

4 Configuration

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

Web-based Management

After you log in, you will see the screen below:

The screenshot shows the D-Link Web-based Management interface. At the top is the **Tool Bar** with the D-Link logo, device status indicators (1000 Link, 10/100 Link, ST, 100 Link, SF, 1000 Link, SF, 10G), and a Refresh Interval dropdown set to 'Never'. Below the Tool Bar is a navigation bar with 'Save', 'Tools', and 'Online Help' options. On the left is the **Function Tree** with a red box around it, listing 'DGS-1100-10/ME' and sub-items: System, Configuration, QoS, RMON, Security, Monitoring, and LLDP. The main area is the **Main Configuration Screen**, also with a red box around it, containing 'Device Information' and 'Device Status and Quick Configurations'.

Device Information			
Device Type	DGS-1100-10/ME V1.00.002	System Time	00:03:11 01 01 2013
System Name		System Up Time	0 days, 0 hours, 3 mins, 7 seconds
System Location		MAC Address	DE-AD-BE-EF-01-02
System Contact		IP Address	10.90.90.90
Boot Version	0.09.03	Subnet Mask	255.0.0.0
Firmware Version	V1.00.002	Hardware Version	A1
Default Gateway	0.0.0.0	Serial Number	1MB1733K0000A
Login Timeout (minutes)	5		

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

Figure 4.1 – Web-based Management

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

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

Click on the D-Link logo at the upper left corner of the screen to be redirected to the local D-Link website.

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

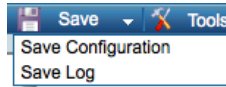


Figure 4.2 – Save Menu

Save Configuration

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



Figure 4.3 – Save Configuration

Save Log

Click **Backup Log** to save the log entries to your local drive. A pop-up message will prompt you for the file path. You can view or edit the log file by using a text editor (e.g., Notepad).



Figure 4.4 – Save Log

Tool Bar > Tool Menu

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



Figure 4.5 – Tool Menu

Reset System

Provides three different reset options for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot.

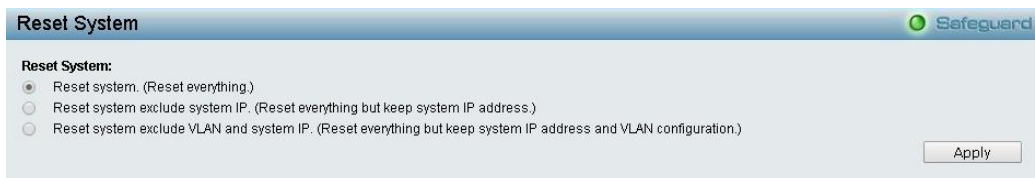


Figure 4.6 – Tool Menu > Reset System

Select a reset method and then click **Apply** to reset the system.

Reboot Device

Click **Reboot** to restart the switch.



Figure 4.7 – Tool Menu > Reboot Device

Configuration Backup & Restore

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



Figure 4.8 – Tool Menu > Configure Backup and Restore

HTTP: Backup or restore the configuration file to or from your local drive.
 Click **Backup** to save the current settings to your disk.
 Click **Browse** to browse your inventory 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: The Switch will reboot after restoring the saved backup settings are applied. All current settings will be lost.

System Log Backup

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

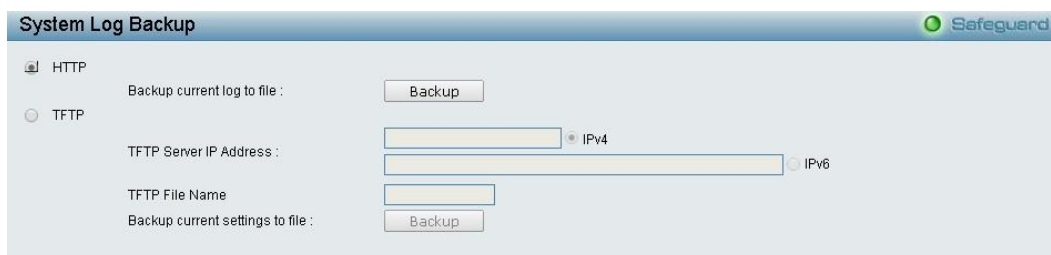


Figure 4.9 – Tool Menu > System Log Backup

HTTP: Click **Backup** to save the current log to your local drive.

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.

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

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

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**.



Figure 4.10 – 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 inventory for a saved firmware file.

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

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:



Figure 4.11 – Online Help

D-Link Support Site: This will re-direct 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.

Function Tree

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

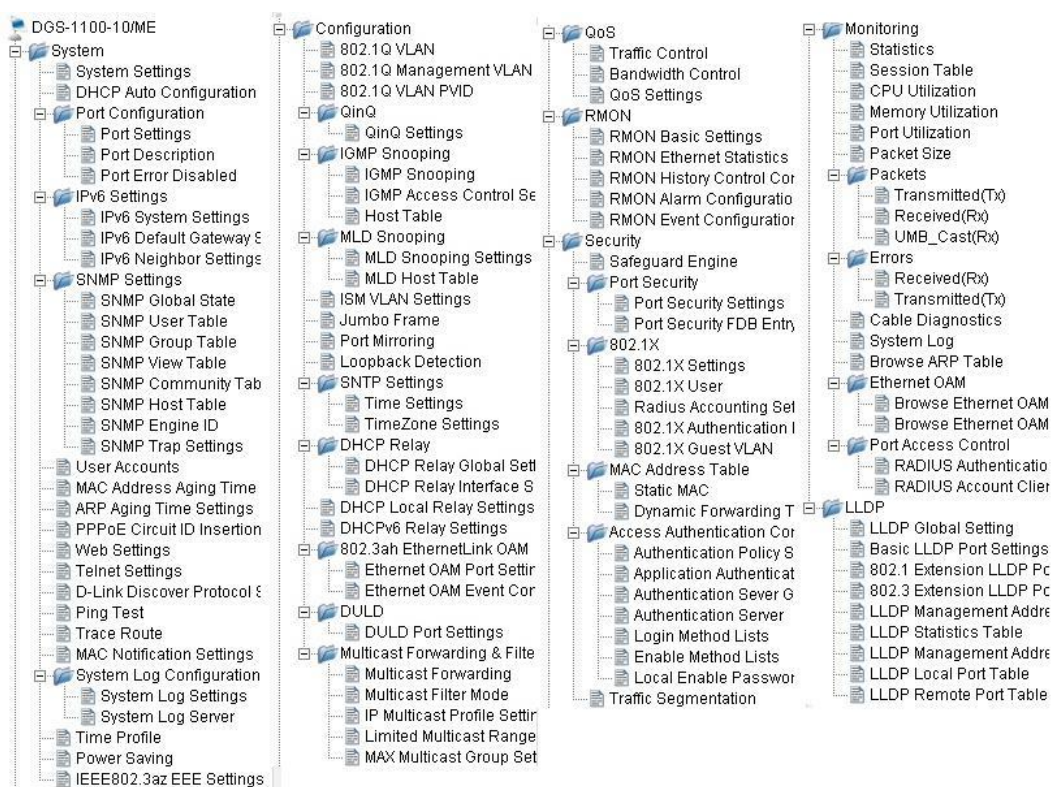


Figure 4.12 –Function Tree

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



Figure4.13 – Device Information

System > System Settings

The System Setting allows you 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 an IP address of **10.90.90.90** and subnet mask of **255.0.0.0**.

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

System Contact: By entering a system contact.

Login Timeout (3-30 minutes): 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.

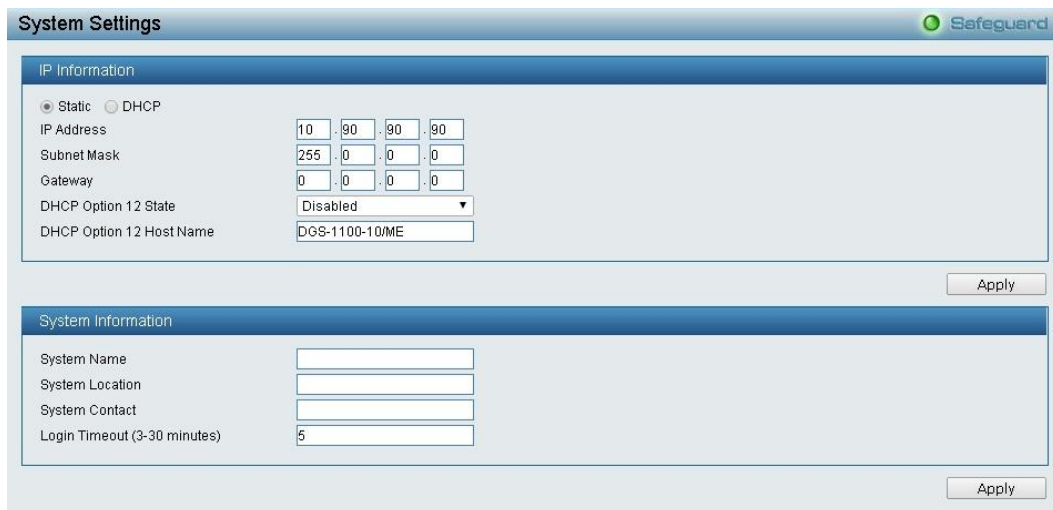


Figure 4.14 – System > System Settings

System > DHCP Auto Configuration

From this page you can 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.

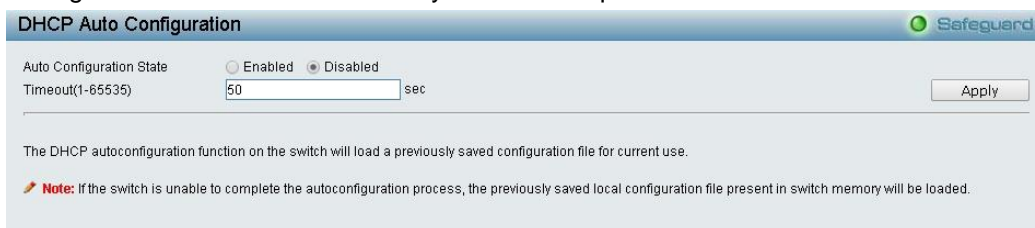


Figure 4.15 – System > DHCP Auto Configuration

Timeout (1-65535): Specify the timeout.

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.

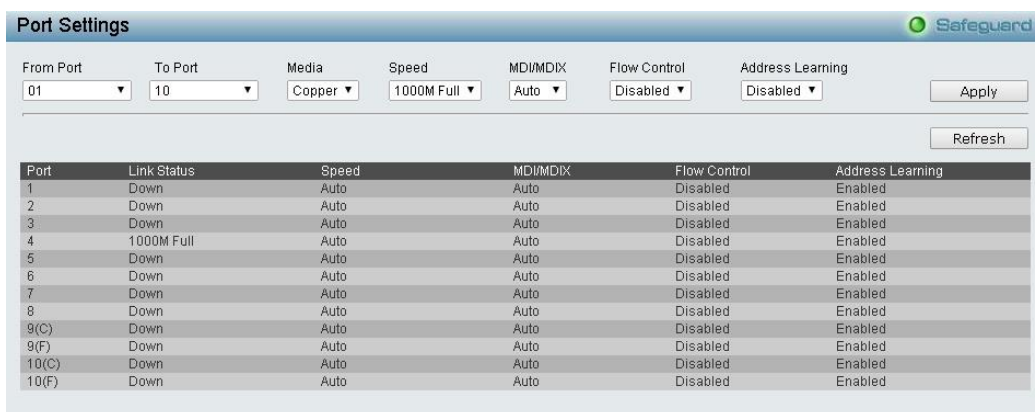


Figure 4.16 – System > Port Configuration > Port Settings

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 a 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, you 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: Enable this function to mitigate traffic congestion. Ports configured for full-duplex use 802.3x flow control and half-duplex ports use backpressure flow control. The default setting is **Disabled**.

Address Learning: Enable or disable the address learning function. The default setting is Enabled.

System > Port Configuration > Port Description

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

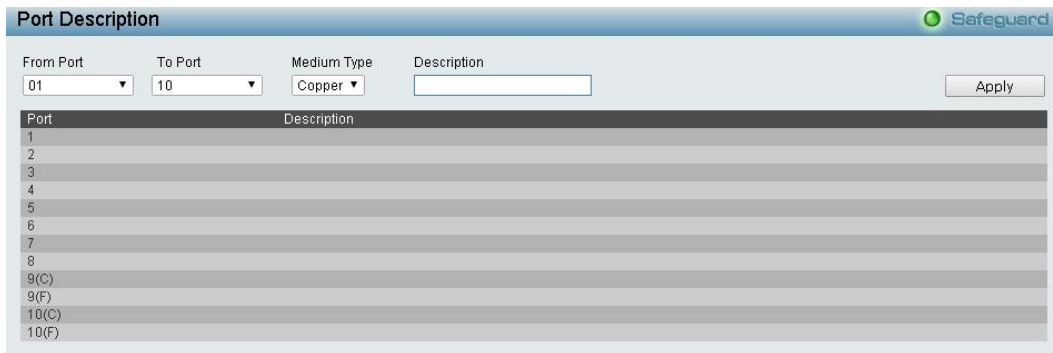


Figure 4.17 – System > Port Configuration > Port Description

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 link down status.



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.

System > IPv6 Settings > IPv6 System Settings

From this page you can configure IPv6 system information.



Figure 4.18 – System > IPv6 Settings > IPv6 System Settings

IPv6 System Settings:

Interface Name: Displays the IPv6 interface name.

IPv6 State: Select to either enable or disable IPv6.

DHCPv6 Client: Select to either enable or disable the switch as an IPv6 client.

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 seconds. The field range is 1-3600, and default is 1 second.

Automatic Link Local State Settings:

Automatic Link Local Address: Select either Enabled or Disabled.

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

System > IPv6 Settings > IPv6 Default Gateway Settings

From this page you can configure the IPv6 gateway settings.

Figure 4.19 – System > IPv6 Settings > 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 or and click the **Delete** button to remove the entry.

System > IPv6 Settings > IPv6 Neighbor Settings

You 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.

Figure 4.20 – System > IPv6 Settings > IPv6 Neighbor Settings

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

Neighbor IPv6 Address: Enter the neighbor IPv6 address.

Link Layer MAC Address: Enter 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, you 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 > 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) that 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.

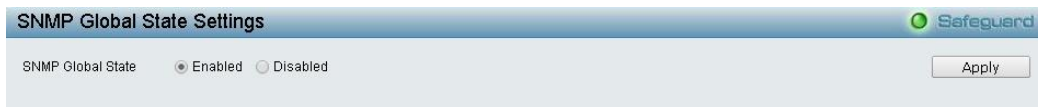


Figure 4.21 – System > SNMP Settings > SNMP Global State

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.

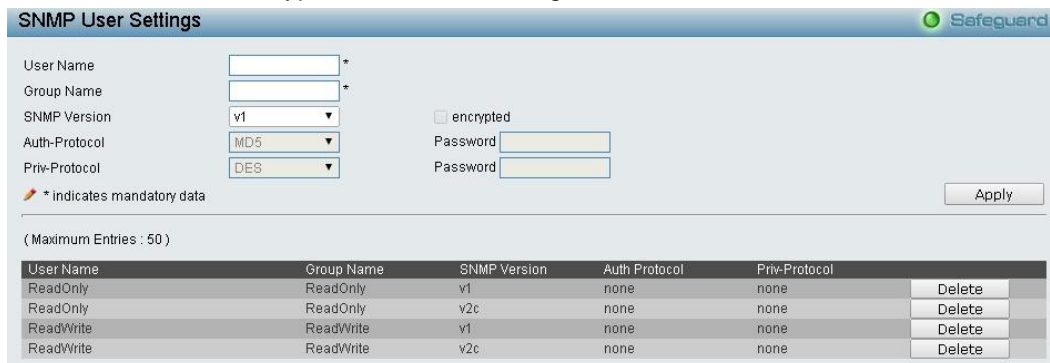


Figure 4.22 – System > SNMP Settings > SNMP User Table

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

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

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

Encrypt: If you selected SNMP v3, tick the box to enable encryption.

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: Select 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 or 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 and security policies for a user group directly.

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

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

Write View Name: Enter 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 manager.

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

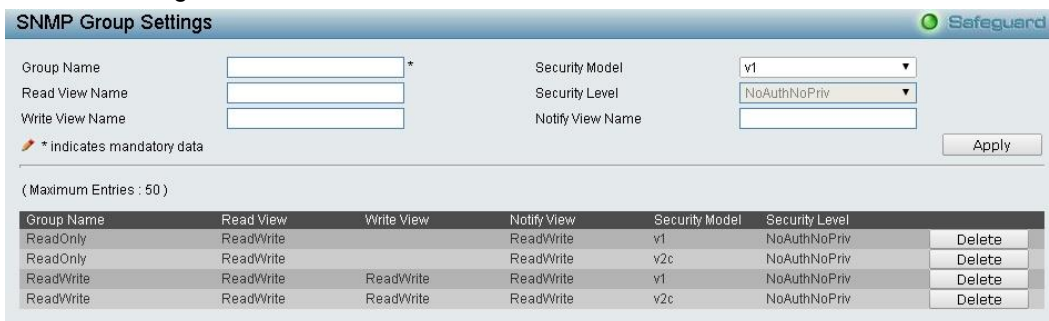


Figure 4.23– System > SNMP Settings > SNMP Group Table

System > SNMP Settings > SNMP View Table

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

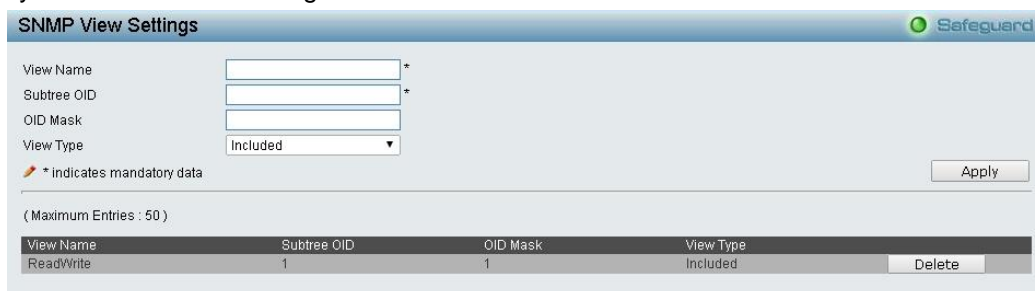


Figure 4.24 – System > SNMP Settings > SNMP View Table

View Name: Enter a view name of 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 or click **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: Enter a name of the community string.

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



Figure 4.25 – System > SNMP Settings > SNMP Community Table

Click **Apply** to create a new SNMP community or click **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.

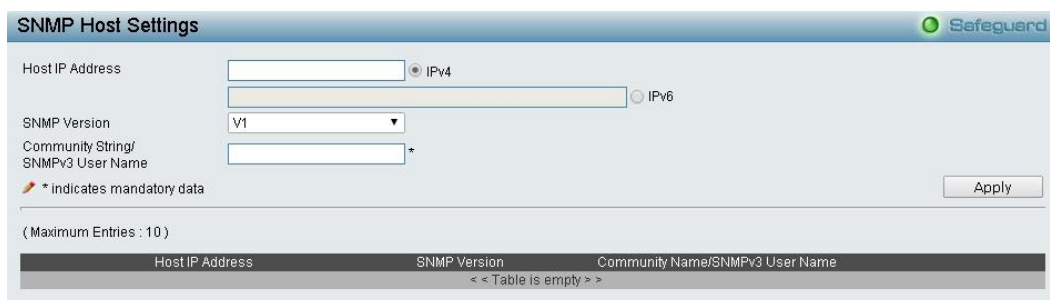


Figure 4.26 – System > SNMP Settings > SNMP Host Table

Click **Apply** to create a new SNMP host or click **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 or click **Delete** to reset back to the default value.

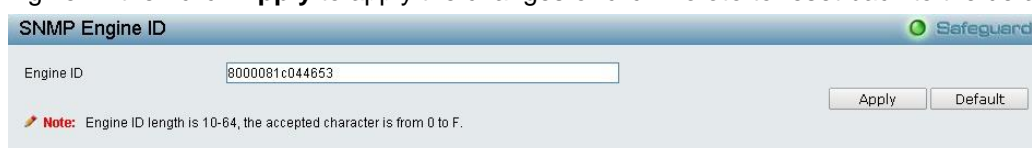


Figure 4.27 – System > SNMP Settings > SNMP Engine ID

System > SNMP Settings > SNMP Trap Settings

From this page you can specify whether the device can send SNMP notifications.

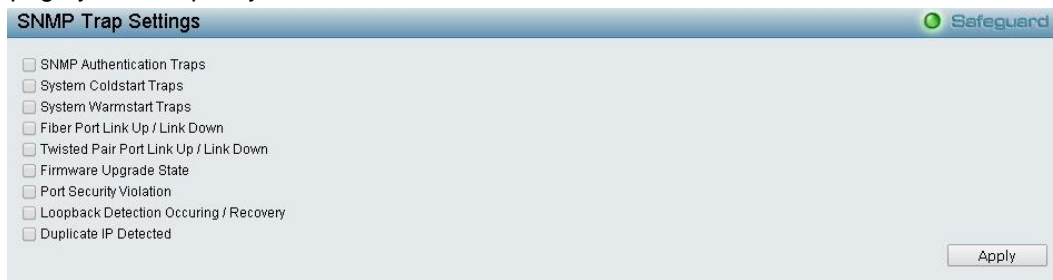


Figure 4.28 – System > SNMP Settings > SNMP Trap Settings

SNMP Authentication Traps: Tick the box to send authentication failure notifications.

System Coldstart Traps: System cold start boot-up information.

System Warmstart Traps: System warm start 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.

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

Port Security Violation: Information of Port Security Violation.

Loopback Detection occurring / recovery: Tick the box to send SNMP Trap when Loopback Detection occurring and recovery.

Duplicate IP Detected: Information of duplicate IP was detected.

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

System > User Accounts

From this page you can control user privileges. Select **Enabled** or **Disable** to configure the Password Encryption State. Add a new user by typing in a **User Name**, **Password** and choose the level of privilege (*Admin, Operator or User*) from the **Access Right** drop-down menu, then click the **Apply** button.

You can modify an 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 the **Delete** button.



Figure 4.29– 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.

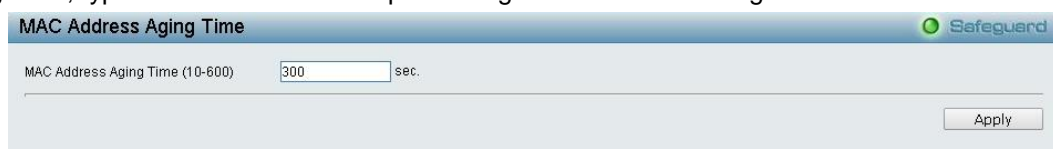


Figure 4.30 – System > MAC Address Aging Time

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.



Figure 4.31 – System > ARP Aging Time Settings

ARP Aging Time (0-65535): Enter the ARP aging time on the Switch. The range is from 0 to 65535 with a default setting of 3 minutes.

System > PPPoE Circuit ID Insertion Settings

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

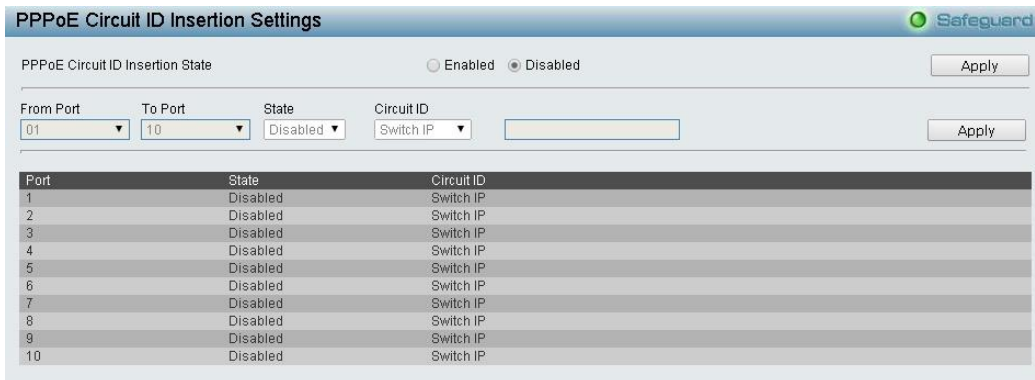


Figure 4.32 – System > PPPoE Circuit ID Insertion Settings

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

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

State: Enable or disable the state of specified ports.

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

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

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

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

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

System > Web Settings

The Web State is **Enabled** by default. If you select Disabled, you will lose the ability to configure the system through the web interface as soon as these settings are applied.



Figure 4.33– 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 you do not want to allow Telnet configuration, then select **Disabled**.



Figure 4.34 – 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 > D-Link Discover Protocol Settings

For the D-Link Discovery Protocol (DDP) supported device, this page is an option for you to disable DDP or configure the DDP packet report timer.

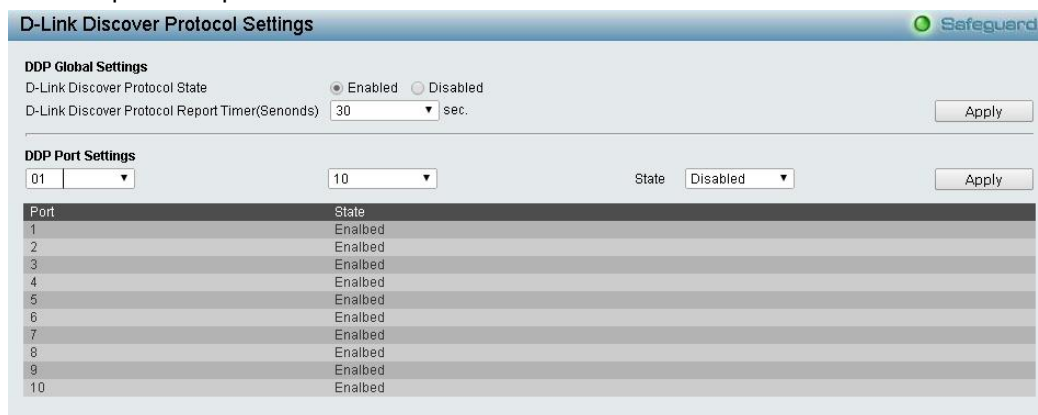


Figure 4.35 – System > D-Link Discover Protocol Settings

D-Link Discover Protocol State: Enable or disable the Discover Protocol state.

D-Link Discover Protocol Report Timer (Seconds): Configure the report timer of D-Link Discover Protocol in seconds. The values are 30, 60, 90, 120 or Never.

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

System > Ping Test

You can Ping either an IPv4 address or an IPv6 address. Ping 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 from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

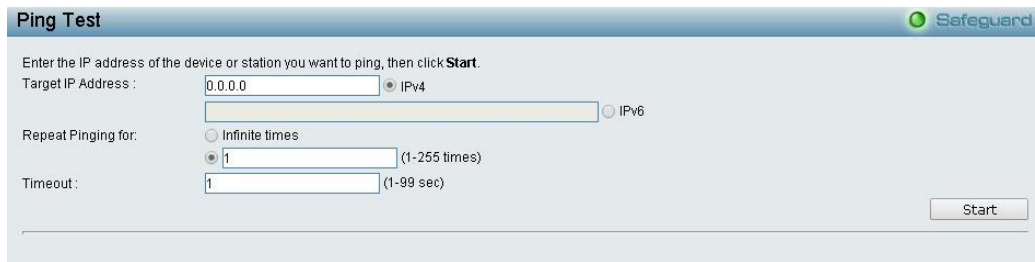


Figure 4.36 – System > Ping Test

The user may tick the Infinite times radio button to tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. You 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 test.

Target IP Address: Enter an IPv4 or IPv6 address to be pinged.

Repeat Pinging for: Enter the number of times desired to attempt to Ping either the IPv4 or the IPv6 address configured in this window. Enter a number of times between 1 and 255.

Timeout: For IPv4, select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. For IPv6, select a timeout period between 1 and 10 seconds for this Ping message to reach its destination. In either case, if the packet fails to find the IP address in this specified time, the Ping packet will be dropped.

System > Trace Route

From this page you can trace a route between the switch and a given host on the network.

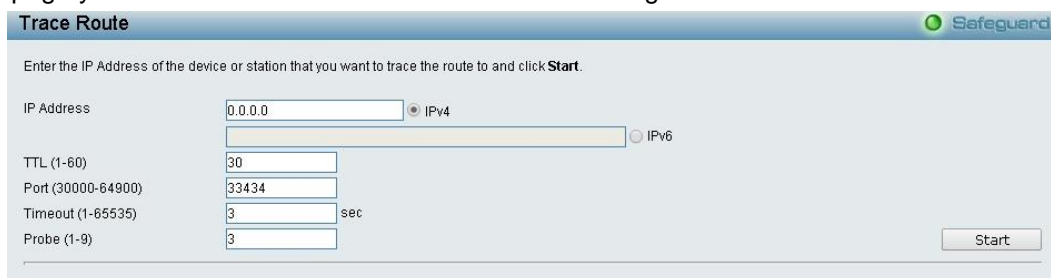


Figure 4.37 – System > Trace Route

IP Address: Enter an IPv4 or IPv6 address of the destination station.

TTL (1-60): The time to live value of the trace route request. This is the maximum number of routers that a trace route packet can pass. The trace route option will cross while seeking the network path between two devices. The range for the TTL is 1 to 60 hops.

Port (30000-64900): Enter a port number. The value range is from 30000 to 64900.

Timeout (1-65535): Defines the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 3 seconds.

Probe (1-9): Enter a number for probing. The range is from 1 to 9. If unspecified, the default value is 3.

System > MAC Notification Settings

The MAC Notification page is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, select enabled or disabled, input the time interval between notification and **history size**, then click the **Apply** button.

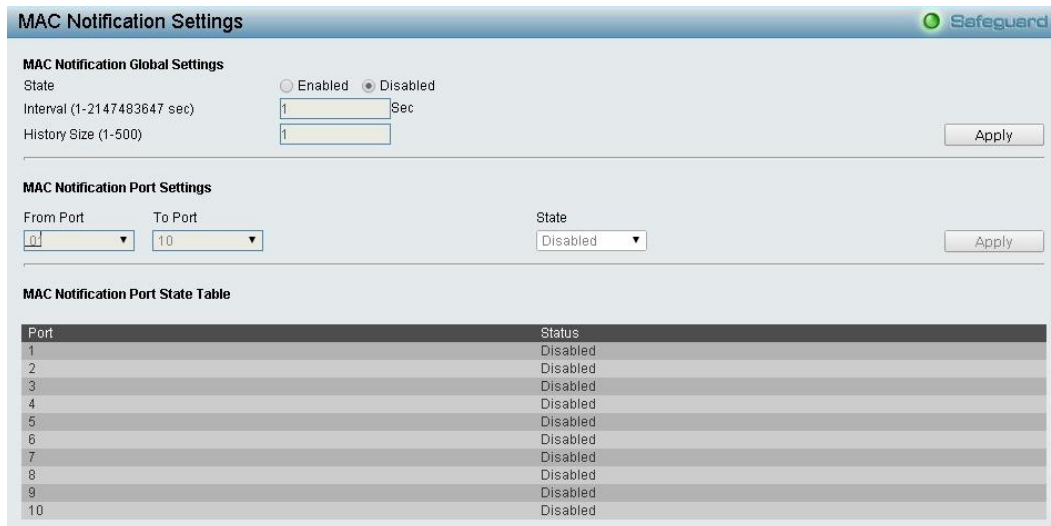


Figure 4.38 – System > MAC Notification Settings

MAC Notification Global Settings:

State: Select to enable or disable MAC notification globally on the Switch.

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

History Size (1-500): Enter 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.

MAC Notification Port Settings:

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** to configure the related settings of remote system log server, then press **Apply** for the changes to take effect.

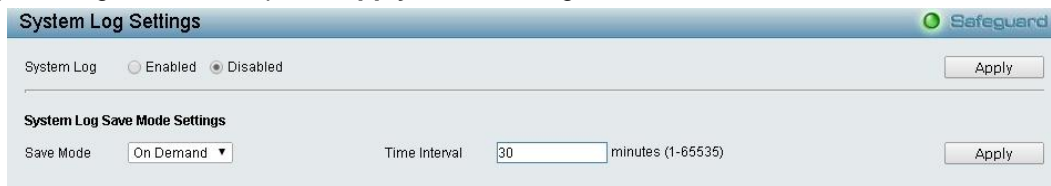


Figure4.39 – System > System Log Configuration > System Log Settings

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

Minutes: Enter a time interval, in minutes, for 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**.

Figure 4.40 - System > System Log Configuration > System Log Server

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

Severity: Select 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.

Facility: Select 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: Enter the UDP port to which the server logs are sent. The possible range is 6000 – 65535, and the default value is 514.

Status: Select the status to enable or disable.

Server IP Address: Select either IPv4 or IPv6 and enter the syslog server IP address.

System > Time Profile

From this page you can configure the time profile settings of the device.

Figure 4.41 – System > Time Profile Settings

Profile Name: Enter a profile name.

Time(HH MM): Select a Start Time and End Time.

Weekdays: Select which days you want to use.

Date: Tick the Date box and select a range from the "From Day" and "To Day" fields.

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 link is down or the connected devices are turned off. Less power will be consumed also when a 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, Cable Length Detection and Link Status Detection are enabled. Select either **Enabled** or **Disabled**. If you select Enabled, make any changes to the settings below and click **Apply**.

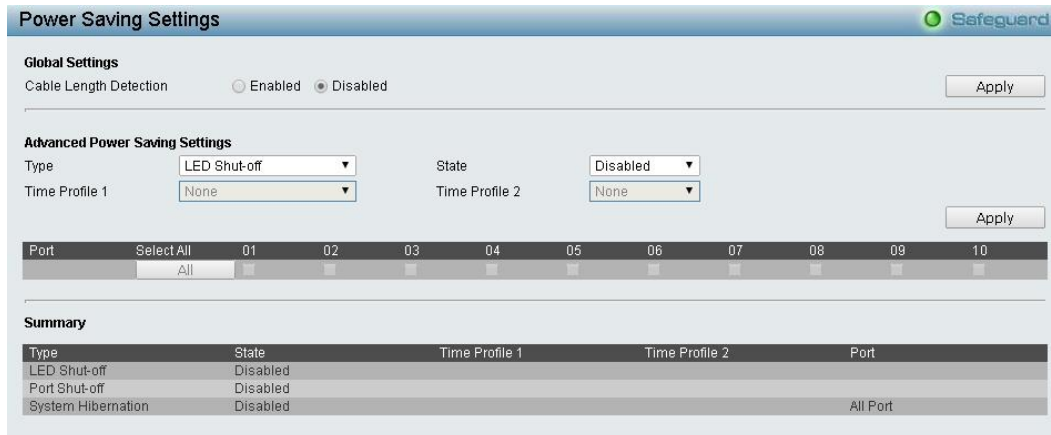


Figure 4.42 – System > Power Saving

Advanced Power Saving Settings:

Type: Select the Power Saving type. Select either LED Shut-off, Port Shut-off, Port Standby or System Hibernation.

LED Shut-off - Select LED Shut-off to turn off the LEDs on the selected port(s). Select the time profile that you want the LEDs to turn off.

Port Shut-off - Select to turn off the selected port(s) on the Switch. Select the time profile that you want the port(s) to turn off.

Port Standby - The system changes to standby state and wait for a wake up event. Select the time profile(s) to place the Switch in port standby mode.

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: Select Enable or Disable.

Time Profile 1: Select the time profile or None.

Time Profile 2: Select the time profile or None.

Port: Select the port or ports to apply to the power saving type selected.

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

System > IEEE802.3az EEE Settings

The IEEE 802.3 EEE standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be IEEE802.3az EEE compliance. By default, the switch enabled the 802.3az EEE function. You can disable this feature by individual port via the IEEE802.3az EEE setting page.

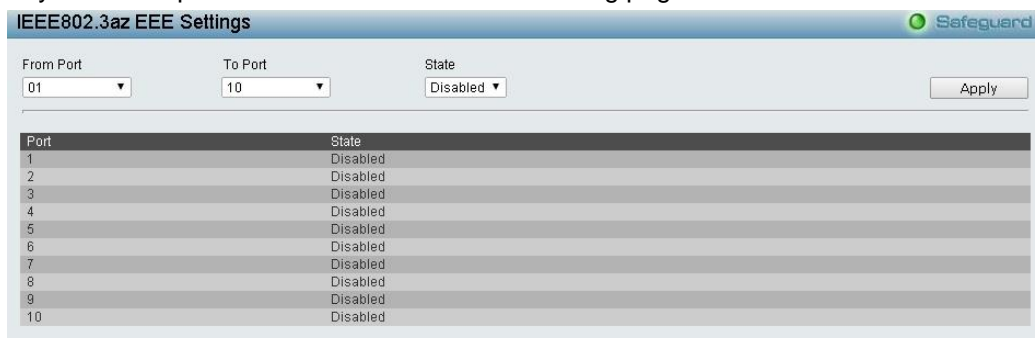


Figure 4.43 – System > IEEE802.3az EEE Settings

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

State: Enabled or Disabled the IEEE802.3az EEE for the specified ports. By default, all ports are enabled.

Click **Apply** to implement changes made.

If the connection speed drops down from 1000M to 100M, or the first link up takes longer time, please follow below steps and check again:

1. Upgrade drivers of your Ethernet adapter or LAN controller for the host PC.
2. Disable EEE function on the switch port.

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.



Figure 4.44 – Configuration > 802.1Q VLAN

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

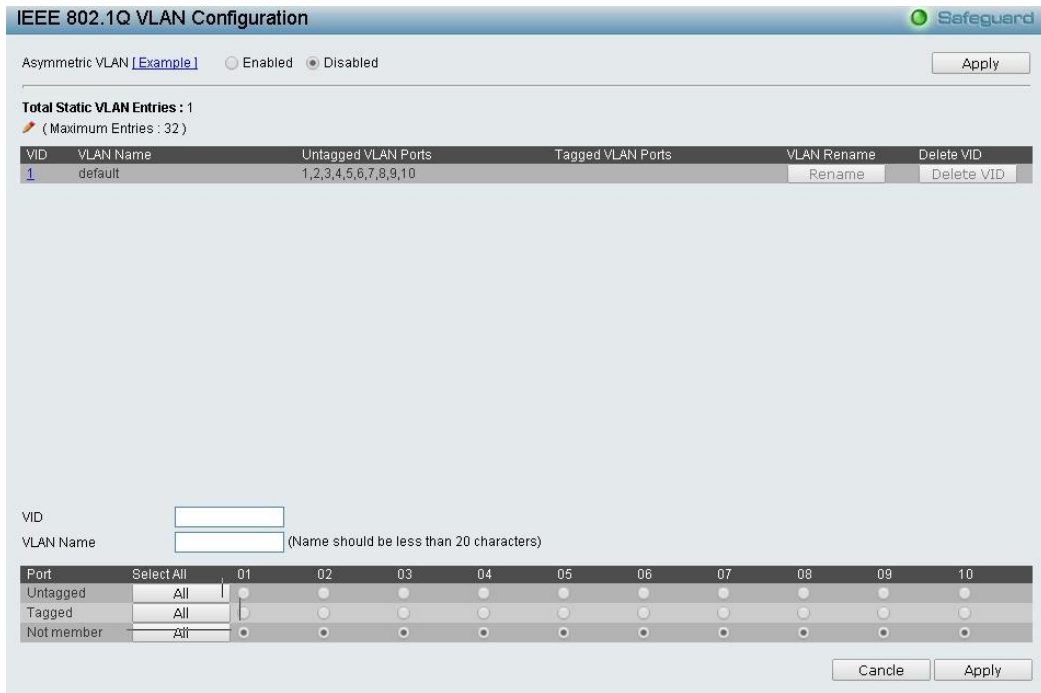


Figure4.45 – Configuration > 802.1Q VLAN > Add VLAN

Click **Apply** and the 802.1Q VLAN Configuration Table will be displayed with updates.



Figure 4.46 - Configuration > 802.1Q VLAN > Example VIDs

Click the VID number to display the VLAN group configuration. Change the port assignment and then click **Apply** to implement changes made.

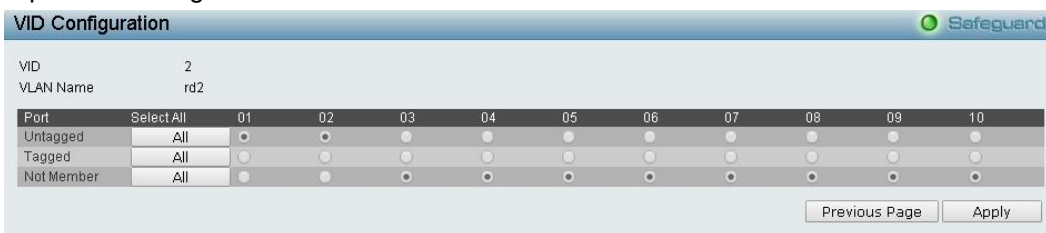


Figure 4.47 - Configuration > 802.1Q VLAN > VID Assignments

Select **Enabled** and click **Apply** to enable asymmetric VLAN.



Figure4.48 - Configuration > 802.1Q VLAN > VID Assignments

Configuration > 802.1Q Management VLAN

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

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



Figure 4.49 – Configuration > 802.1Q Management VLAN

Configuration > 802.1Q VLAN PVID

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

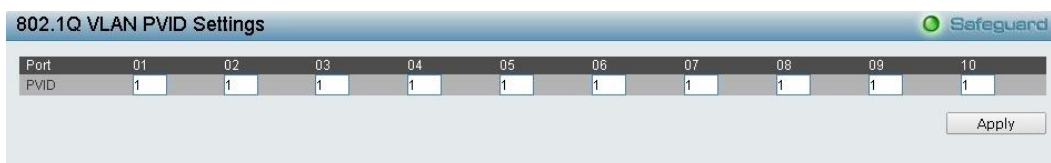


Figure 4.50 – Configuration > 802.1Q VLAN PVID

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.



Figure4.51 - 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: Select either *UNI* or *NNI*.

UNI – User-to-network interface which specifies that communication between the specified user and a specified network will occur.

NNI –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-1100-10/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-1100-10/ME will forward multicast traffic only to connections that have group members attached.

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



Figure 4.52 – Configuration > IGMP Snooping > IGMP Snooping

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

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

Click the **Edit** button to enter the Querier Timers Settings page.

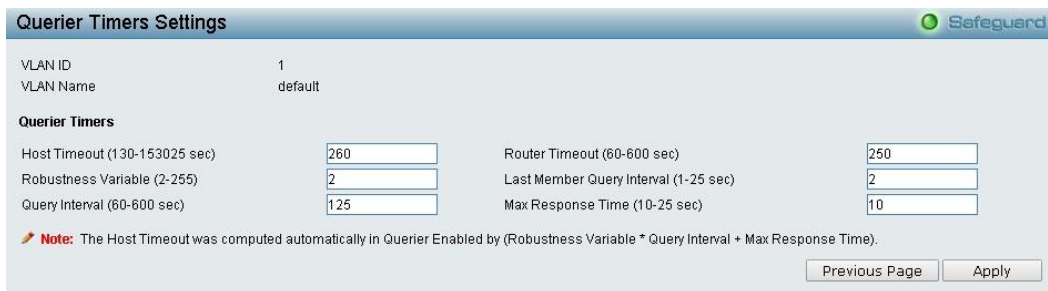


Figure 4.53 – Configuration > IGMP Snooping > Querier Timer Settings

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.

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

Click the **Edit** button to enter the Router Port Settings which you can configure what 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.



Figure 4.54 – Configuration > IGMP Snooping > IGMP Snooping-Router Port Settings

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



Figure 4.55– Configuration > IGMP Snooping > IGMP Snooping-Multicast Entry Table

Configuration > IGMP Snooping > IGMP Access Control Settings

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



Figure 4.56 - Configuration > IGMP Snooping > IGMP Access Control Settings

Configuration > IGMP Snooping > Host Table

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

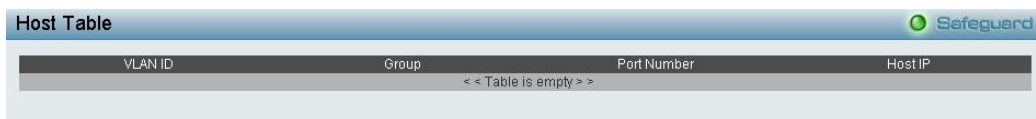


Figure 4.57 - Configuration > IGMP Snooping > Host Table

Configuration > MLD Snooping > MLD Snooping Settings

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



Figure 4.58 - Configuration > MLD Snooping > MLD Snooping Settings

MLD Snooping: Enable or disable the MLD Snooping.

The VLAN Settings of MLD snooping:

Click the **Edit** button to enter the Querier Timers Settings page.



Figure 4.59 – Configuration > MLD Snooping > Querier Timer 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 sec): 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.

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

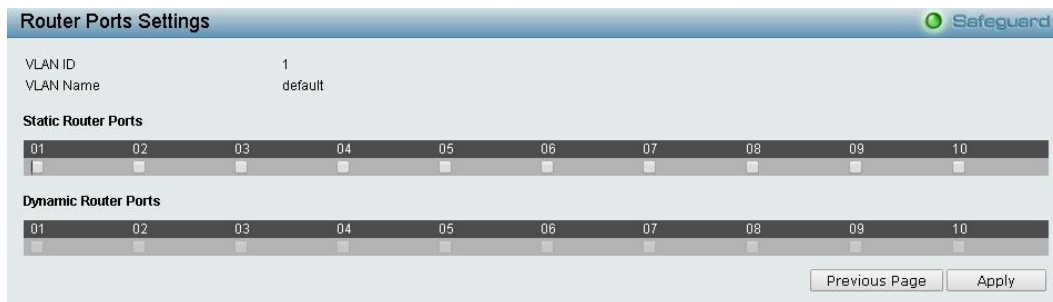


Figure 4.60 – Configuration > MLD Snooping > MLD Snooping-Router Port Settings

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



Figure 4.61– Configuration > MLD Snooping > MLD Snooping-Multicast Entry Table

Configuration > MLD Snooping > MLD Host Table

The MLD Host Table page displays the MLD Snooping information.

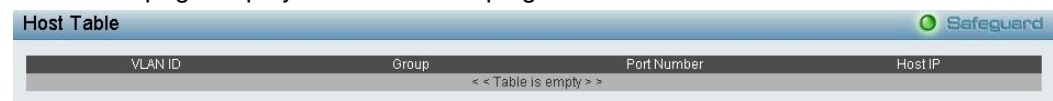


Figure 4.62 - Configuration > MLD Snooping > MLD Host Table

Configuration > 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.

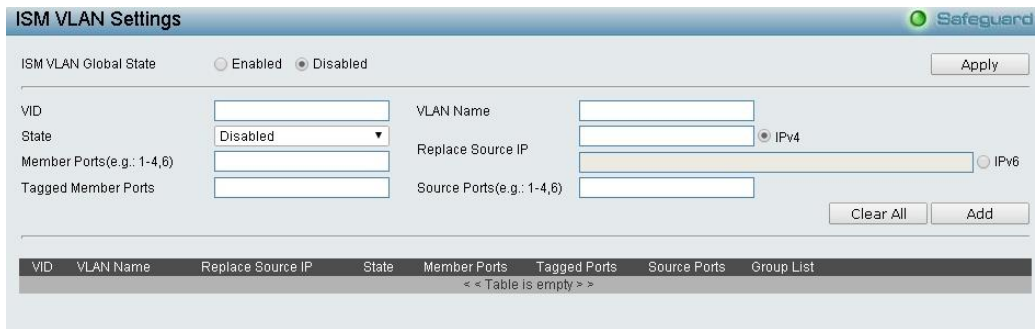


Figure 4.63 - Configuration > ISM VLAN Settings

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

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

VID: Add the corresponding VLAN ID of the Multicast VLAN. You 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.

Replace Source: This field is used to replace the source IPv4 or 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.

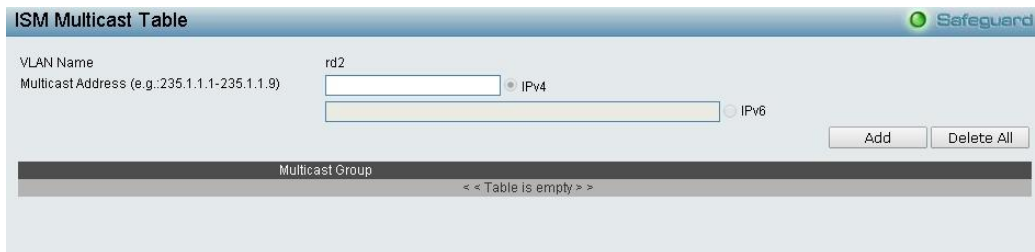


Figure4.64 - Configuration > IGMP Snooping > ISM VLAN Settings

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

Click **Add** to create a new enter or click **Delete All** to remove all entries.

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** and then click **Apply** to turn on the jumbo frame support.

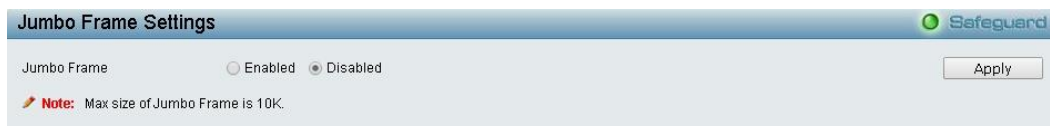


Figure 4.65 – Configuration > Jumbo Frame Settings

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.

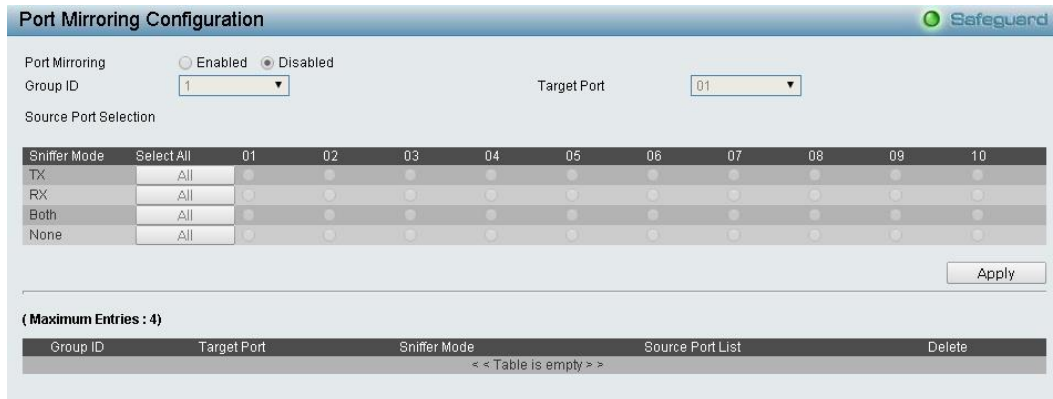


Figure 4.66 – Configuration > Port Mirroring

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 shut down 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 drop-down menu.

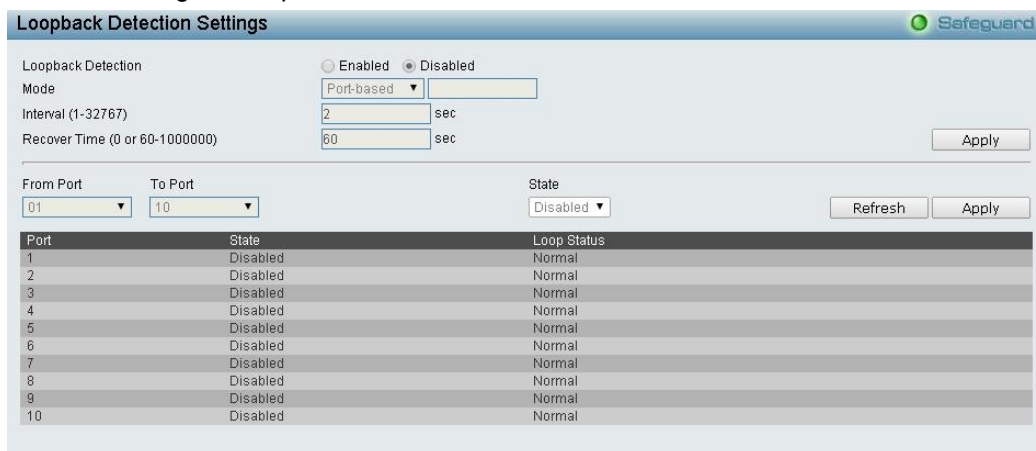


Figure 4.67 – Configuration > Loopback Detection

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.

Figure 4.68 – 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, you can select from one of two options:

Manually set current time: Enter 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.

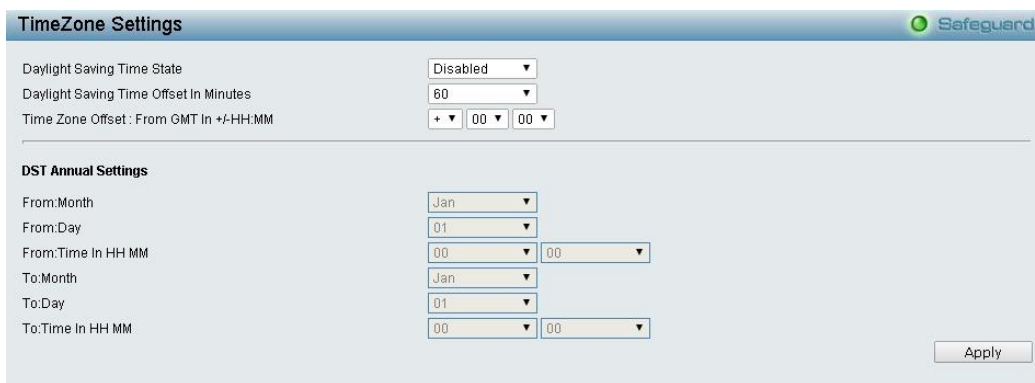


Figure 4.69 – Configuration > SNTP > TimeZone Settings

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 Relay > DHCP Relay Global Settings

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



Figure 4.70 - Configuration > DHCP Relay > DHCP Relay Global Settings

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

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

DHCP Relay Time Threshold (0-65535): Allows an entry between 0 and 65535 seconds, and defines the maximum time limit for routing a DHCP packet. If a value of 0 is entered, the Switch will not process the value in the **seconds** field of the 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 DHCP packet.

DHCP Relay Agent Information Option 82 State: This field can be toggled between Enabled and Disabled using the drop-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 drop-down menu. It is used to enable or disable the Switch's 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 drop-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 Relay > DHCP Relay Interface Settings

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



Figure 4.71 - Configuration > DHCP Relay > DHCP 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 server. Up to four server IPs can be configured per IP Interface.

Configuration > DHCP Local Relay Settings

From this page you can 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.



Figure4.72 - Configuration > DHCP Local Relay Settings

DHCP 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.



Figure4.73 - 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 an entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded. The default hop count is 4.

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

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

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

Interface: Enter a name of the interface.

Server IP: Enter the server IP address.

Click **Apply** to implement changes made.

Configuration > 802.3ah EthernetLink 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 you to configure the Ethernet OAM settings.

Figure 4.74 - Configuration > 802.3ah EthernetLink OAM > Ethernet OAM Port Settings

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

Mode: Select either active mode or passive mode. The default mode is active.

State: Select 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: Select whether to process or to ignore the received Ethernet OAM remote loopback command. The default method is *Ignore*.

Click **Apply** to implement changes made.

Configuration > 802.3ah EthernetLink OAM > Ethernet OAM Event Configuration

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

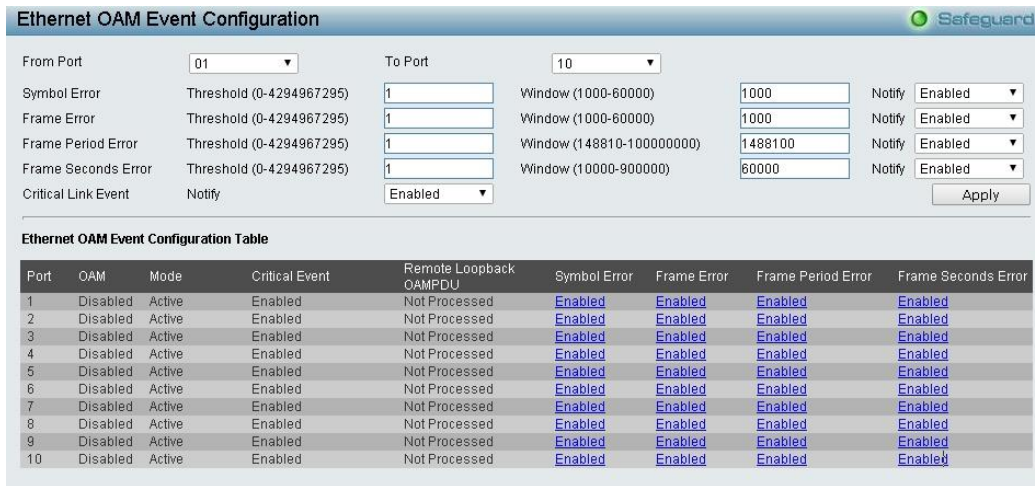


Figure 4.75 - Configuration > 802.3ah EthernetLink OAM > Ethernet OAM Event Configuration

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:

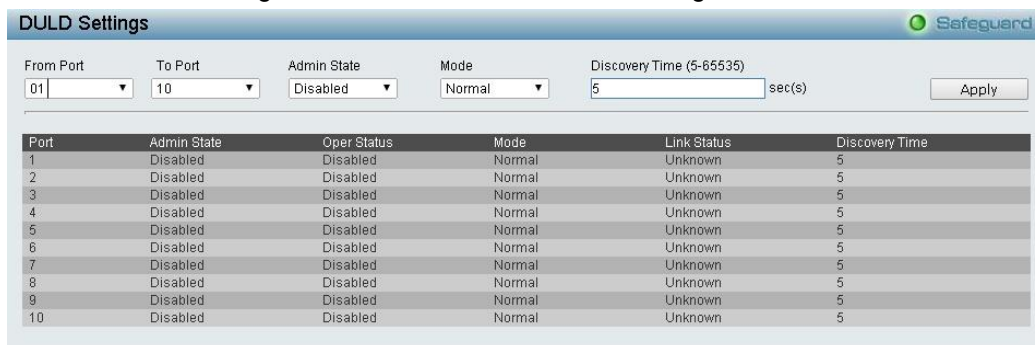


Figure4.76 - Configuration > DULD > DULD Port Settings

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 & Filter > Multicast Forwarding

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

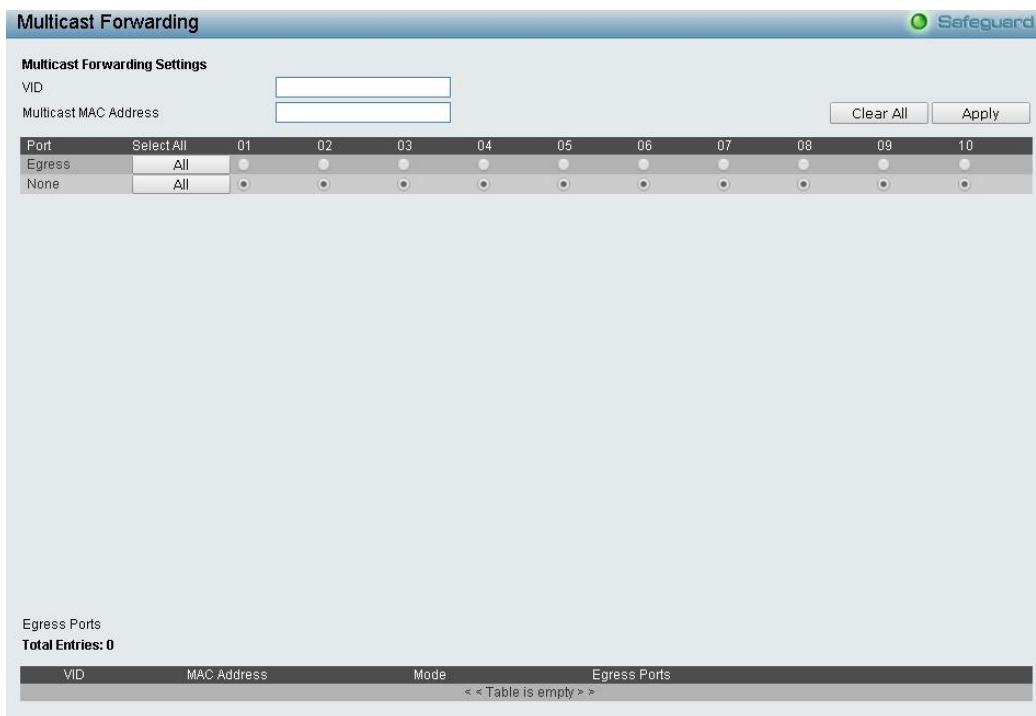


Figure 4.77 - Configuration > Multicast Forwarding & Filter > Multicast Forwarding

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** to implement changes made.

Configuration > Multicast Forwarding & Filter > Multicast Filter Mode

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



Figure4.78 - Configuration > Multicast Forwarding & Filter > Multicast Filter Mode

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

Multicast Filtering Mode: Select an action from the drop-down menu when the Switch 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.

Configuration > Multicast Forwarding & Filter > IP Multicast Profile Settings

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



Figure 4.79 - Configuration > IGMP Snooping > IP Multicast Profile Settings

Profile Type: Select either IPv4 or IPv6.

Profile ID: Select the Profile ID.

Profile Name: Enter a Profile Name.

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

Configuration > Multicast Forwarding & Filter > Limited Multicast Range Settings

The Limited Multicast Range Settings page allows you to configure the Limited Multicast. Specify the port range, select the Access IP Type (IPv4 or IPv6), and select to permit or deny access. Click **Apply** to implement changes made.

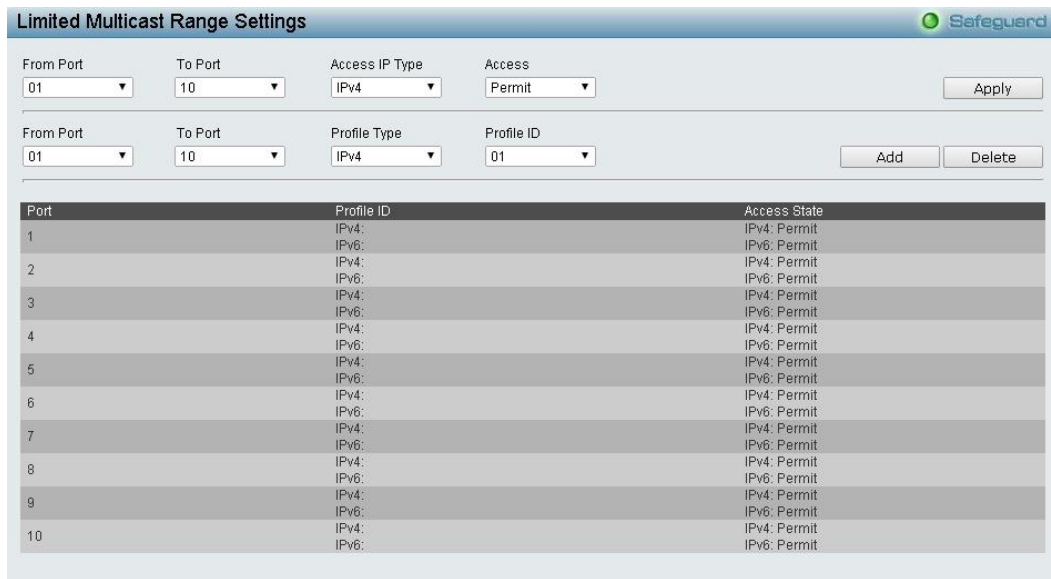


Figure 4.80 - Configuration > IGMP Snooping > Limited Multicast Range Settings

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

Profile Type: Select **IPv4** or **IPv6**.

Profile ID: Select the Profile ID.

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

Configuration > Multicast Forwarding & Filter > Max Multicast Group Settings

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

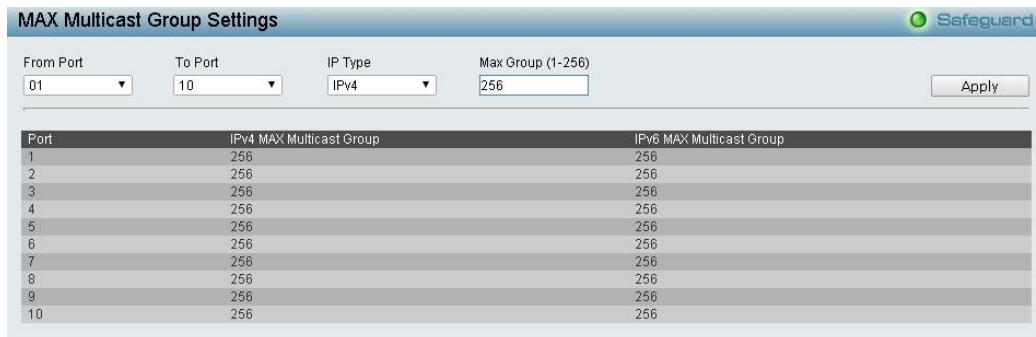


Figure4.81- Configuration > IGMP Snooping > Max Multicast Group Settings

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

IP Type: Select **IPv4** or **IPv6**.

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

Click **Apply** to implement changes made.

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.

Port	Storm Control Type	Action	Threshold	Count Down	Interval	Port status	Shutdown Forever
1	None	Drop	0 Kbps	0	0	Normal	
2	None	Drop	0 Kbps	0	0	Normal	
3	None	Drop	0 Kbps	0	0	Normal	
4	None	Drop	0 Kbps	0	0	Normal	
5	None	Drop	0 Kbps	0	0	Normal	
6	None	Drop	0 Kbps	0	0	Normal	
7	None	Drop	0 Kbps	0	0	Normal	
8	None	Drop	0 Kbps	0	0	Normal	
9	None	Drop	0 Kbps	0	0	Normal	
10	None	Drop	0 Kbps	0	0	Normal	

Figure4.82 – QoS > Traffic Control

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

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 countdown 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: Ports that are in 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.



Figure 4.83 – QoS > Bandwidth Control

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

Type: Select **RX** (receive), **TX** (transmit), or **Both**. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit: Select **Enabled** to remove any bandwidth limit on the selected port range. Select **Disabled** and enter a bandwidth rate limit.

Rate (16-1000000): If you selected **Disabled** from the *No Limit* drop-down menu, enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 16 and 1000000.

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



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 > QoS Settings

QoS is an implementation of the IEEE 802.1p standard that allows you 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.

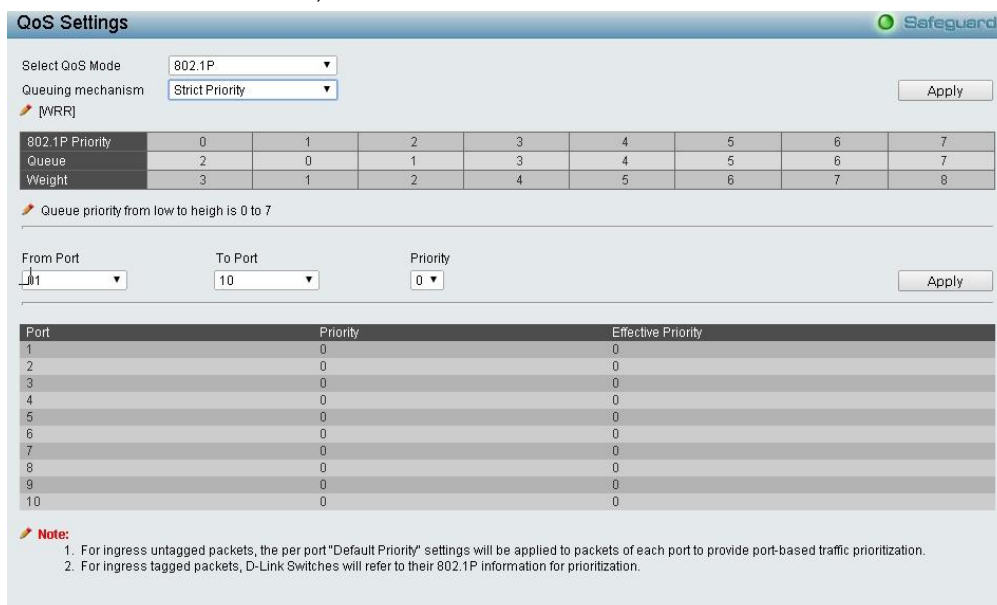


Figure 4.84 - QoS > QoS Settings

Select QoS Mode: Select **PortBase**, **802.1p**, or **DSCP**.

Quening Mechanism:

Strict Priority: Selecting this 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.

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

Priority: Defines the priority assigned to the port. The priority range is between 0 and 7 with 0 being assigned to the lowest priority and 7 assigned to the highest.

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

RMON > RMON Basic Settings

You 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** for the settings to take effect.

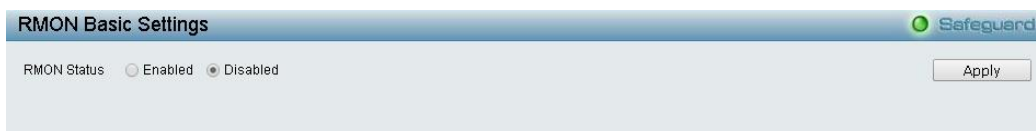


Figure 4.85 - RMON > RMON Basic Settings

RMON > RMON Ethernet Statistics Configuration

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



Figure 4.86 - RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:

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

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

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

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

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.

Figure 4.87 - RMON > RMON History Control Configuration

The History Control Configuration contains the following fields:

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

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

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

Interval (1 ~ 3600secs): Enter 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: Enter the RMON station or user that requested the RMON information.

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

RMON > RMON Alarm Configuration

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

Figure 4.88 - RMON > RMON Alarm Settings

The configuration contains the following fields:

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

Variable: Enter the selected MIB variable value.

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

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

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

Interval (1 ~ 2^31-1): Enter 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): Enter the falling counter value that triggers the falling threshold alarm.

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

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

RMON > RMON Event Configuration

The RMON Event page contains fields for defining, modifying and viewing RMON events statistics.

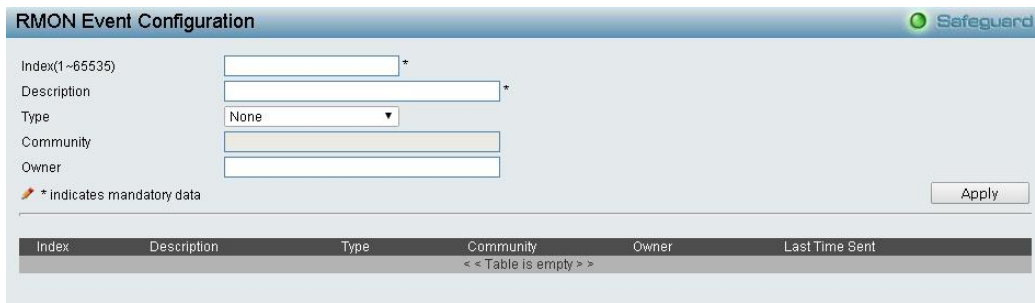


Figure4.89 - RMON > RMON Event Configuration

The RMON Events Page contains the following fields:

Index (1~ 65535): Enter an event index number.

Description: Enter a user-defined event description.

Type: Select an 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: Enter the community to which the event belongs.

Owner: Enter the user that defined the event.

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

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.

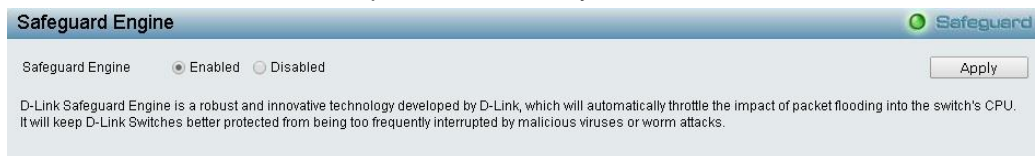


Figure 4.90 – Security > Safeguard Engine

Security > Port Security > Port Security Settings

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 port's (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.

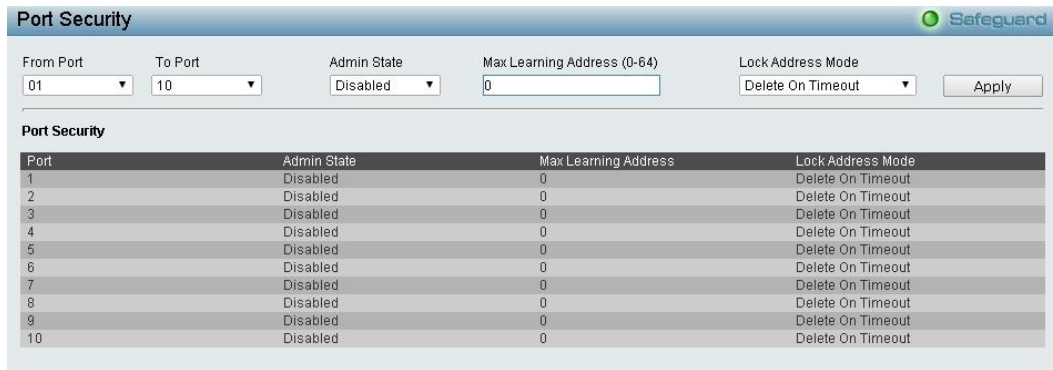


Figure 4.91 - Security > Port Security > Port Security Settings

The Port Security page contains the following fields:

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

Admin State: Select either **enable** or **disable** Port Security (locked MAC address table for the selected ports).

Max. Learning Address (0-64): Enter 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: Select how the MAC address table locking will be implemented 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** for the settings to take effect.

Security > Port Security > Port Security FDB Entry

The Port Security FDB Entry page allows the Switch's dynamic forwarding table to be viewed. When the Switch learns an association between a MAC address, VLAN and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.



Figure 4.92 - Security > Port Security > Port Security FDB Entry

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

Click **Clear** to remove any lock entries on the selected port range.

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: Authentication Protocol:

802.1X Port Access Control

From Port: To Port:

QuietPeriod (0-65535): sec. SuppTimeout (1-65535): sec.

ServerTimeout (1-65535): sec. MaxReq (1-10): times

TxPeriod (1-65535): sec. ReAuthPeriod (1-65535): sec.

ReAuthentication: Port Control:

Capability: Direction:

Port	AdmDir	OperDir	Port Control	Auth Status	Tx Period	Quiet Period	Supp Timeout	Server Timeout	Max Req	ReAuth Period	ReAuth	Capability
1	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
2	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
3	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
4	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
5	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
6	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
7	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
8	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
9	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None
10	Both	Both	ForceAuthorized	Authorized	30	60	30	30	2	3600	Disable	None

Figure 4.93 - 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: Select 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): Enter 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): Enter 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): Enter 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: Select whether regular reauthentication will take place on this port. The default setting is *Disabled*.

Capability: Select 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-5challenge) 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 you to control the port authorization state.

Select **ForceAuthorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.

If **ForceUnauthorized** is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.

If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is *Auto*.

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

Both – Specify the control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

In – Disables the support in the present firmware release.

Click **Apply** to implement configuration changes.

Security > 802.1X > 802.1X User

The **802.1X User** page allows you 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.

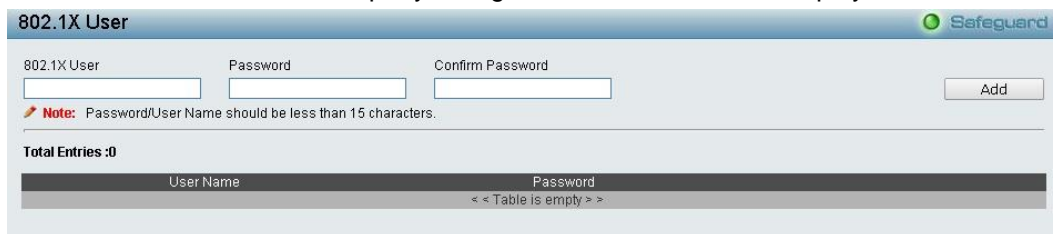


Figure4.94 - Security > 802.1X > 802.1X User

Click **Add** to add a new 802.1X user.

Security > 802.1X > Radius Accounting Settings

The Radius Accounting Settings allows you to configure the accounting state of 802.1X.

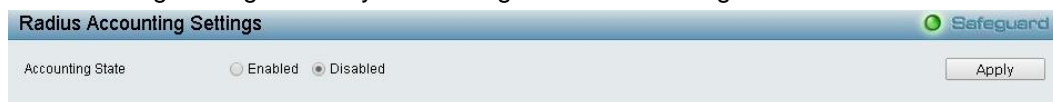


Figure 4.95 - Security > 802.1X > Radius Accounting Settings

Security > 802.1X > 802.1X Authentication RADIUS

This page allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

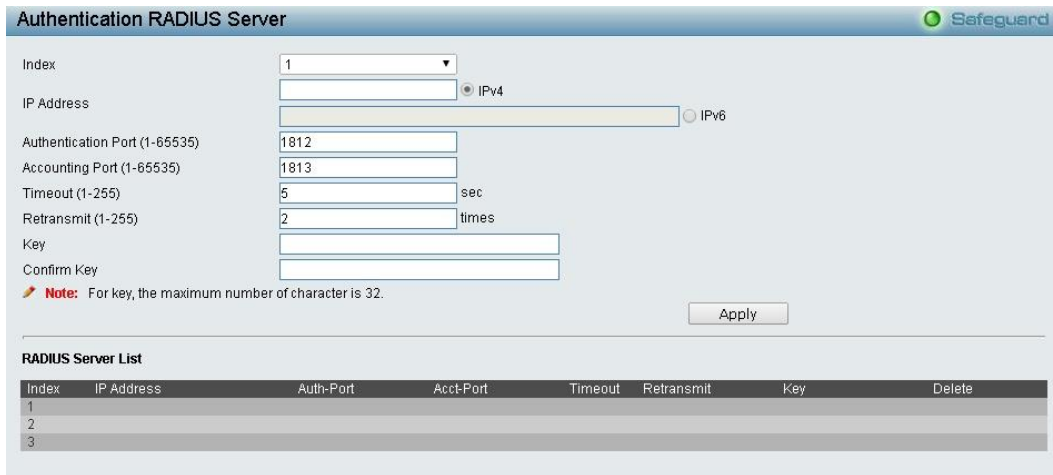


Figure 4.96 - Security > 802.1X > 802.1X Authentication RADIUS

Index: Select 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): Enter the RADIUS authentic server(s) UDP port. The default port is 1812.

Accounting Port (1 - 65535): Enter the RADIUS account server(s) UDP port. The default port is 1813.

Timeout (1 – 255 sec): Enter 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: Enter 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

From this page you can set an existing VLAN to a Guest VLAN.

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.

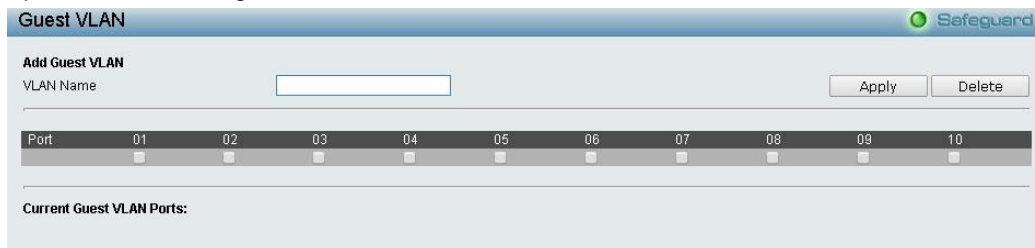


Figure4.97 - Security > 802.1X > 802.1X Guest VLAN

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).



Figure 4.98 - Security > MAC Address Table > Static Mac Address

The **Static MAC Address List** table displays static MAC addresses that are 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.

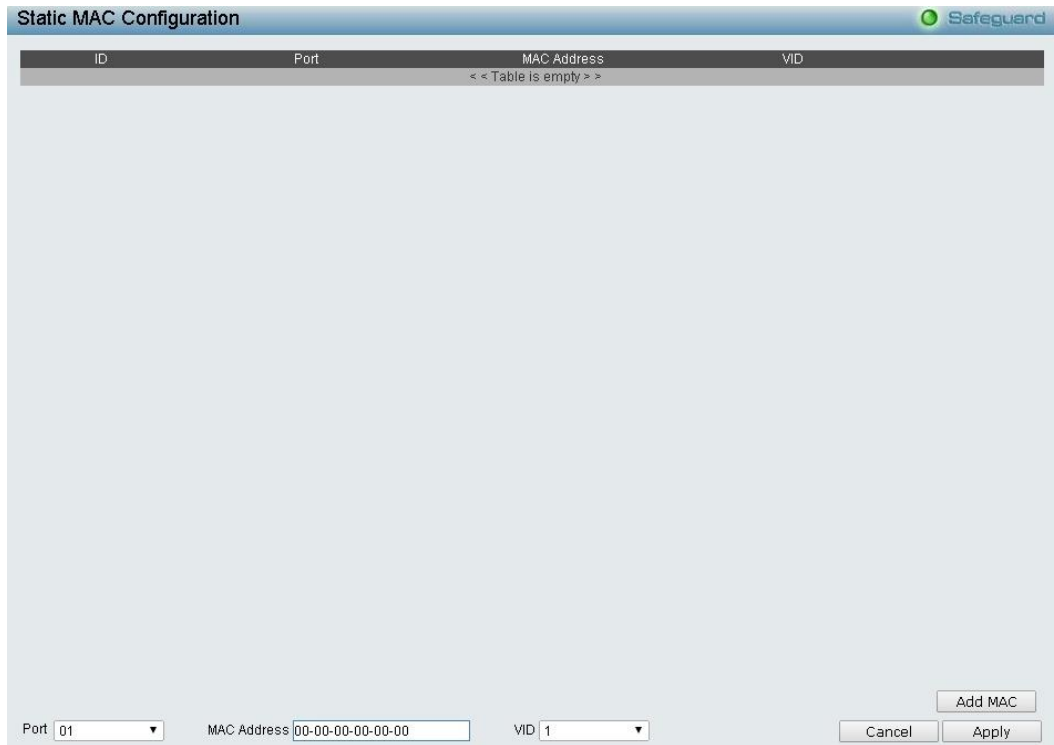


Figure 4.99 - Security > MAC Address Table > Static Mac Address-add MAC

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.



Figure 4.100 - 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 you 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: Click 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.

Figure 4.101 – Security > Access Authentication control > Authentication Policy Settings

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

Response Timeout (0 - 255): 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): Enter 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 you to configure switch configuration applications for login at the user level and at the administration level utilizing a previously configured method list.

Application	Login Method List	Enable Method List
Telnet	default	default
HTTP	default	default

Figure 4.102 – 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: Select 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: Select 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. You 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.

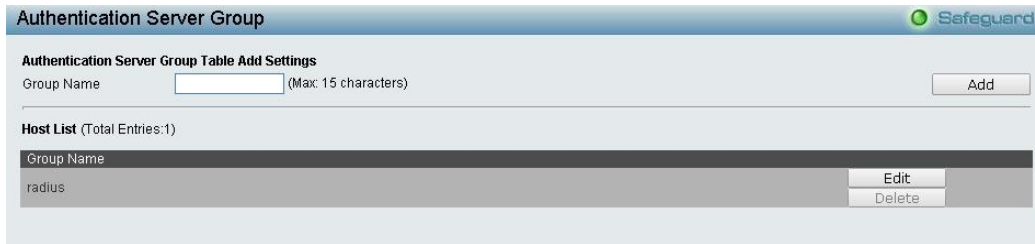


Figure 4.103 – Security > Access Authentication control > Authentication Server Group

Enter a group name of no more than 15 alphanumeric characters to define the user group. 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 and the following window will appear.



Figure 4.104 – Security > Access Authentication control > Authentication Server Group-Edit

Select **Group Name**, **Protocol** and **IP address** then click **Add** to implement the changes.



NOTE: You 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

From this page you can 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.

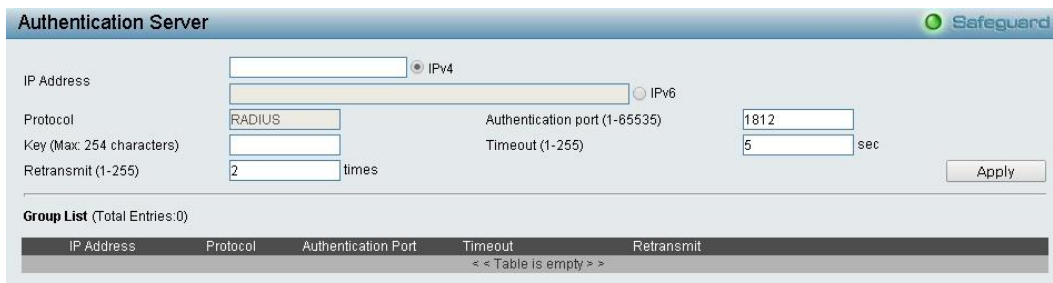


Figure 4.105 – Security > Access Authentication control > Authentication Server

To add an Authentication Server Host:

IP Address: Select **IPv4** or **IPv6** and then enter the server IP address.

Protocol: The protocol used by the server host. Select from 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 configured RADIUS servers. 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

From this page you can 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**. To modify the Login Method List, click **Edit**.

Method List Name	Priority 1	Priority 2	Priority 3	Priority 4	
default	local	none	none	none	Edit Delete

Figure 4.106 – 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: You may add one or a combination of up to four of the following authentication methods to this method list:

- none** – Selecting this parameter will require authentication to access the Switch.
- local** – Selecting this parameter will require the user to be authenticated using the local user account database on the Switch.
- radius** – Selecting 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, click to Delete the entry desired to be deleted. To modify an Enable Method List, click **Edit** to make any changes and click **Apply**.

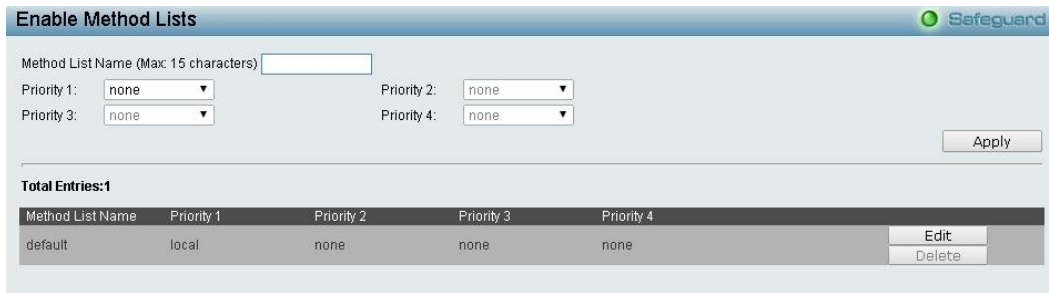


Figure 4.107 – Security > Access Authentication control > Enable Method Lists

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: You may add one or a combination of up to four of the following authentication methods to this method list:

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

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

radius – Selecting 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 you 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 that is locally set on the Switch.

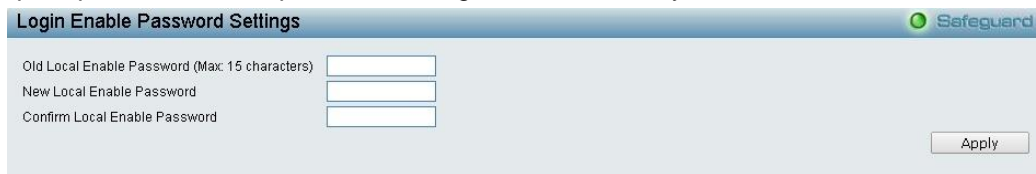


Figure 4.108 – Security > Access Authentication control > Local Enable Password Settings

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 a 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.

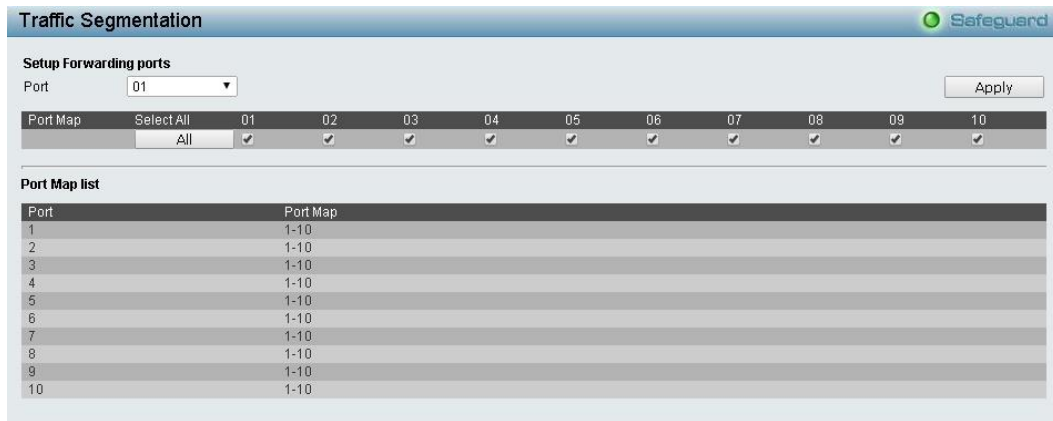


Figure 4.109 – Security > Traffic Segmentation

Configure traffic segmentation by selecting a port or ports from the drop-down menu, then next to *Port Map*, select what ports to map to. Click **Apply**.

Click **Select All** to select all port maps or click **Clear** to uncheck port maps.

Monitoring > Statistics

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

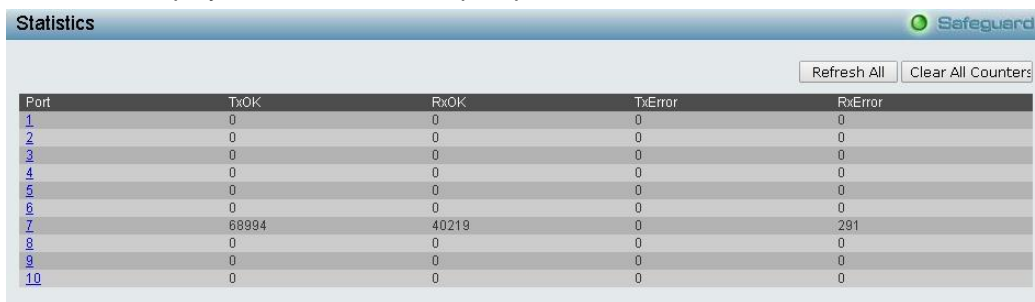


Figure4.110 – Monitoring > Port Statistics

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.



Figure 4.111 – 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 you 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.

ID	Login Time	Live Time	From	Level	Name
1	1/1/2013 00:36:20	06:36:36	10.90.90.98	3	anonymous
2	1/1/2013 01:47:39	05:25:17	10.90.90.98	3	anonymous
3	1/1/2013 06:19:17	00:53:39	10.90.90.98	3	anonymous

Figure 4.112 – 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.

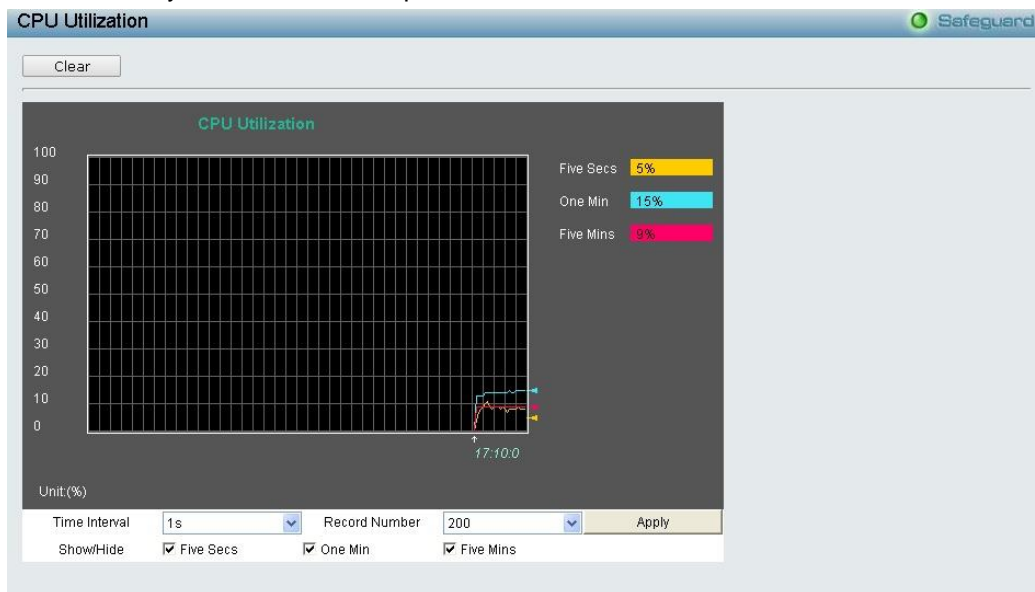


Figure4.113 – Monitoring > CPU Utilization

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 the 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: Click to clear all statistics counters in 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.

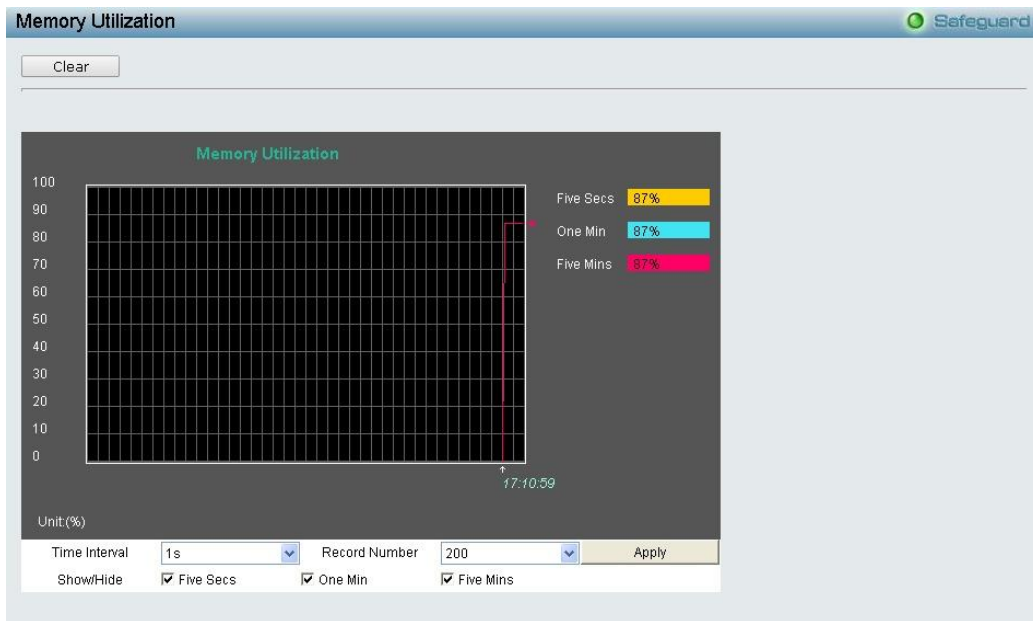


Figure 4.114 – Monitoring > Memory Utilization

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 the 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: Click to clear all statistic counters on this window.

Monitoring > Port Utilization

The Port Utilization page displays the percentage of the total available bandwidth being used on the port.



Figure 4.115 – Monitoring > Port Utilization

You 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 the 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: Click to clear all statistic 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** drop-down menu. You may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

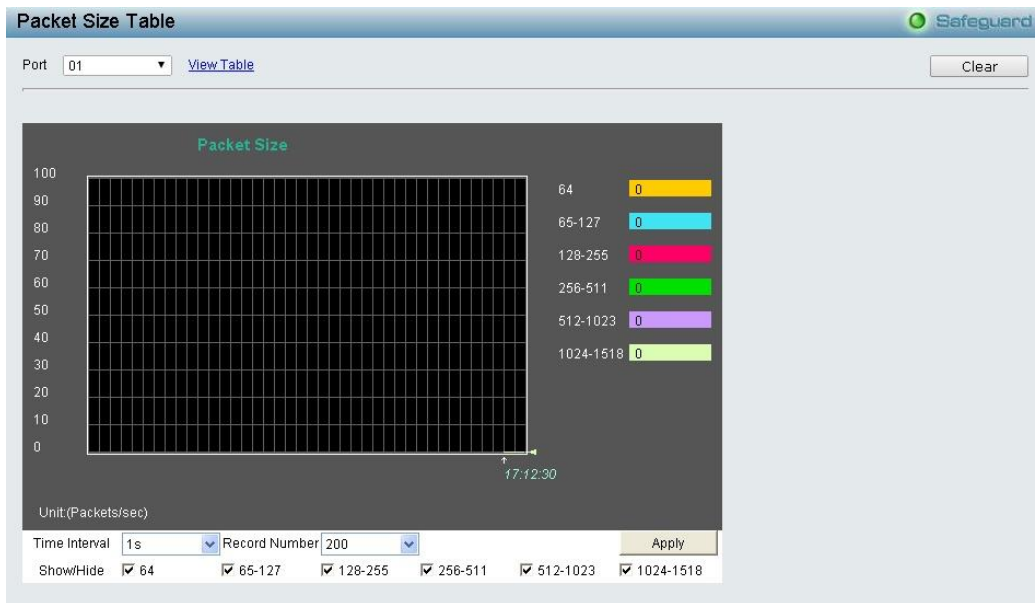


Figure 4.116 – Monitoring > Packet Size

To view the **Packet Size Analysis Table**, click the link [View Table](#), which will show the following table:

The screenshot shows the 'Packet Size Table' window with the 'View Table' link selected. The table below displays the following data:

Packets Size	Frames Counts	Frames/Sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0

Figure 4.117 – 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 the 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: Click to clear all statistic counters on this window.

View Table: Click to display a table rather than a line graph.

View Line Chart: Click 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** drop-down menu. You may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

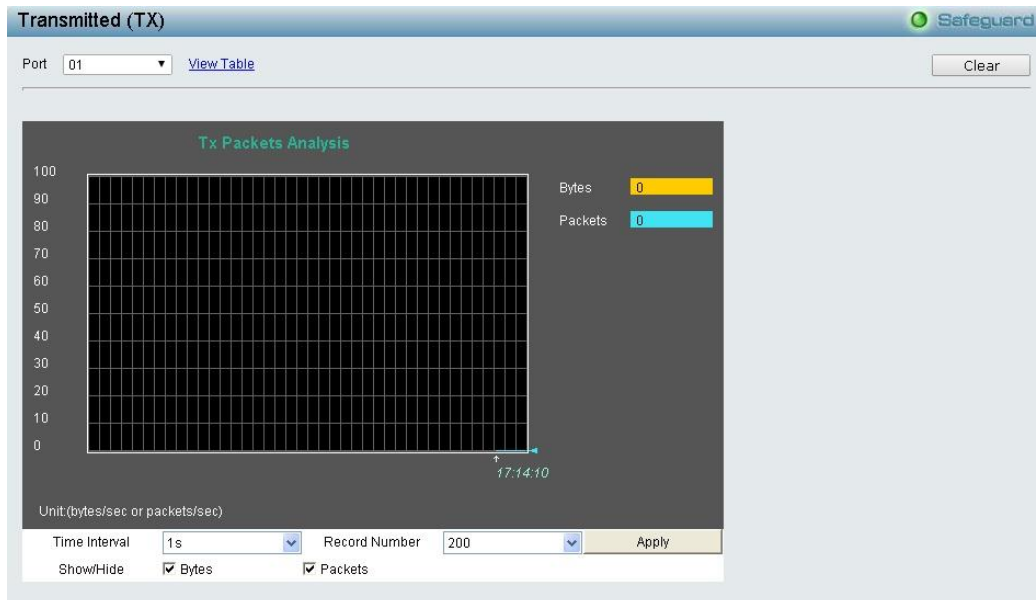


Figure 4.118 - Monitoring > Packets > Transmitted (TX) (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link [View Table](#), which will show the following table:

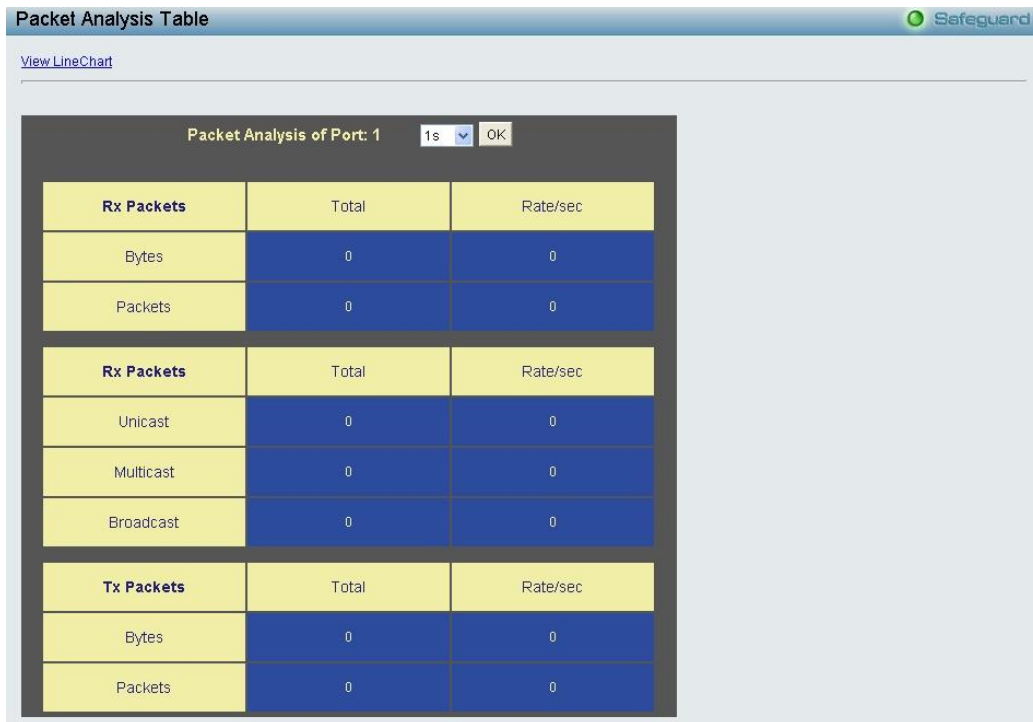


Figure 4.119 - Monitoring > Packets > Transmitted (TX) (table for Bytes and Packets)

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 the 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: Click to clear all statistic counters on this window.

View Table: Click to display a table rather than a line graph.

View Line Chart: Click 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** drop-down menu. You may also use the real-time graphic of the Switch at the top of the web page by clicking on a port.

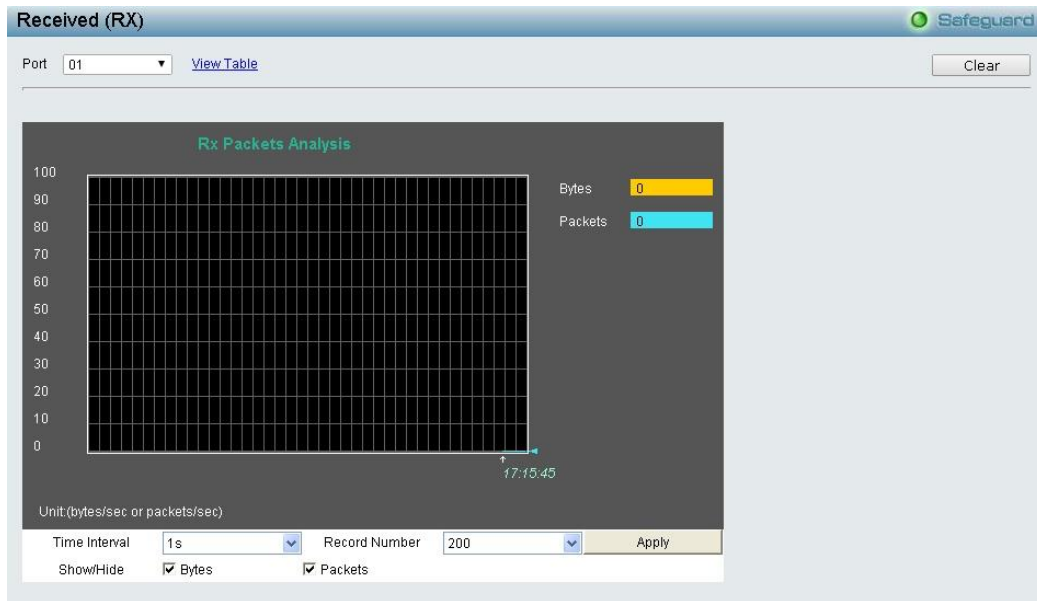


Figure 4.120 - Monitoring > Packets > Received (RX) (line graph for Bytes and Packets)

To view the **Received Packets Table**, click the link [View Table](#), which will show the following table:

Packet Analysis of Port: 1		
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 4.121 - Monitoring > Packets > 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:** Click to clear all statistic counters on this window.
- View Table:** Click to display a table rather than a line graph.
- View Line Chart:** Click 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** drop-down menu. You may also use the real-time graphic of the Switch at the top of the web page by clicking on a port.

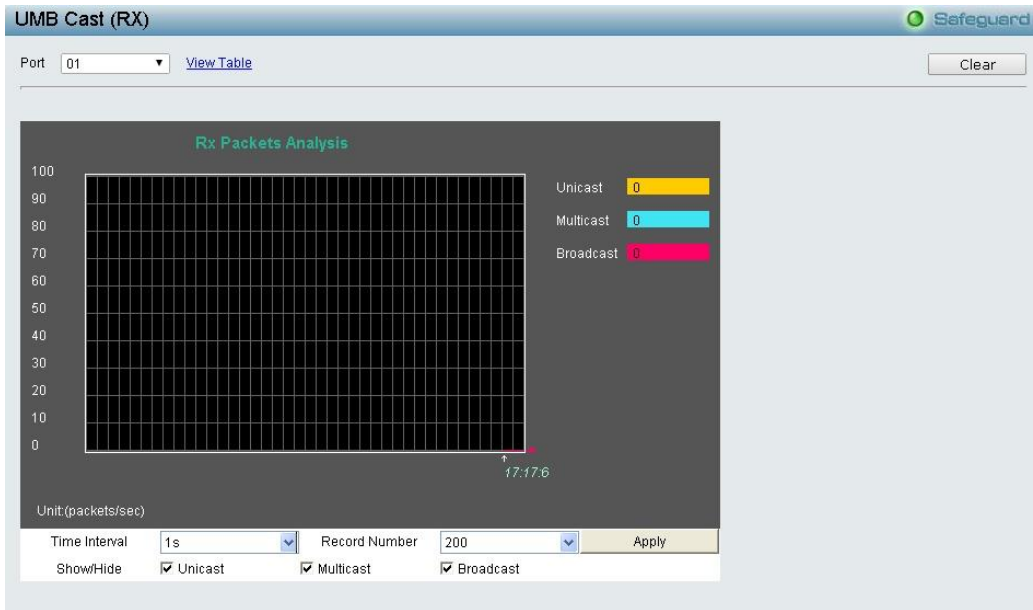


Figure 4.122 - Monitoring > Packets > UMB Cast (RX) (line graph for Unicast, Multicast and Broadcast Packets)

To view the **UMB Cast Table**, click the [View Table](#) link, which will show the following table:

Packet Analysis of Port: 1		
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 4.123 - 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 the 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: Click to clear all statistic counters on this window.

View Table: Click to display a table rather than a line graph.

View Line Chart: Click 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** drop-down menu. You may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

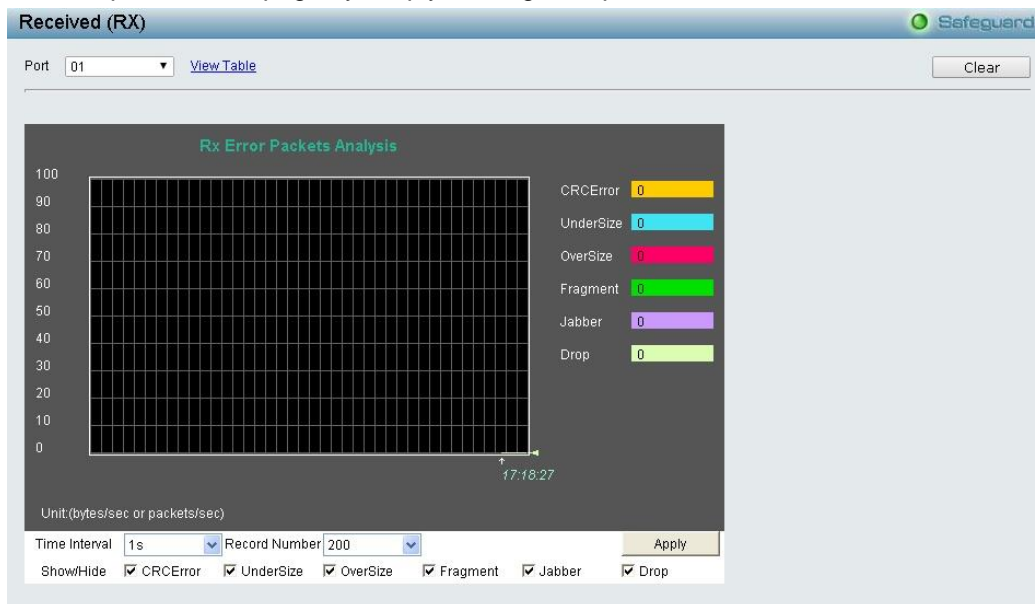


Figure4.124 - Monitoring > Errors > Received (RX) (line graph)

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

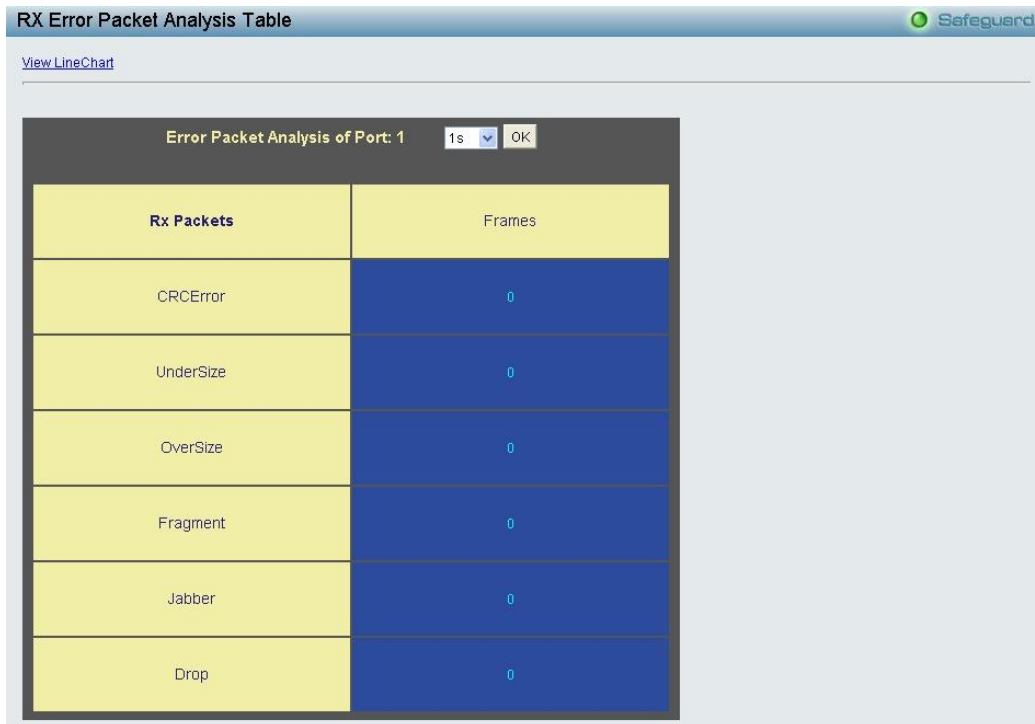


Figure 4.125 - Monitoring > Errors > Received (RX) (table)

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 the 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 than 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 than 1518 octets, or if a VLAN frame is 1522 octets, and less than 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: Click to clear all statistic counters on this window.

View Table: Click to display a table rather than a line graph.

View Line Chart: Click 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** drop-down menu. You may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

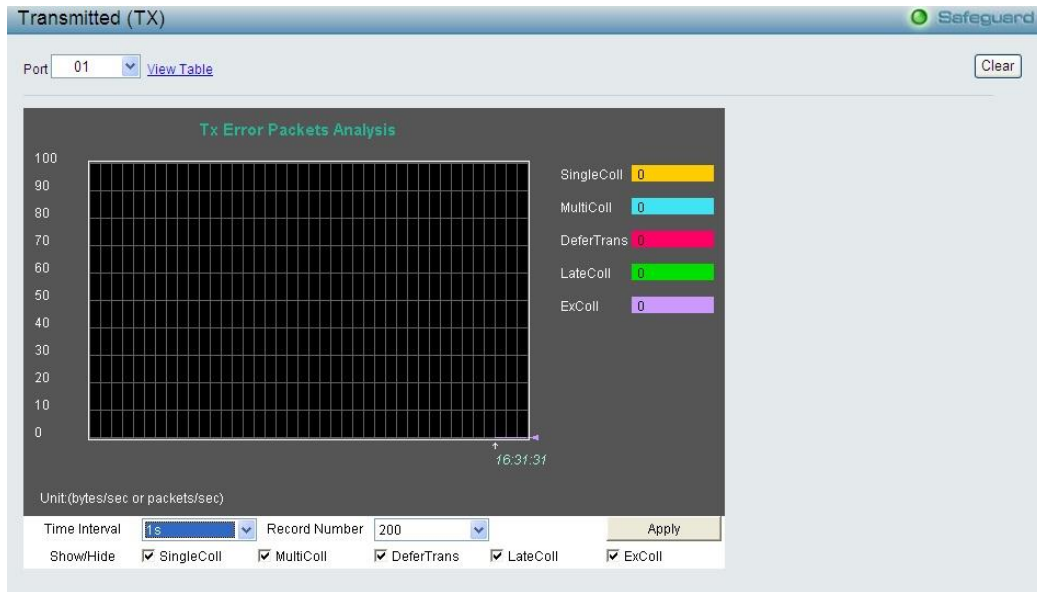


Figure 4.126 - Monitoring > Errors > Transmitted (TX) (line graph)

To view the **Transmitted Error Packets Table**, click the link [View Table](#), which will show the following table:

Tx Error	Frames
ExDefer	0
LateColl	0
ExColl	0
SingColl	0
Collision	0

Figure 4.127 - 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 the 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: Click to clear all statistic counters on this window.

View Table: Click to display a table rather than a line graph.

View Line Chart: Click 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 determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.

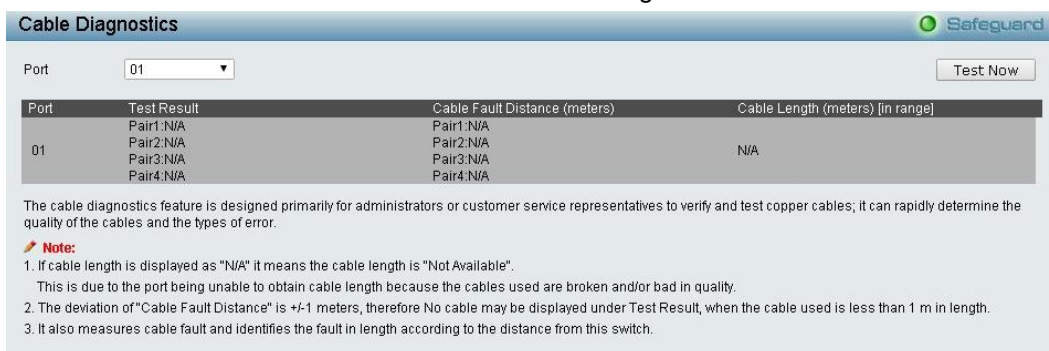


Figure 4.128 - Monitoring > Cable Diagnostics

Test Result: The description of the cable diagnostic results.

- **OK** means the cable has a good 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 an error 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 available on Gigabit ports.

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.



Figure 4.129 - 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 or click to delete 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 find a specific client, enter its IP address and select a type from the drop-down menu, click **Find**. To clear the ARP Table, click **Clear All**.

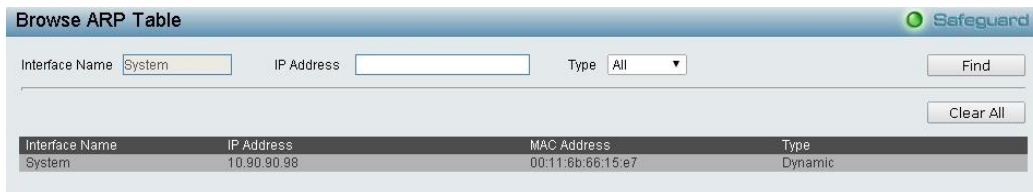


Figure 4.130 - Monitoring > Browse ARP Table

Interface Name: Displays the name of ARP mappings.

IP Address: Displays 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: Displays the ARP mapping ports.

Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

This window allows you 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:

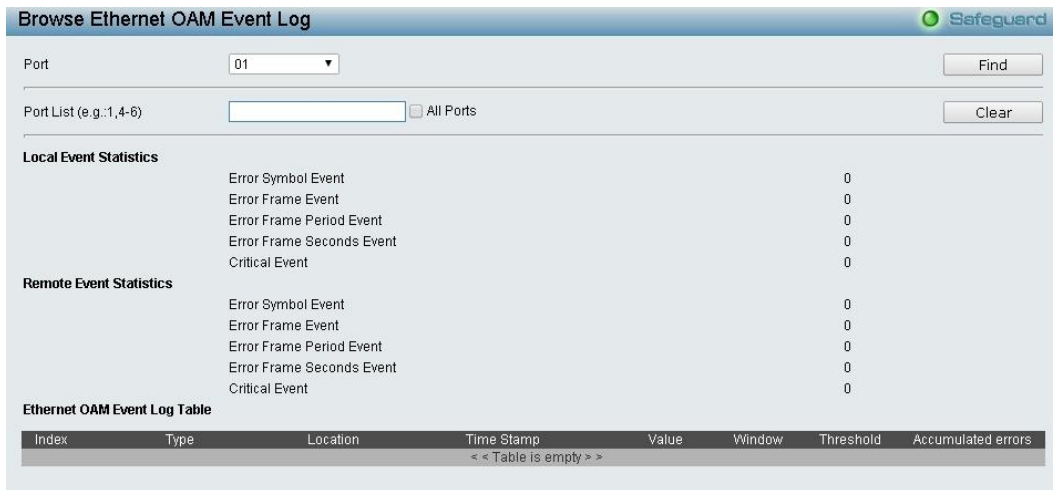


Figure 4.131 - Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

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

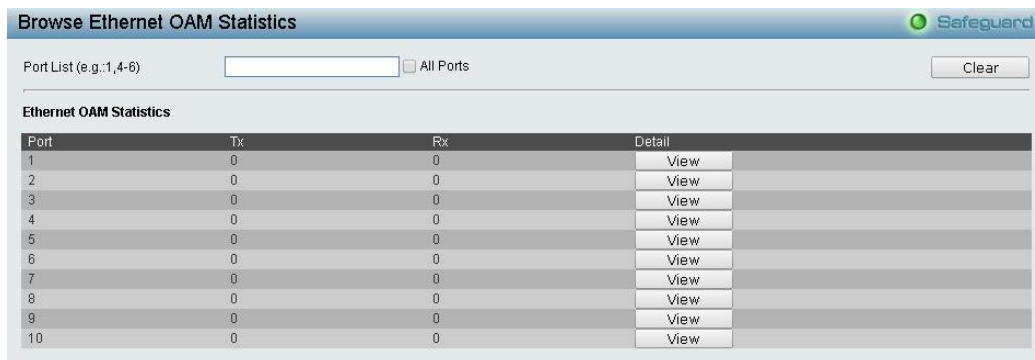


Figure 4.132 - Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

Enter a **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	Reqs
1	0	FutureNAS	0.0.0.0	0	0	0
2	0	FutureNAS	0.0.0.0	0	0	0
3	0	FutureNAS	0.0.0.0	0	0	0

Figure 4.133 - Monitoring > Port Access Control > RADIUS Authentication

You 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 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.

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 displays one row for each RADIUS authentication server that the client shares a secret with.

ServerIndex	InvalidServerAddr	Identifier	Server IP Addr	Server Port Number	Timeouts
1	0	FutureNAS	0.0.0.0	0	0
2	0	FutureNAS	0.0.0.0	0	0
3	0	FutureNAS	0.0.0.0	0	0

Figure 4.134 - Monitoring > Port Access Control > RADIUS Account Client

You 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 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.

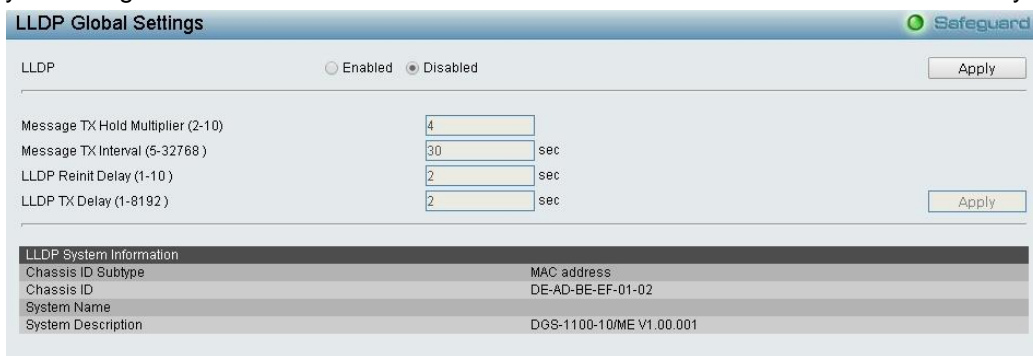


Figure 4.135 – LLDP > LLDP Global Settings

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: $1 < txDelay < (0.25 \times msgTxInterval)$. 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.

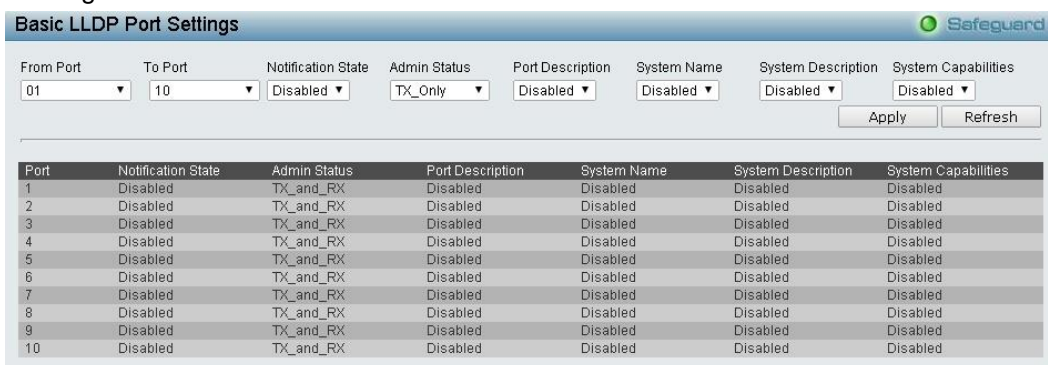


Figure 4.136– LLDP > Basic LLDP Port Settings

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.

Port	Port VLAN ID	VLAN	Protocol Identity
1	Disabled	1	(NONE)
2	Disabled	1	(NONE)
3	Disabled	1	(NONE)
4	Disabled	1	(NONE)
5	Disabled	1	(NONE)
6	Disabled	1	(NONE)
7	Disabled	1	(NONE)
8	Disabled	1	(NONE)
9	Disabled	1	(NONE)
10	Disabled	1	(NONE)

Figure 4.137 – 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.

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.

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.

Protocol Identity: Specifies the Protocol Identity to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the EAPOL.

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.

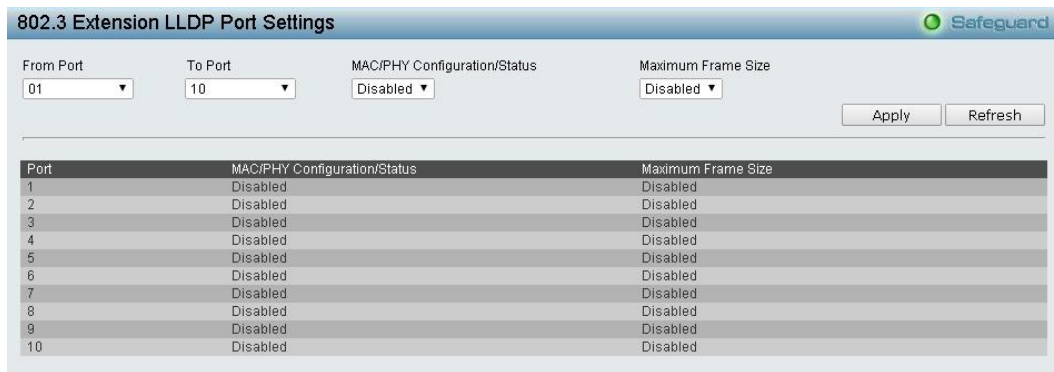


Figure4.138 – LLDP > 802.3 Extension LLDP Port Settings

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

MAC/PHY Configuration/Status: Select either **Enabled** or **Disabled**.

Maximum Frame Size: Select either **Enabled** or **Disabled**.

Once configured 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 you to set management address which is included in LLDP information transmitted.

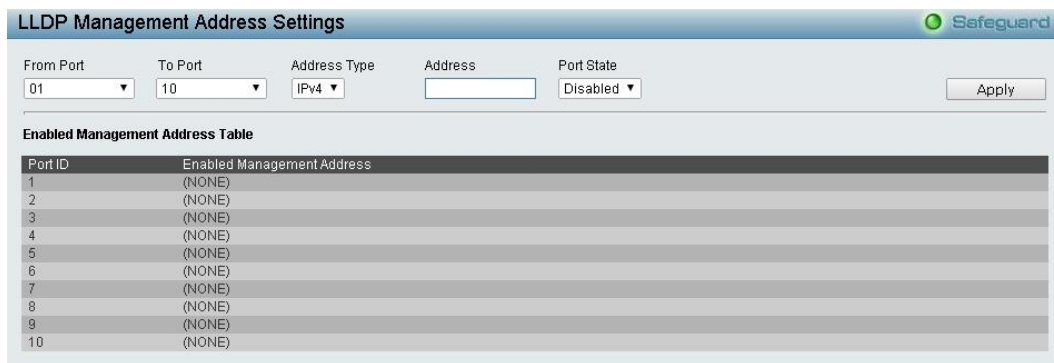


Figure4.139 – LLDP > LLDP Management Address Settings

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

Address Type: Specify the LLDP address type on the port. The value is always IPv4.

Address: Specify the address.

Port State: Select either **Enabled** or **Disabled**.

Click **Apply** to implement changes made.

LLDP > LLDP Statistics Table

The LLDP Statistics page displays an overview of all LLDP traffic.

LLDP Statistics Table

LLDP Statistics System

Last Change Time	0
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Age Out	0

LLDP Statistics Ports

No.	TxPort FramesTotal	RxPortFrames DiscardedTotal	RxPort FramesErrors	RxPort FramesTotal	RxPortTLVs DiscardedTotal	RxPortTLVs UnrecognizedTotal	RxPort AgeoutsTotal
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0

Figure 4.140 – 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 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 the table being 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 Find

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	

Figure 4.141 – LLDP > LLDP Management Address Table

Management Address: Select **IPv4 address** or **IPv6 address** and then enter the IP 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.

No.	Port ID Subtype	Port ID	Port Description	Normal	Detailed
1	Interface Alias	Fa0/1		View	View
2	Interface Alias	Fa0/2		View	View
3	Interface Alias	Fa0/3		View	View
4	Interface Alias	Fa0/4		View	View
5	Interface Alias	Fa0/5		View	View
6	Interface Alias	Fa0/6		View	View
7	Interface Alias	Fa0/7		View	View
8	Interface Alias	Fa0/8		View	View
9	Interface Alias	Fa0/9		View	View
10	Interface Alias	Fa0/10		View	View

Figure 4.142 –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.

No.	1
Port ID Subtype	Interface Alias
Port ID	Fa0/1
Port Description	
Port VID	1
Management Address Count	1
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	See detail
Maximum Frame Size	1522
Show LLDP Local Port Brief Table	
Show LLDP Local Port Detailed Table	

Figure 4.143 – 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 : Fa0/1
Port Description :
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
VLAN Name Entries Count : 1
Entry : 1
Vlan ID : 1
Vlan Name : default
Protocol Identity Entries Count : 0
(NONE)
MAC/PHY Configuration/Status :
Auto-negotiation Support : Not Supported
Auto-negotiation Enabled : Disabled
Auto-negotiation Advertised Capability : 0000(hex)
Auto-negotiation Operational MAU Type : 0000(hex)
Maximum Frame Size : 1522
Show LLDP Local Port Brief Table
Show LLDP Local Port Normal Table
    
```

Figure 4.144 – 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 the port number and click **Search** to display additional information.



Figure 4.145 – LLDP > LLDP Remote Port Table

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



Figure 4.146 – LLDP > LLDP Remote Port Normal Table

To view the detail settings for a remote port, click **View Detailed** and the following page is displayed.



Figure 4.147 – LLDP > LLDP Remote Port Detailed Table