it comes from and **Event** shows the content of this trap message. Click **Refresh** to redisplay all traps, click **Clear** to clear all entries. Click **Exit** to exit

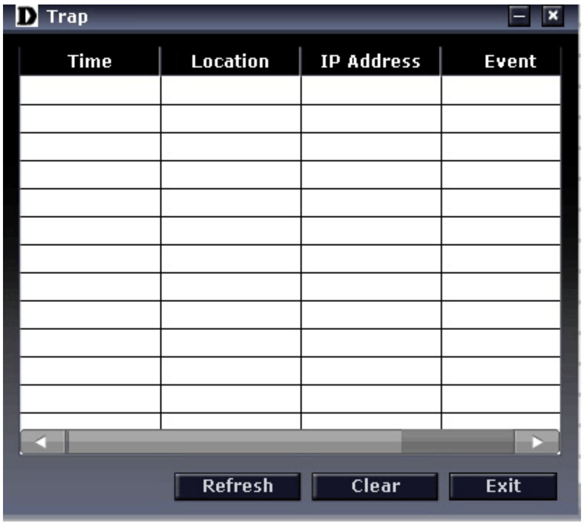


Figure 4.4 – SmartConsole Trap

The trap icon in the SmartConsole Settings will change while receiving new trap messages. Please see below for detailed description.

Icon	Description
🗎	No new traps
✉	New traps was received

Monitor List

By clicking on this icon you will see below options:

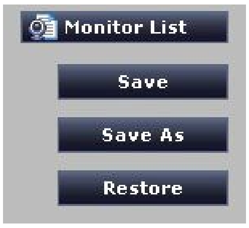
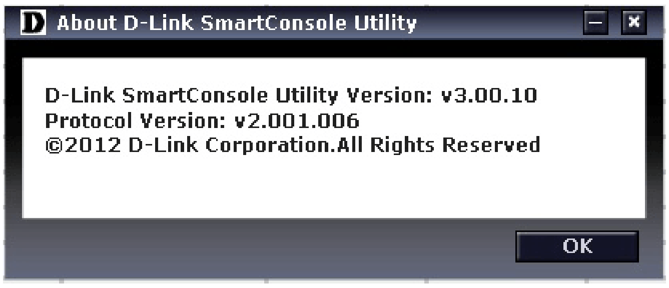


Figure 4.5 – SmartConsole Monitor List

Save: Records the setting of the Device List as default for the next time the SmartConsole Utility is used.
Save As: Records the setting of the Device List in an appointed filename and file path.
Restore: Manually reload a Device List setting file.

About

Click this icon to launch the SmartConsole Info window.


About D-Link SmartConsole Utility

D-Link SmartConsole Utility Version: v3.00.10
Protocol Version: v2.001.006
©2012 D-Link Corporation.All Rights Reserved

Figure 4.6 – SmartConsole About

Device Configuration

The Device Configuration in the SmartConsole Utility has five icons:

Device Settings

Password Settings

Firmware Upgrade

DHCP Refresh

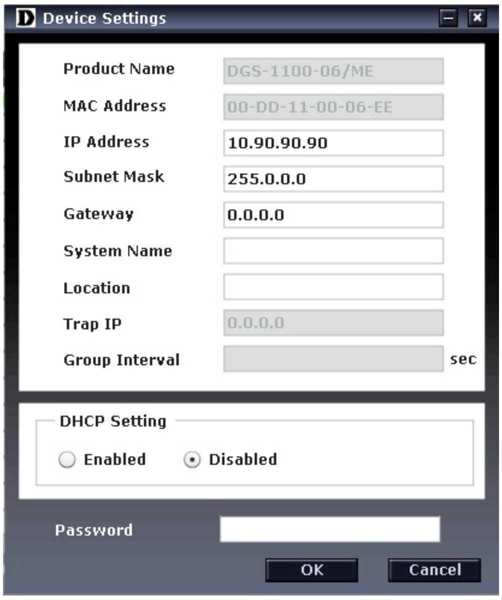
Web Access

and the −, +, Discover device buttons for the Device List.

Device Settings

Select a switch from the Device List. Click on this icon to launch the Device Settings window. Here you can configure the Product Name, MAC Address, IPv4 Address, Subnet Mask, Gateway, System Name, Location, Trap IP, Group Interval, and DHCP Client Setting of the Switch.

To apply the configuration, insert the correct device password in the Confirm Password box and then click **OK.**



Device Settings

Product Name: DGS-1100-06/ME
MAC Address: 00-DD-11-00-06-EE
IP Address: 10.90.90.90
Subnet Mask: 255.0.0.0
Gateway: 0.0.0.0
System Name:
Location:
Trap IP: 0.0.0.0
Group Interval: sec

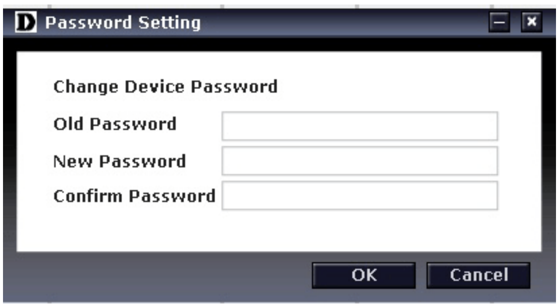
DHCP Setting
○ Enabled ● Disabled

Password:

Figure 4.7 – SmartConsole Device Settings

Password Settings

Select a switch from the Device List. Click on this icon to launch the Device Password Manager window. Here you can enter a new password and confirm it.



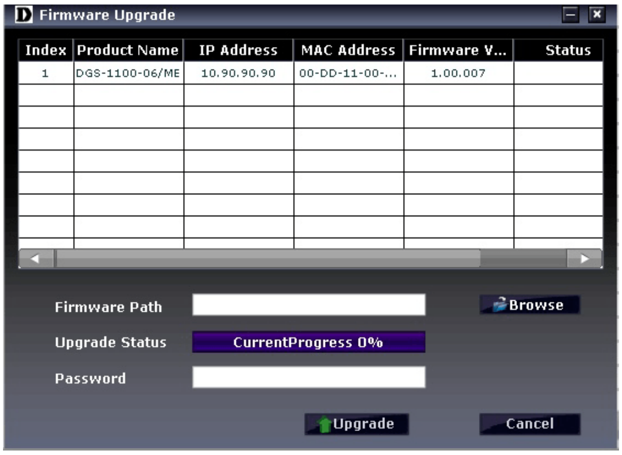
Password Setting

Change Device Password
Old Password:
New Password:
Confirm Password:

Figure 4.8 – SmartConsole Password Settings

Firmware Upgrade

Select one or many switches of the same model name from the Device List. Click on this icon to launch the Firmware Upgrade window. Specify the Firmware Path (or Browse for one) that you are going to use. Input the correct password of the device, and then click **Upgrade.** The state will show "OK" after completion, or “Fail” if the firmware upgrade fails or cannot be completed for any reason.



Firmware Upgrade

Index	Product Name	IP Address	MAC Address	Firmware V...	Status
1	DGS-1100-06/ME	10.90.90.90	00-DD-11-00-...	1.00.007	

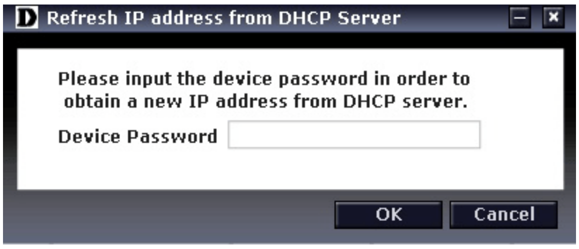
Firmware Path:
Upgrade Status: CurrentProgress 0%
Password:

Figure 4.9 – Firmware Upgrade

CAUTION: Do not disconnect the PC or remove the power cord from the device until the upgrade completes. The software may be corrupted because of the incomplete firmware upgrade.

DHCP Refresh:

If a DHCP-client enabled switch in the Device List shows the default IP is still used, it means the device did not receive an IPv4 address from the DHCP server successfully. Select that switch and click the DHCP refresh icon. Enter the correct Device Password and then click **OK.** The device will renew the IPv4 address from the DHCP server.



Refresh IP address from DHCP Server

Please input the device password in order to obtain a new IP address from DHCP server.

Device Password

Figure 4.10 – DHCP Refresh

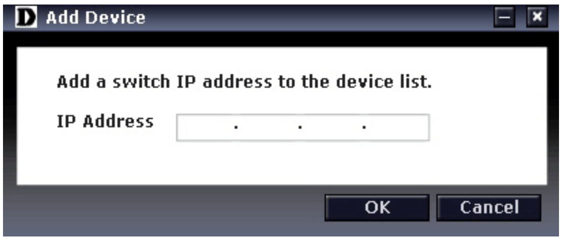
Web Access

Select a switch from the Device List. Click this icon to launch your Internet browser (eg. The Internet Explorer). Here you can configure the Switch through the Web-based Management utility. You may also get into the Web-based Management by double-clicking the device in the device list.

Add(+), Delete(-) and Discover the device

Click the **Discovery** button to display all of the Web-Smart devices located in the same domain with the management PC.

Click the **+** and insert a device IP address to add a device into the Discover List, or select a device and click the **–** button to remove it.

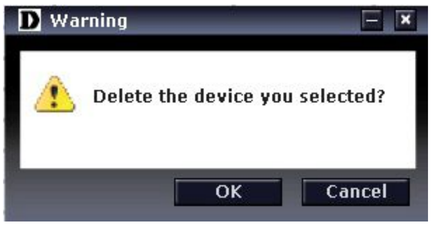


Add Device

Add a switch IP address to the device list.

IP Address . . .

Figure 4.11 – SmartConsole Add device



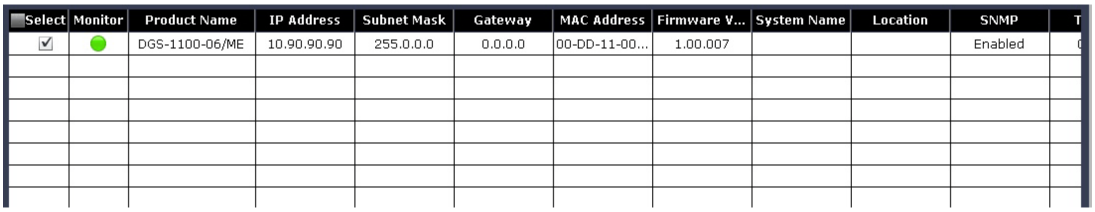
Warning

Delete the device you selected?

Figure 4.12 – SmartConsole Delete device

Device List

This list displays all discovered Web-Smart devices on the network.



Select	Monitor	Product Name	IP Address	Subnet Mask	Gateway	MAC Address	Firmware V...	System Name	Location	SNMP	T
☑	●	DGS-1100-06/ME	10.90.90.90	255.0.0.0	0.0.0.0	00-DD-11-00...	1.00.007			Enabled	0

Figure 4.13 – SmartConsole Device List

Definitions of the Device List features:

Select: Click the **Select** to choose a switch for configuration settings.

Monitor: Click the Monitor button and the SmartConsole will collect the trap and log data from the device. The ● in the monitor means the device was discovered by SmartConsole. Click the icon to have the device to continue updating the information, such as system log or trap to the SmartConsole Utility. The icon will appear ● . When the device was detected as not reachable, the icon will change to ● . Please check if the power or the cable of this device is disconnected.

Product Name: Displays the device product name.

IP Address: Displays the current IP addresses of devices.

Subnet Mask: Displays the Subnet Mask setting of the device.

Gateway: Displays the Gateway setting of the device.

MAC Address: Displays the device MAC Addresses.

Firmware version: Displays the current Firmware version of this device.

System Name: Displays the appointed device system name.

Location: Displays the location of the appointed device.

SNMP: Displays the SNMP status of the device.

Trap IP: Displays the IP address of the host where the Trap information will be sent.

DHCP: Specify if the device gets the IP address from a DHCP server.

Group Interval: Displays the intervals (in seconds) that the Switch will be discovered in the SmartConsole Device List.

NOTE: If the devices are marked red in the device list, it means that a firmware upgrade is required again.

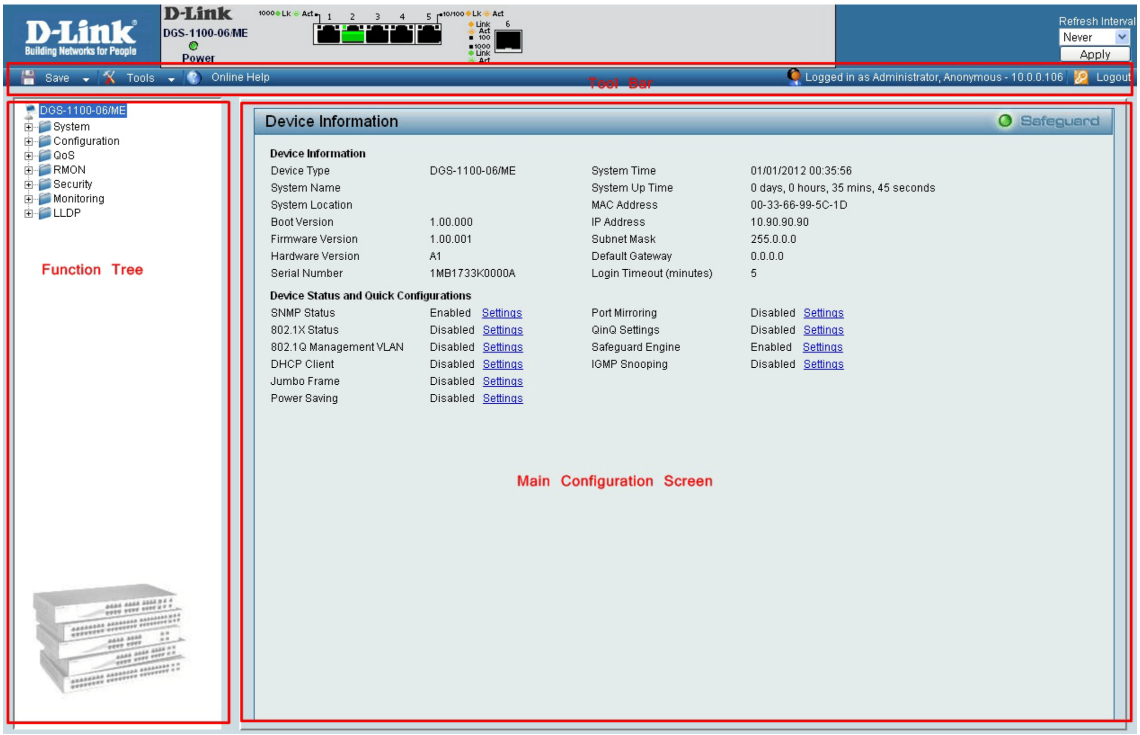
NOTE: If the IP address of device is showed with IPv6 address, then it can not be configured with Smartconsole Utility. The user needs to double click the selected device and login the web for configuration.

5 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 Information

Device Type	DGS-1100-06/ME	System Time	01/01/2012 00:35:56
System Name		System Up Time	0 days, 0 hours, 35 mins, 45 seconds
System Location		MAC Address	00-33-66-99-5C-1D
Boot Version	1.00.000	IP Address	10.90.90.90
Firmware Version	1.00.001	Subnet Mask	255.0.0.0
Hardware Version	A1	Default Gateway	0.0.0.0
Serial Number	1MB1733K0000A	Login Timeout (minutes)	5

Device Status and Quick Configurations

SNMP Status	Enabled Settings	Port Mirroring	Disabled Settings
802.1X Status	Disabled Settings	QinQ Settings	Disabled Settings
802.1Q Management VLAN	Disabled Settings	Safeguard Engine	Enabled Settings
DHCP Client	Disabled Settings	IGMP Snooping	Disabled Settings
Jumbo Frame	Disabled Settings		
Power Saving	Disabled Settings		

Figure 5.1 – 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.

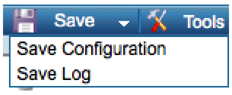
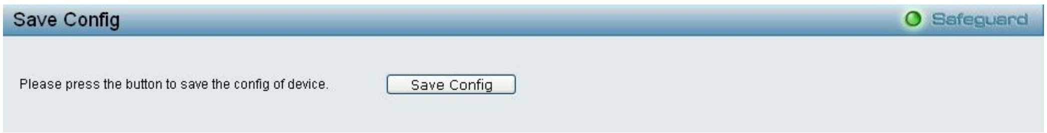


Figure 5.2 – Save Menu

Save Configuration

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

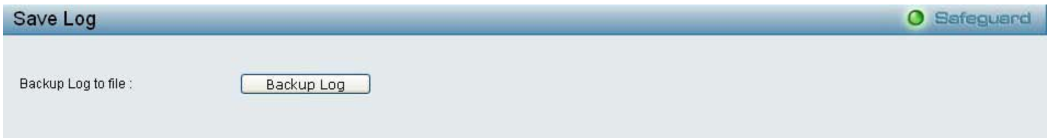


Please press the button to save the config of device.

Figure 5.3 – 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 5.4 – 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.

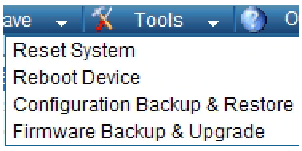
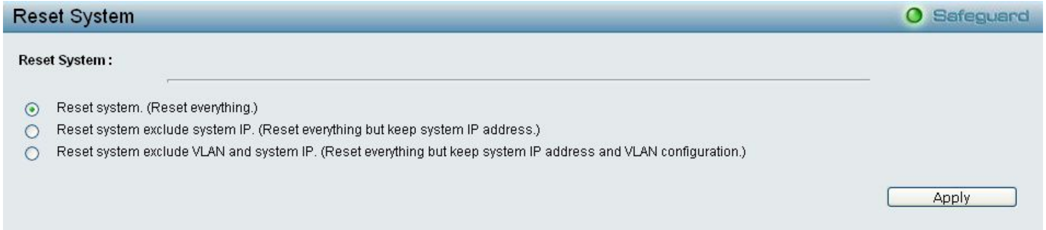


Figure 5.5 – Tool Menu

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.)

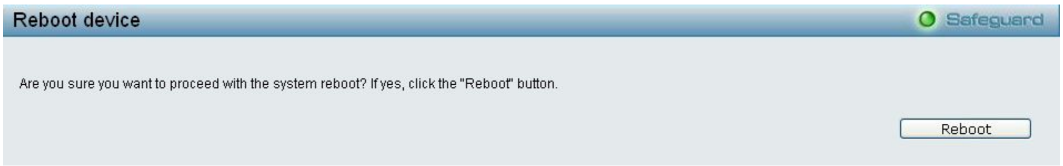
○ Reset system exclude VLAN and system IP. (Reset everything but keep system IP address and VLAN configuration.)

Figure 5.6 – 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.

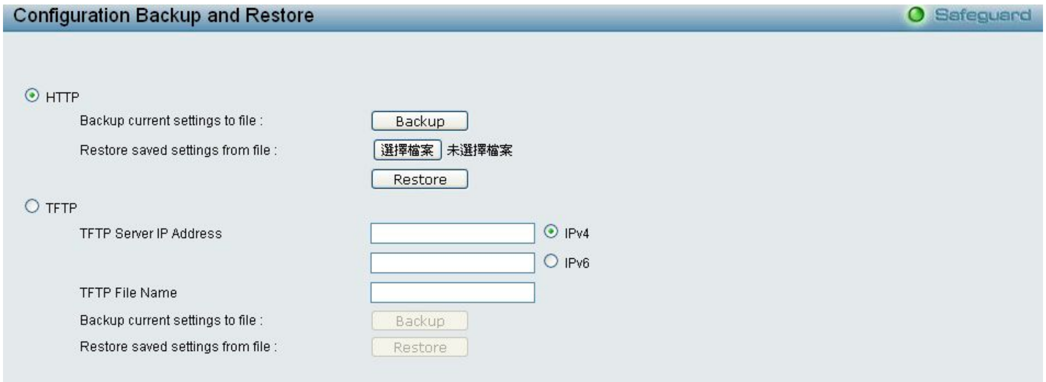

Reboot device

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

Figure 5.7 – 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

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

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

Figure 5.8 – 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.

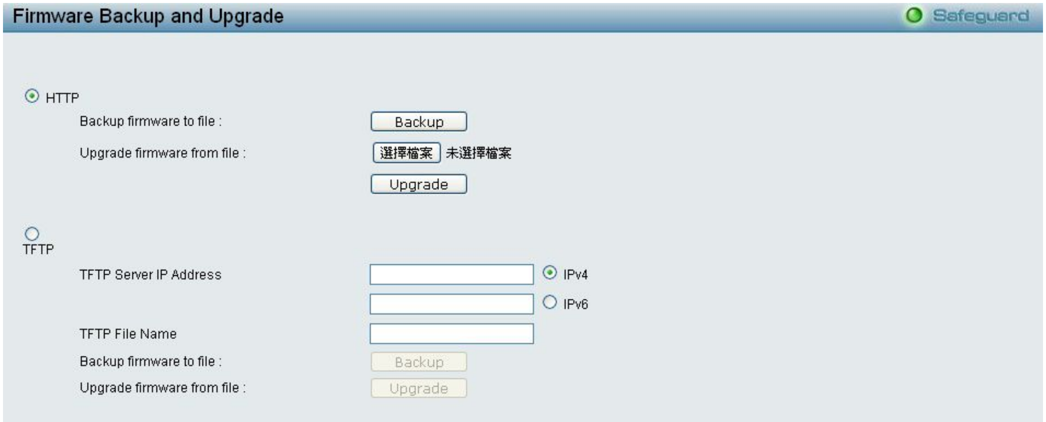
Click **Backup** to save the current settings to the TFTP server.

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

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

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

Figure 5.9 – 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.

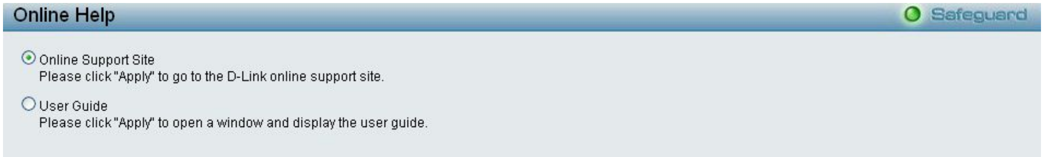
Click **Backup** to save the firmware to the TFTP server.

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 5.10 – 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.

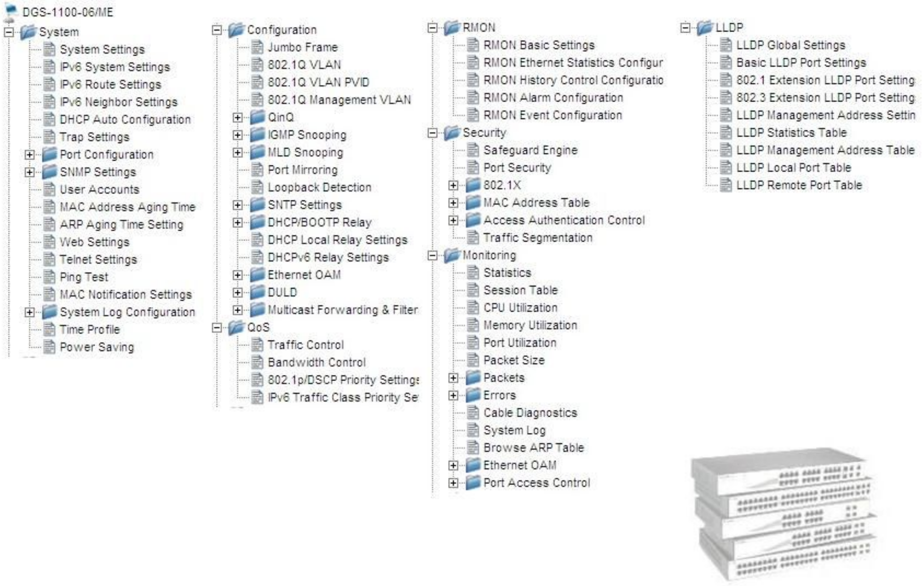


Figure 5.11 –Function Tree

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:

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.

Jumbo Frame: Click **Settings** to link to Configuration > Jumbo Frame. Default is disabled.

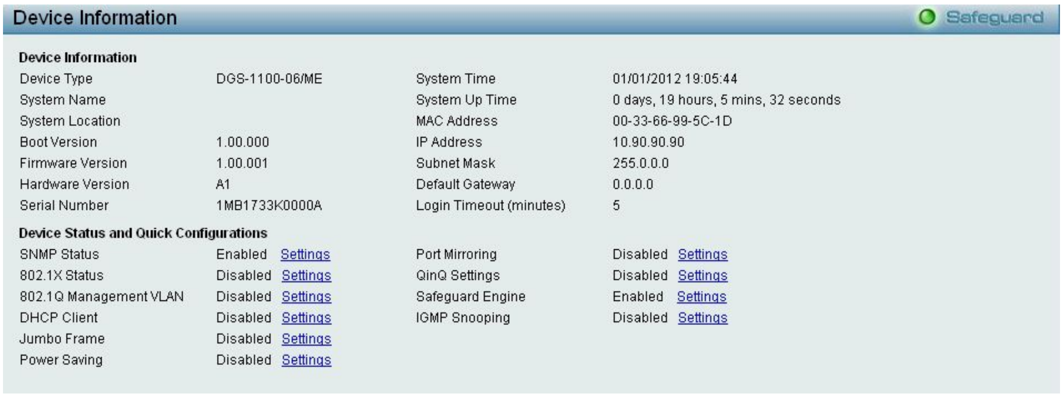
Power Saving: Click **Settings** to link to System > Power Saving. Default is disabled.

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

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

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

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



Device Information

Safeguard

Device Information

Device Type	DGS-1100-06/ME	System Time	01/01/2012 19:05:44
System Name		System Up Time	0 days, 19 hours, 5 mins, 32 seconds
System Location		MAC Address	00-33-66-99-5C-1D
Boot Version	1.00.000	IP Address	10.90.90.90
Firmware Version	1.00.001	Subnet Mask	255.0.0.0
Hardware Version	A1	Default Gateway	0.0.0.0
Serial Number	1MB1733K0000A	Login Timeout (minutes)	5

Device Status and Quick Configurations

SNMP Status	Enabled Settings	Port Mirroring	Disabled Settings
802.1X Status	Disabled Settings	QinQ Settings	Disabled Settings
802.1Q Management VLAN	Disabled Settings	Safeguard Engine	Enabled Settings
DHCP Client	Disabled Settings	IGMP Snooping	Disabled Settings
Jumbo Frame	Disabled Settings		
Power Saving	Disabled Settings		

Figure 5.12 – Device Information

System > System Settings

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

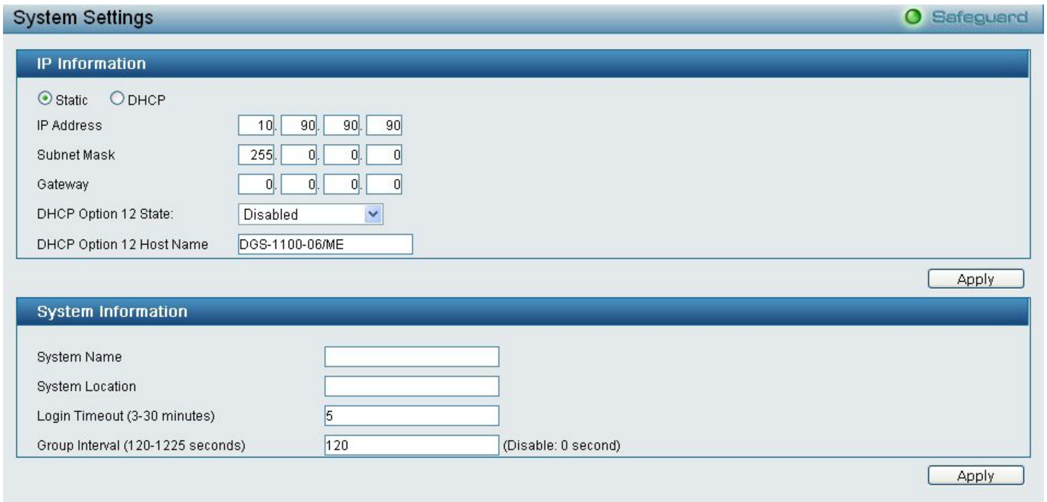
IP Information: There are two ways for the switch to obtain an IP address: Static and DHCP (Dynamic Host Configuration Protocol).

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.



System Settings

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	DGS-1100-06/ME

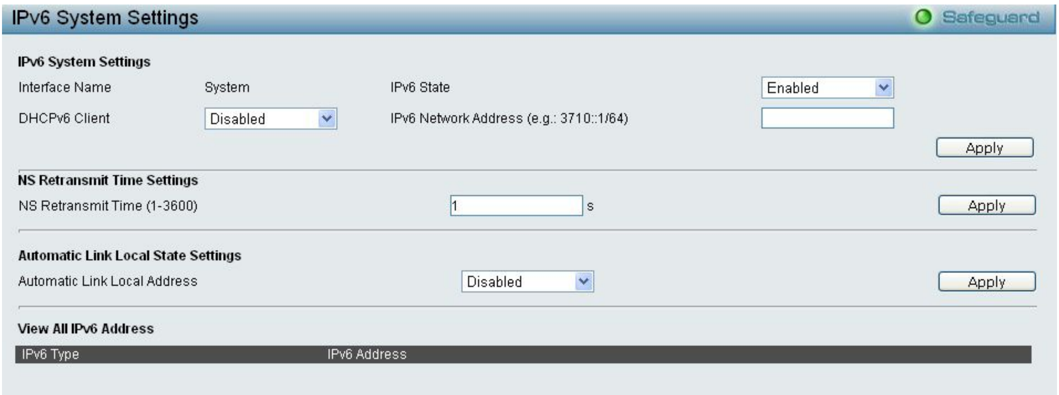
System Information

System Name	
System Location	
Login Timeout (3-30 minutes)	5
Group Interval (120-1225 seconds)	120 (Disable: 0 second)

Figure 5.13 – System > System Settings

System > IPv6 System Settings

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



IPv6 System Settings

IPv6 System Settings

Interface Name	System	IPv6 State	Enabled
DHCPv6 Client	Disabled	IPv6 Network Address (e.g.: 3710::1/64)	

NS Retransmit Time Settings

NS Retransmit Time (1-3600) 1 s

Automatic Link Local State Settings

Automatic Link Local Address Disabled

View All IPv6 Address

IPv6 Type	IPv6 Address

Figure 5.14 – 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.

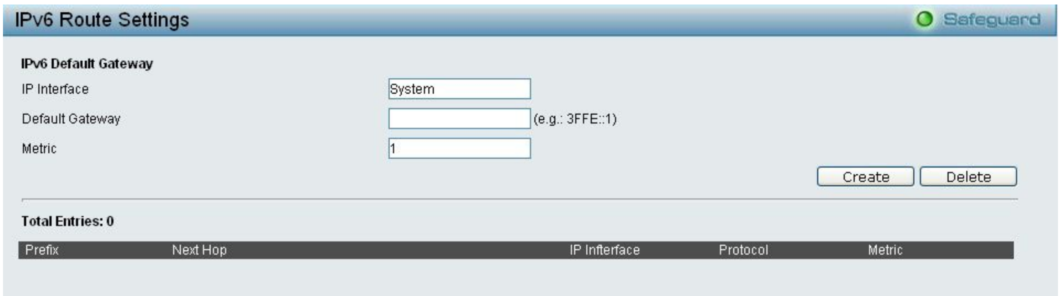
Automatic Link Local State Settings:

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

IPv6 Default Gateway

IP Interface: System

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

Metric: 1

Total Entries: 0

Prefix	Next Hop	IP Interface	Protocol	Metric

Figure 5.15 – System > IPv6 Route Settings

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

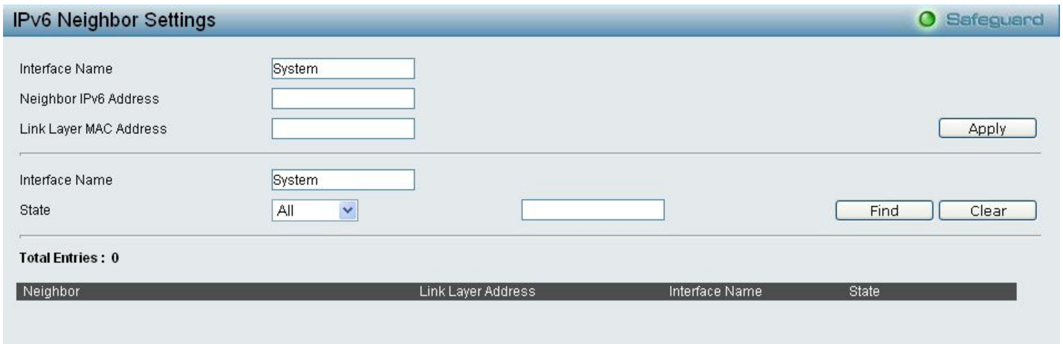
Default Gateway: The corresponding IPv6 address for the next hop Gateway address in IPv6 format..

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.



IPv6 Neighbor Settings

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 5.16 – 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.

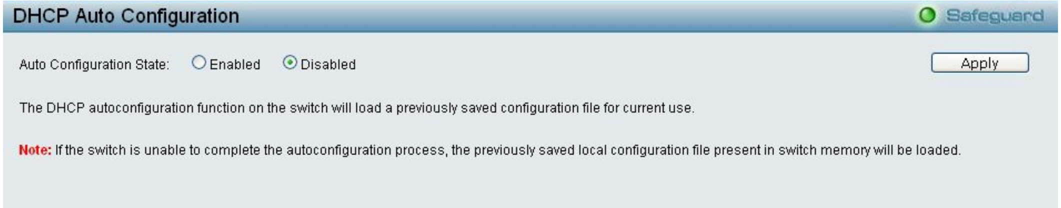
State: Use the drop-down menu to select All, Address, Static or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

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

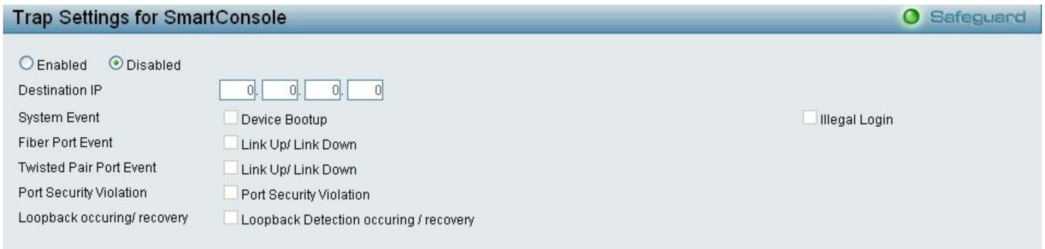
The DHCP autoconfiguration function on the switch will load a previously saved configuration file for current use.

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 5.17 – 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.



○ 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	
Port Security Violation	☐ Port Security Violation	
Loopback occuring/ recovery	☐ Loopback Detection occuring / recovery	

Figure 5.18 – 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.

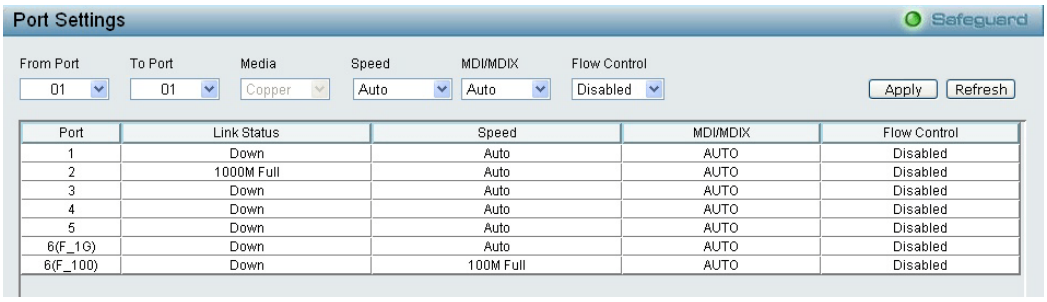
Twisted Pair Port Event: Events when pair port connection port link up / link down.

Port Security Violation: Events of port security violation.

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

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	Apply	Refresh

Port	Link Status	Speed	MDI/MDIX	Flow Control
1	Down	Auto	AUTO	Disabled
2	1000M Full	Auto	AUTO	Disabled
3	Down	Auto	AUTO	Disabled
4	Down	Auto	AUTO	Disabled
5	Down	Auto	AUTO	Disabled
6(F_1G)	Down	Auto	AUTO	Disabled
6(F_100)	Down	100M Full	AUTO	Disabled

Figure 5.19 – System > Port Configuration > Port Settings

Media: Specify the media type of the port.

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.

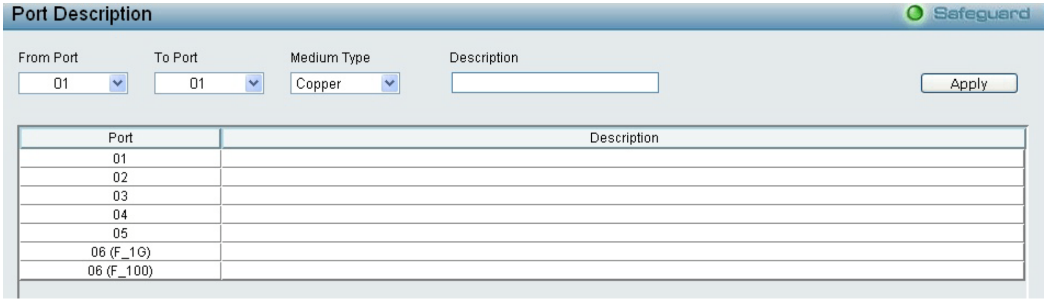
This switch provides a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

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	To Port	Medium Type	Description	
01	01	Copper		Apply

Port	Description
01	
02	
03	
04	
05	
06 (F_1G)	
06 (F_100)	

Figure 5.20 – System > Port Configuration > Port Description

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

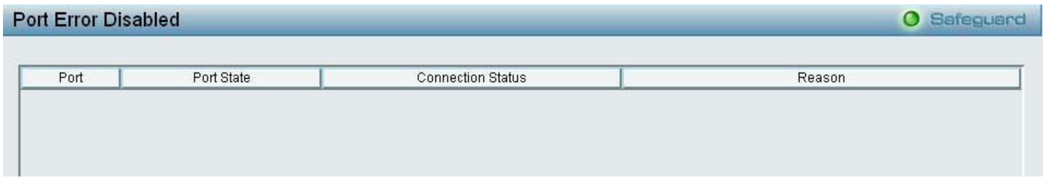
Medium Type: Specify the media type of the port

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 5.21 – 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.

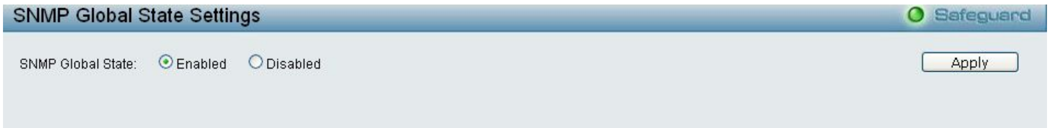
Reason: Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

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.



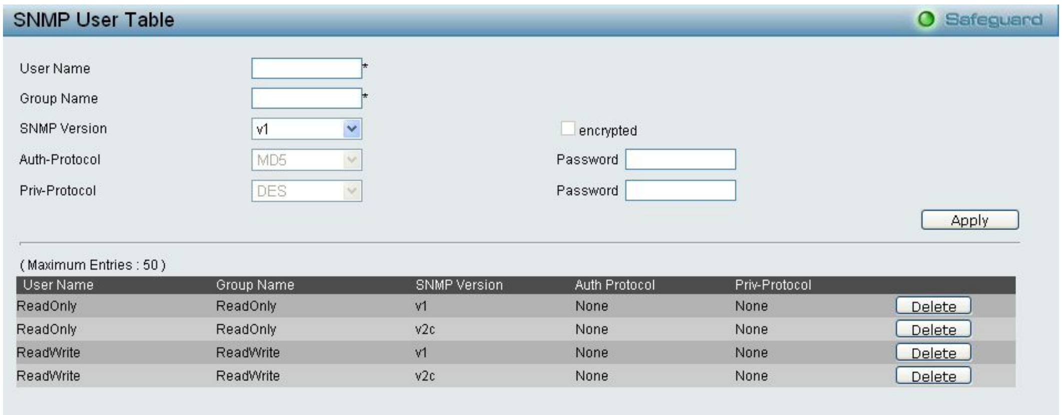
SNMP Global State Settings

SNMP Global State: ● Enabled ○ Disabled

Figure 5.22 – 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 5.23 – 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.

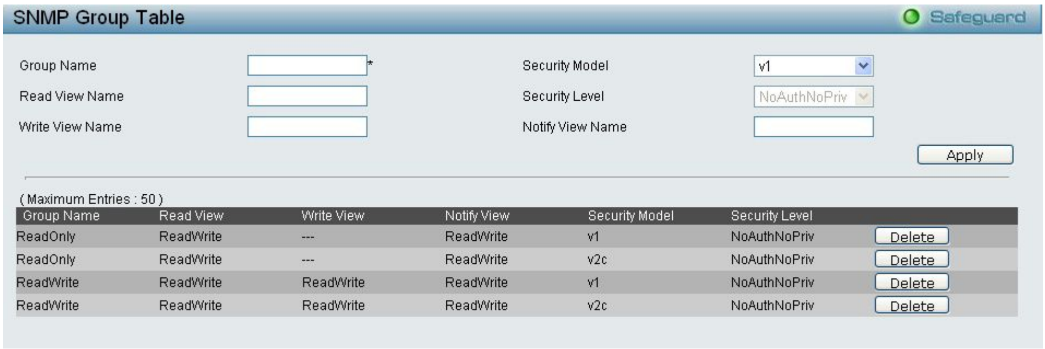
Security Level: This function is only available when you select SNMPv3 security level.

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	

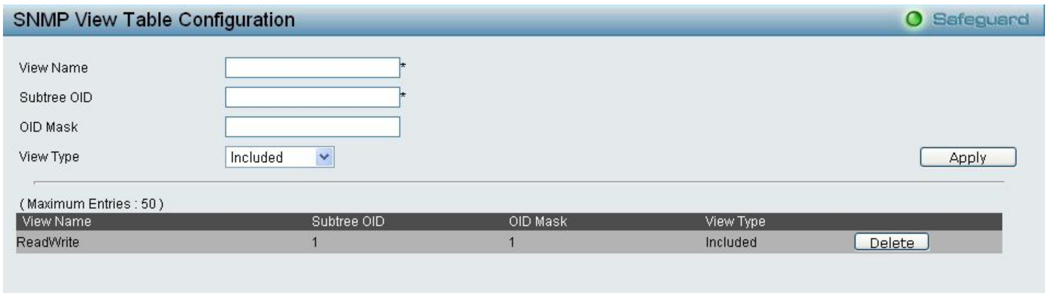
(Maximum Entries : 50)

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 5.24– 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

(Maximum Entries : 50)

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

Figure 5.25 – 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.

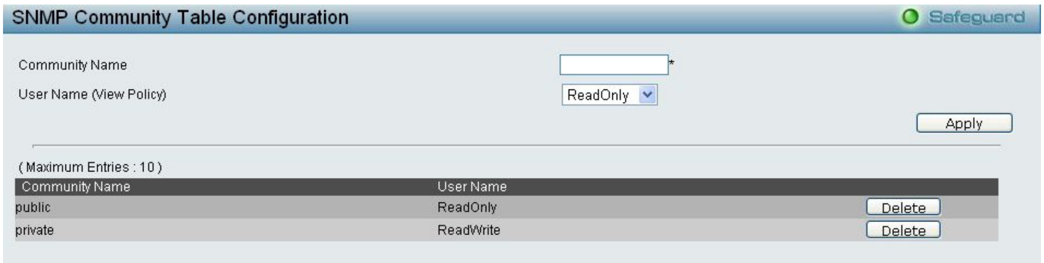
Click **Apply** to create a new view, **Delete** to remove an existing view.

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 5.26 – System > SNMP Settings > SNMP Community Table

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

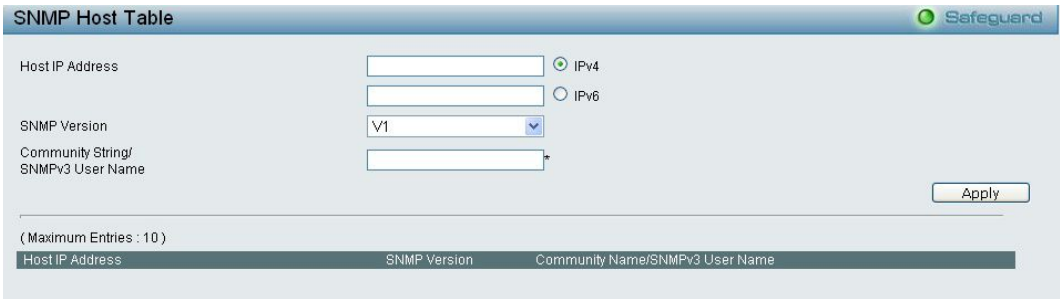
System > SNMP Settings > SNMP Host Table

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

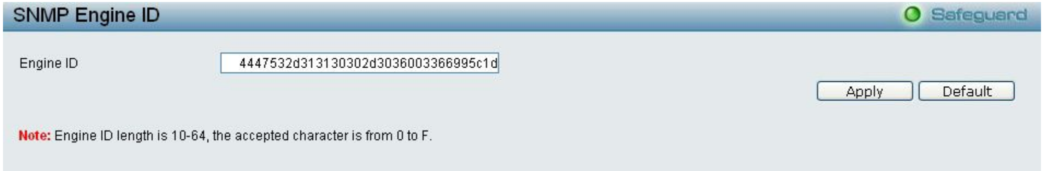
Figure 5.27– System > SNMP Settings > SNMP Host Table

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

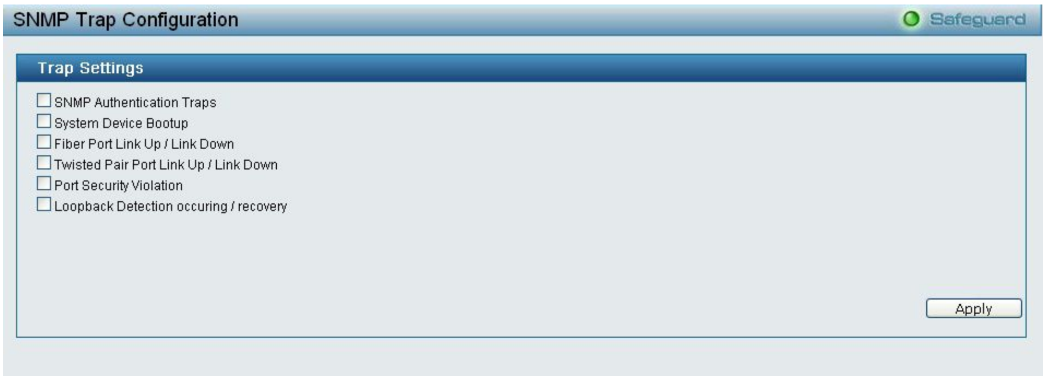
Engine ID: 4447532d313130302d3036003366995c1d

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

Figure 5.28 – 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 Device Bootup
- □ Fiber Port Link Up / Link Down
- □ Twisted Pair Port Link Up / Link Down
- □ Port Security Violation
- □ Loopback Detection occuring / recovery

Figure 5.29 – 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.

Port Security Violation: Information of Port Security Violation.

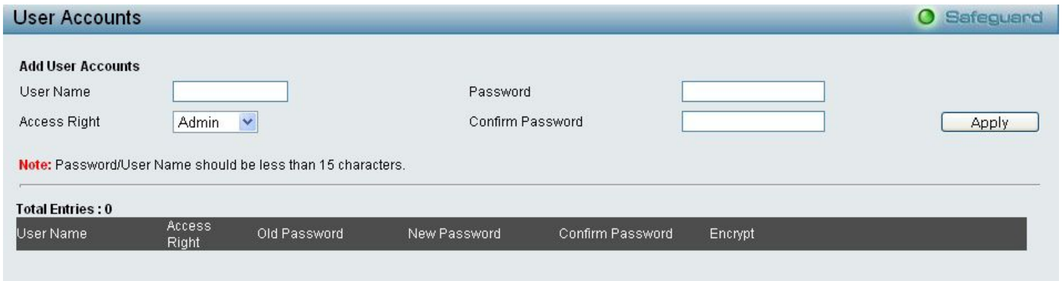
Loopback Detection occurring / recovery: Specify the device to send SNMP Trap when Loopback Detection occurring and recovery.

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.

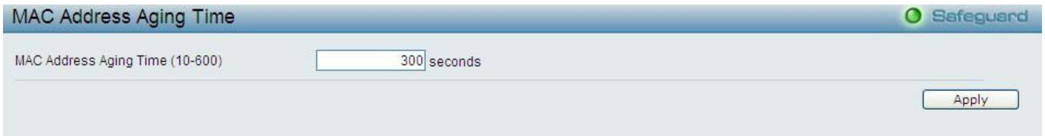
Total Entries : 0

User Name	Access Right	Old Password	New Password	Confirm Password	Encrypt

Figure 5.30– 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

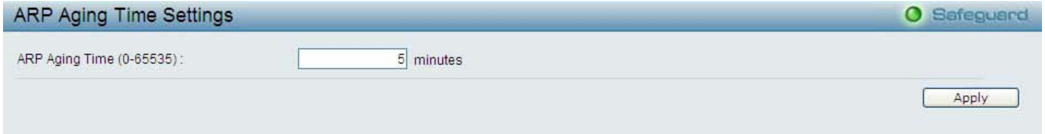
MAC Address Aging Time (10-600) 300 seconds

Figure 5.31 – 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

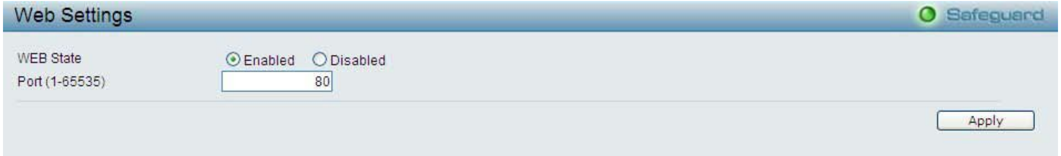
ARP Aging Time (0-65535) : 5 minutes

Figure 5.32 – 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 > 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

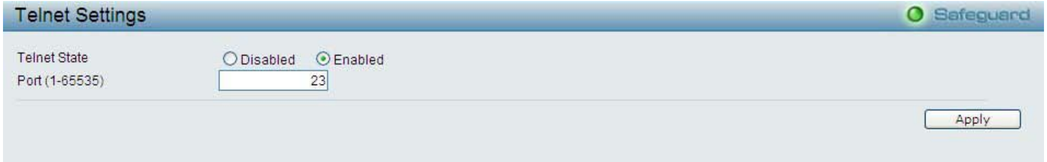
Port (1-65535) 80

Figure 5.33– 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

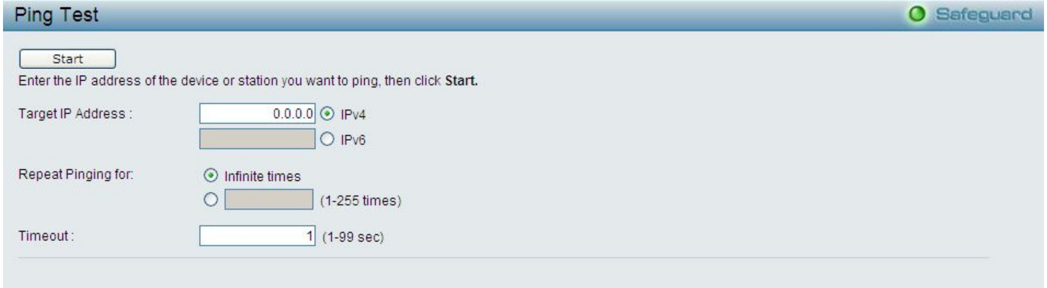
Port (1-65535) 23

Figure 5.34 – 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 > 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.



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)

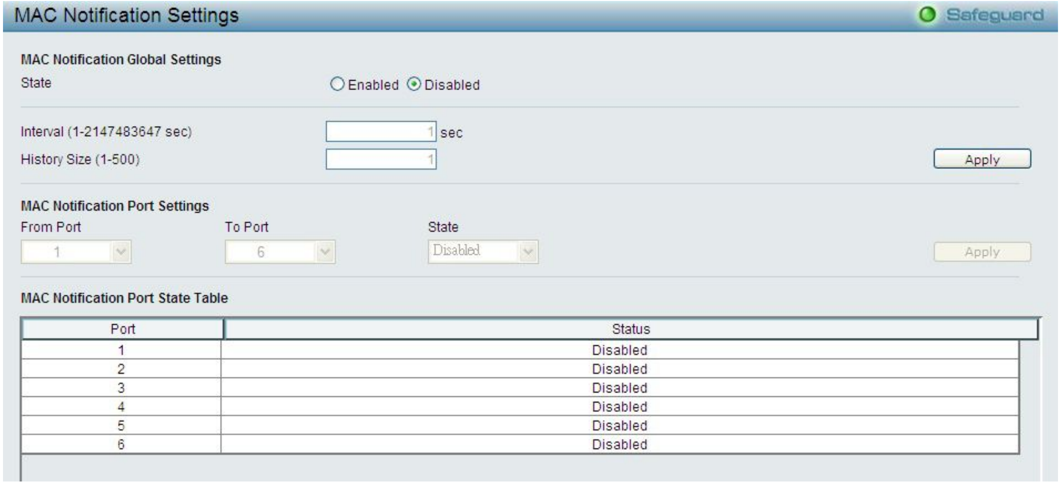
Figure 5.35 – System > Ping Test

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 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 6 State Disabled

MAC Notification Port State Table

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

Figure 5.36 – 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.

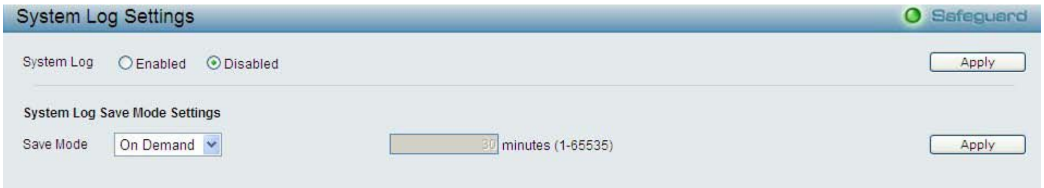
To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters. , then click the **Apply** button.

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 [Apply]

System Log Save Mode Settings

Save Mode: On Demand | 30 minutes (1-65535) [Apply]

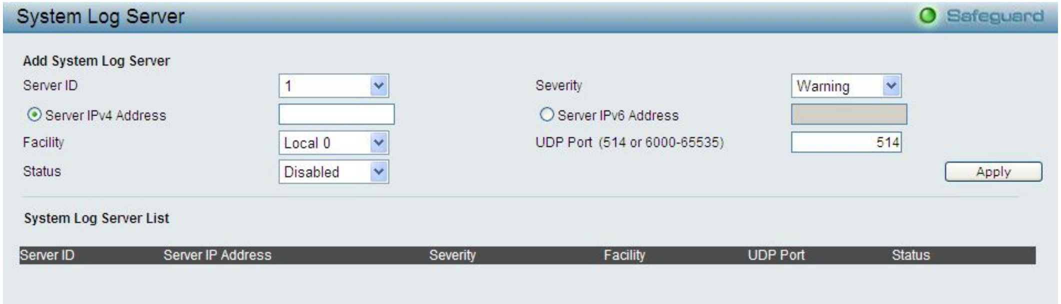
Figure 5.37 – System > System Log Configuration > System Log Settings

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

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 5.38 - 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.

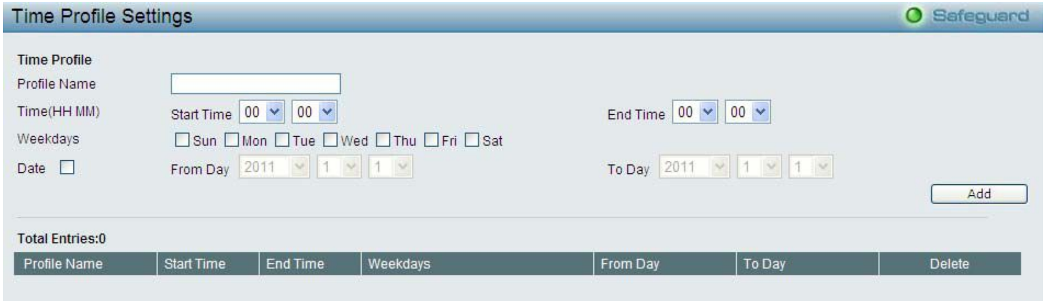
Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7).

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 > Time Profile

The Time Profile page allows users to configure the time profile settings of the device.



Time Profile Settings

Safeguard

Time Profile

Profile Name

Time(HH MM) Start Time 00 00 End Time 00 00

Weekdays □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Date □ From Day 2011 1 1 To Day 2011 1 1

Add

Total Entries:0

Profile Name	Start Time	End Time	Weekdays	From Day	To Day	Delete

Figure 5.39 – System > Time Profile Settings

Profile Name: Specifies the profile name.

Time(HH MM): Specifies the Start Time and End Time.

Weekdays: Specifies the work day.

Date: Select Date and specifies the From Day and To Day of the time profile.

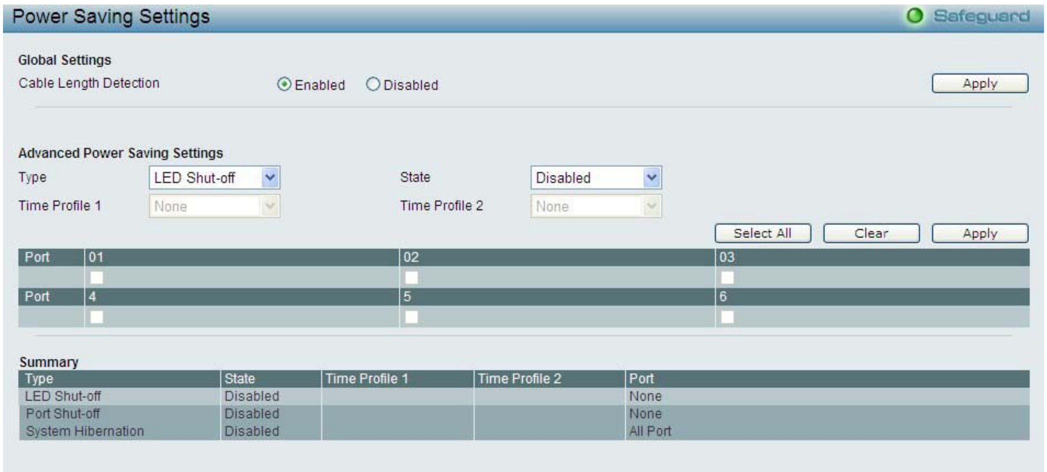
Click **Add** to create a new time profile or click **Delete** to delete a time profile from the table.

NOTE: The time must be set after current time, otherwise it will take effect on the next cycle time.

System > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 20 meters).

By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Cable Length Detection and Link Status Detection are enabled. Click **Apply** to make the change effective.



Power Saving Settings

Safeguard

Global Settings

Cable Length Detection ● Enabled ○ Disabled Apply

Advanced Power Saving Settings

Type LED Shut-off State Disabled

Time Profile 1 None Time Profile 2 None

Select All Clear Apply

Port	01	02	03
	□	□	□
Port	4	5	6
	□	□	□

Summary

Type	State	Time Profile 1	Time Profile 2	Port
LED Shut-off	Disabled			None
Port Shut-off	Disabled			None
System Hibernation	Disabled			All Port

Figure 5.40 – System > Power Saving

Advanced Power Saving Settings:

Type: Specifies the Power Saving type to be LED Shut-off, Port Shut-off, Port Standby or System Hibernation.

> **LED Shut-off -** The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means the LED can not be turned on after Time Profile time's up when the state is disabled. On the contrary, if the LED is enabled, the Time Profile function will work.
>
> **Port Shut-off -** The Port Shut-off state has high priority (the priority rule is the same as LED.) Therefore, if the Port Shut-off sate is already disabled the Time Profile function will not take effect.

Port Standby - The system changes to standby state and wait for a wake up event. Each port on the system enters sleep state by schedule.

System Hibernation - In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

State: Specifies the power saving state to be Enabled or Disabled.

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

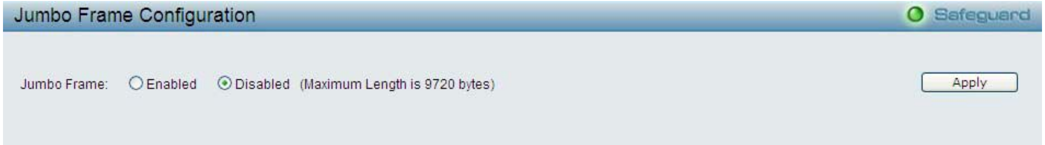
Port: Specifies the ports to be configure of the Power Saving.

Click **Select All** configure all ports, or click **Clear** to uncheck all port. Then click **Apply** to implement changes made.

Configuration > Jumbo Frame

Jumbo Frame support is designed to enhance Ethernet networking throughput and significantly reduce the CPU utilization of large file transfers like large multimedia files or large data files by enabling more efficient larger payloads per packet. The Jumbo Frame page allows network managers to enable Jumbo Frames on the device.

The Jumbo Frame default is disabled, Select Enabled then click Apply to turn on the jumbo frame support.



Jumbo Frame Configuration

Jumbo Frame: ○ Enabled ● Disabled (Maximum Length is 9720 bytes)

Figure 5.41 – Configuration > Jumbo Frame Settings

Configuration > 802.1Q VLAN

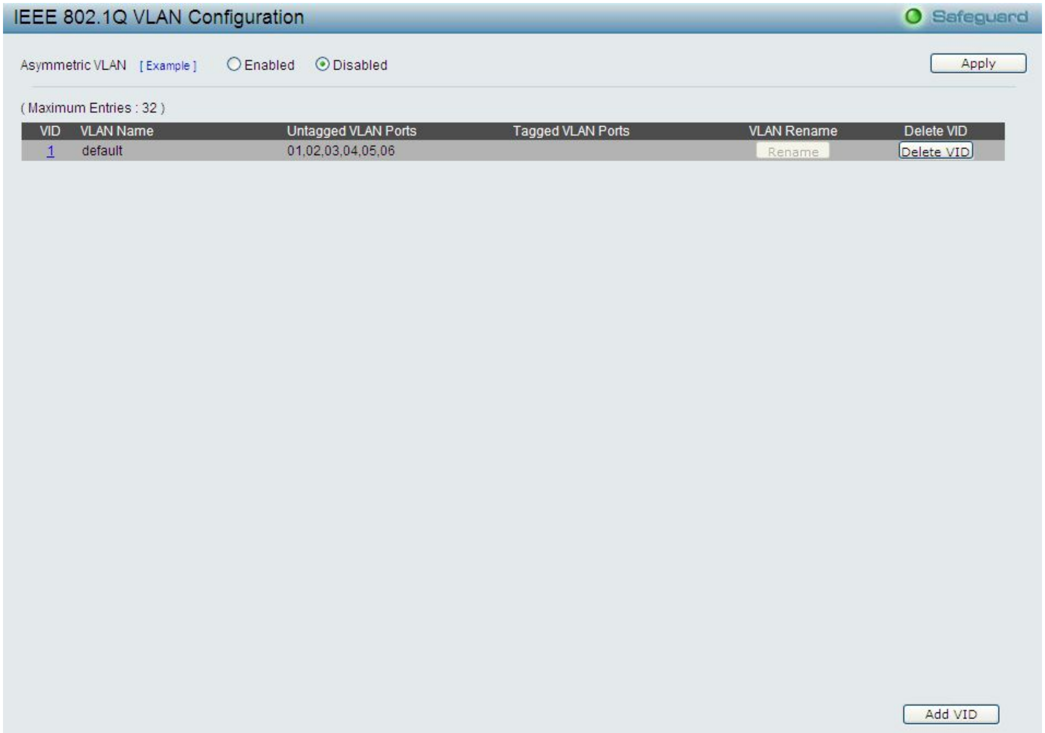
A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

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

Safeguard

Asymmetric VLAN [Example] ○ Enabled ● Disabled Apply

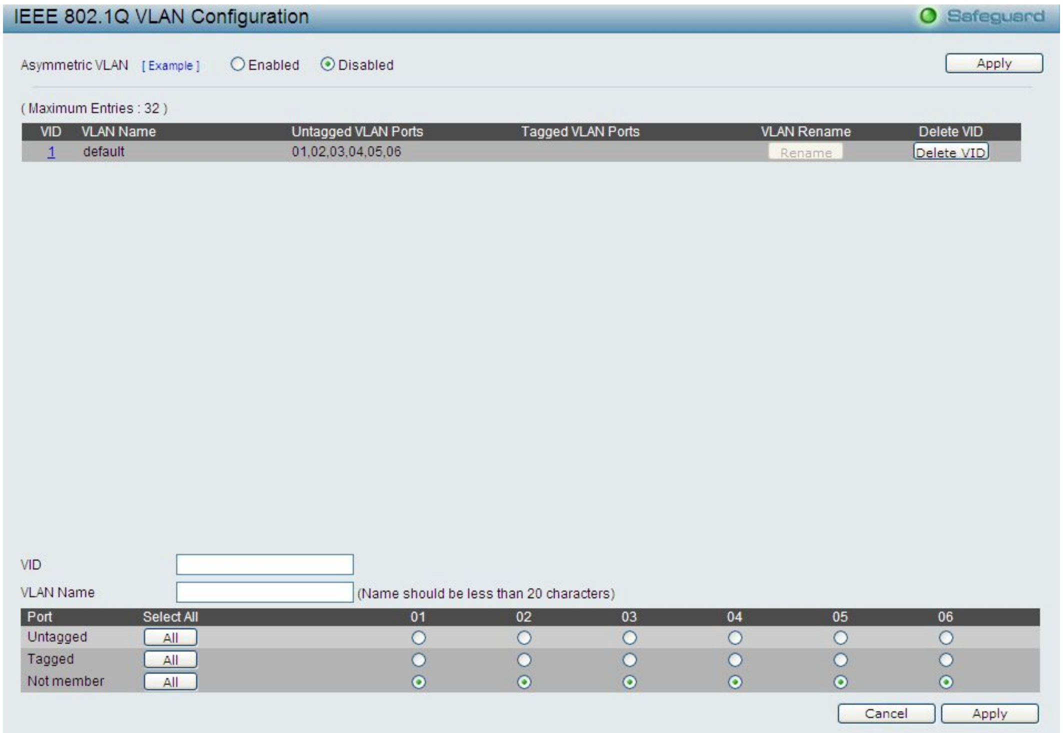
(Maximum Entries : 32)

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
1	default	01,02,03,04,05,06		Rename	Delete VID

Add VID

Figure 5.42 – Configuration > 802.1Q VLAN

Click **Add VID** to create a new VID group, assigning ports from 01 to 06 as **Untag**, **Tag** or **Not Member**. A port can be untagged in only one VID. To save the VID group, click **Apply.**



IEEE 802.1Q VLAN Configuration

Safeguard

Asymmetric VLAN [Example] ○ Enabled ● Disabled Apply

(Maximum Entries : 32)

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
1	default	01,02,03,04,05,06		Rename	Delete VID

VID

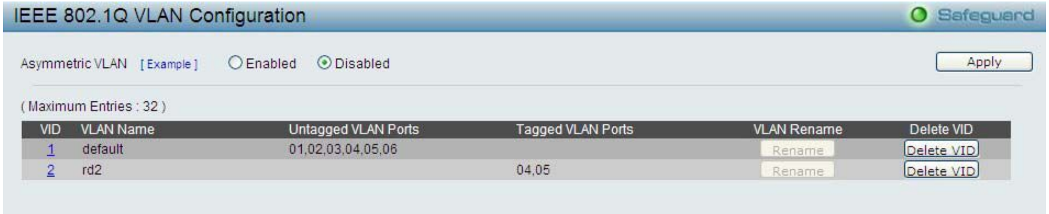
VLAN Name (Name should be less than 20 characters)

Port	Select All	01	02	03	04	05	06
Untagged	All	○	○	○	○	○	○
Tagged	All	○	○	○	○	○	○
Not member	All	●	●	●	●	●	●

Cancel Apply

Figure 5.43 – Configuration > 802.1Q VLAN > Add VLAN

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



IEEE 802.1Q VLAN Configuration — Safeguard

Asymmetric VLAN [Example] ○ Enabled ● Disabled — Apply

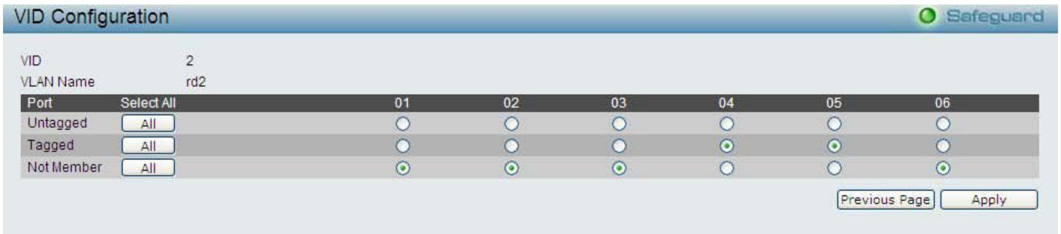
(Maximum Entries : 32)

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
1	default	01,02,03,04,05,06		Rename	Delete VID
2	rd2		04,05	Rename	Delete VID

Figure 5.44 - 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 — Safeguard

VID 2

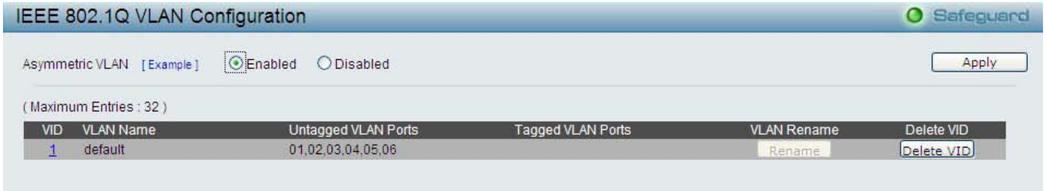
VLAN Name rd2

Port	Select All	01	02	03	04	05	06
Untagged	All	○	○	○	○	○	○
Tagged	All	○	○	○	●	●	○
Not Member	All	●	●	●	○	○	●

Previous Page — Apply

Figure 5.45 - 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 — Safeguard

Asymmetric VLAN [Example] ● Enabled ○ Disabled — Apply

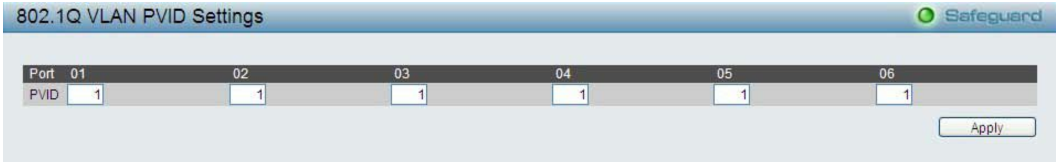
(Maximum Entries : 32)

VID	VLAN Name	Untagged VLAN Ports	Tagged VLAN Ports	VLAN Rename	Delete VID
1	default	01,02,03,04,05,06		Rename	Delete VID

Figure 5.46 - Configuration > 802.1Q VLAN > VID Assignments

Configuration > 802.1Q VLAN PVID

The 802.1Q VLAN PVID setting allows user to configure the PVID for each ports. Click **Apply** to implement changes made.



802.1Q VLAN PVID Settings — Safeguard

Port	01	02	03	04	05	06
PVID	1	1	1	1	1	1

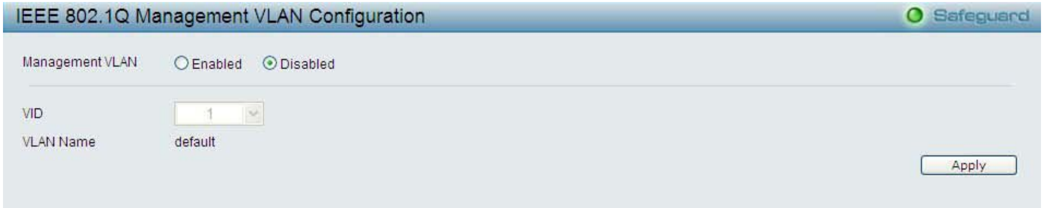
Apply

Figure 5.47 – Configuration > 802.1Q VLAN PVID

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 — Safeguard

Management VLAN ○ Enabled ● Disabled

VID 1

VLAN Name default

Apply

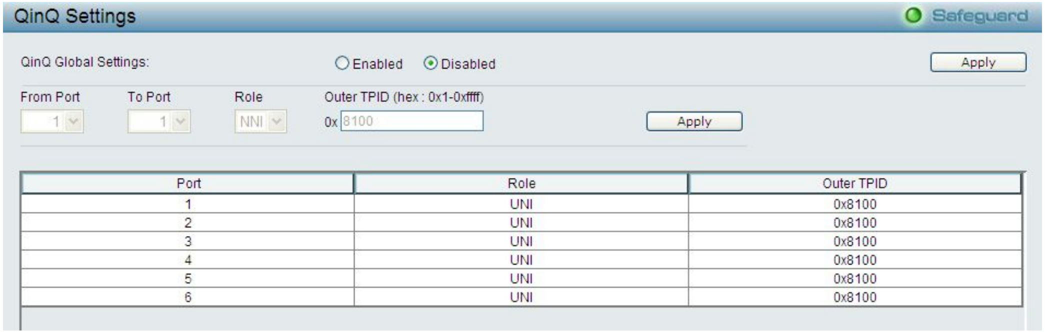
Figure 5.48 – Configuration > 802.1Q Management VLAN

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 Global Settings: ○ Enabled ● Disabled

From Port: 1
To Port: 1
Role: NNI
Outer TPID (hex : 0x1-0xffff): 0x 8100

Port	Role	Outer TPID
1	UNI	0x8100
2	UNI	0x8100
3	UNI	0x8100
4	UNI	0x8100
5	UNI	0x8100
6	UNI	0x8100

Figure 5.49 - 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.

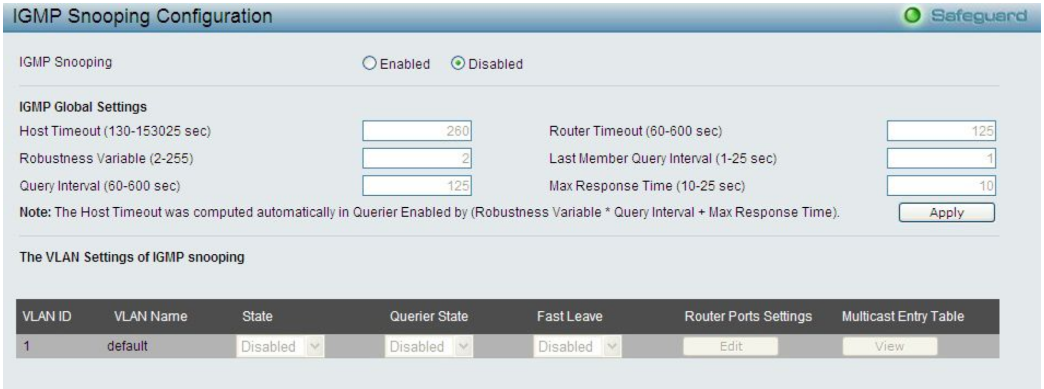
Click **Apply** to implement changes made.

Configuration > IGMP Snooping > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the DGS-1100-06/ME 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 DGS-1100-06/ME 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

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

The VLAN Settings of IGMP snooping

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

Figure 5.50 – 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.

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.

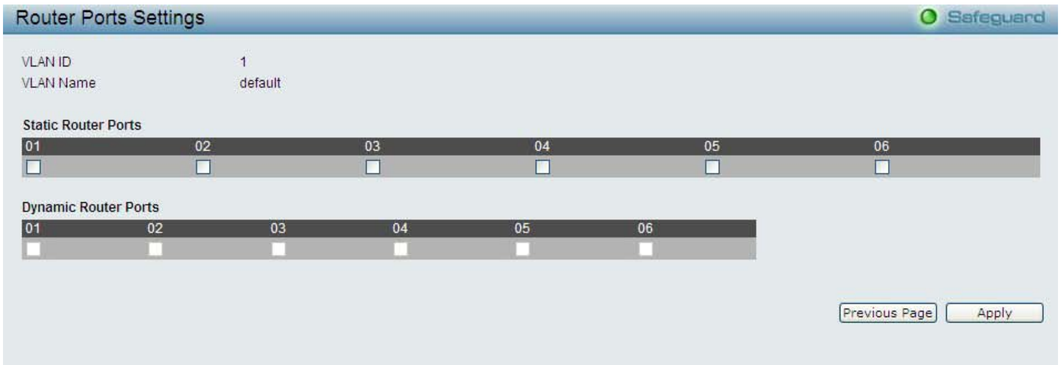
Last Member Query Interval (1-25 sec): The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" 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,** and **Fast Leave** 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** 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

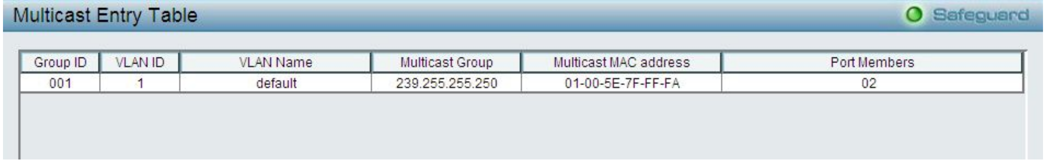
01	02	03	04	05	06
□	□	□	□	□	□

Dynamic Router Ports

01	02	03	04	05	06
□	□	□	□	□	□

Figure 5.51 – Configuration > IGMP Snooping > IGMP Snooping-Router Port Settings

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



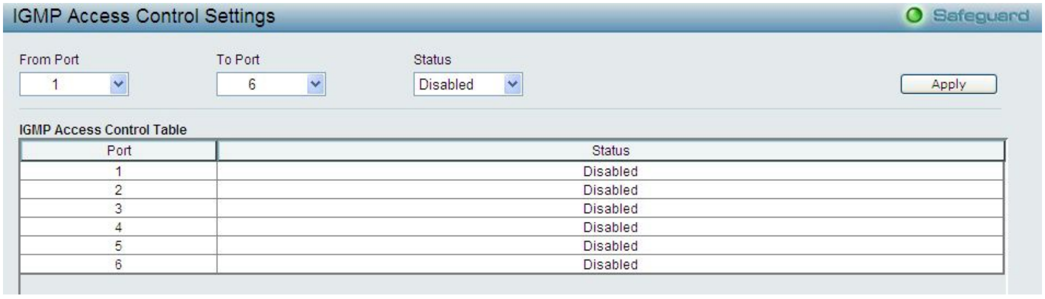
Multicast Entry Table

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	02

Figure 5.52– Configuration > IGMP Snooping > IGMP Snooping-Multicast Entry Table

Configuration > IGMP Snooping > IGMP Access Control Settings

The IGMP Access Control Settings page allows user to enable or disable the IGMP access control of ports. Click **Apply** to implement changes made.



IGMP Access Control Settings

From Port	To Port	Status
1	6	Disabled

IGMP Access Control Table

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

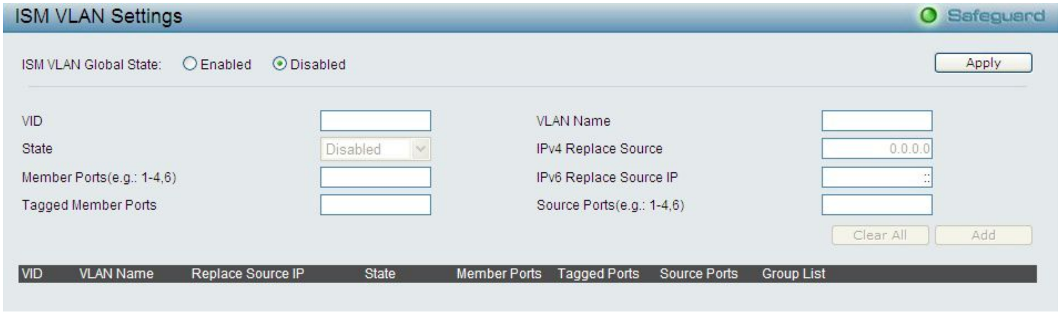
Figure 5.53 - Configuration > IGMP Snooping > IGMP Access Control Settings

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 Global State: ○ Enabled ● Disabled

VID		VLAN Name	
State	Disabled	IPv4 Replace Source	0.0.0.0
Member Ports(e.g.: 1-4,6)		IPv6 Replace Source IP	::
Tagged Member Ports		Source Ports(e.g.: 1-4,6)	

VID	VLAN Name	Replace Source IP	State	Member Ports	Tagged Ports	Source Ports	Group List

Figure 5.54 - 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.

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.

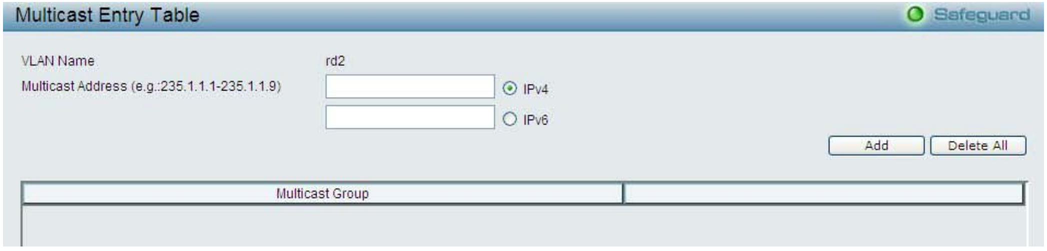
IPv6 Replace Source IP: This field is used to replace the source IPv6 address of incoming packets sent by the host before being forwarded to the source port.

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.



VLAN Name rd2

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

Multicast Group	

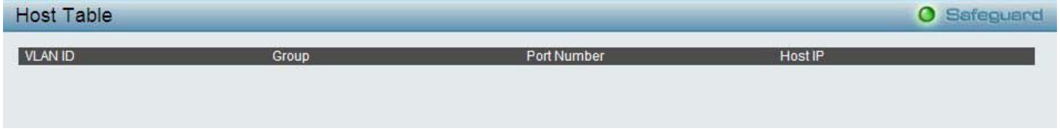
Figure 5.55 - Configuration > IGMP Snooping > ISM VLAN Settings

Multicast Address: Select IPv4 or IPv6 and specify the IP address.

Click **Add** to create a new entry, click **Delete All** to remove all entries.

Configuration > IGMP Snooping > Host Table

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

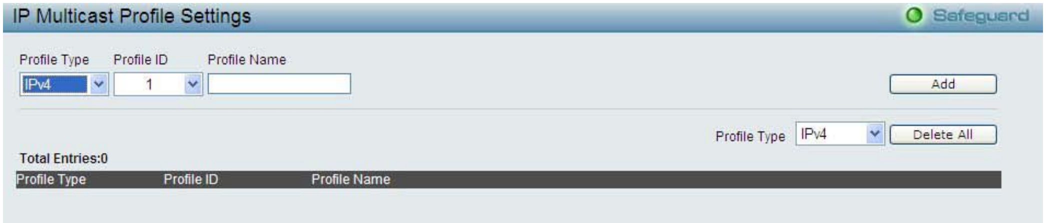


VLAN ID	Group	Port Number	Host IP

Figure 5.56 - 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.



IP Multicast Profile Settings

Profile Type	Profile ID	Profile Name
IPv4	1	

Profile Type IPv4

Total Entries:0

Profile Type	Profile ID	Profile Name

Figure 5.57 - Configuration > IGMP Snooping > IP Multicast Profile Settings

Profile Type: Specify the profile type to be IPv4 or IPv6.

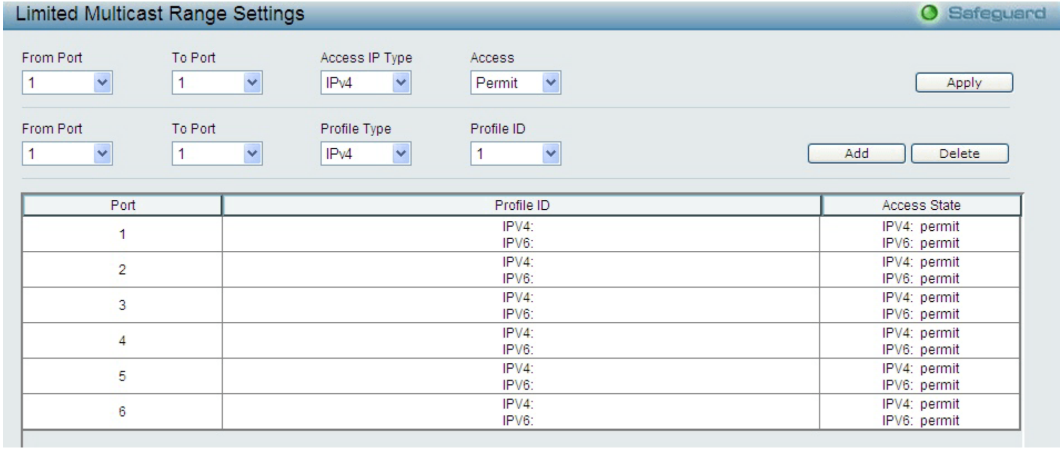
Profile ID: Specify the Profile ID.

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.



Limited Multicast Range Settings

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

From Port	To Port	Profile Type	Profile ID
1	1	IPv4	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: IPV6:	IPV4: permit IPV6: permit
6	IPV4: IPV6:	IPV4: permit IPV6: permit

Figure 5.58- Configuration > IGMP Snooping > Limited Multicast Range Settings

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

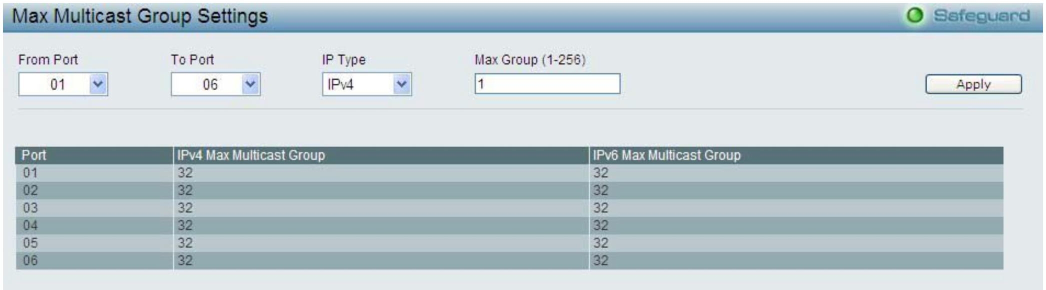
Profile Type: Specify the profile type is IPv4 or IPv6.

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	06	IPv4	1

Port	IPv4 Max Multicast Group	IPv6 Max Multicast Group
01	32	32
02	32	32
03	32	32
04	32	32
05	32	32
06	32	32

Figure 5.59- Configuration > IGMP Snooping > Max Multicast Group Settings

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

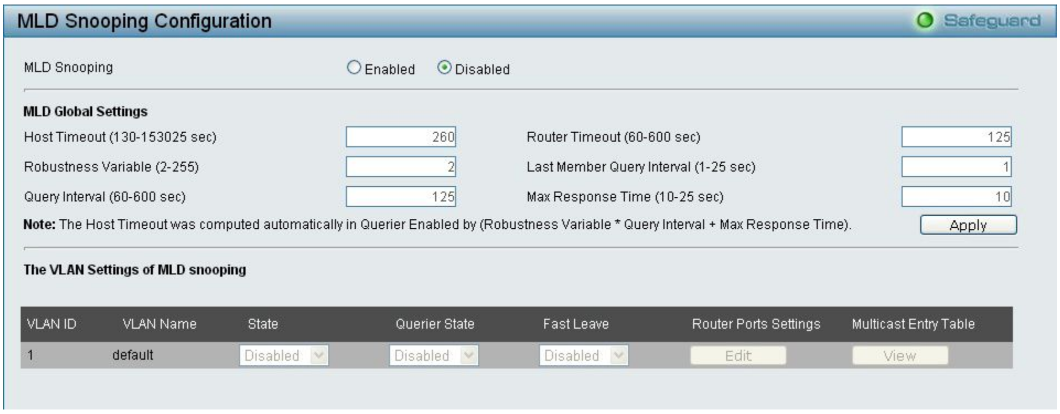
IP Type: Specify the IP type is IPv4 or IPv6.

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

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	Router Ports Settings	Multicast Entry Table
1	default	Disabled	Disabled	Disabled	Edit	View

Figure 5.60 - 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 the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.

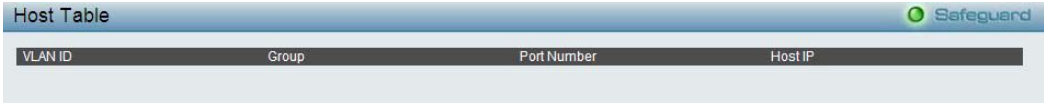
Query Interval (60-600 sec): The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of MLD messages can increase or decrease; larger values cause MLD Queries to be sent less often. Default is 125 seconds.

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.

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.



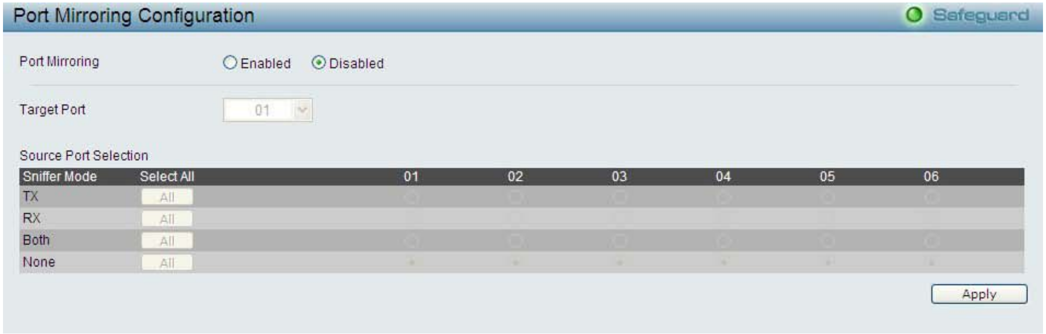
Host Table

VLAN ID	Group	Port Number	Host IP

Figure 5.61 - 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
TX	All	○	○	○	○	○	○
RX	All	○	○	○	○	○	○
Both	All	○	○	○	○	○	○
None	All	●	●	●	●	●	●

Figure 5.62 – Configuration > Port Mirroring

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.

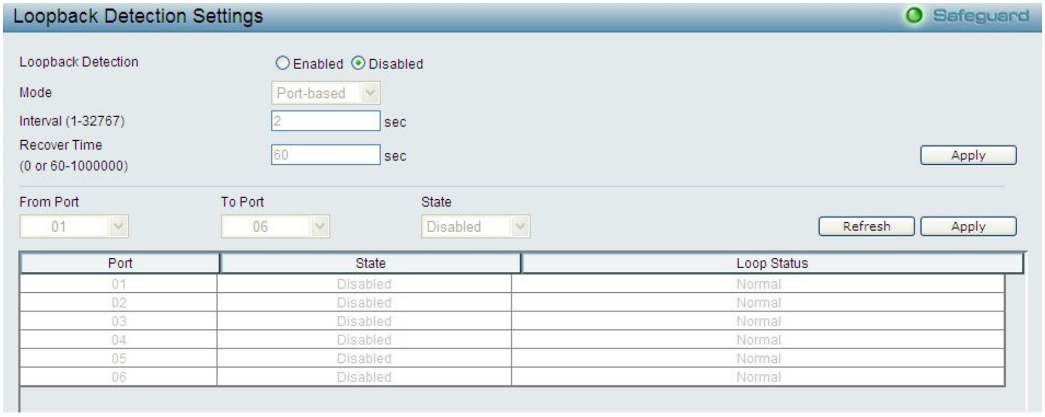
Both (TX and RX) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click “all” to include all ports into port mirroring.

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 Settings

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 06 State Disabled

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

Figure 5.63 – 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.

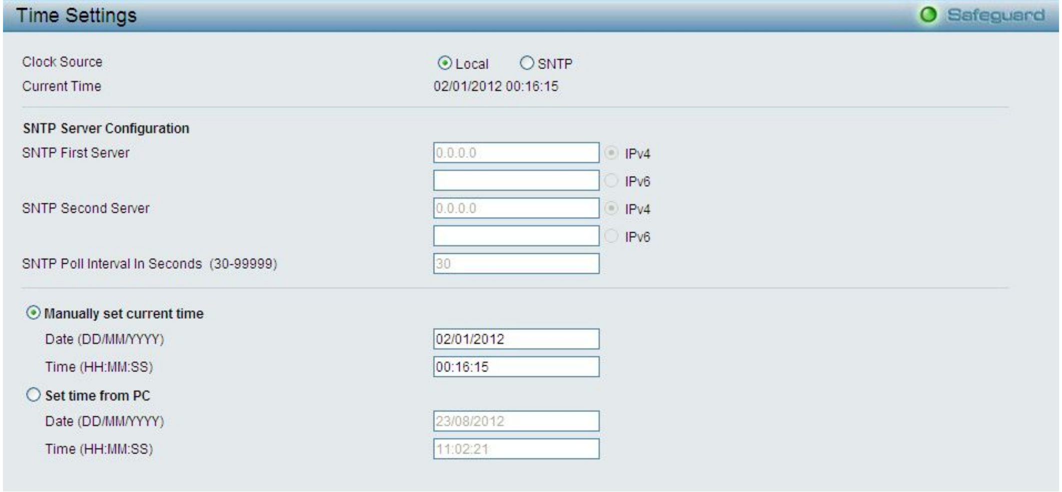
To Port: The ending of a consecutive group of ports may be configured starting with the selected port.

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

Click **Apply** to implement changes made and click **Refresh** to renew the page.

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.



Time Settings

Clock Source	● Local ○ SNTP
Current Time	02/01/2012 00:16:15
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)	02/01/2012
Time (HH:MM:SS)	00:16:15
○ **Set time from PC**	
Date (DD/MM/YYYY)	23/08/2012
Time (HH:MM:SS)	11:02:21

Figure 5.64 – 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.

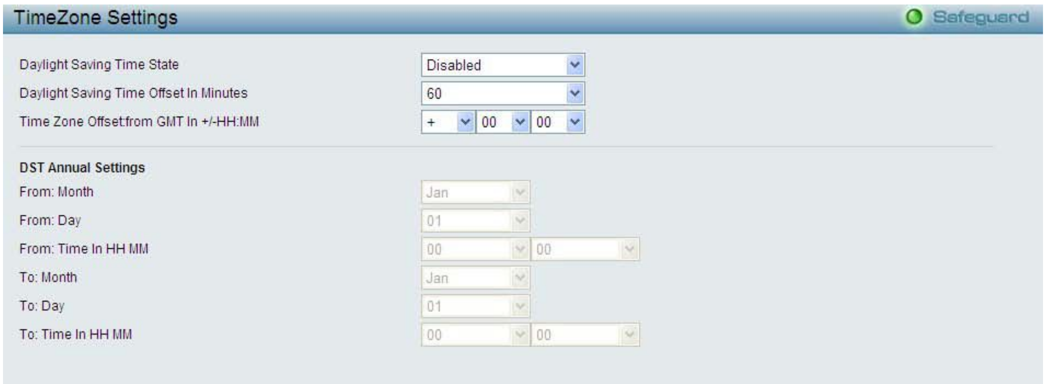
When selecting **Local** for the clock source, users can select from one of two options:

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.



TimeZone Settings

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 5.65 – 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.

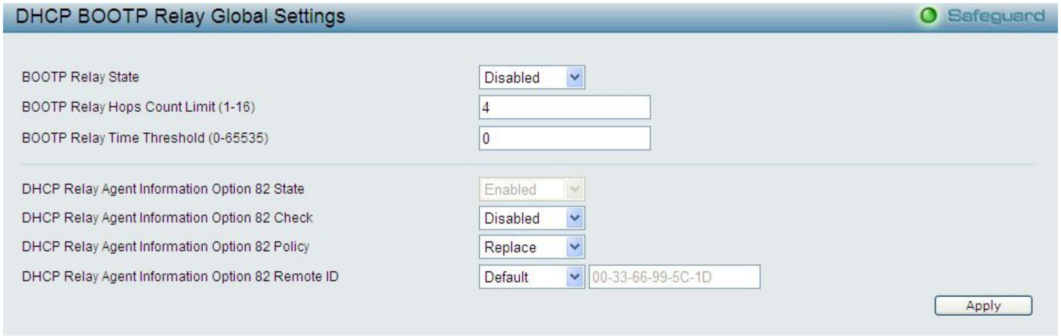
To: Month / Day: Enter the month DST and date DST will end on, each year.

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 00-33-66-99-5C-1D

Figure 5.66 - 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.

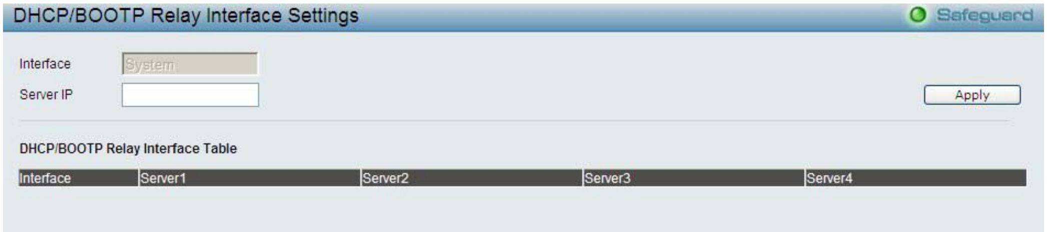
Keep -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.

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

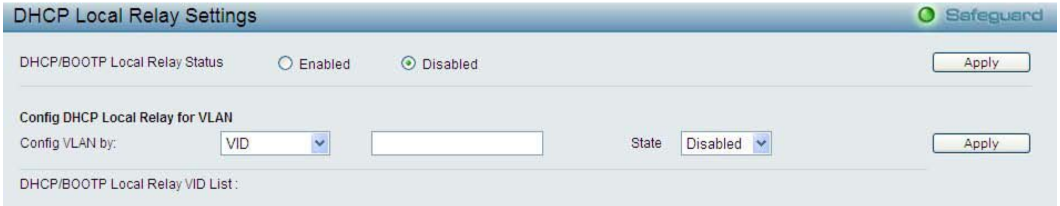
Figure 5.67 - Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

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.

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 5.68 - 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.

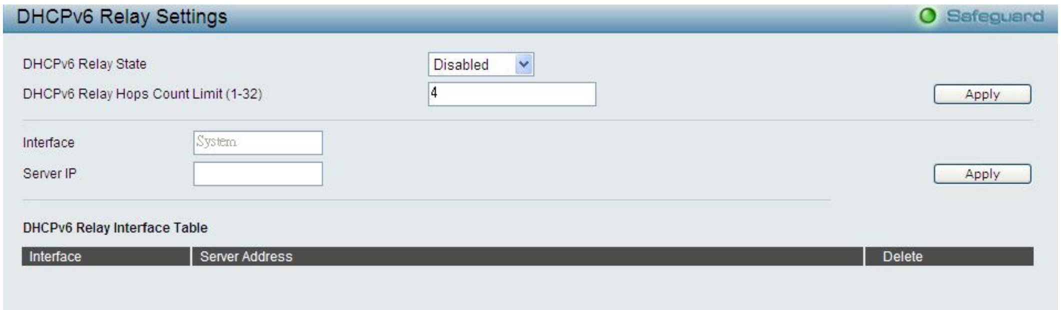
Disabled – Disables DHCP Local Relay on the VLAN.

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

Interface: System

Server IP:

DHCPv6 Relay Interface Table

Interface	Server Address	Delete

Figure 5.69 - 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.

Interface: Enter a name of the interface.

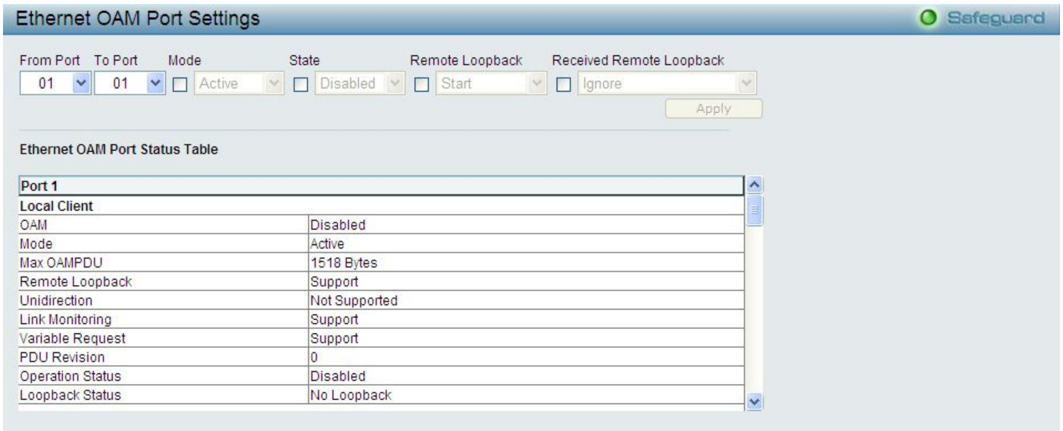
Server IP: Enter the server IP address.

Click **Apply** to implement changes made.

Configuration > Ethernet OAM > Ethernet OAM Port Settings

Ethernet OAM (Operations, Administration, and Maintenance) is a data link layer protocol which provides network administrators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions on point-to-point and emulated point-to-point Ethernet link.

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

Figure 5.70 - Configuration > Ethernet OAM > Ethernet OAM Port Settings

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

Mode: Specify to operate in either active mode or passive mode. The default mode is active.

State: Specify to enable or disable the OAM function. The default state is disabled.

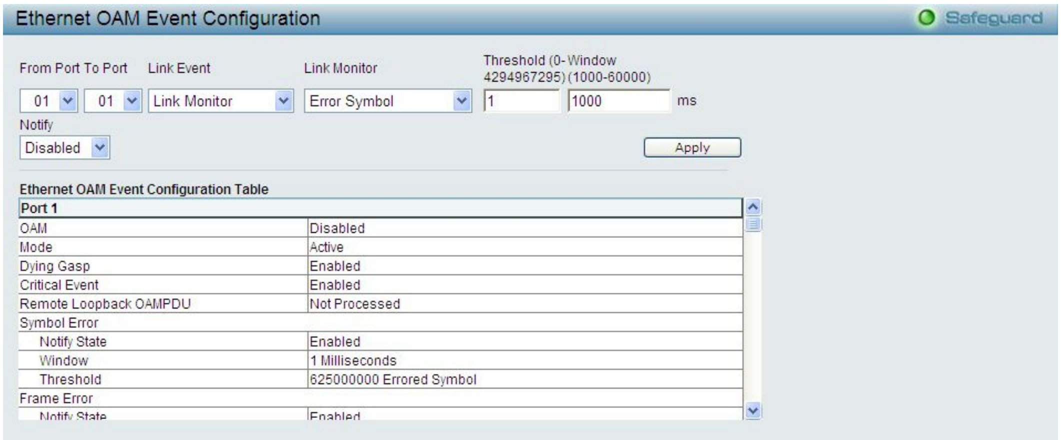
Remote Loopback: If start is specified, it will request the peer to change to the remote loopback mode. If stop is specified, it will request the peer to change to the normal operation mode.

Received Remote Loopback: Specify whether to process or to ignore the received Ethernet OAM remote loopback command. The default method is I*gnore*.

Click **Apply** to implement changes made.

Configuration > Ethernet OAM > Ethernet OAM Event Configuration

The Ethernet OAM Event Configuration page allows user to configure the Ethernet OAM Event 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	1 Milliseconds
Threshold	625000000 Errored Symbol
Frame Error	
Notify State	Enabled

Figure 5.71 - Configuration > Ethernet OAM > Ethernet OAM Event Configuration

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

Link Event: Choose the type of Link Event, *Link Monitor* or *Critical Link Event*, to configure.

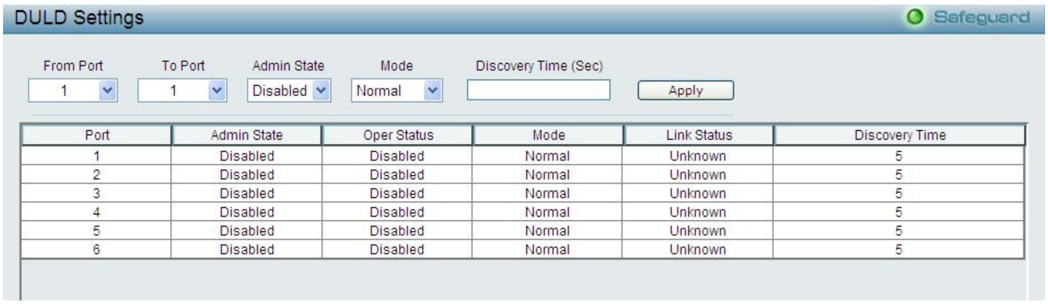
Link Monitor: The option is used to configure ports Ethernet OAM link monitoring error symbols, error frames, error frame period, and error frame seconds. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. If the number of error symbols or error frames is equal to or greater than the specified threshold within the period specified by the **Window** option, and the event notification state (**Notify**) is enabled, it generates an event to notify the remote OAM peer.
Use the Link Monitor menu to define the type of link monitor, and set the threshold, window and notifications status.
Threshold: Specify the number of error symbols, error frames, error frame period, or error frame seconds in the period that is required to be equal to or greater than in order for the event to be generated. Threshold value can range from 0 – 4294967295.
Window: For error symbol and error frame, the available range is 1000 to 60000 ms and default value 1000ms. For error frame period the range is 14881 to 89286000, the default value is 148810 for FE port. For error frame seconds the range is 10000 to 900000, the default value is 60000.

Click **Apply** to implement changes made.

Configuration > DULD > DULD Port Settings

The Switch features a D-Link Unidirectional Link Detection (DULD) module. The unidirectional link detection provides a mechanism that can be used to detect unidirectional link for Ethernet switches whose PHYs do not support unidirectional OAM operation. This function is established based on OAM, so OAM should be enabled before starting detection.

To view this window, click Configuration > DULD > DULD Port Settings, as shown below:



From Port: 1
To Port: 1
Admin State: Disabled
Mode: Normal
Discovery Time (Sec):

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

Figure 5.72 - Configuration > DULD > DULD Port Settings

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

Admin State: Enable or disable the administration state. This indicates these ports unidirectional link detection status. The default state is *Disabled*.

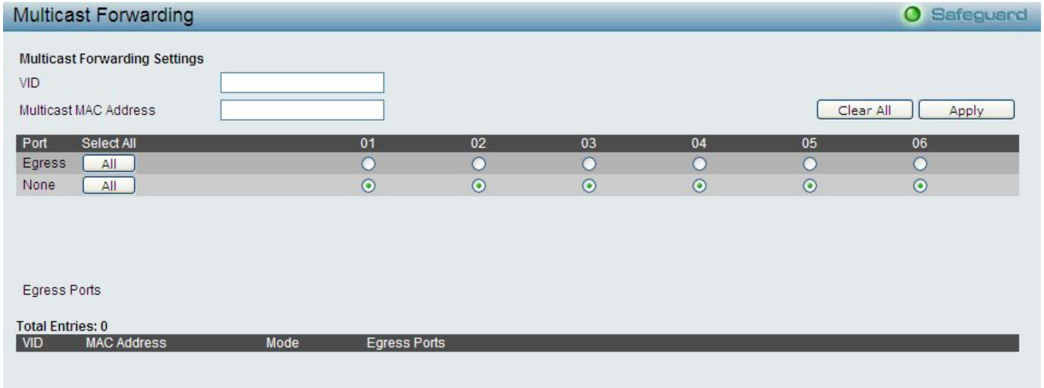
Mode: Toggle between Shutdown and Normal. When Shutdown is selected if any unidirectional link is detected, this feature will disable the port and log an event. When Normal is selected, this feature will only log an event when a unidirectional link is detected.

Discovery Time (sec): Enter the port neighbor discovery time between 5 and 65535 seconds. If the discovery is timed out, the unidirectional link detection will start. The default discovery time is 5 seconds.

Click **Apply** to create a new entry.

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 Settings

VID

Multicast MAC Address

Port	Select All	01	02	03	04	05	06
Egress	All	○	○	○	○	○	○
None	All	●	●	●	●	●	●

Egress Ports

Total Entries: 0

VID	MAC Address	Mode	Egress Ports

Figure 5.73 - 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.

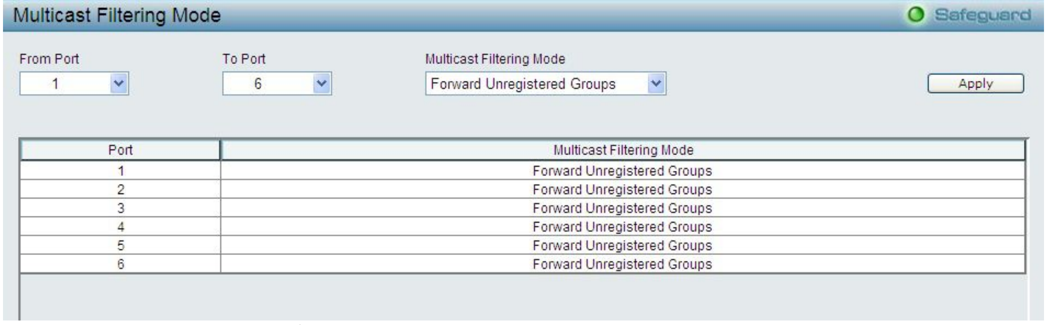
Port Settings: Allows the selection of ports that will be members of the static multicast group and ports either that are forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP.

> **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.



From Port: 1

To Port: 6

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

Figure 5.74 - Configuration > Multicast Forwarding & Filtering > Multicast Filtering

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

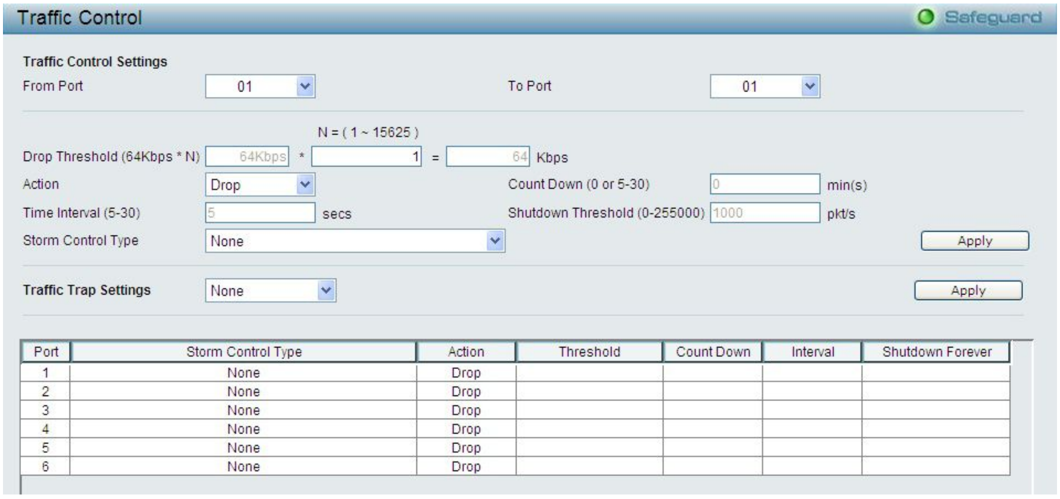
Multicast Filtering Mode: This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.

> **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 ~ 15625)

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				

Figure 5.75 – 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 15625.

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.

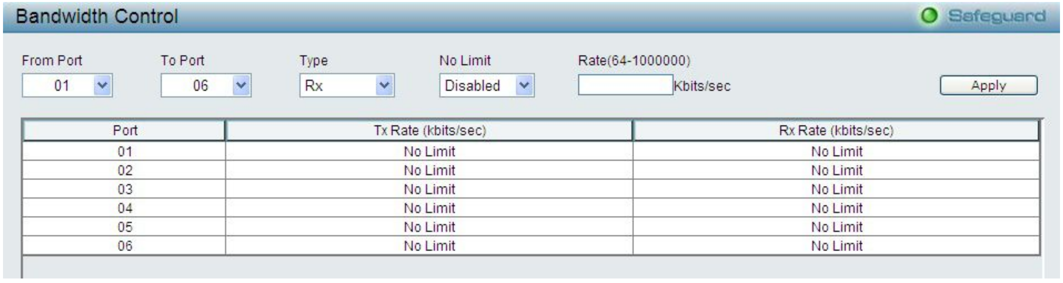
NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation.

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(64-1000000)
01	06	Rx	Disabled	Kbits/sec

Port	Tx Rate (kbits/sec)	Rx Rate (kbits/sec)
01	No Limit	No Limit
02	No Limit	No Limit
03	No Limit	No Limit
04	No Limit	No Limit
05	No Limit	No Limit
06	No Limit	No Limit

Figure 5.76 – 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.

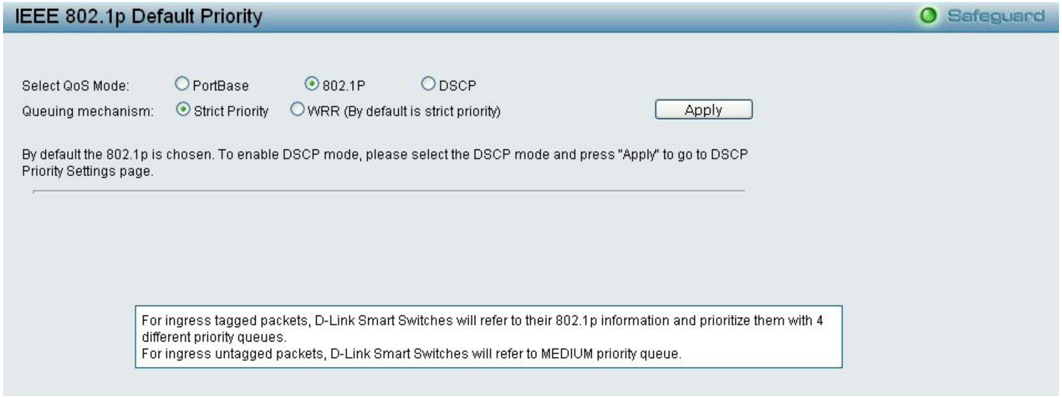
Rate (64-1024000): This field allows you to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 64 and 1024000.

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 > 802.1p/DSCP Priority Settings

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.



IEEE 802.1p Default Priority

Select QoS Mode: ○ PortBase ● 802.1P ○ DSCP

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

By default the 802.1p is chosen. To enable DSCP mode, please select the DSCP mode and press "Apply" to go to DSCP Priority Settings page.

For ingress tagged packets, D-Link Smart Switches will refer to their 802.1p information and prioritize them with 4 different priority queues.
For ingress untagged packets, D-Link Smart Switches will refer to MEDIUM priority queue.

Figure 5.77 - QoS > 802.1p/DSCP Priority Settings

Select QoS Mode: Specifies the QoS mode to be PortBase, 802.1p or DSCP.

Quening Mechanism:

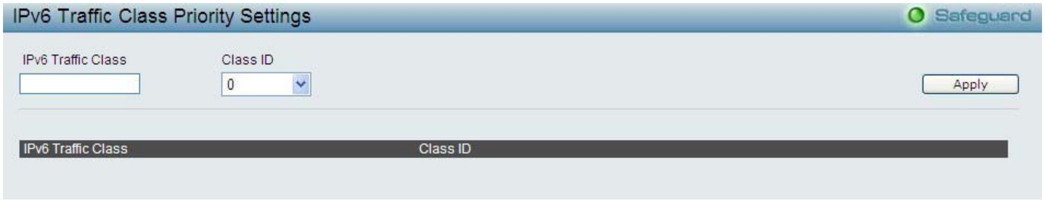
Strict Priority: Denoting a Strict scheduling will set the highest queue to be emptied first while the other queues will follow the weighted round-robin scheduling scheme

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

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

QoS > IPv6 Traffic Class Priority Settings

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



Class ID: 0

IPv6 Traffic Class	Class ID

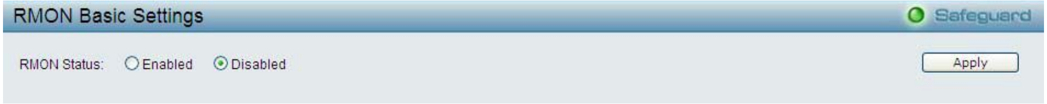
Figure 5.78 - QoS > IPv6 Traffic Class Priority Settings

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.

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.

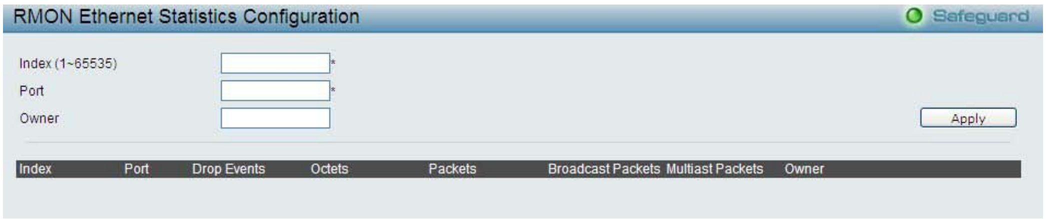


RMON Status: ○ Enabled ● Disabled

Figure 5.79 - 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	Port	Drop Events	Octets	Packets	Broadcast Packets	Multiast Packets	Owner

Figure 5.80 - RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:

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

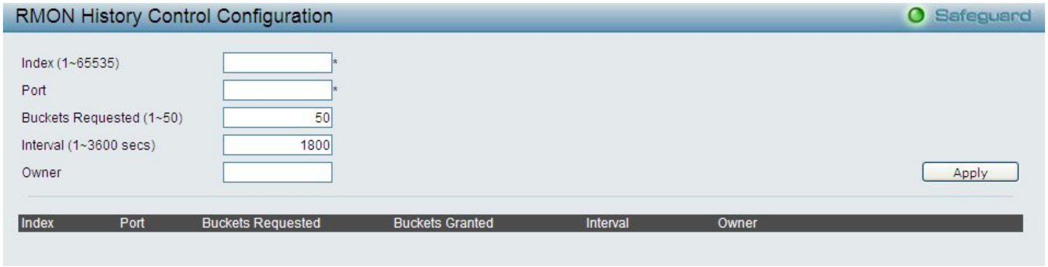
Port: Specifies the port from which the RMON information was taken.

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.



RMON History Control Configuration

Index (1~65535)	*
Port	*
Buckets Requested (1~50)	50
Interval (1~3600 secs)	1800
Owner	

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner

Figure 5.81 - 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.

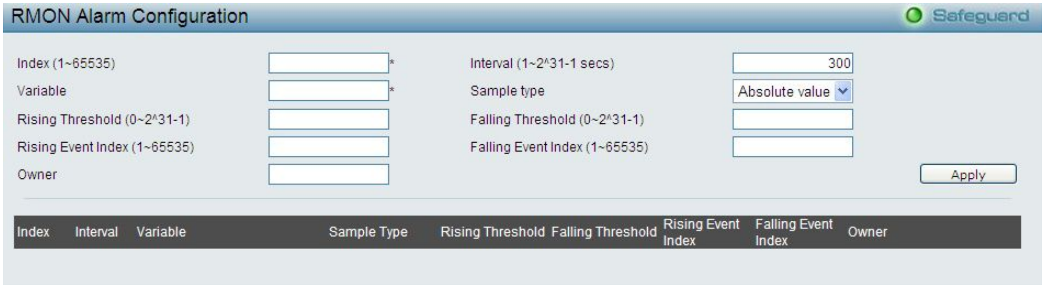
Interval (1 ~ 3600): Indicates in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes).

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.



RMON Alarm Configuration

Index (1~65535)	*	Interval (1~2^31-1 secs)	300
Variable	*	Sample type	Absolute value
Rising Threshold (0~2^31-1)		Falling Threshold (0~2^31-1)	
Rising Event Index (1~65535)		Falling Event Index (1~65535)	
Owner			

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

Figure 5.82 - 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.

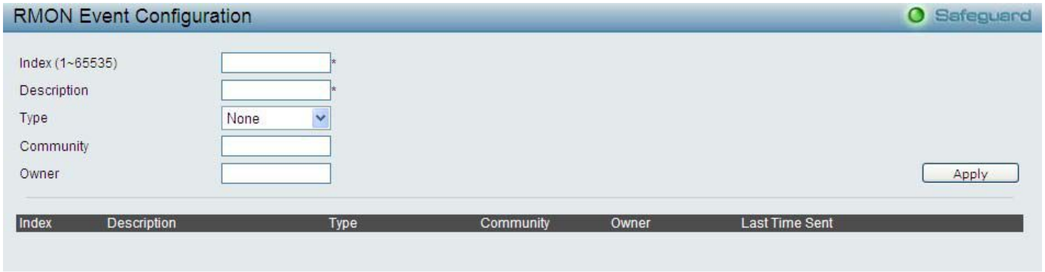
Falling Threshold (0 ~ 2^31-1): Displays the falling counter value that triggers the falling threshold alarm.

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 5.83 - 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.

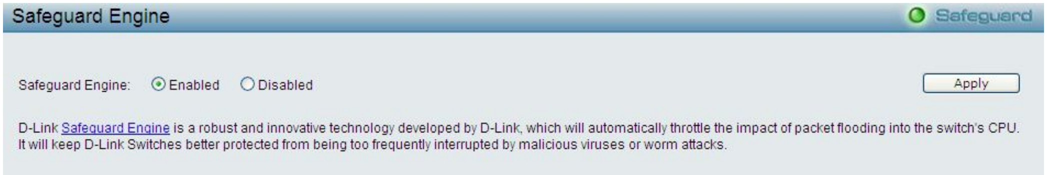
Community: Specifies the community to which the event belongs.

Owner: Specifies the time that the event occurred.

Click **Apply** to add a new RMON event.

Security > 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

Safeguard Engine: ● Enabled ○ Disabled

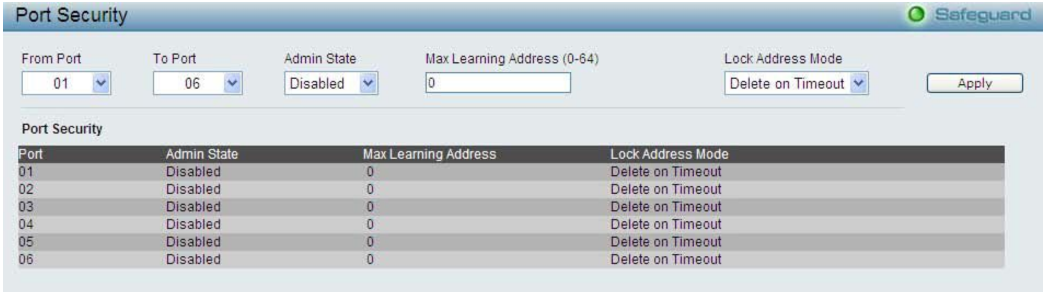
D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU. It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.

Figure 5.84 – Security > Safeguard Engine

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	06	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

Figure 5.85 - 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.

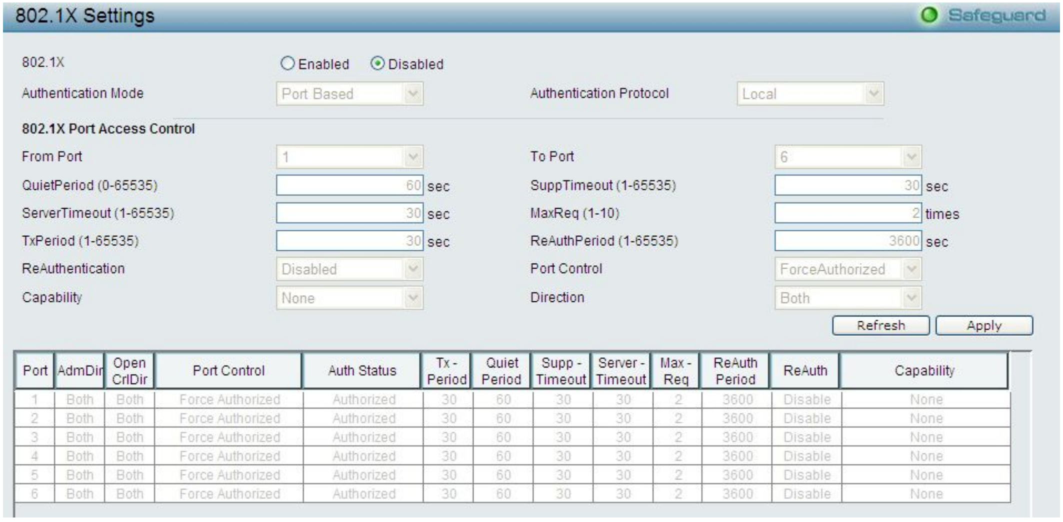
Click **Apply** to make configurations make effects.

Security > 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	6	
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

Figure 5.86 - 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***.**

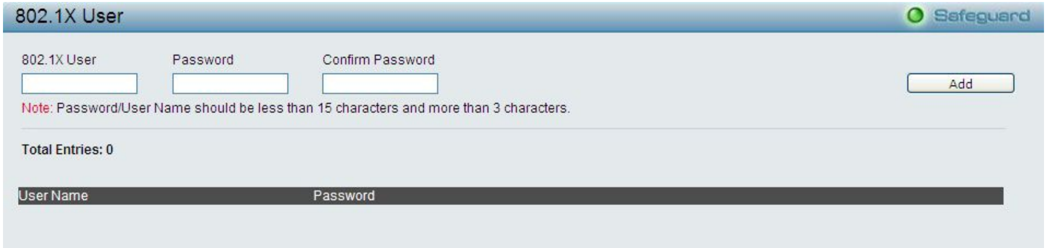
Direction: Sets the administrative-controlled direction on the port. The possible field values are:

> **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.

<u>Security > 802.1X > 802.1X User</u>

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.



802.1X User

802.1X User | Password | Confirm Password

Note: Password/User Name should be less than 15 characters and more than 3 characters.

Total Entries: 0

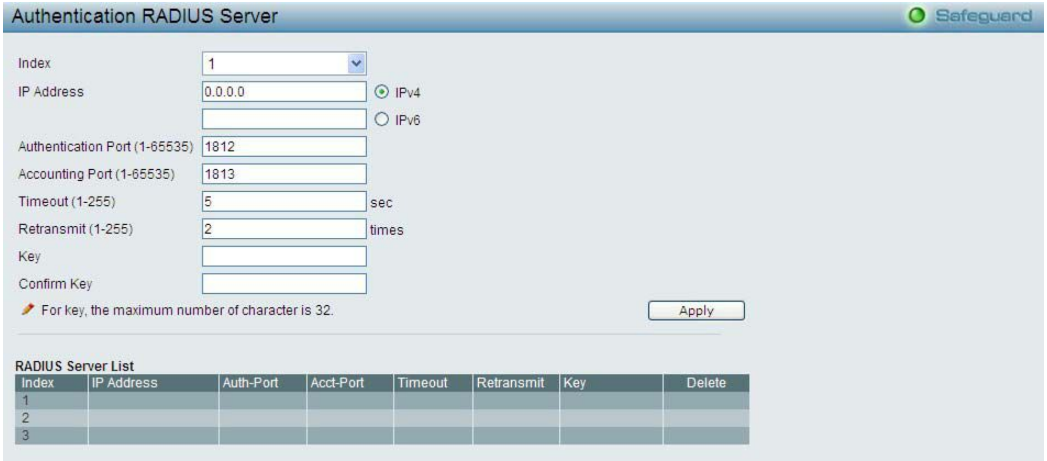
User Name	Password

Figure 5.87 - 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	0.0.0.0	● 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 5.88 - 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.

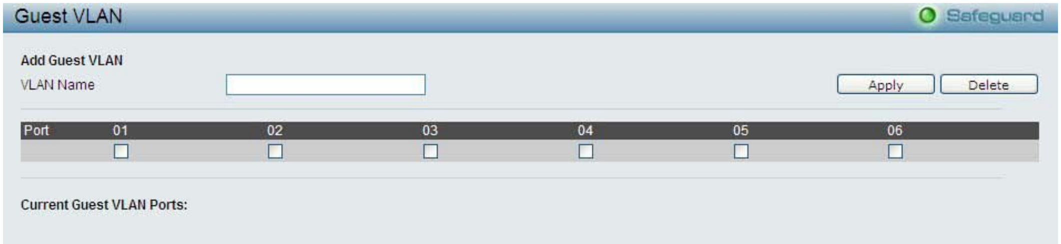
Confirm Key: Confirm the shared key is the same as that of the RADIUS server.

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

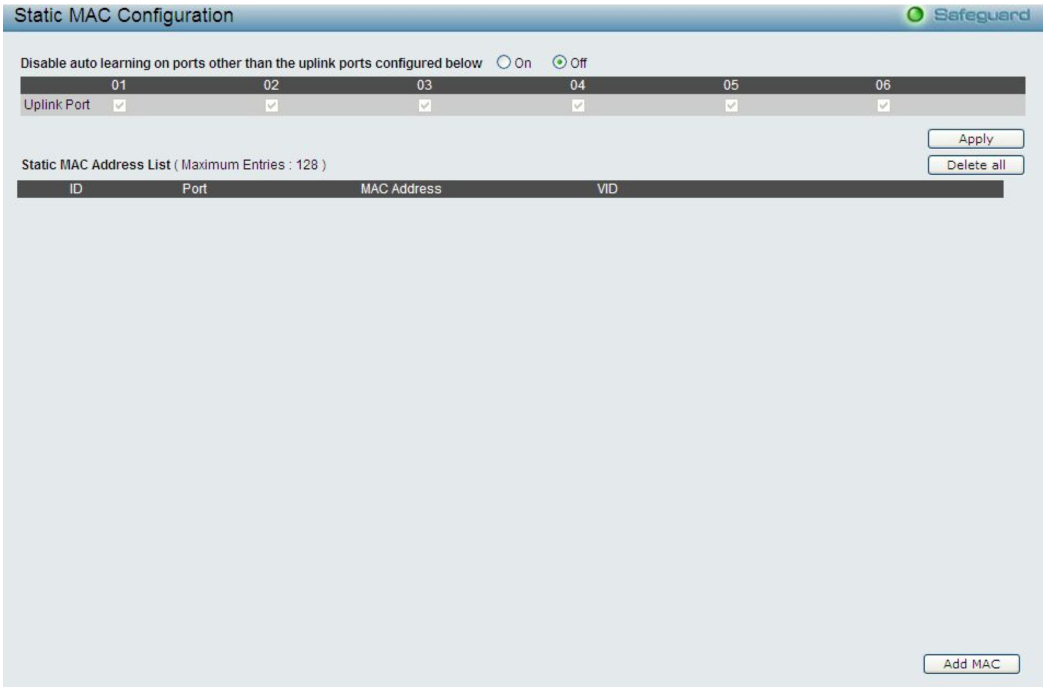
Port	01	02	03	04	05	06
	□	□	□	□	□	□

Current Guest VLAN Ports:

Figure 5.89 - 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).



Static MAC Configuration

Safeguard

Disable auto learning on ports other than the uplink ports configured below ○ On ● Off

	01	02	03	04	05	06
Uplink Port	☑	☑	☑	☑	☑	☑

Apply

Static MAC Address List (Maximum Entries : 128)

Delete all

ID	Port	MAC Address	VID

Add MAC

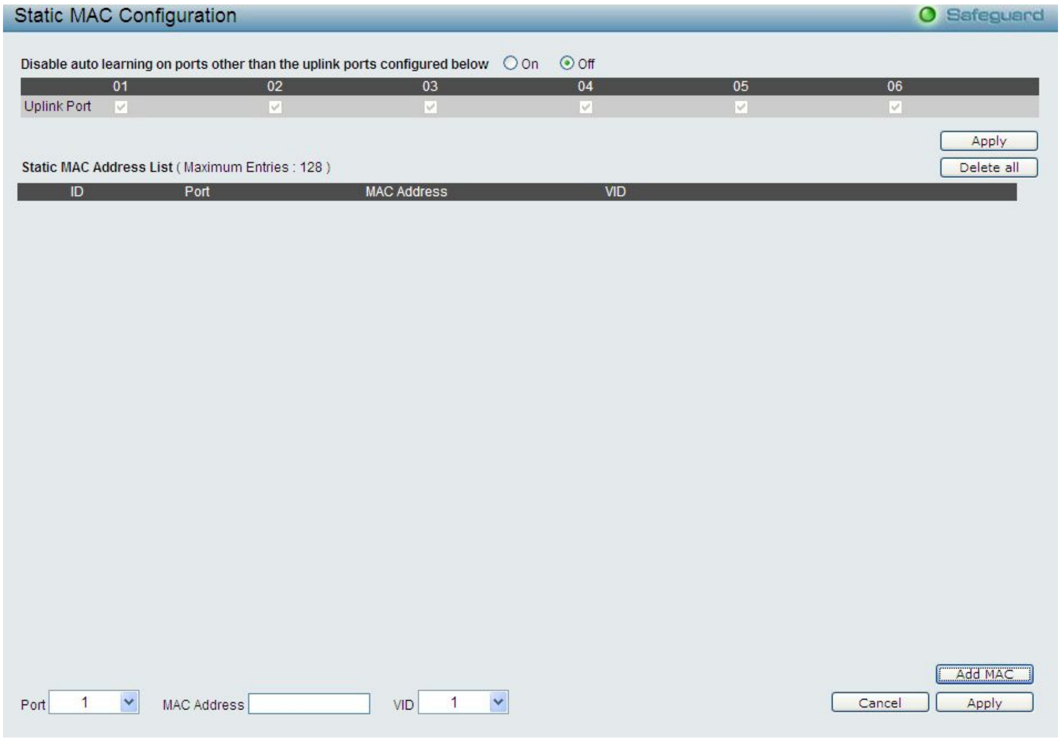
Figure 5.90 - Security > MAC Address Table > Static Mac Address

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.



Disable auto learning on ports other than the uplink ports configured below ○ On ● Off

	01	02	03	04	05	06
Uplink Port	☑	☑	☑	☑	☑	☑

Static MAC Address List (Maximum Entries : 128)

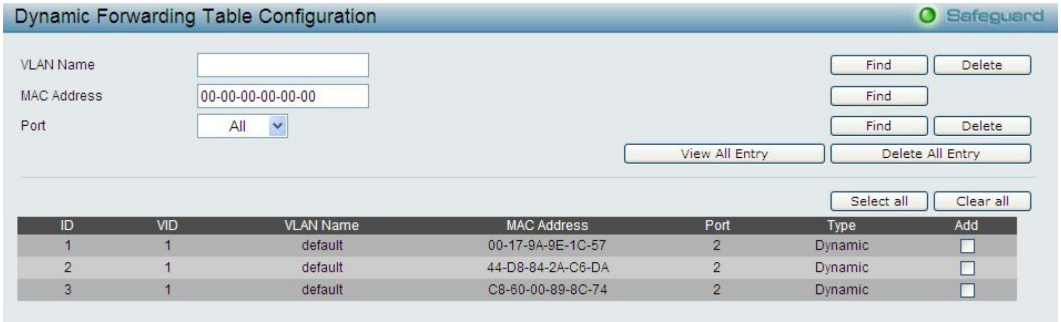
ID	Port	MAC Address	VID

Port 1 MAC Address VID 1

Figure 5.91 - 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.



VLAN Name

MAC Address 00-00-00-00-00-00

Port All

ID	VID	VLAN Name	MAC Address	Port	Type	Add
1	1	default	00-17-9A-9E-1C-57	2	Dynamic	□
2	1	default	44-D8-84-2A-C6-DA	2	Dynamic	□
3	1	default	C8-60-00-89-8C-74	2	Dynamic	□

Figure 5.92 - 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.

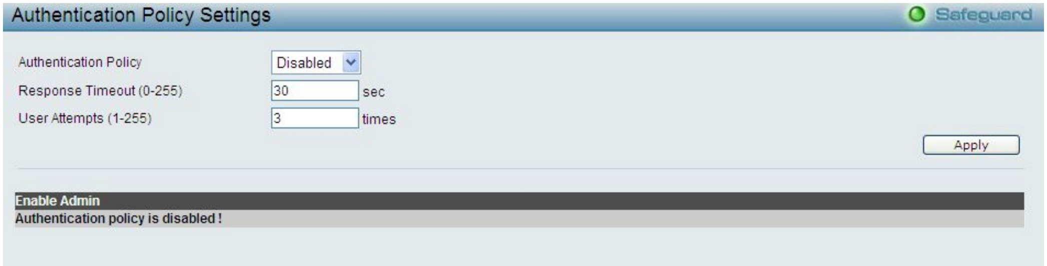
Port: The port to which the MAC address above corresponds.

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 5.93 – Security > Access Authentication control > Authentication Policy Settings

Authentication Policy: Use the pull-down menu to enable or disable the Authentication Policy on the Switch.

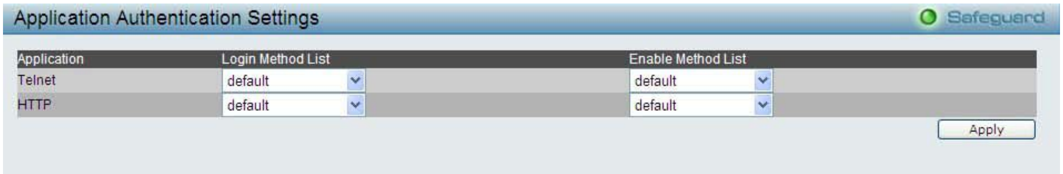
Response Timeout (0 - 255): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.

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 (Telnet, 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
Telnet	default	default
HTTP	default	default

Figure 5.94 – 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 Telnet application 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.

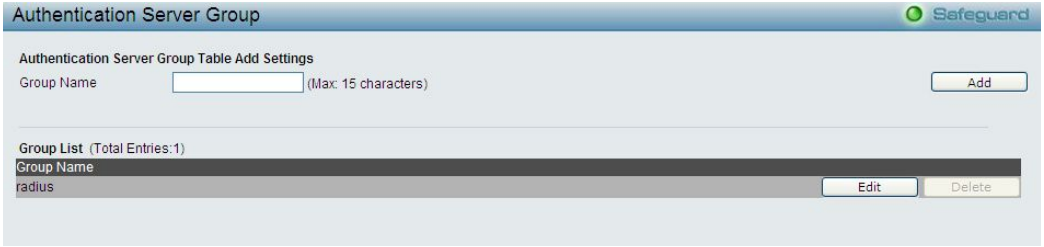
Enable Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

Click **Apply** to implement configuration changes.

Security > Access Authentication Control > Authentication Server Group

A server group is a technique used to group 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

Authentication Server Group Table Add Settings

Group Name (Max: 15 characters) Add

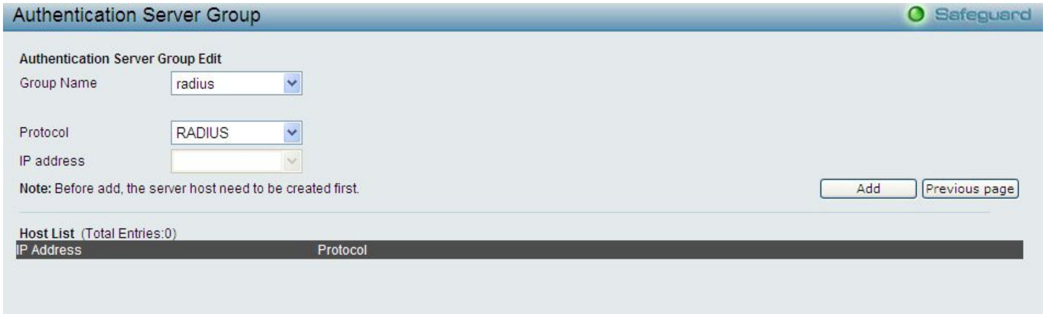
Group List (Total Entries:1)

Group Name		
radius	Edit	Delete

Figure 5.95 – 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

Authentication Server Group Edit

Group Name: radius

Protocol: RADIUS

IP address:

Note: Before add, the server host need to be created first.

Host List (Total Entries:0)

IP Address	Protocol

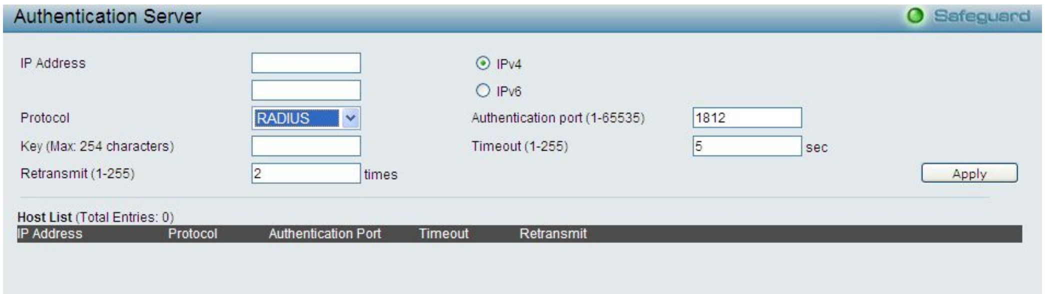
Figure 5.96 – Security > Access Authentication control > Authentication Server Group-Edit

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.

Security > Access Authentication Control > Authentication Server

This Authentication Server page will set user-defined **Authentication Server Hosts** for the 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 RADIUS server host on a remote host. The RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. The maximum supported number of server hosts is *16*.



Authentication Server

IP Address: ● IPv4 ○ IPv6

Protocol: RADIUS

Authentication port (1-65535): 1812

Key (Max: 254 characters):

Timeout (1-255): 5 sec

Retransmit (1-255): 2 times

Host List (Total Entries: 0)

IP Address	Protocol	Authentication Port	Timeout	Retransmit

Figure 5.97 – 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:

RADIUS – Enter this parameter if the server host utilizes the RADIUS protocol.

Authentication 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 *1812* but the user may set a unique port number for higher security.

Key(Max: 254 characters): Authentication key to be shared with a configured RADIUS servers only. Specify an alphanumeric string up to *254* characters.

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. The default value is *2*.

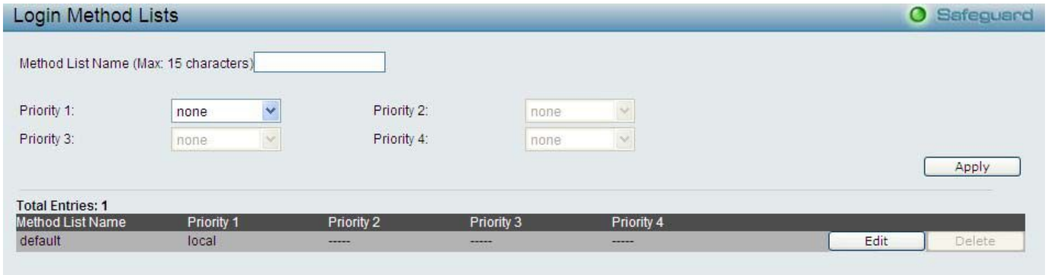
Click **Apply** to add a new Authentication Server Host.

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.



Login 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	local	-----	-----	-----	Edit	Delete

Figure 5.98 – 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.

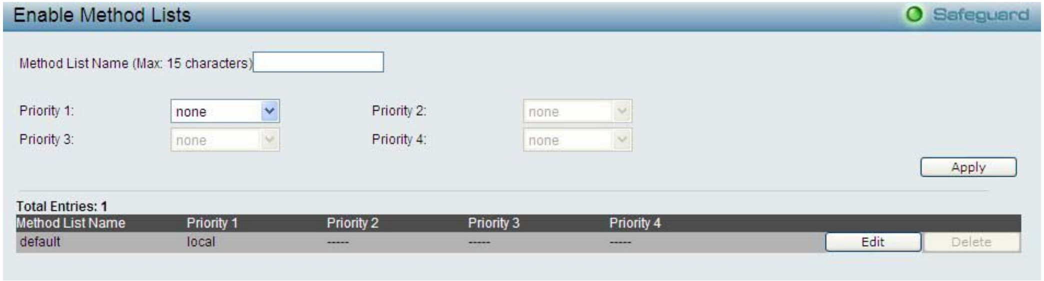
local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

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**.



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 5.99 – 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:

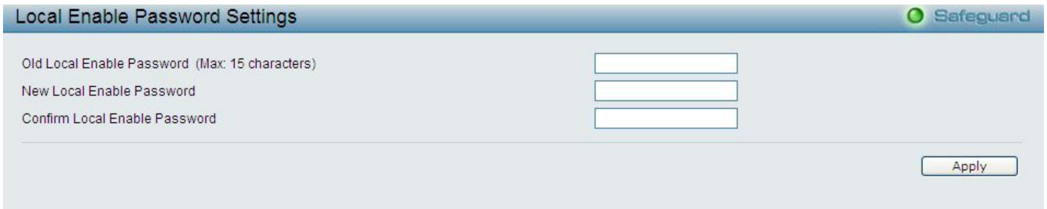
none – Adding this parameter will require an authentication to access the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

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.



Old Local Enable Password (Max: 15 characters)

New Local Enable Password

Confirm Local Enable Password

Figure 5.100 – Security > Access Authentication control > Local Enable Password Settings

To set the Local Enable Password, set the following parameters and click **Apply**:

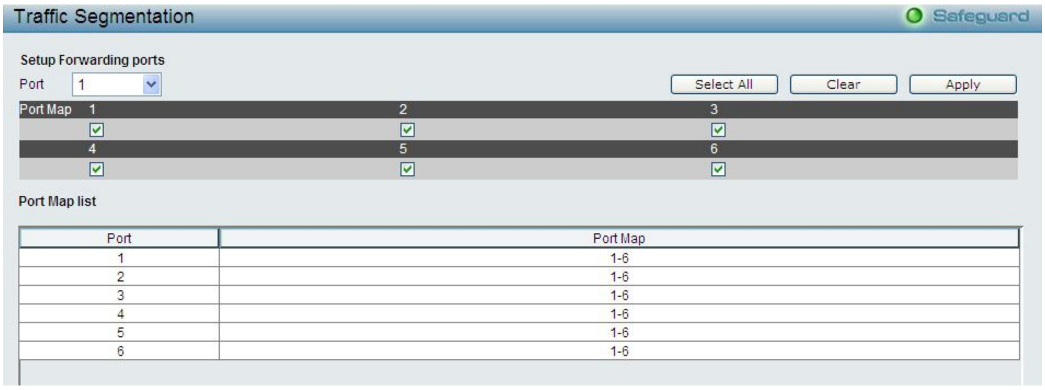
Old Local Enable Password: If a password was previously configured for this entry, enter it here in order to change it to a new password.

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.



Setup Forwarding ports

Port 1

Port Map	1	2	3
	☑	☑	☑
	4	5	6
	☑	☑	☑

Port Map list

Port	Port Map
1	1-6
2	1-6
3	1-6
4	1-6
5	1-6
6	1-6

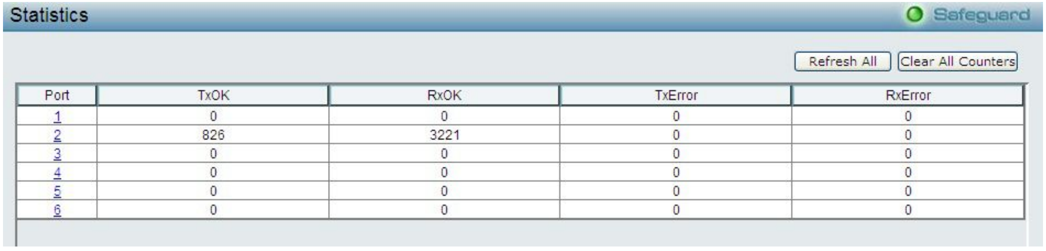
Figure 5.101 – Security > Traffic Segmentation

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.

Monitoring > Statistics

The Statistics screen displays the status of each port packet count.



Port	TxOK	RxOK	TxError	RxError
1	0	0	0	0
2	826	3221	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0

Figure 5.102 – Monitoring > Port Statistics

Refresh All: Renews the details collected and displayed.

Clear All: To reset the details displayed.

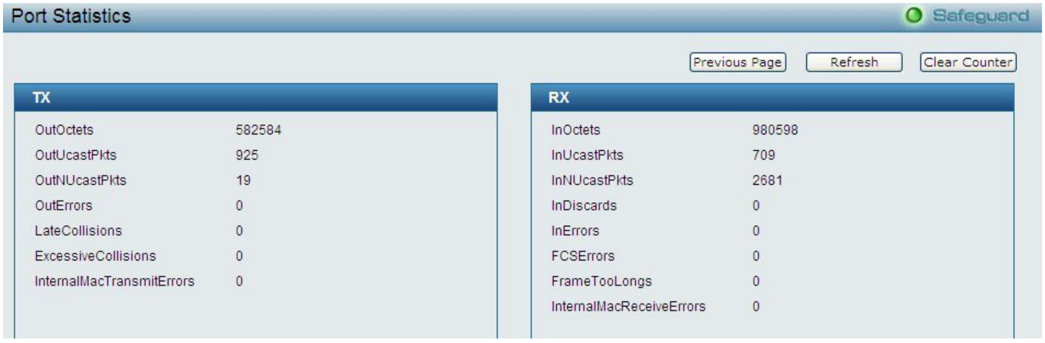
TxOK: Number of packets transmitted successfully.

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	582584	InOctets	980598
OutUcastPkts	925	InUcastPkts	709
OutNUcastPkts	19	InNUcastPkts	2681
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

Figure 5.103 – Monitoring > Port Statistics

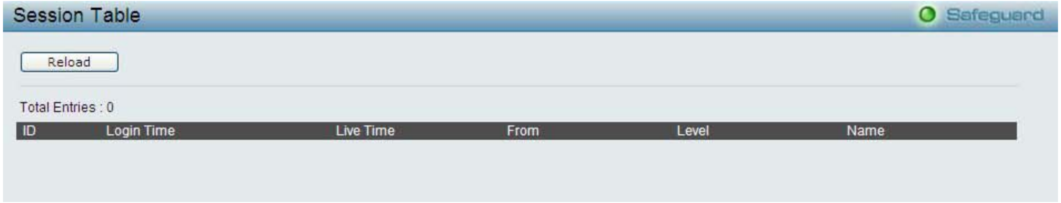
Previous Page: Go back to the Statistics main page.

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.



Session Table

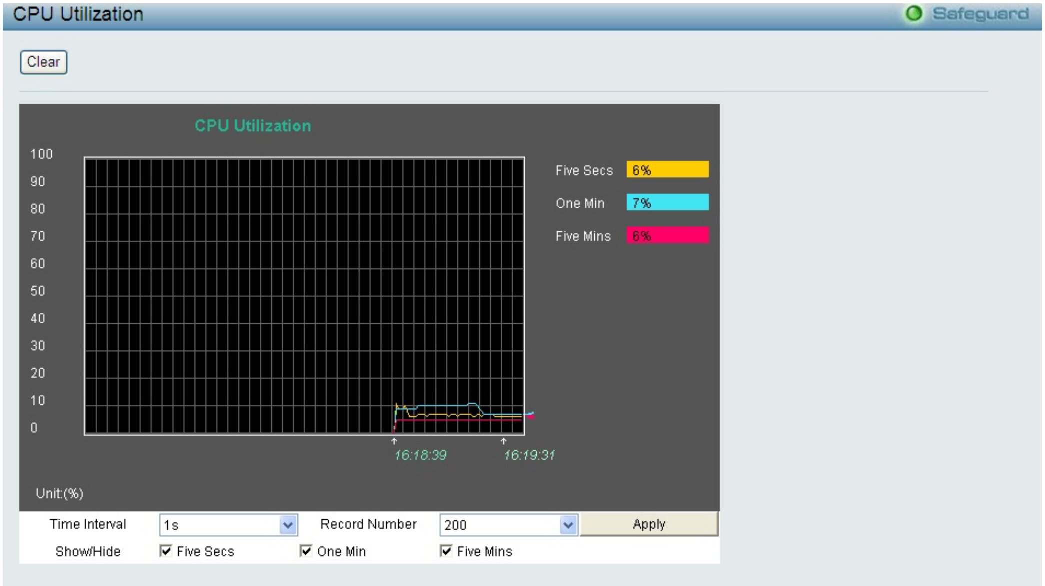
Total Entries : 0

ID	Login Time	Live Time	From	Level	Name

Figure 5.104 – 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.



CPU Utilization

Five Secs 6%
One Min 7%
Five Mins 6%

Time Interval 1s
Record Number 200

Show/Hide ☑ Five Secs ☑ One Min ☑ Five Mins

Figure 5.105 – 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.

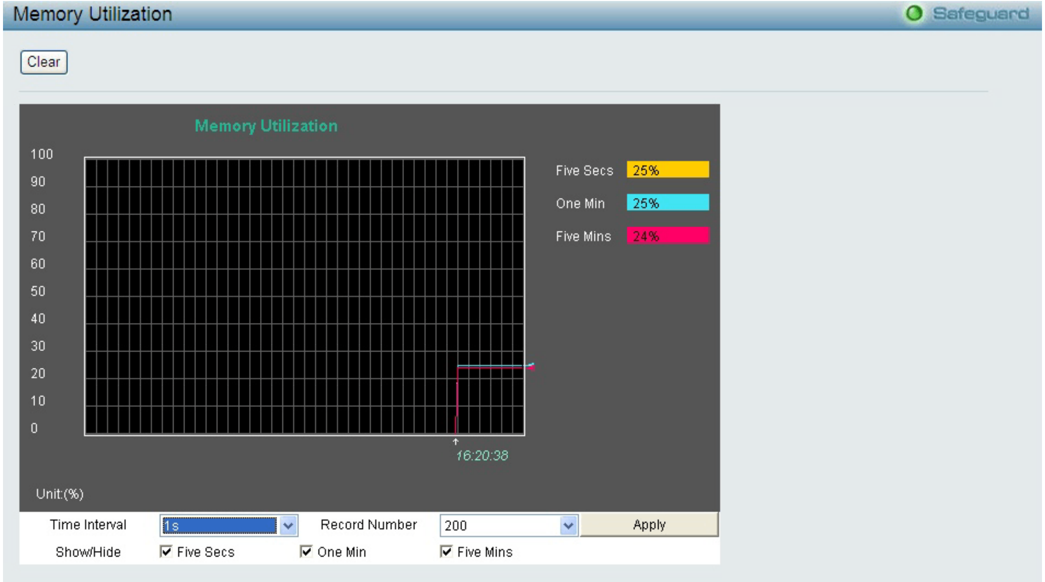
Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

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.



Memory Utilization

Clear

Time Interval: 1s

Record Number: 200

Apply

Show/Hide: ☑ Five Secs ☑ One Min ☑ Five Mins

Figure 5.106 – 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.

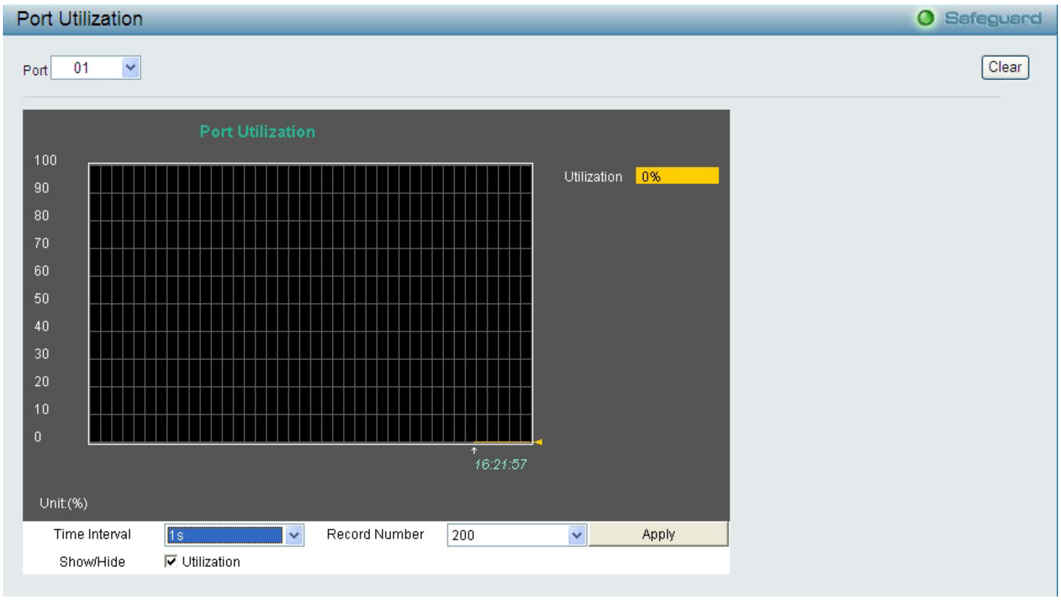
Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

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

Clear

Time Interval: 1s

Record Number: 200

Apply

Show/Hide: ☑ Utilization

Figure 5.107 – 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.

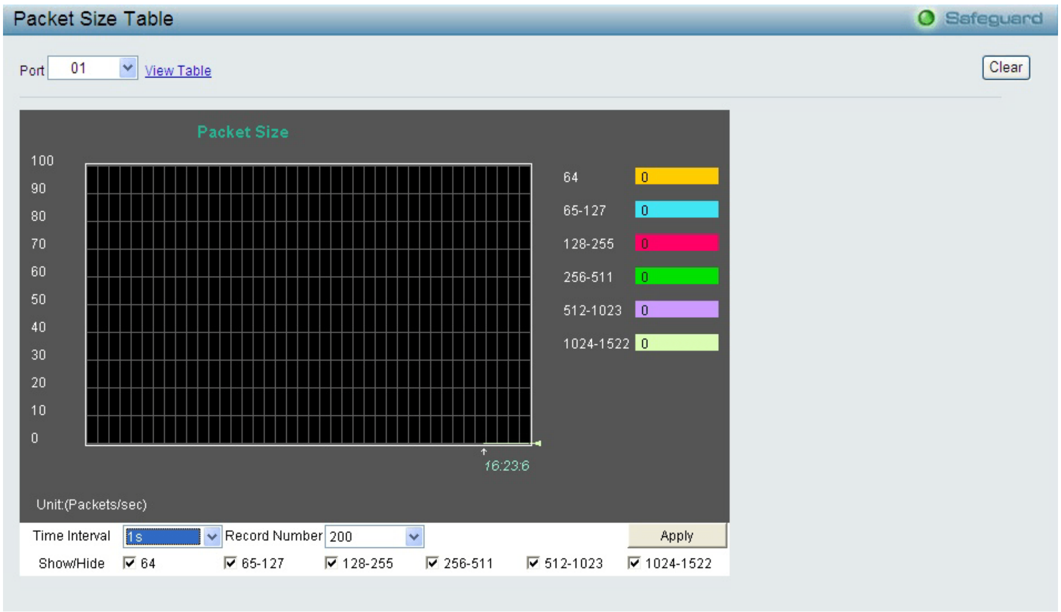
Record Number: Select number of times the Switch will be polled between *20* and *200*. The default value is *200*.

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.



Packet Size Table

Port 01 View Table

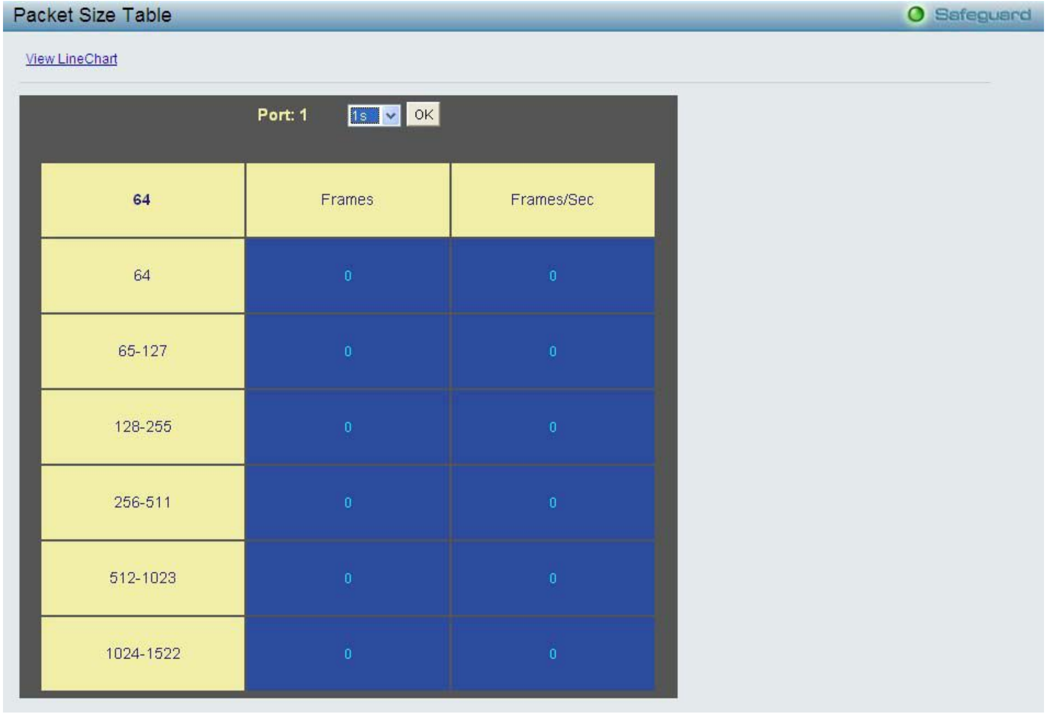
Time Interval 1s Record Number 200

Show/Hide ☑ 64 ☑ 65-127 ☑ 128-255 ☑ 256-511 ☑ 512-1023 ☑ 1024-1522

64	0
65-127	0
128-255	0
256-511	0
512-1023	0
1024-1522	0

Figure 5.108 – Monitoring > Packet Size

To view the **Packet Size Analysis Table**, click the link View Table, which will show the following table:



Packet Size Table

View LineChart

Port: 1 1s OK

64	Frames	Frames/Sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1522	0	0

Figure 5.109 – 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).

1024-1522: 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 *1024-1522* packets received.

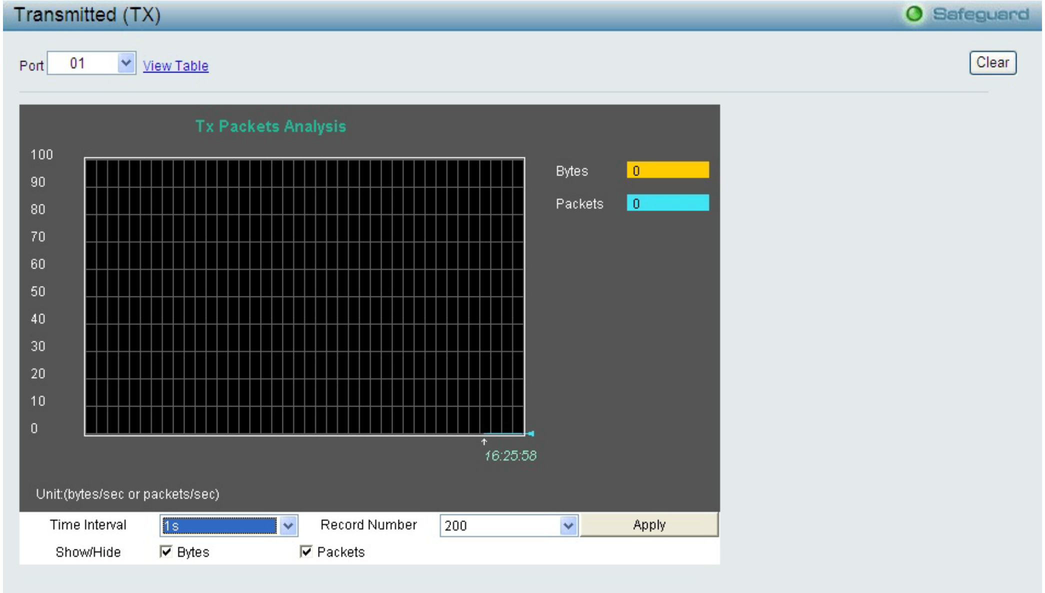
Clear: Clicking this button clears all statistics counters on this window.

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

Bytes 0

Packets 0

Unit:(bytes/sec or packets/sec)

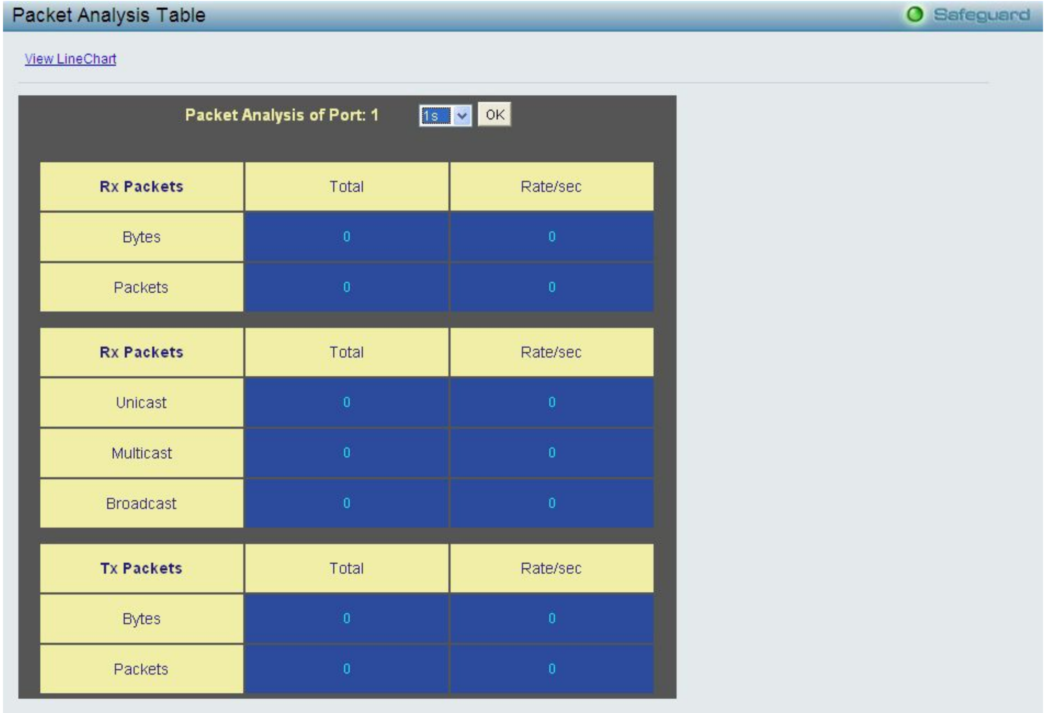
Time Interval 1s

Record Number 200

Show/Hide ☑ Bytes ☑ Packets

Figure 5.110 - 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:



Rx Packets	Total	Rate/sec
Bytes	0	0
Packets	0	0

Rx Packets	Total	Rate/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

Tx Packets	Total	Rate/sec
Bytes	0	0
Packets	0	0

Figure 5.111 - 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.

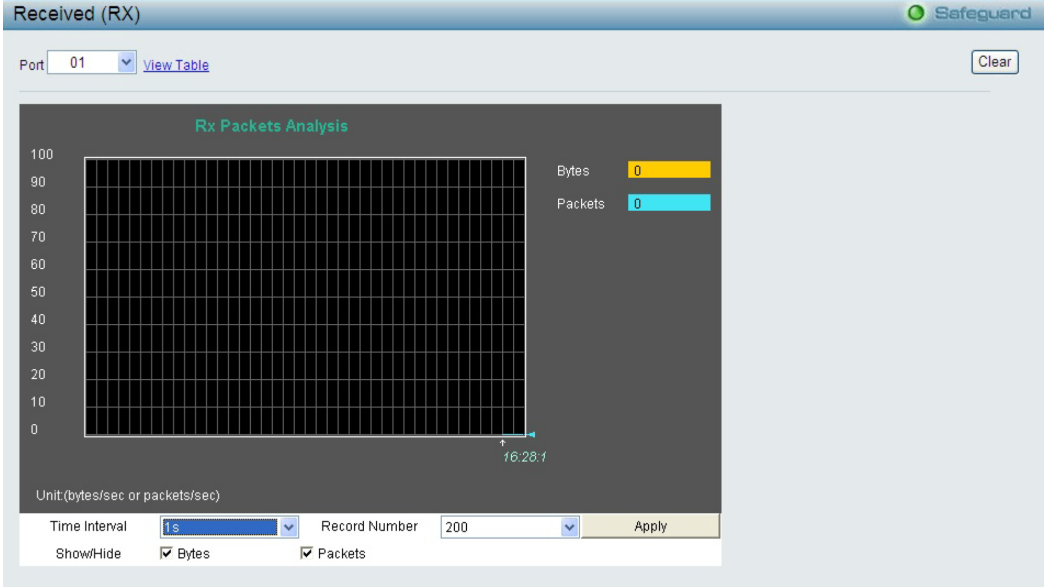
Clear: Clicking this button clears all statistics counters on this window.

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 01 View Table

Clear

Time Interval 1s

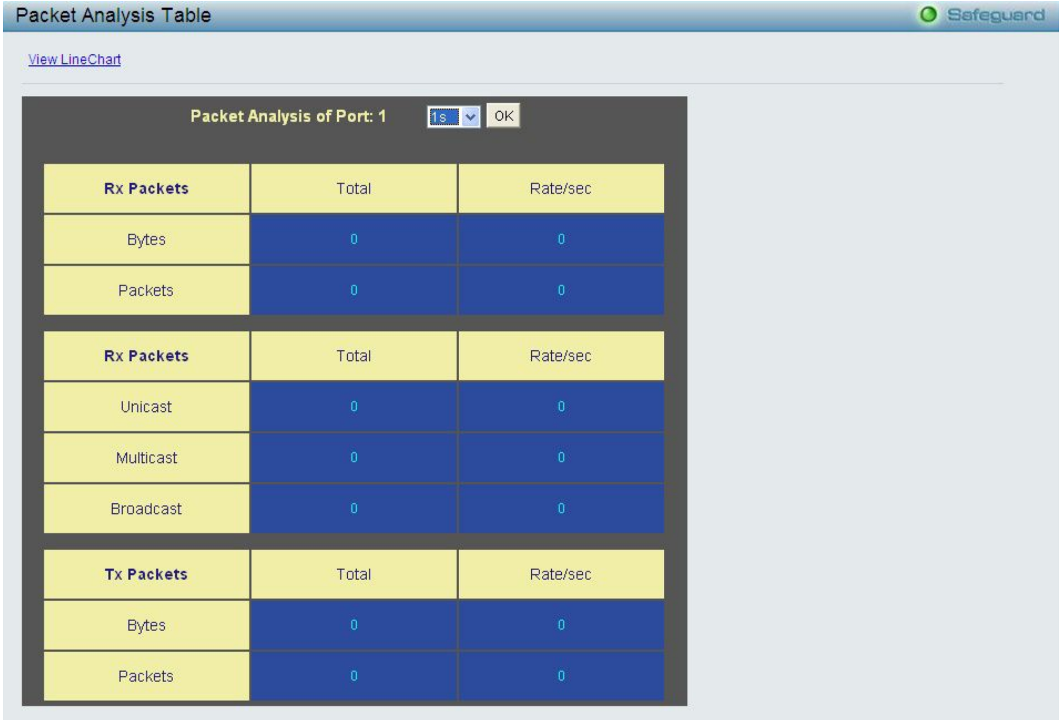
Record Number 200

Apply

Show/Hide ☑ Bytes ☑ Packets

Figure 5.112 - 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

Packet Analysis of Port: 1 1s OK

Rx Packets	Total	Rate/sec
Bytes	0	0
Packets	0	0

Rx Packets	Total	Rate/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

Tx Packets	Total	Rate/sec
Bytes	0	0
Packets	0	0

Figure 5.113 - 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.

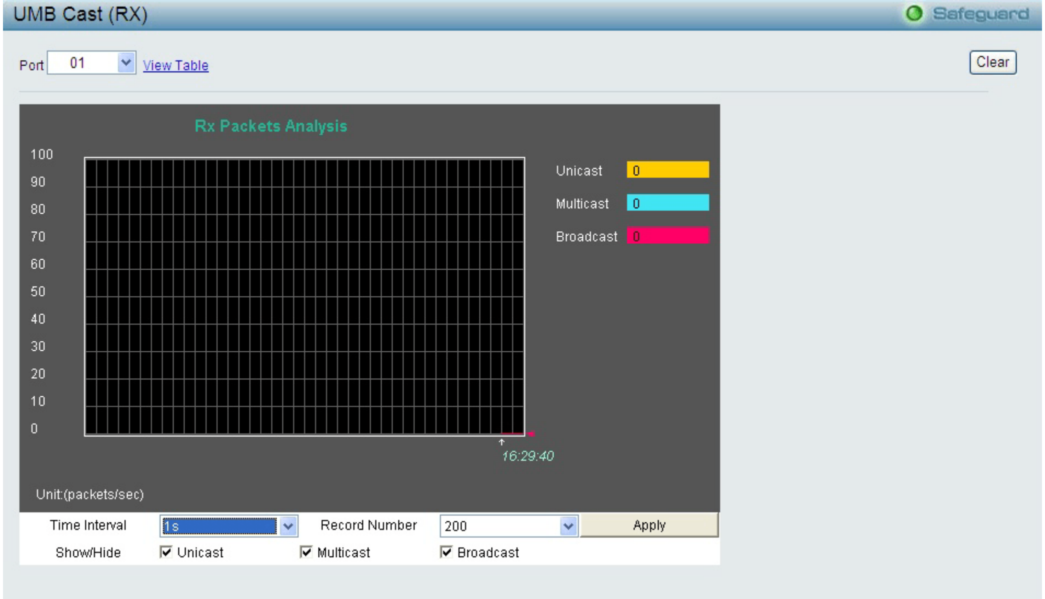
Clear: Clicking this button clears all statistics counters on this window.

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.



Port 01

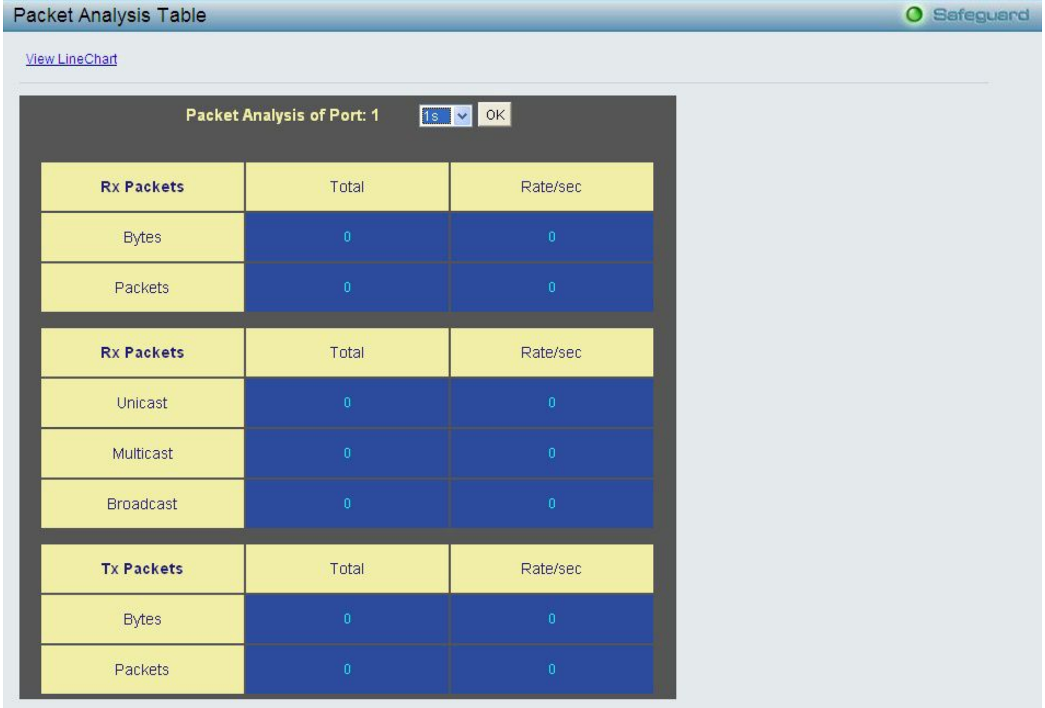
Unicast 0
Multicast 0
Broadcast 0

Time Interval 1s
Record Number 200

Show/Hide ☑ Unicast ☑ Multicast ☑ Broadcast

Figure 5.114 - 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 of Port: 1 1s

Rx Packets	Total	Rate/sec
Bytes	0	0
Packets	0	0
Rx Packets	Total	Rate/sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0
Tx Packets	Total	Rate/sec
Bytes	0	0
Packets	0	0

Figure 5.115 - 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.

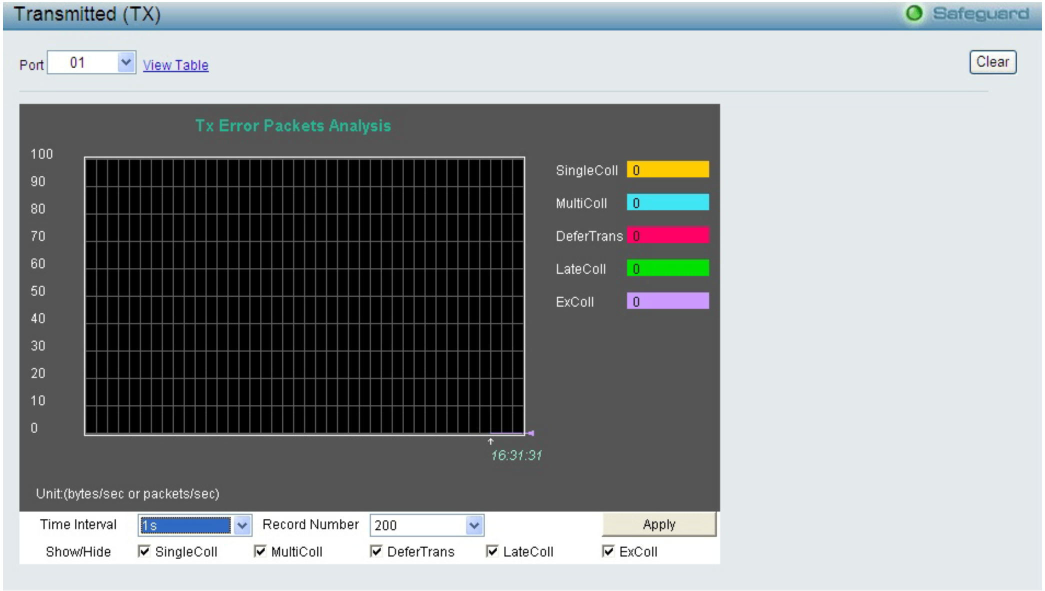
Clear: Clicking this button clears all statistics counters on this window.

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 > 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.



Transmitted (TX)

Port 01 View Table Clear

Tx Error Packets Analysis

SingleColl 0

MultiColl 0

DeferTrans 0

LateColl 0

ExColl 0

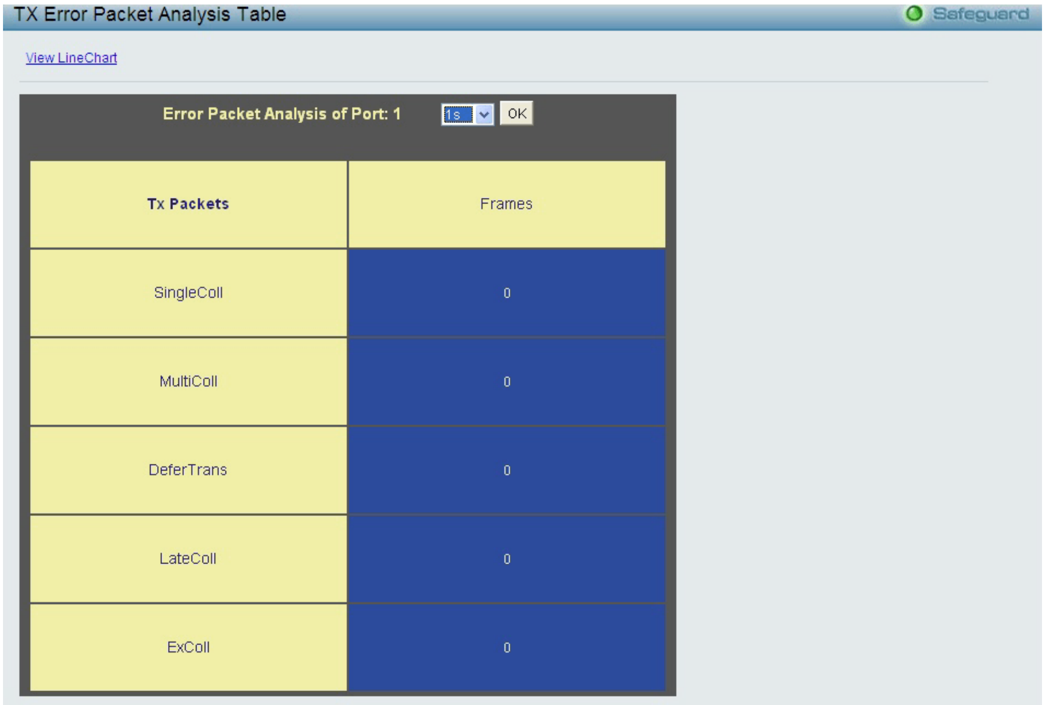
Unit:(bytes/sec or packets/sec)

Time Interval 1s Record Number 200 Apply

Show/Hide ☑ SingleColl ☑ MultiColl ☑ DeferTrans ☑ LateColl ☑ ExColl

Figure 5.116 - Monitoring > Errors > Transmitted (TX) (line graph)

To view the **Transmitted Error Packets Table**, click the link View Table, which will show the following table:



TX Error Packet Analysis Table

Error Packet Analysis of Port: 1 1s OK

Tx Packets	Frames
SingleColl	0
MultiColl	0
DeferTrans	0
LateColl	0
ExColl	0

Figure 5.117 - 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*.

SingColl: Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.

MultiColl: Multi Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by multi collision.

DeferTrans: The number of frames for which the first transmission attempt was delayed because the medium was busy.

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.

Show/Hide: Check whether or not to display SingColl, MultiColl, DeferTrans, LateColl and ExColl errors.

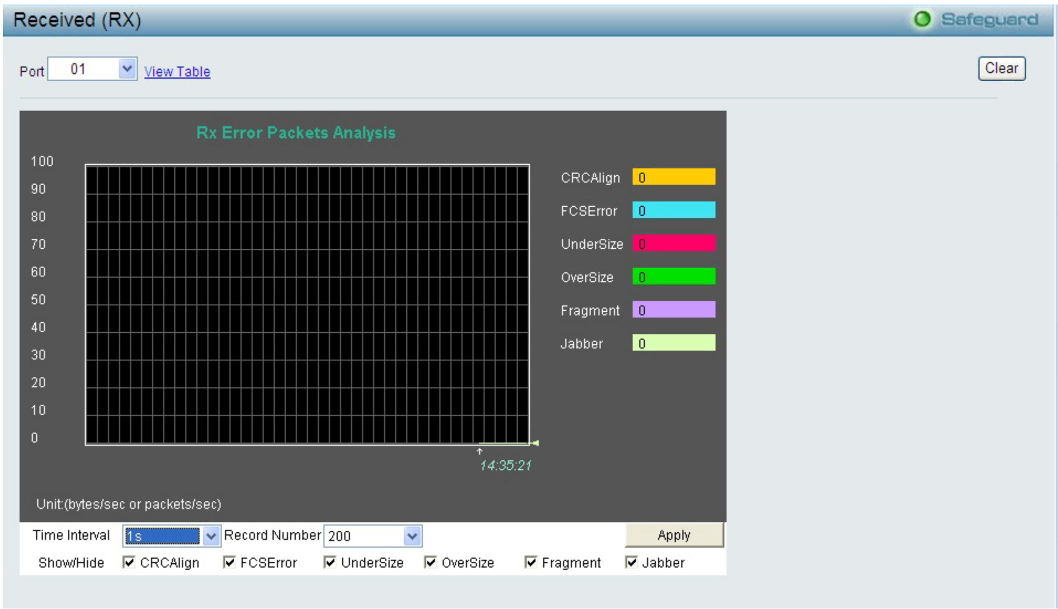
Clear: Clicking this button clears all statistics counters on this window.

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 > 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 01 View Table Clear

Rx Error Packets Analysis

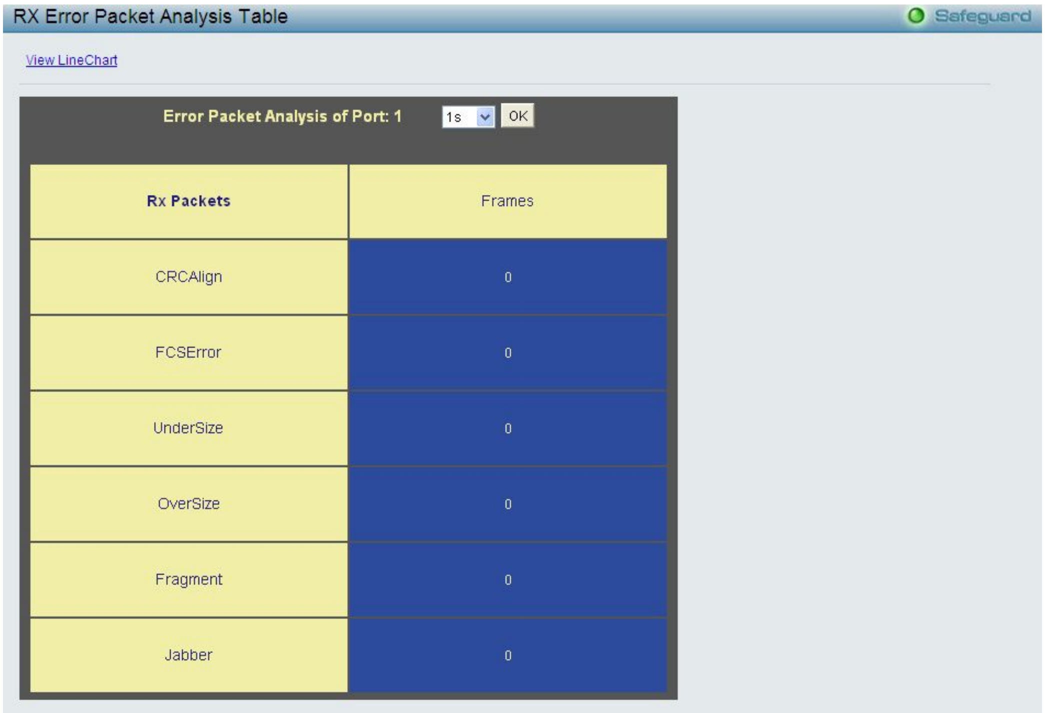
CRCAlign 0
FCSError 0
UnderSize 0
OverSize 0
Fragment 0
Jabber 0

Time Interval 1s Record Number 200 Apply

Show/Hide ☑ CRCAlign ☑ FCSError ☑ UnderSize ☑ OverSize ☑ Fragment ☑ Jabber

Figure 5.118 - 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

View LineChart

Error Packet Analysis of Port: 1 1s OK

Rx Packets	Frames
CRCAlign	0
FCSError	0
UnderSize	0
OverSize	0
Fragment	0
Jabber	0

Figure 5.119 - 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 Align: 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*.

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.

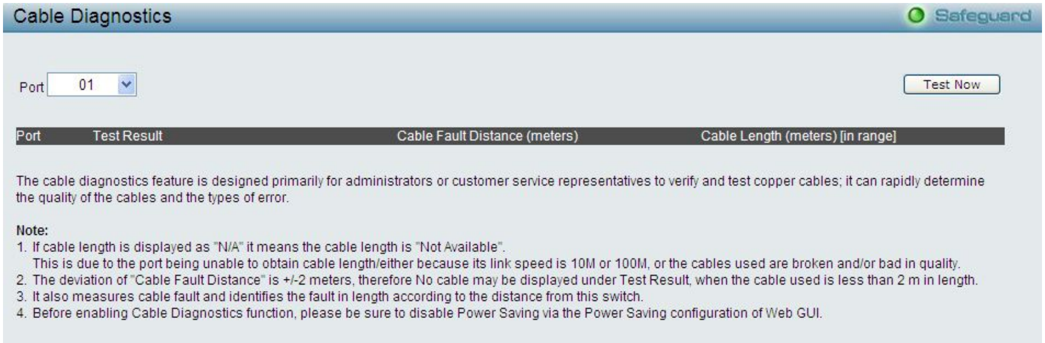
View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > 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/either because its link speed is 10M or 100M, or the cables used are broken and/or bad in quality.
2. The deviation of "Cable Fault Distance" is +/-2 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 2 m in length.
3. It also measures cable fault and identifies the fault in length according to the distance from this switch.
4. Before enabling Cable Diagnostics function, please be sure to disable Power Saving via the Power Saving configuration of Web GUI.

Figure 5.120 - 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.

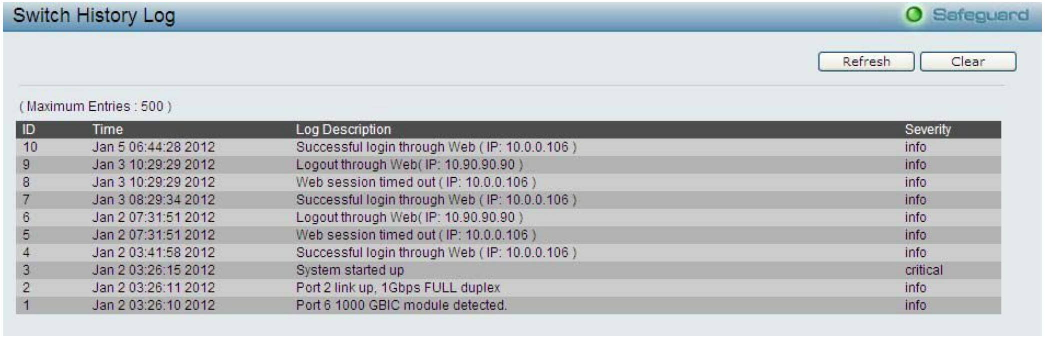
NOTE: Cable length detection is effective on Gigabit ports only.

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
10	Jan 5 06:44:28 2012	Successful login through Web (IP: 10.0.0.106)	info
9	Jan 3 10:29:29 2012	Logout through Web(IP: 10.90.90.90)	info
8	Jan 3 10:29:29 2012	Web session timed out (IP: 10.0.0.106)	info
7	Jan 3 08:29:34 2012	Successful login through Web (IP: 10.0.0.106)	info
6	Jan 2 07:31:51 2012	Logout through Web(IP: 10.90.90.90)	info
5	Jan 2 07:31:51 2012	Web session timed out (IP: 10.0.0.106)	info
4	Jan 2 03:41:58 2012	Successful login through Web (IP: 10.0.0.106)	info
3	Jan 2 03:26:15 2012	System started up	critical
2	Jan 2 03:26:11 2012	Port 2 link up, 1Gbps FULL duplex	info
1	Jan 2 03:26:10 2012	Port 6 1000 GBIC module detected.	info

Figure 5.121 - 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.

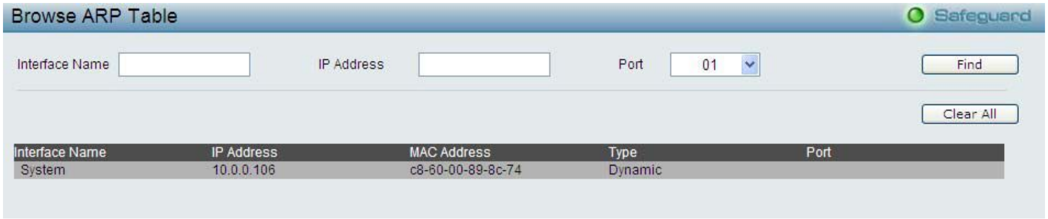
Log Description: Displays the description of event recorded.

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	IP Address	MAC Address	Type	Port
System	10.0.0.106	c8-60-00-89-8c-74	Dynamic	

Figure 5.122 - 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.

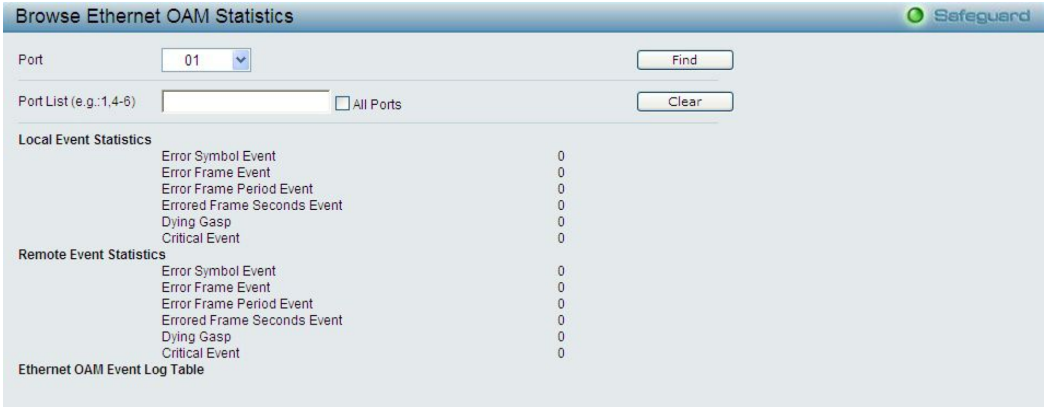
Static – Indicates the MAC address is a static IP address.

Port: Defines the ARP mapping ports.

Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

This window allows the user to view the Ethernet OAM event log information. The Switch can buffer up to 1000 event logs. The event log will provide and record detailed information about each OAM event. Specify the port number and port list you wish to view and click **Find**. To remove an entry, enter the appropriate information and click **Clear**.

To view this window, click **Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log** as shown below:



Port 01

Port List (e.g.:1,4-6) □ All Ports

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

Figure 5.123 - Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

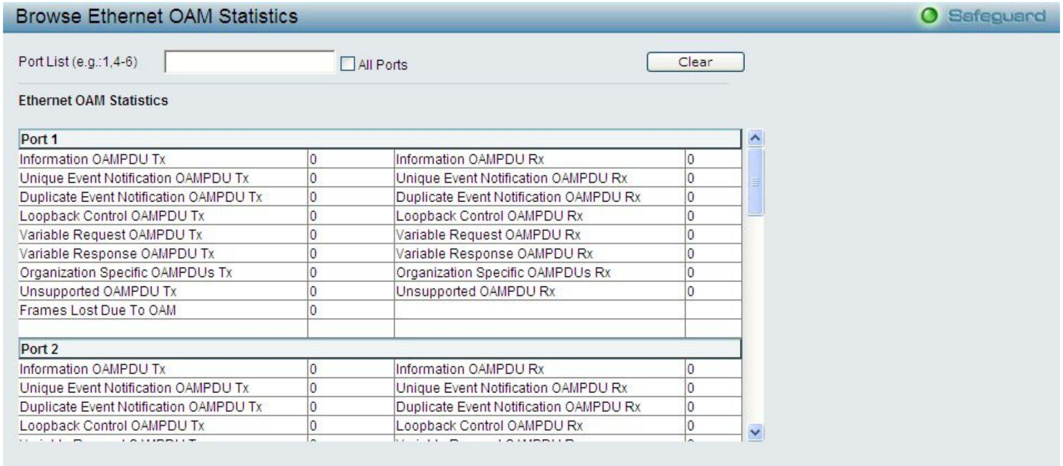
Select **Port** and click **Find** to display the Ethernet OAM event log information.

Fill in **Port** or check **All Ports** then click **Clear** to remove Ethernet OAM event log information.

Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

This window displays the Ethernet OAM Statistic information on each port of the Switch. To clear information for a particular port or list of ports enter the ports and click **Clear**.

To view this window, click **Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics** as shown below:



Port List (e.g.:1,4-6) □ All Ports

Ethernet OAM Statistics

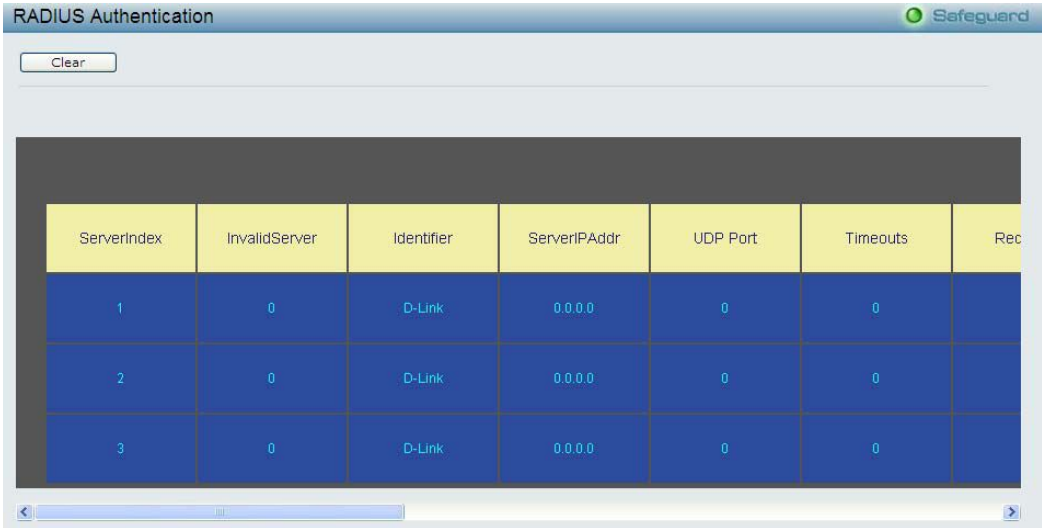
Port 1			
Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	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

Figure 5.124 - Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

Fill in **Port** or check **All Ports** then click **Clear** to remove Ethernet OAM Statistics.

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.



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 5.125 - 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.

InvalidServer: The number of invalid server.

ServerIPAddr: The server IP address.

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.

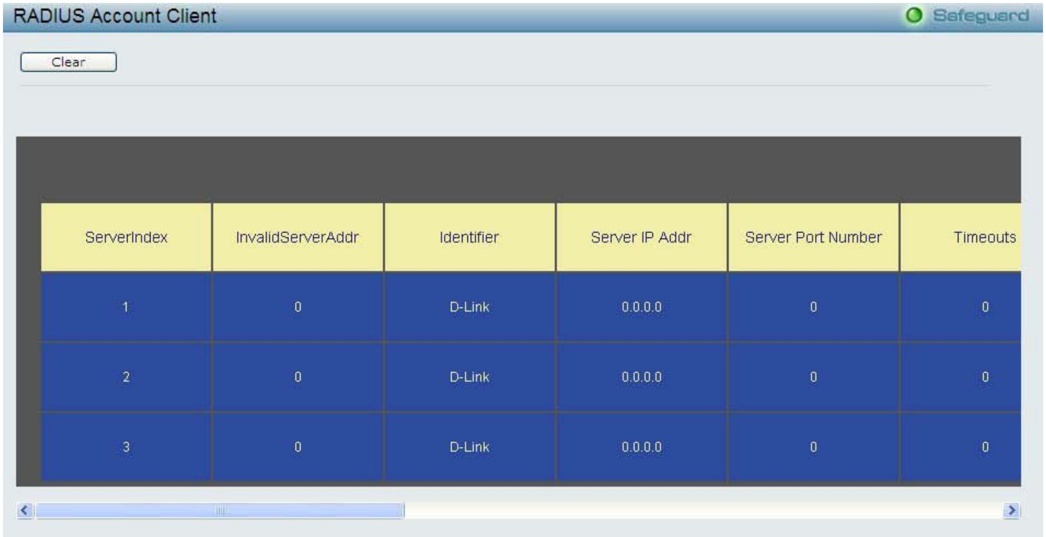
BadAuthenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.

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.



RADIUS Account Client

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 5.126 - 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.

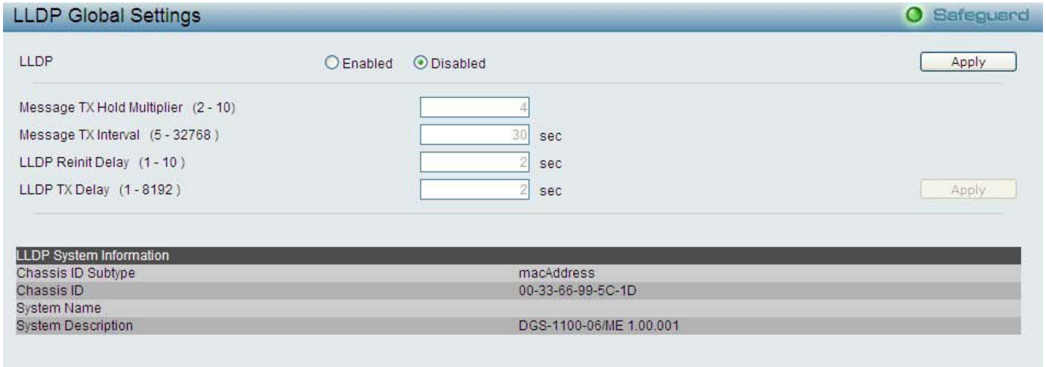
BadAuthenticators: The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.

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.

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

Safeguard

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	00-33-66-99-5C-1D
System Name	
System Description	DGS-1100-06/ME 1.00.001

Figure 5.127 – 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**.

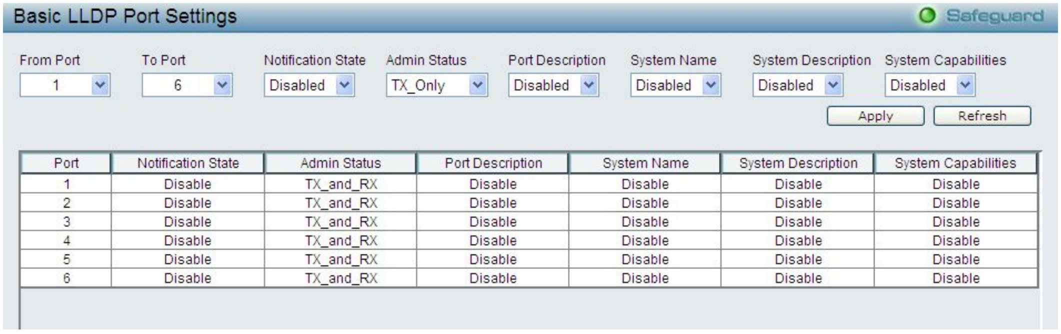
Message TX Interval (5-32768): This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is **30** seconds.

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

Safeguard

From Port	To Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	6	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

Figure 5.128– 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:

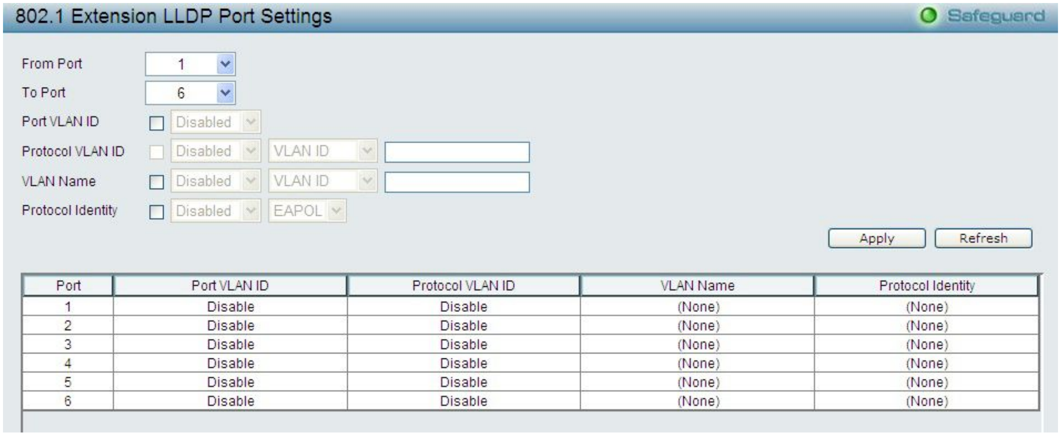
Enabled – Enables the System Capabilities TLV on the port.

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.



From Port 1

To Port 6

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	VLAN Name	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)

Figure 5.129 – 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.

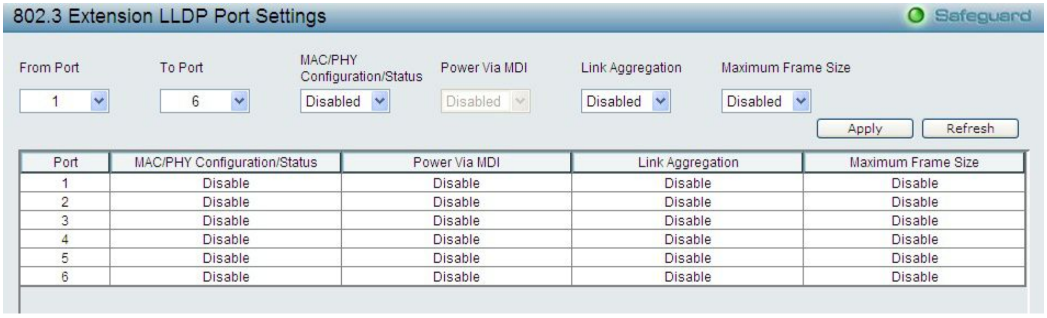
VLAN Name : Specifies the VLAN name to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN Name.

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	6	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

Figure 5.130 – 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:

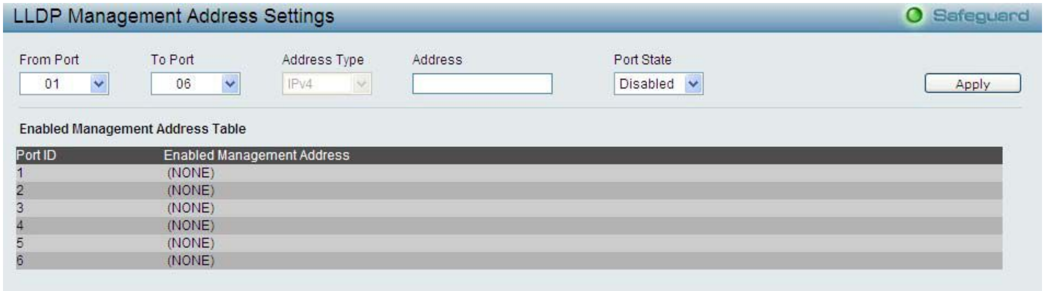
Enabled – Enables the Maximum Frame Size configured on the port.

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	06	IPv4		Disabled

Enabled Management Address Table

Port ID	Enabled Management Address
1	(NONE)
2	(NONE)
3	(NONE)
4	(NONE)
5	(NONE)
6	(NONE)

Figure 5.131 – 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:

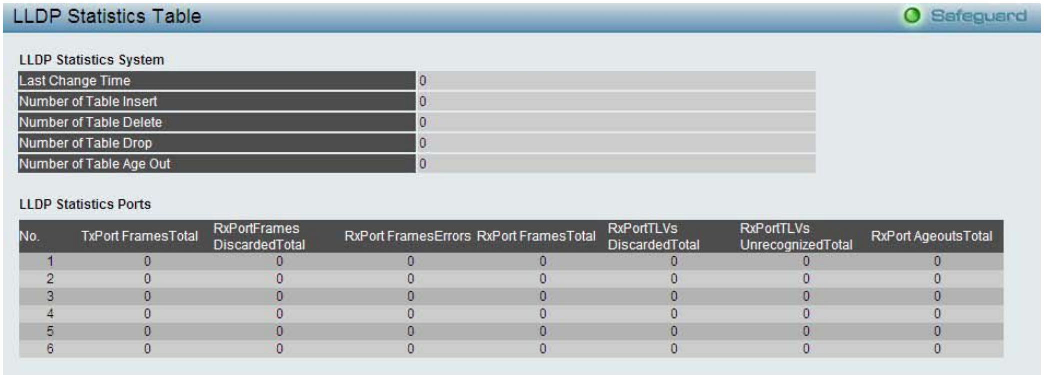
Enabled – Enables the port state configured on the port.

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

Figure 5.132 – 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.

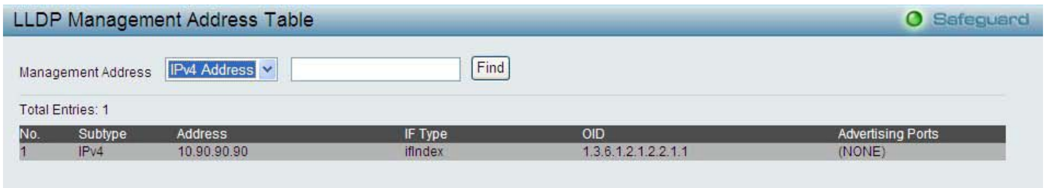
RxPortTLVsDiscarded – Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

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)

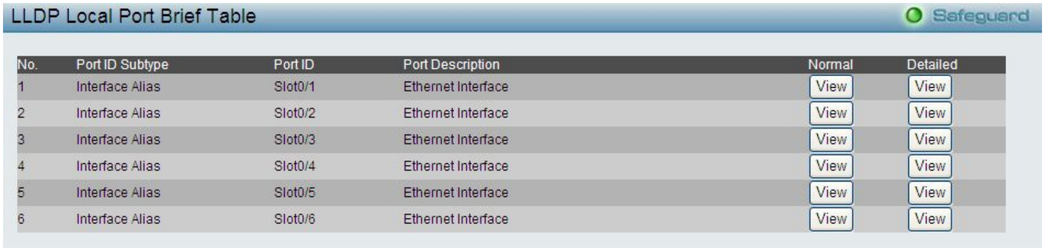
Figure 5.133 – LLDP > LLDP Management Address Table

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.



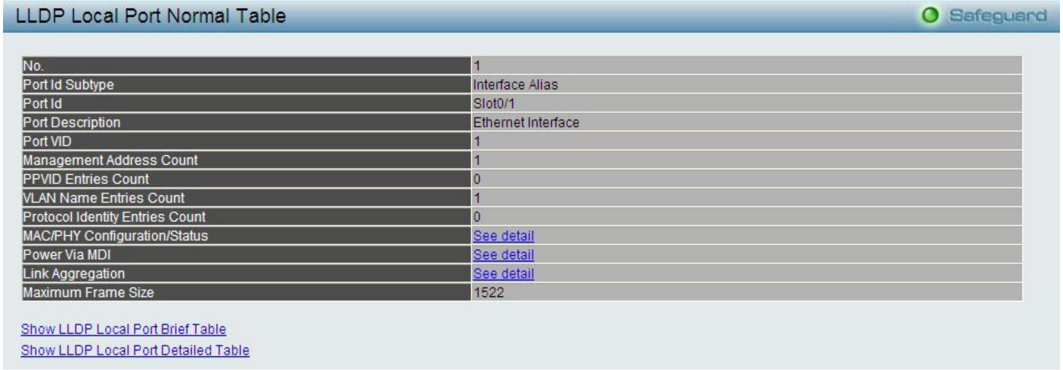
LLDP Local Port Brief Table

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

Figure 5.134 –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.



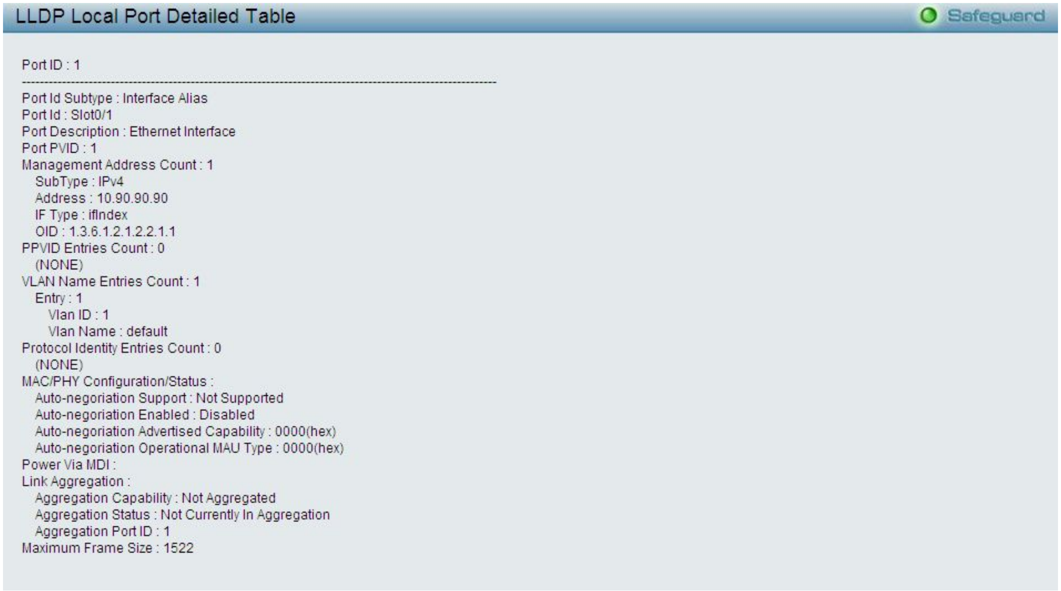
LLDP Local Port Normal Table

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 5.135 – LLDP > LLDP Local Port Normal Table

Click **View** of Detailed column to display detail information.

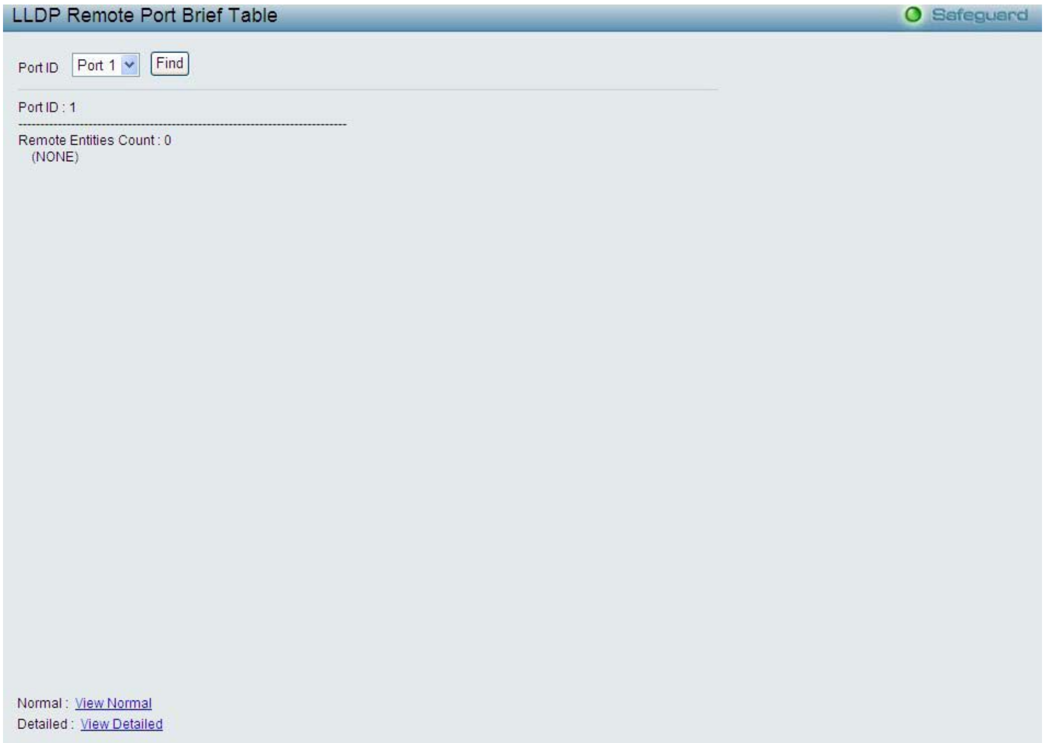


```
Port ID : 1
------------------------------------------------------------------------------------------------
Port Id Subtype : Interface Alias
Port Id : Slot0/1
Port Description : Ethernet Interface
Port PVID : 1
Management Address Count : 1
   SubType : IPv4
   Address : 10.90.90.90
   IF Type : 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 5.136 – 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.

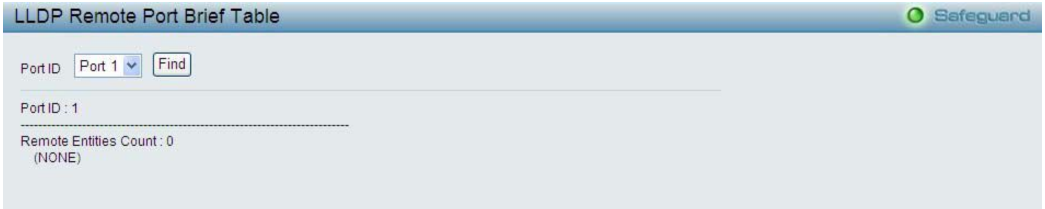


```
Port ID : 1
------------------------------------------------------------------
Remote Entities Count : 0
   (NONE)
```

Normal : View Normal
Detailed : View Detailed

Figure 5.137 – LLDP > LLDP Remote Port Table

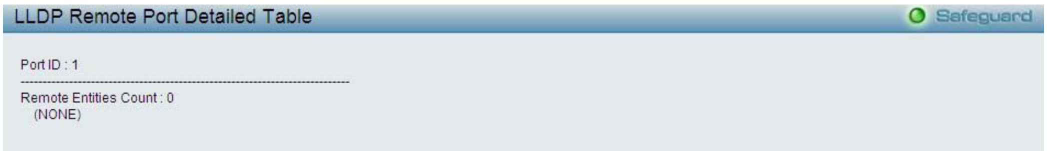
To view the settings for a remote port, click **View Normal** and the following page displays.



```
Port ID : 1
------------------------------------------------------------------
Remote Entities Count : 0
   (NONE)
```

Figure 5.138 – 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)
```

Figure 5.139 – LLDP > LLDP Remote Port Detailed Table

Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link DGS-1100-06/ME 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 - Technical Specifications

Hardware Specifications

Key Components / Performance

- Switching Capacity: 12Gbps
- Max. Forwarding Rate: 8.9Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory: 128KB
- DDRII for CPU: 128M Bytes
- Flash Memory: 16M Bytes

Port Functions

- 5 10/100/1000Base-TX ports compliant with the following standards:

  - IEEE 802.3

  - IEEE 802.3u

  - IEEE 802.3ab

  - Supports Half/Full-Duplex operations

  - IEEE 802.3x Flow Control support for Full-Duplex mode

  - Auto MDI/MDIX

  - Auto-negotiation
- 1 SFP port 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)

  - DEM-302s-LX (1000BASE-LX, 2km)

  - DGS-712 (1000Base-T)
- 1 SFP port 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)

  - DEM-302S-BXD (1000BASE-BX, TX-1550/RX-1310nm, 2km)

  - DEM-302X-BXU (1000BASE-BXU, TX-1310/RX-1550nm, 2km)

Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply

  Acoustic Value: 0dB (Fan-less)
- Operation Temperature -5~50°C
- Storage Temperature -40~70°C
- Operation Humidity: 10%~90% RH
- Storage Humidity: 5%~90% RH

Emission (EMI) Certifications

- CE Class A

Safety Certifications

- cUL, LVD

Features

L2 Features

- Supports up to 4K MAC address
- Supports 256 static MAC
- IGMP snooping:

  - Supports 32 IGMP Snooping groups

  - Supports at least 32 static multicast groups
- Limited IP Multicast:
  - Support up to 24 profiles and each profile can add up to 32 multicast groups
  - Able to configure the maximum multicast group number for a port, ranging from 1-32
- MLD Snooping:
  - Supports 32 MLD snooping groups
  - Supports 32 static multicast addresses
- Loopback Detection
- Port mirroring
- SNTP
- LLDP

VLAN

- 802.1Q VLAN
- Total 32 static VLAN groups
- Management VLAN
- ISM VLAN
- Supports Port-based Q-in-Q

QoS (Quality of Service)

- Be able to classify packets according to follow contents:

  - Switch port

  - 802.1p priority

  - DSCP

  - IPv6 Traffic Class
- Supports Strict / WRR mode in queue handling

- Support Port based bandwidth control

AAA

- 802.1X Local/RADIUS server
- 802.1X port-based/MAC-based access control
- RADIUS Accounting
- 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)

Security

- Static MAC : Support 128 Static MAC entries
- Port Security:Support 64 MACs per port
- Traffic Segmentation
- D-Link Safeguard Engine
- Broadcast Storm Control

OAM

- Cable Diagnostics
- 802.3ah:
  - 802.3ah D-Link extension: D-Link Unidirectional Link Detection (DULD)

Management

- Web-based GUI or SmartConsole Utility
- D-Link proprietary CLI
- Telnet Server: Support up to 4 telnet session simultaneously
- SNMP v1/v2c/v3
- Bootp/DHCP Client
- DHCP Relay: Support DHCP local relay, option 82.
- DHCPv6 Relay: Support DHCP local relay and option 37
- SNMP Trap
- RMON v1: Support 4 groups 1, 2, 3, 9
- Password access control
- Web-based configuration backup / restoration
- Reset, Reboot
- IPv6 Neighbor Discovery:
  - Supports Max 512 ND entries
  - Support up to 64 static ND entries

D-Link Green Technology

- Power Saving: save energy in 4 ways:

  - Power Saving by Time Profile: Ports or the system can be turned on/off by giving schedule.

  - Power Saving by LED Shut-Off: Posered LEDs can be turned on/off by port or system through schedule.

  - Power Saving by Port Shut-Off: Each port on the system can be turned on/off by schedule.

  - Power Saving by System Hibernation: System enters hibernation by schedule. In this mode, switches get most power-saving fingures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

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).

D-Link®

Building Networks for People