D-Link
Building Networks for People

DGS-1210-28

Web UI Reference Guide
Web Smart Switch

Ver. 4.00

Table of Contents

Table of Contents i
About This Guide 1
Terms/Usage 1
Copyright and Trademarks 1
1 Product Introduction 2
DGS-1210-28 3
Front Panel 3
Rear Panel 3
2 Hardware Installation 4
Step 1: Unpacking 4
Step 2: Switch Installation 4
Desktop or Shelf Installation 4
Rack Installation 4
Step 3 : Plugging in the AC Power Cord with Power Cord Clip 5
Power Failure 8
3 Getting Started 9
Management Options 9
Using Web-based Management 9
Supported Web Browsers 9
Connecting to the Switch 9
Login Web-based Management 10
Smart Wizard 10
Web-based Management 10
D-Link Network Assistant (DNA) 10
4 Configuration 12
Smart Wizard Configuration 12
IP Information 12
Password 12
SNMP 13
Web-based Management 15
Tool Bar > Save Menu 16
Save Configuration 16
Save Log 16
Tool Bar > Tool Menu 16
Reset 16
Reset System 16
Reboot Device 16
Configuration Backup and Restore 17
Firmware Backup and Upgrade 17
Tool Bar > Smart Wizard 18
Tool Bar > Online Help 18
Function Tree 18
Device Information 19
System > System Settings 20
System > IPv6 System Settings 21
System > IPv6 Route Settings 21
System > IPv6 Neighbor Settings 22

System > Password 22
System > Port Settings 22
System > Port Description 23
System > DHCP Auto Configuration 24
System > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings 24
System > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings 25
System > DHCP Local Relay Settings 26
System > DHCPv6 Relay Settings 26
System > SysLog Host 27
System > Time Profile 27
System > Power Saving 28
System > IEEE802.3az EEE Settings 29
System > D-Link Discover Protocol Settings 29
VLAN > 802.1Q VLAN 29
VLAN > 802.1Q VLAN PVID 30
VLAN > 802.1Q Management VLAN 30
VLAN > Voice VLAN > Voice VLAN Global Settings 30
VLAN > Voice VLAN > Voice VLAN Port Settings 32
VLAN > Voice VLAN > Voice Device List 32
VLAN > Auto Surveillance VLAN Settings 33
L2 Functions > Jumbo Frame 34
L2 Functions > Port Mirroring 34
L2 Functions > Loopback Detection 34
L2 Functions > MAC Address Table > Static MAC 35
L2 Functions > MAC Address Table > Dynamic Forwarding Table 36
L2 Functions > Spanning Tree > STP Global Settings 36
L2 Functions > Spanning Tree > STP Port Settings 37
L2 Functions > Link Aggregation > Port Trunking 38
L2 Functions > Link Aggregation > LACP Port Settings 39
L2 Functions > Multicast > IGMP Snooping 39
L2 Functions > Multicast > MLD Snooping 41
L2 Functions > Multicast > Multicast Forwarding 42
L2 Functions > Multicast > Multicast Filtering Mode 43
L2 Functions > SNTP > Time Settings 43
L2 Functions > SNTP > TimeZone Settings 44
L2 Functions > LLDP > LLDP Global Settings 45
L2 Functions > LLDP > LLDP Port Settings 45
L2 Functions > LLDP > 802.1 Extension TLV 46
L2 Functions > LLDP > 802.3 Extension TLV 47
L2 Functions > LLDP > LLDP Management Address Settings 48
L2 Functions > LLDP > LLDP Management Address Table 48
L2 Functions > LLDP > LLDP Local Port Table 49
L2 Functions > LLDP > LLDP Remote Port Table 50
L2 Functions > LLDP > LLDP Statistics 51
QoS > Bandwidth Control 52
QoS > 802.1p/DSCP/ToS 53
Security > Trusted Host 54
Security > Port Security 54
Security > Traffic Segmentation 55

Security > Safeguard Engine 55
Security > Storm Control 56
Security > ARP Spoofing Prevention 56
Security > DHCP Server Screening 57
Security > SSL Settings 57
Security > DoS Prevention Settings 57
Security > SSH > SSH Settings 58
Security > SSH > SSH Authmode and Algorithm Settings 58
Security > SSH > SSH User Authentication Lists 59
Security > Smart Binding > Smart Binding Settings 60
Security > Smart Binding > Smart Binding 61
Security > Smart Binding > White List 61
Security > Smart Binding > Black List 61
AAA > RADIUS Server 62
AAA > 802.1X > 802.1X Global Settings 63
AAA > 802.1X > 802.1X Port Settings 63
AAA > 802.1X > 802.1X User 64
ACL > ACL Wizard 65
ACL > ACL Access List 72
ACL > ACL Access Group 73
ACL > ACL Hardware Resource Status 74
SNMP > SNMP > SNMP Global Settings 74
SNMP > SNMP > SNMP User 74
SNMP > SNMP > SNMP Group Table 75
SNMP > SNMP > SNMP View 76
SNMP > SNMP > SNMP Community 76
SNMP > SNMP > SNMP Host 76
SNMP > SNMP > SNMP Engine ID 77
SNMP > RMON > RMON Global Settings 77
SNMP > RMON > RMON Statistics 77
SNMP > RMON > RMON History 78
SNMP > RMON > RMON Alarm Settings 78
SNMP > RMON > RMON Event 79
Monitoring > Port Statistics 79
Monitoring > Cable Diagnostics 80
Monitoring > System Log 81
5 Command Line Interface 82
To connect a switch via TELNET: 82
Logging on to the Command Line Interface: 82
CLI Commands: 82
? 83
download 83
upload 84
config ipif system 85
config ipif system 86
logout 86
ping 87
ping6 87
create iproute 88

delete iproute 88
show iproute 88
reboot 89
reset config 89
show ipif 90
show switch 90
config account admin password 91
save 91
debug info 92
Appendix A - Ethernet Technology 93
Gigabit Ethernet Technology 93
Fast Ethernet Technology 93
Switching Technology 93
Appendix B - Technical Specifications 94
Hardware Specifications 94
Key Components / Performance 94
Port Functions 94
Physical & Environment 94
Emission (EMI) Certifications 94
Safety Certifications 94
Features 94
L2 Features 94
VLAN 94
QoS (Quality of Service) 94
Security 95
OAM 95
Management 95
D-Link Green Technology 95
Appendix C – Rack mount Instructions 96

About This Guide

This guide provides instructions to install the D-Link Gigabit Web Smart Switch DGS-1210-28, and to configure Web-based Management step-by-step.

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

This guide is mainly divided into four parts:

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

Terms/Usage

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

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

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

Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2013 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

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

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

Product Introduction

Thank you and congratulations on your purchase of D-Link Web Smart Switch Products.

D-Link's next generation Web Smart Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provides advanced features including network security, traffic segmentation, QoS and versatile management.

Flexible Port Configurations. The DGS-1210-28 is the new generation of Web Smart series. It provides a variety of port counts 24 10/100/1000Mbps ports plus 4 SFP ports.

D-Link Green Technology. D-Link Green devices are about providing eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DGS-1210-28 such as shutting down a port, or turning off some LED indicators, or adjusting the power usage according to the Ethernet cable connected to it.

Extensive Layer 2 Features. Implemented as complete L2 devices, these switches include functions such as IGMP snooping, port mirroring, Spanning Tree, 802.3ad LACP and Loopback Detection to enhance performance and network resiliency.

Traffic Segmentation, QoS and Auto Surveillance VLAN. The switches support 802.1Q VLAN standard tagging to enhance network security and performance. The switches also support 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802.1p traffic in the network. Auto Surveillance VLAN will automatically place the vedio traffic from pre-defined IP surveillance devices to an assigned VLAN with higher priority, so it can be separated from normal data traffic. Asymmetric VLAN is implemented in these switches for a more efficient use of shared resources, such as server or gateway devices.

Network Security. D-Link’s innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features like 802.1X port-based authentication provide access control of the network with external RADIUS servers. ACL is a powerful tool to screen unwanted IP or MAC traffic. Storm Control can help to keep the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the network device integrity.

Versatile Management. The new generation of D-Link Web Smart Switches provides growing businesses with a simple and easy management of their network, using an intuitive SmartConsole utility or a Web-Based management interface that allows administrators to remotely control their network down to the port level. The SmartConsole easily allows customers to discover multiple D-Link web smart switches with the same L2 network segment connected to the user’s local PC. With this utility, users do not need to change the IP address of the PC and provide easy initial settings of the smart switches. The switches within the same L2 network segment connected to the user’s local PC are displayed on the screen for instant access. It allows extensive switch configuration settings, and basic configuration of discovered devices, such as a password change or firmware upgrade.

Users can also access the switch via TELNET. Some basic tasks can be performed such as changing the Switch IP address, resetting the settings to factory defaults, setting the administrator password, rebooting the Switch, or upgrading the Switch firmware by using the Command Line Interface (CLI).

In addition, users can utilize the SNMP MIB (*Management Information Base*) to poll the switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate the switches with other third-party devices for management in an SNMP-enabled environment. D-Link Web Smart Switches also come with the D-View plug-in module that works with D-View 6 SNMP Management Software, and provides easy-to-use graphic interface and facilitates the operation efficiency.

DGS-1210-28

24-Port 10/100/1000Mbps plus 4 SFP Slot Web Smart Switch.

Front Panel

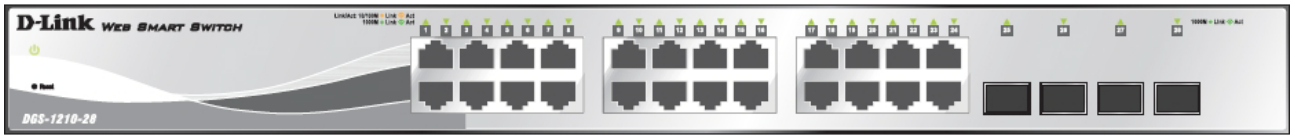


Figure 1.1 – DGS-1210-28 Front Panel

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

Port Link/Act/Speed LED (1-24): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.

Port Link/Act/Speed LED (25F, 26F, 27F, 28F): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an green light, this indicates that the port is running on 1000M.

Reset: Press the Reset button for 5 seconds to reset the Switch back to the default settings. All previous changes will be lost.

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

Rear Panel

Figure 1.2 – DGS-1210-28 Rear Panel

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

Hardware Installation

This chapter provides unpacking and installation information for the D-Link Web-Smart Switch.

Step 1: Unpacking

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

- One D-Link Web-Smart Switch
- One AC power cord
- Four rubber feet
- Screws and two mounting brackets
- One Multi-lingual Getting Started Guide
- One CD with User Manual, D-Link Network Assistant (DNA) Utility program, D-Link Network Assistant User Guide and D-View Module

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

Step 2: Switch Installation

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

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

Desktop or Shelf Installation

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

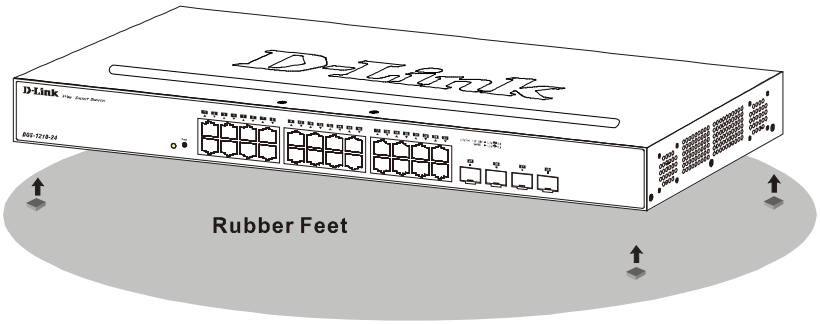


Figure 2.1 – Attach the adhesive rubber pads to the bottom

Rack Installation

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

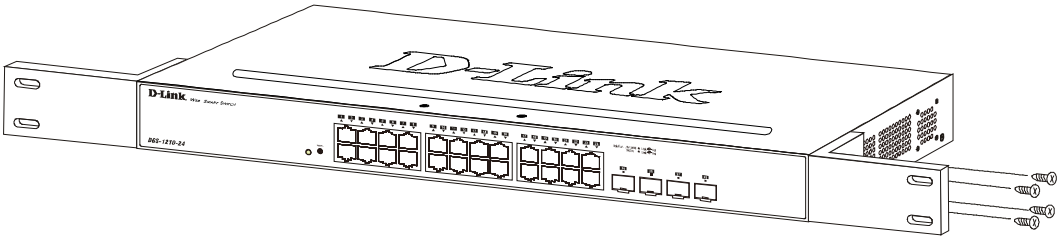


Figure 2.2 – Attach the mounting brackets to the Switch

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

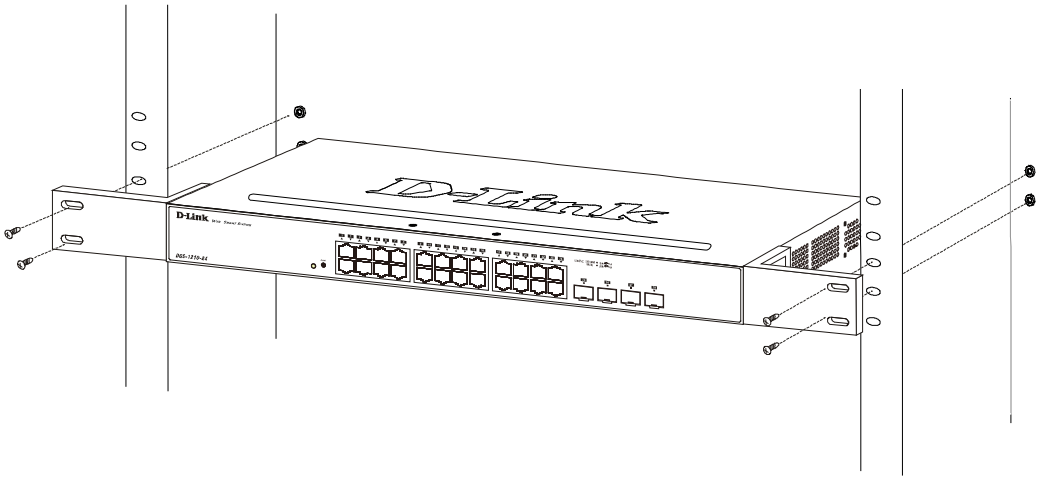


Figure 2.3 – Mount the Switch in the rack or chassis

Please be aware of following safety Instructions when installing:

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

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

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

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

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

Step 3 : Plugging in the AC Power Cord with Power Cord Clip

To prevent accidental removal of the AC power cord, it is recommended to install the power cord clip together with the power cord.

A) With the rough side facing down, insert the Tie Wrap into the hole below the power socket.

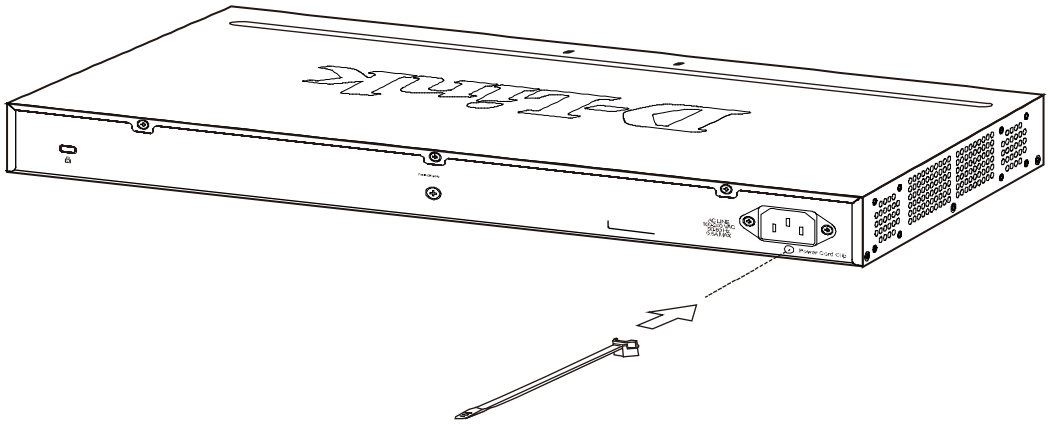


Figure2.4 – Insert Tie Wrap to the Switch

B) Plug the AC power cord into the power socket of the Switch.

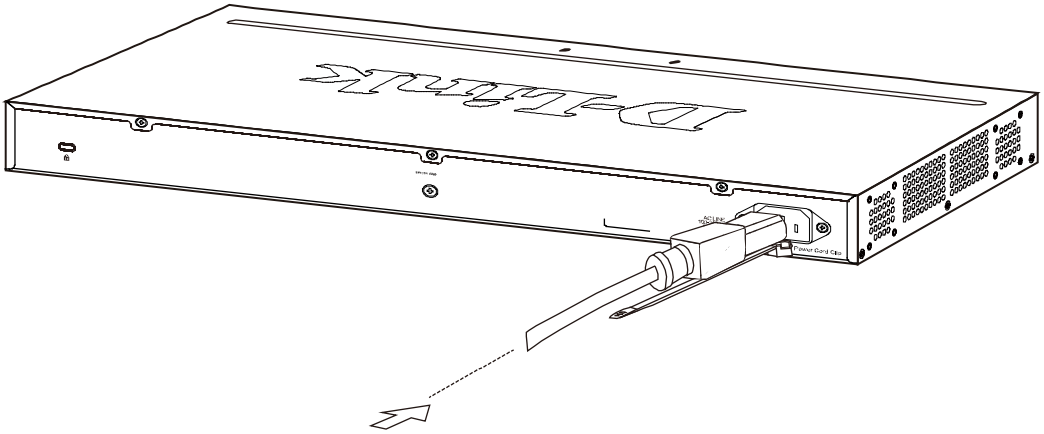


Figure 2.5 – Connect the power cord to the Switch

C) Slide the Retainer through the Tie Wrap until the end of the cord.

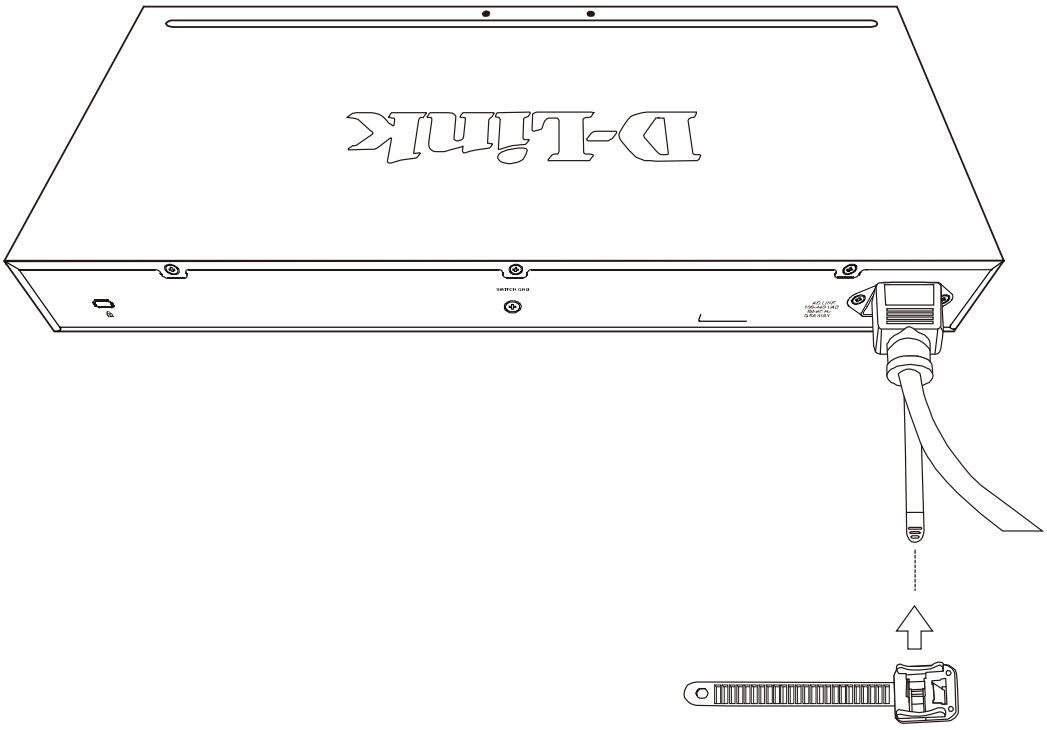


Figure 2.6 – Slide the Retainer through the Tie Wrap

D) Circle the tie of the Retainer around the power cord and into the locker of the Retainer.

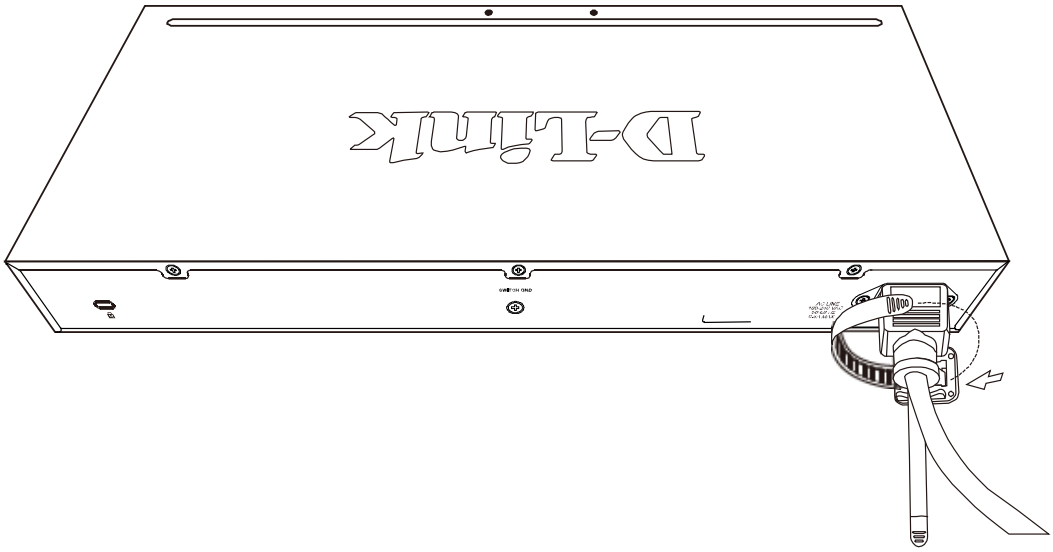


Figure 2.7 – Circle around the power cord

E) Fasten the tie of the Retainer until the power cord is secured.

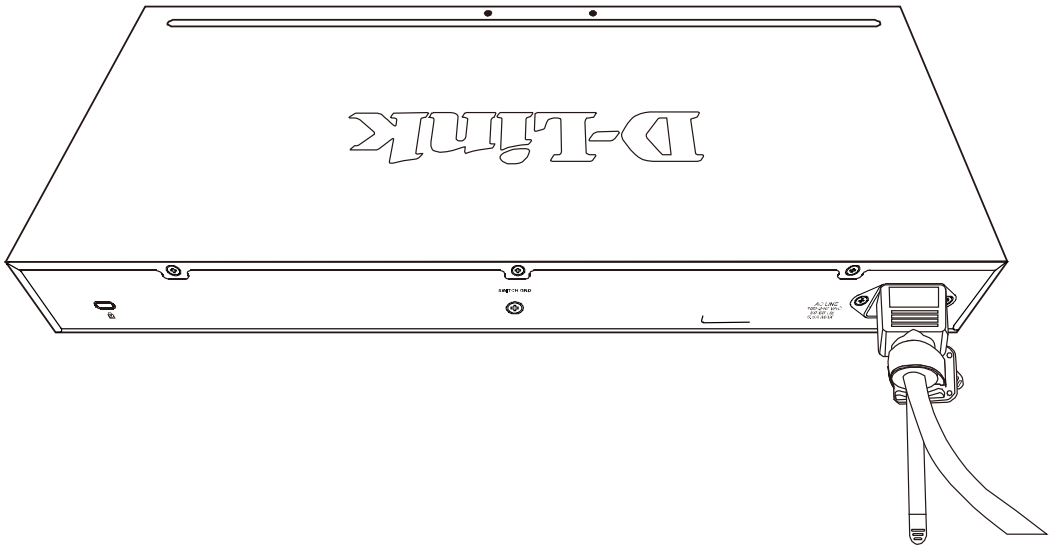


Figure 2.8 – Secure the power cord

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

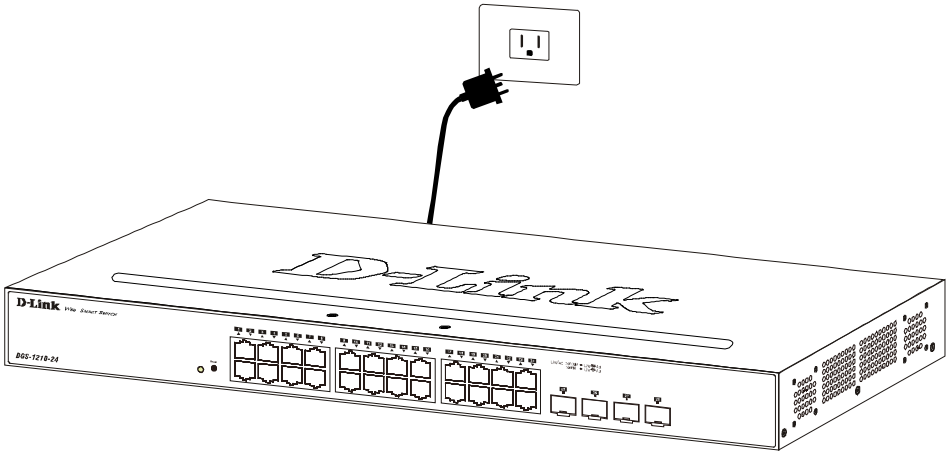


Figure 2.9 – Plugging the switch into an outlet

Power Failure

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

Getting Started

This chapter introduces the management interface of D-Link Web-Smart Switch.

Management Options

The D-Link Web Smart Switch can be managed through any port on the device by using the Web-based Management, or through any PC using the D-Link Network Assistant (DNA).

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

However, if you want to manage multiple D-Link Web Smart Switches, the D-Link Network Assistant (DNA) is a more convenient choice. By using the D-Link Network Assistant (DNA), you do not need to change the IP address of your PC and it is easier to initialize multiple Smart Switches.

Please refer to the following installation instructions for the Web-based Management and the D-Link Network Assistant (DNA).

Using Web-based Management

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

Supported Web Browsers

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

- Internet Explorer 6 or later version
- Netscape 8 or later version
- Firefox 3.0 or later version
- Chrome 5.0 or later version
- Safari 4.0 or later version
- Opera 10 or later version
- Mozilla the latest version

Connecting to the Switch

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

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

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

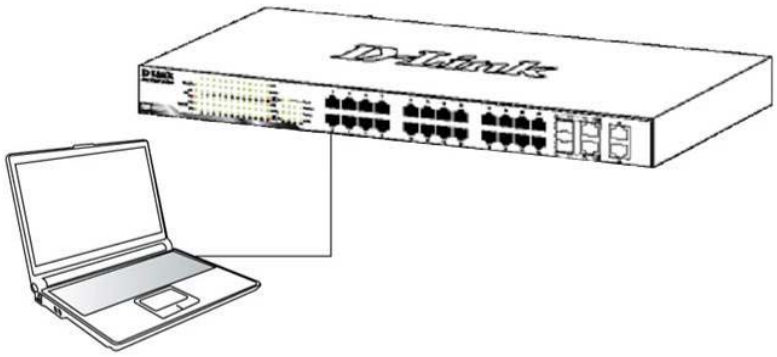


Figure 3.1 – Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management, you may either click the Web Access button at the top of the SmartConsole Utility or open the web browser and enter **10.90.90.90** (the factory-default IP address) in the address bar. Then press <Enter>.

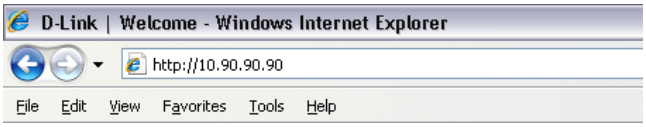


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser

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

The web configuration can also be accessed through the SmartConsole Utility. Open the SmartConsole Utility and double-click the switch as it appears in the Monitor List. This will automatically load the web configuration in your web browser.

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

The switch supports 10 languages including English, Traditional Chinese, Simplified Chinese, German, Spanish, French, Italian, Portuguese, Japanese and Russian. By default, the password is **admin** and the language is **English**.

Figure 3.3 – Logon Dialog Box

Smart Wizard

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

Web-based Management

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface. Please refer to Chapter 3 Configuration for detailed instructions.

D-Link Network Assistant (DNA)

The D-Link Network Assistant (DNA), included in the installation CD, is a program that allows administrators to quickly discover all D-Link smart switches and D-Link Discover Protocol (DDP) supported devices (for a list of supported models, refer to the *D-Link Network Assistant (DNA) User Guide*), that are in the same subnet as the PC, collect traps and log messages, and provide quick access to basic configurations of the switch. This tool is only for computers running Windows 7, Vista, XP, or 2000 on both 32/64bit systems. There are two options for the installation of the DNA; one is through the Autorun program on the installation CD and the other is manual installation.

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

For detailed explanations of the DNA functions, please refer to *D-Link Network Assistant (DNA) User Guide*.

Configuration

The features and functions of the D-Link Web Smart Switch can be configured for optimum use through the Web-based Management Utility.

Smart Wizard Configuration

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link Web Smart Switch. If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Ignore the Wizard next time** for the next time you logon to the Web-based Management.

IP Information

IP Information will guide you to do basic configurations in 3 steps for the IP Information, access password, and SNMP. Select **Static**, **DHCP** or **BOOTP**, and enter the desired new **IP Address**, select the **Netmask** and enter the **Gateway** address, then click the **Next** button to enter the next Password setting page. (No need to enter IP Address, Netmask and Gateway if DHCP and BOOTP are selected.) The Smart Wizard is for the quick setting in IPv4 environment. For IPv6 network, please go to System > IPv6 System Settings. If you are not changing the settings, click **Exit** button to go back to the main page. Or you can click on **Ignore the wizard next time** to skip wizard setting when the switch boots up.

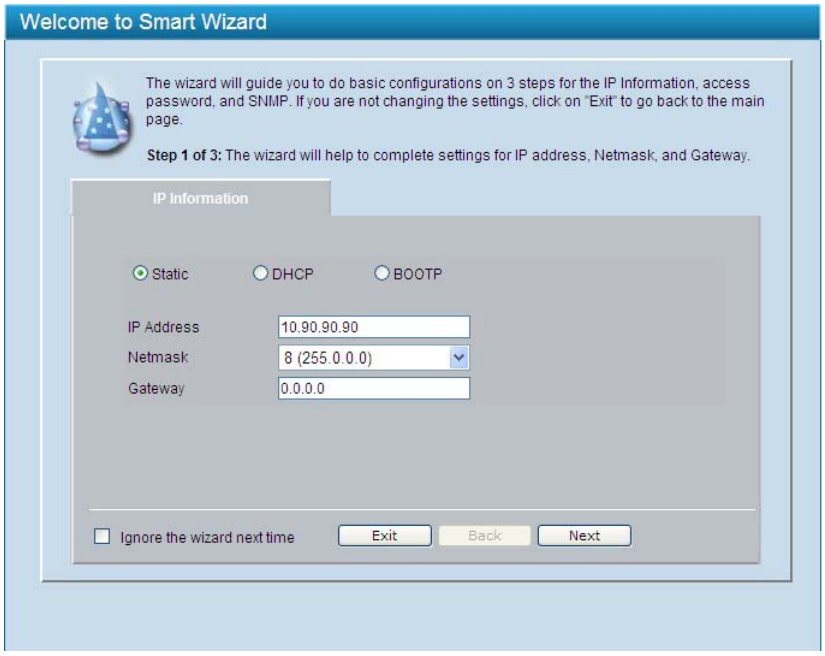


Figure 4.1 – IP Information in Smart Wizard

NOTE: The Smart Wizard supports quick settings for IPv4 network.

Password

Type the desired new password in the **Password** box and again in the **Confirm Password,** then click the **Next** button to the **SNMP** setting page.

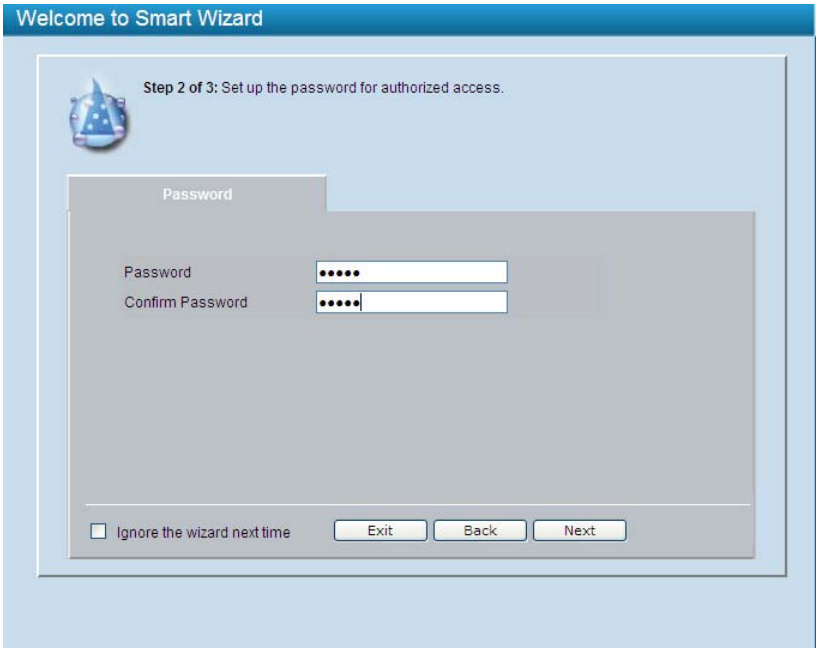


Figure 4.2 – Password in Smart Wizard

SNMP

The SNMP Setting allows you to quickly enable/disable the SNMP function. The default SNMP Setting is Disabled. Click **Enabled** and then click **Apply** to make it effective.

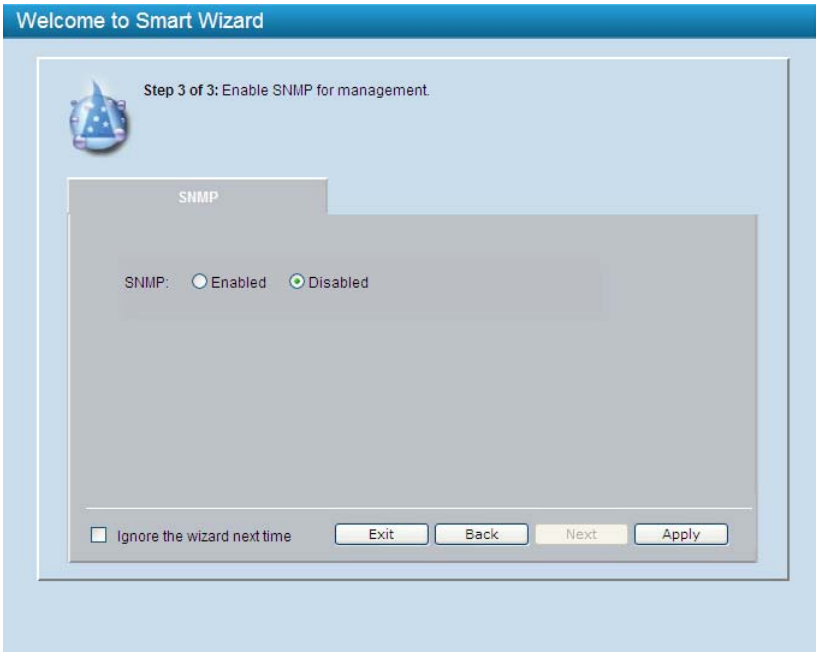


Figure 4.3 – SNMP in Smart Wizard

NOTE: Changing the system IP address will disconnect you from the current connection. Please enter the correct IP address in the Web browser again and make sure your PC is in the same subnet with the switch. See Login Web-based Management for a detailed description.

If you want to change the settings, click **OK** and start a new web browser.

Figure 4.4 – Confirm the changes of IP address in Smart Wizard

Web-based Management

After clicking the **Exit** button in Smart Wizard you will see the screen below:

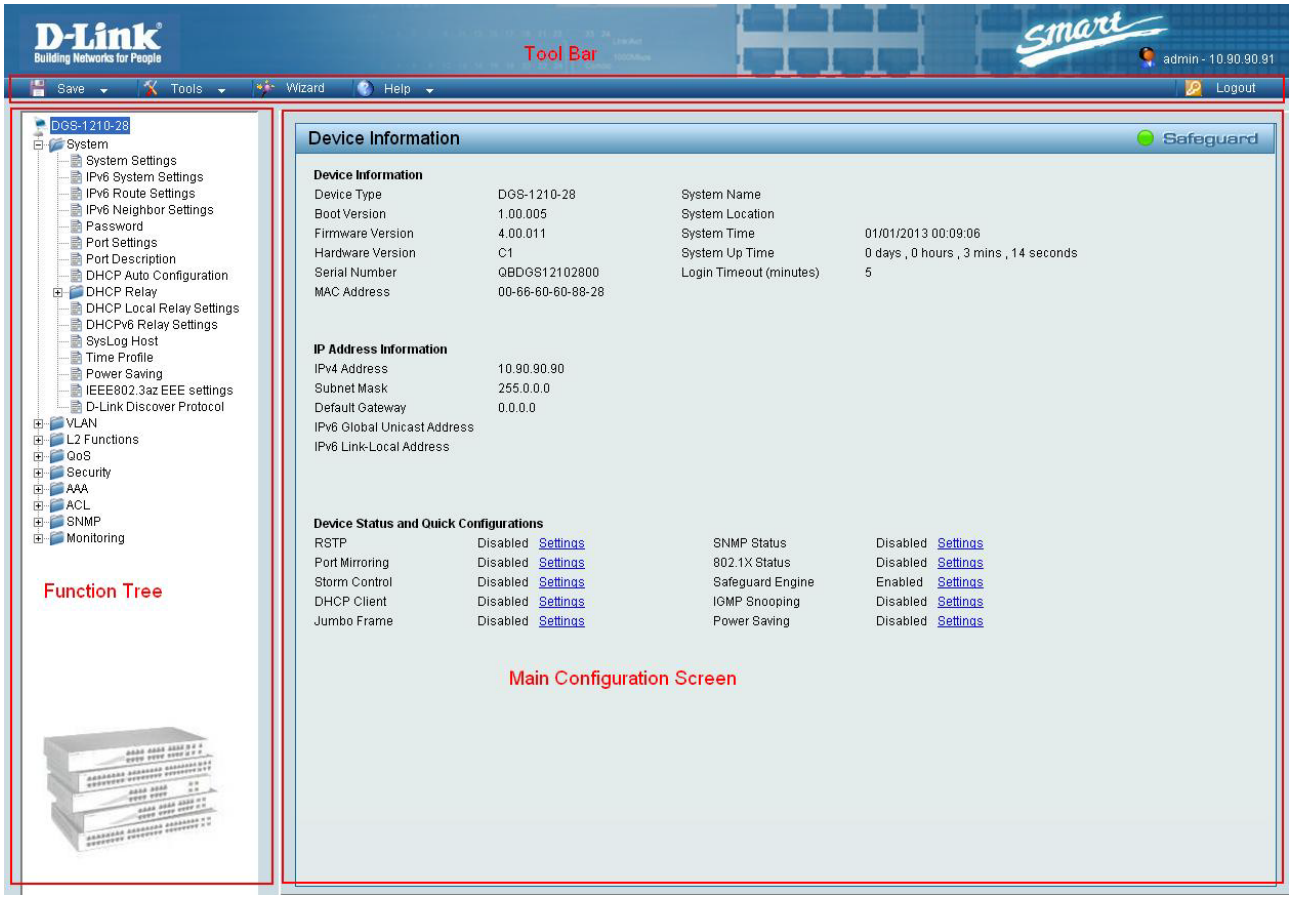


Figure 4.5 – Web-based Management

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

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

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

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

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

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

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

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

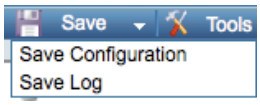


Figure 4.6 – Save Menu

Save Configuration

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

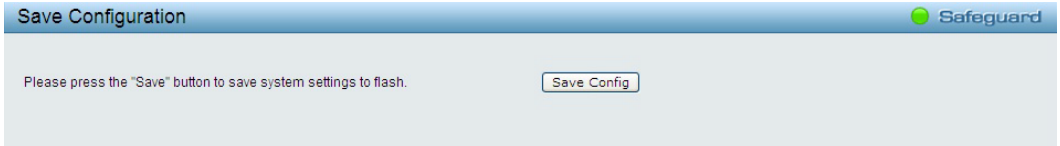


Figure 4.7 – Save Configuration

Save Log

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

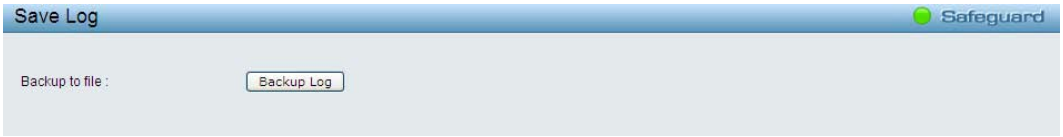


Figure 4.8 – Save Log

Tool Bar > Tool Menu

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

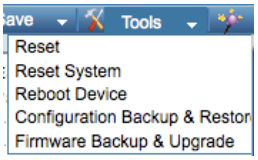


Figure 4.9 – Tool Menu

Reset

Provide a safe reset option for the Switch. All configuration settings in non-volatile RAM will be reset to factory default except for the IP address.

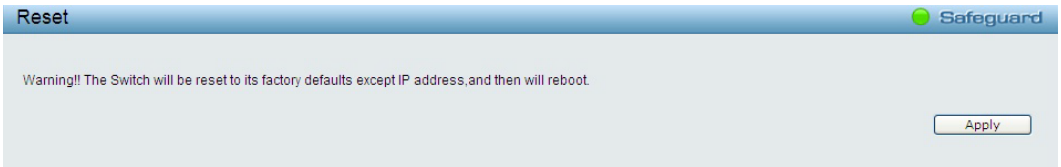


Figure 4.10 – Tool Menu > Reset

Reset System

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

Figure 4.11 – Tool Menu > Reset System

Reboot Device

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

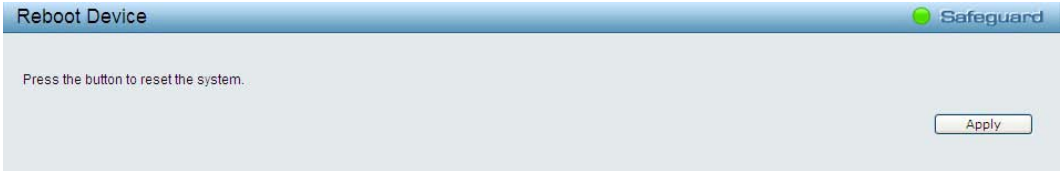


Figure 4.12 – Tool Menu > Reboot Device

Configuration Backup and 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**.

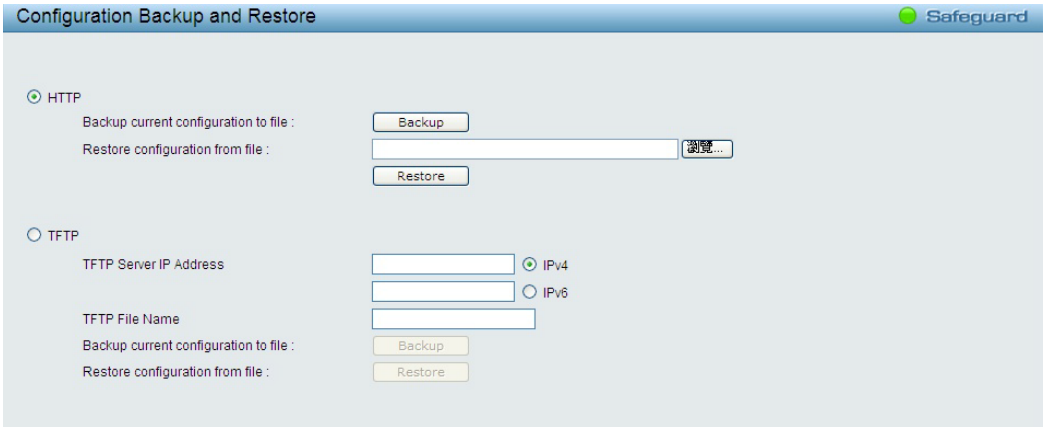


Figure 4.13 – Tool Menu > Configure Backup and Restore

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

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

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

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

TFTP: TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows you to transfer files to a remote TFTP server. Specify **TFTP Server IP Address** with 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 settings to the TFTP server.

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

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

Firmware Backup and 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**.

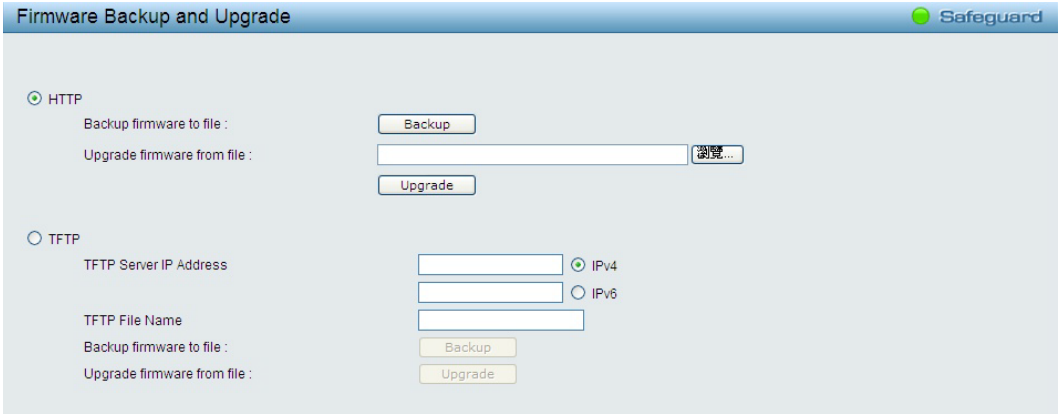


Figure 4.14 – Tool Menu > Firmware Backup and Upload

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

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

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

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

TFTP: Backup or upgrade the firmware to or from a remote TFTP server. Specify **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the configuration file you want to save to / restore from.

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 > Smart Wizard

By clicking the Smart Wizard button, you can return to the Smart Wizard if you wish to make any changes there.

Tool Bar > Online Help

The Online Help provides two ways of online support: **D-Link Support Site** will lead you to the D-Link website where you can find online resources such as updated firmware images; **User Guide** can offer an immediate reference for the feature definition or configuration guide.

Figure 4.15 – Online Help

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.

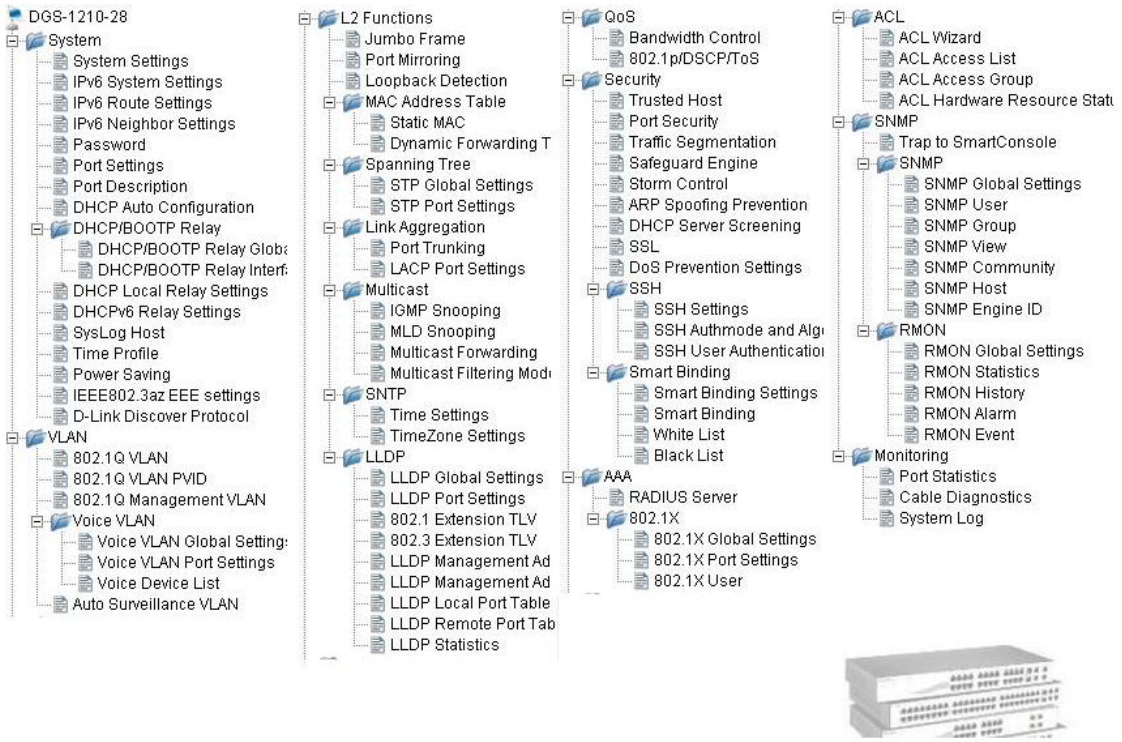


Figure 4.16 –Function Tree

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:

RSTP: Click **Settings** to link to L2 Functions > Spanning Tree > STP Global Settings. Default is disabled.

Port Mirroring: Click **Settings** to link to L2 Functions > Port Mirroring. Default is disabled.

Storm Control: Click **Settings** to link to Security > Storm Control. Default is disabled.

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

Jumbo Frame: Click **Settings** to link to L2 Functions > Jumbo Frame. Default is disabled.

SNMP Status: Click **Settings** to link to SNMP > SNMP > SNMP Global Settings. Default is disabled.

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

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

IGMP Snooping: Click **Settings** to link to L2 Functions > Multicast > IGMP Snooping. Default is disabled.

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

Figure 4.17 – Device Information

System > System Settings

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

Figure 4.18 – System > System Settings

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

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

DHCP Option 12 State: Speicfy the DHCP option 12 state is enabled or disabled.

DHCP Option 12 Host Name: Specify the host name for DHCP.

System Information: By entering a **System Name** and **System Location**, the device can more easily be recognized through the SmartConsole Utility and from other Web-Smart devices on the LAN.

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

System > IPv6 System Settings

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

Figure 4.19 – System > IPv6 System Settings

IPv6 System Settings:

Interface Name: Displays the interface name of IPv6.

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

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

IPv6 Network Address: Specifies the IPv6 Network Address.

NS Retransmit Time Settings:

NS Retransmit Time (1-3600): Specifies the NS retransmit time for IPv6. The field range is 1-3600, and default is 1 second.

Automatic Link Local State Settings:

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

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

System > IPv6 Route Settings

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

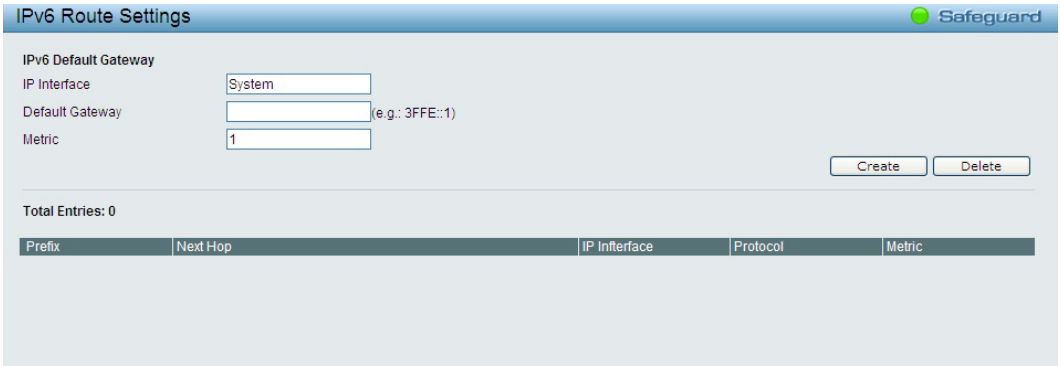


Figure 4.20 – System > IPv6 Route Settings

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

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

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

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

System > IPv6 Neighbor Settings

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

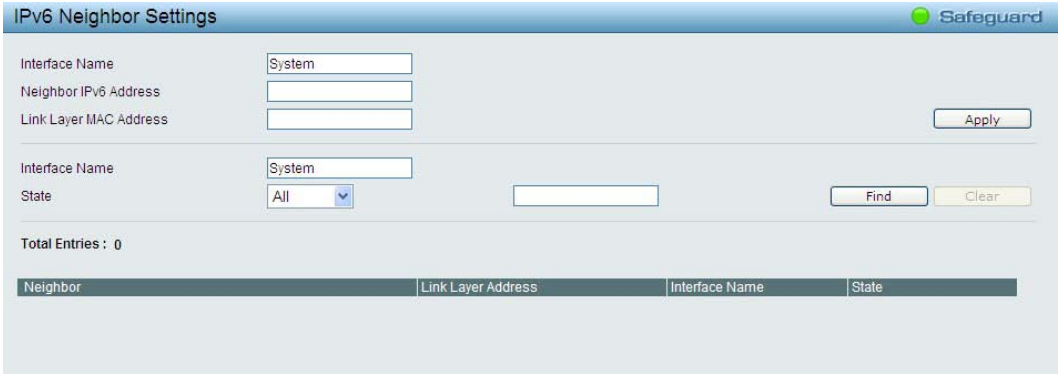


Figure 4.21 – System > IPv6 Neighbor Settings

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

Neighbor IPv6 Address: Specifies the neighbor IPv6 address.

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

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

Interface Name: Specifies the interface name of the IPv6 neighbor. To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window.

State: Select and enter the neighbor IPv6 state here. Options to choose from are *All*, *Address*, *Static*, and *Dynamic*. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

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

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

System > Password

Setting a password is a critical tool for managers to secure the Web-Smart Switch. After entering the old password and the new password twice, click **Apply** for the changes to take effect.

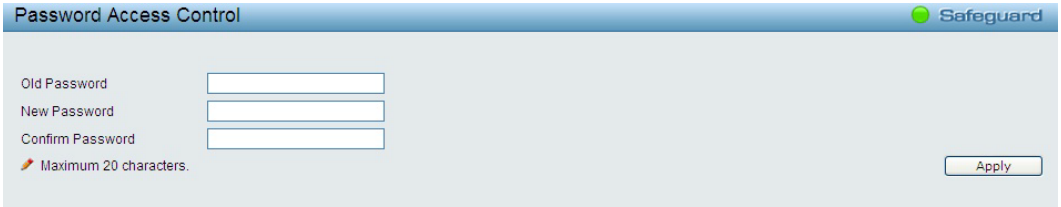
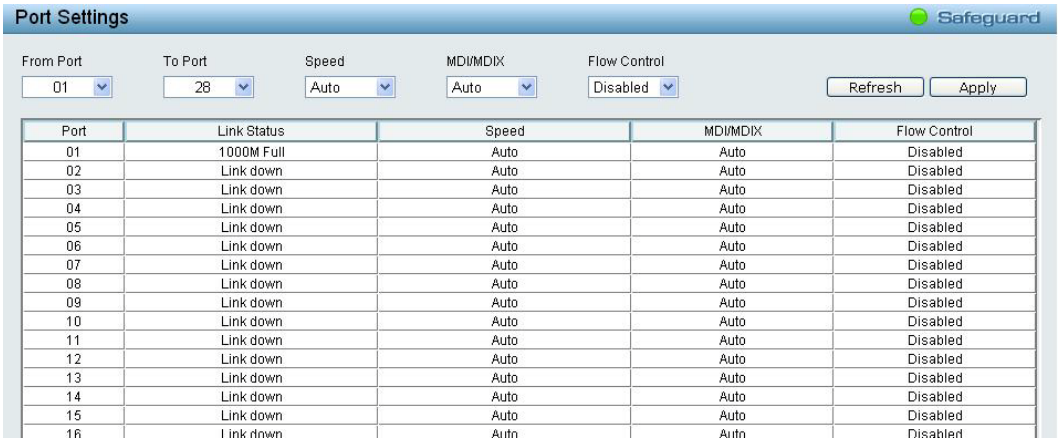


Figure 4.22 – System > Password Access Control

System > Port Settings

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



Port	Link Status	Speed	MDI/MDIX	Flow Control
01	1000M Full	Auto	Auto	Disabled
02	Link down	Auto	Auto	Disabled
03	Link down	Auto	Auto	Disabled
04	Link down	Auto	Auto	Disabled
05	Link down	Auto	Auto	Disabled
06	Link down	Auto	Auto	Disabled
07	Link down	Auto	Auto	Disabled
08	Link down	Auto	Auto	Disabled
09	Link down	Auto	Auto	Disabled
10	Link down	Auto	Auto	Disabled
11	Link down	Auto	Auto	Disabled
12	Link down	Auto	Auto	Disabled
13	Link down	Auto	Auto	Disabled
14	Link down	Auto	Auto	Disabled
15	Link down	Auto	Auto	Disabled
16	Link down	Auto	Auto	Disabled

Figure 4.23 – System > Port Settings

Speed: Gigabit Fiber connections can operate in 1000M Auto or Disabled. Copper connections can operate in Forced Mode settings (1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto, 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.

NOTE: All ports do not support MDI/MDI-X function when the speed links to 1000M force mode.

MDI/MDIX:

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

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

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

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

Link Status: Reporting **Down** indicates the port is disconnected.

System > Port Description

Port description can be given on this page.

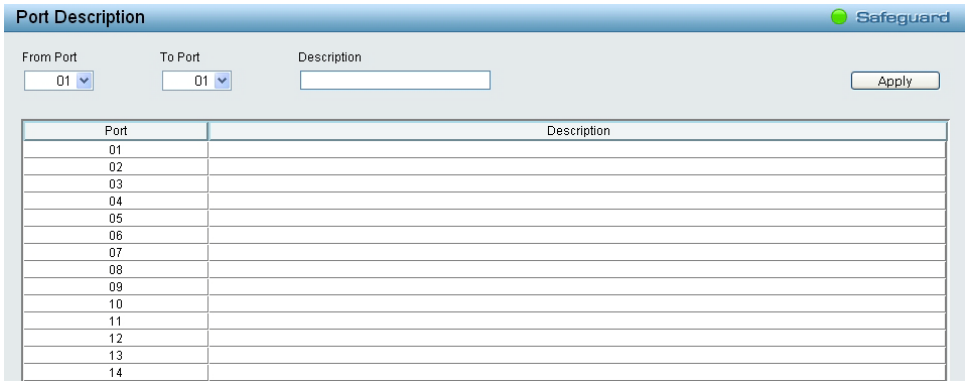


Figure 4.24 – System > Port Description

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

Description: Specify the description of ports.

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

System > DHCP Auto Configuration

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

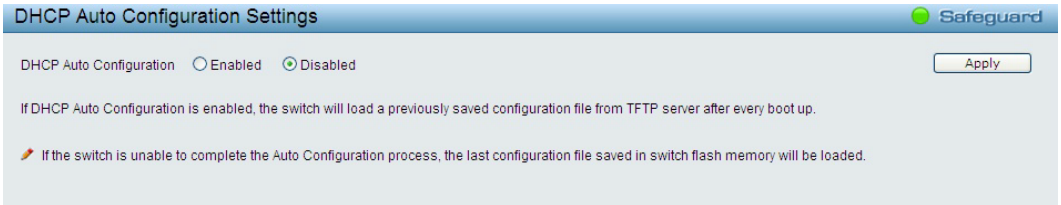


Figure 4.25 – System > DHCP Auto Configuration

System > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings

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

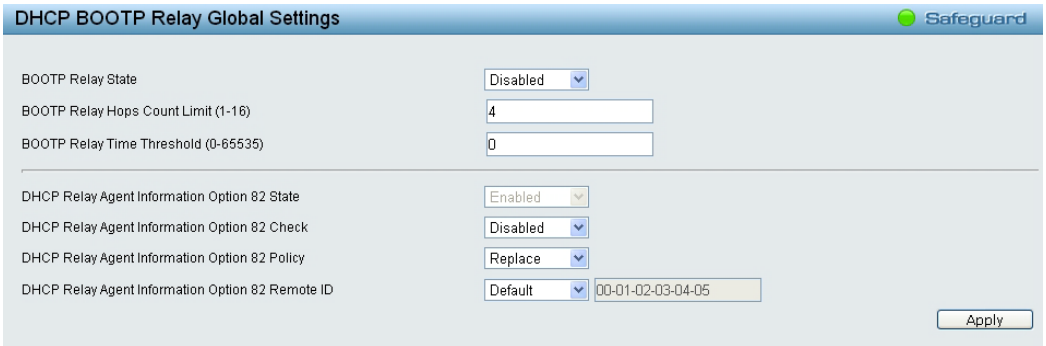


Figure 4.26 – System > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings

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

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

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

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

Enabled – When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

Disabled - If the field is toggled to Disabled the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.

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

Enabled – When the field is toggled to Enabled, the relay agent will check the validity of the packet's option 82 fields. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.

Disabled - When the field is toggled to Disabled, the relay agent will not check the validity of the packet's option 82 fields.

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

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

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

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

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

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

System > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

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

Figure 4.27 – System > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

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

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

Click **Apply** to implement changes made.

System > DHCP Local Relay Settings

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

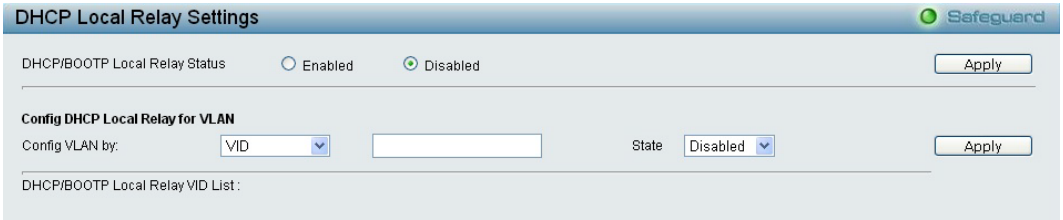


Figure 4.28 - System > DHCP Local Relay Settings

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

Enabled – Enables DHCP Local Relay on the device.

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

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

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

Enabled – Enables DHCP Local Relay on the VLAN.

Disabled – Disables DHCP Local Relay on the VLAN.

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

Click **Apply** to implement changes made.

System > DHCPv6 Relay Settings

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

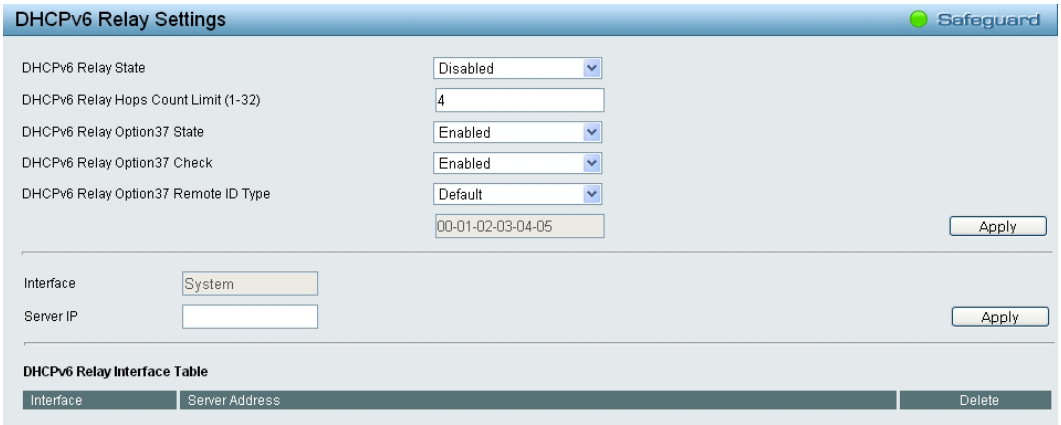


Figure 4.29 - System > DHCPv6 Relay Settings

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

Enabled – Enables DHCPv6 Relay on the device.

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

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

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

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

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

Interface: Enter a name of the interface.

Server IP: Enter the server IP address.

Click **Apply** to implement changes made.

System > SysLog Host

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

Figure 4.30 – System > SysLog Host Settings

Server IP Address: Select IPv4 or IPv6 then specify the IP address of the system log server.

UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is 1 – 65535, and the default value is 514.

Time Stamp: Select Enable to time stamp log messages.

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

Warning - The lowest level of a device warning. The device is functioning, but an operational problem has occurred.

Informational - Provides device information.

All - Displays all levels of system logs.

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

System > Time Profile

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

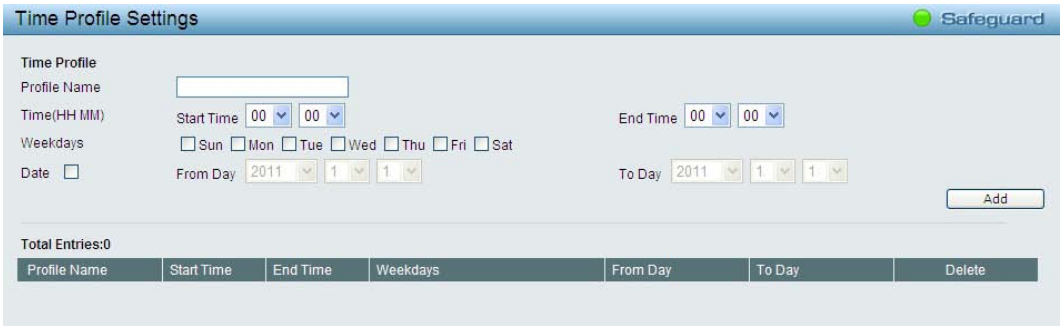


Figure 4.31 – System > Time Profile

Profile Name: Specifies the profile name.

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

Weekdays: Specifies the work day.

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

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

System > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off.

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

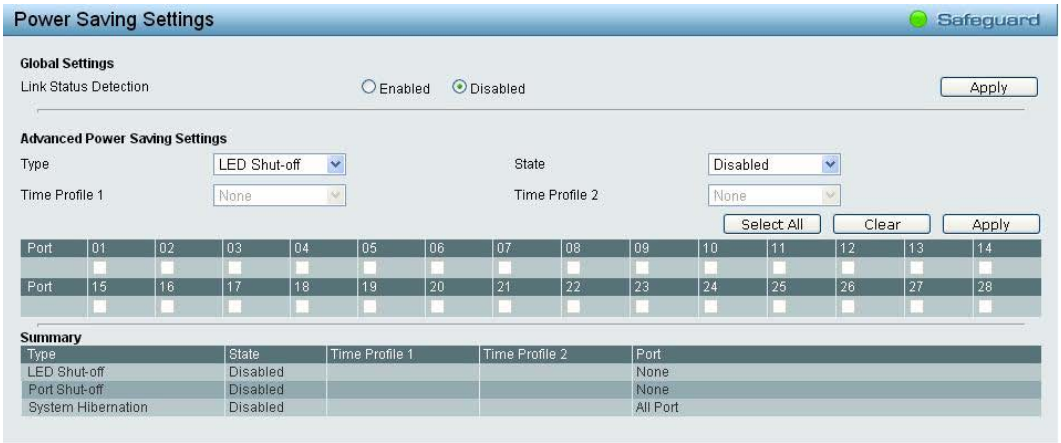


Figure 4.32 – System > Power Saving

Advanced Power Saving Settings:

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

> **LED Shut-off -** The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means the LED can not be turned on after Time Profile time's up when the state is disabled. On the contrary, if the LED is enabled, the Time Profile function will work.
>
> **Port Shut-off -** The Port Shut-off state has high priority (the priority rule is the same as LED.) Therefore, if the Port Shut-off sate is already disabled the Time Profile function will not take effect.
>
> **System Hibernation -** In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

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

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

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

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

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. Users can disable this feature by individual port via the IEEE802.3az EEE setting page.

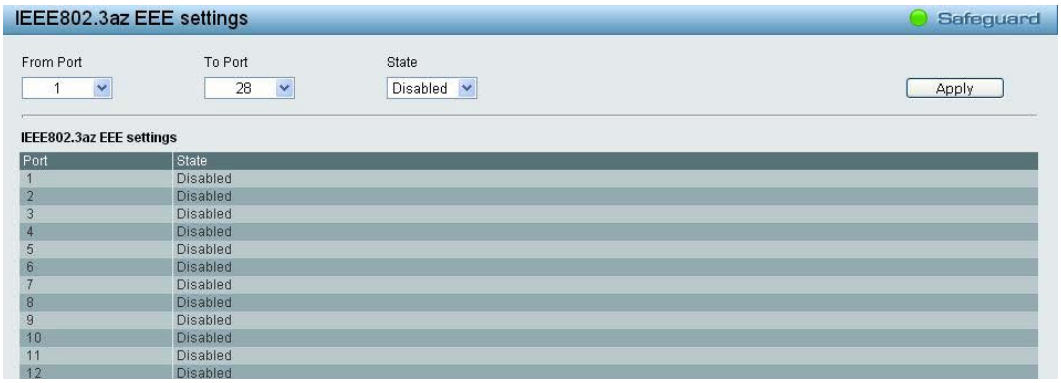


Figure 4.33 – System > IEEE802.3az EEE Settings

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.

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.

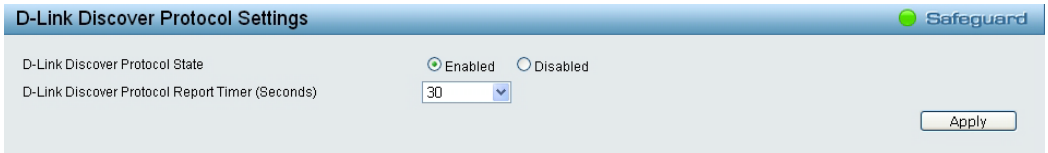


Figure 4.34 – System > D-Link Discover Protocol Settings

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** to implement changes made.

VLAN > 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.

Add New VID: Click to create a new VID group, assigning ports from 01 to 28 as **Untag**, **Tag**, or **Not Member**. A port can be untagged in only one VID. To save the VID group, click **Apply.**

You may change the name accordingly to the desired groups, such as R&D, Marketing, email, etc.

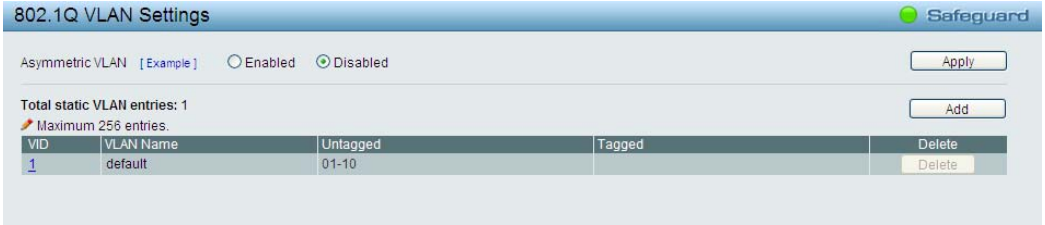


Figure 4.35 – Configuration > 802.1Q VLAN

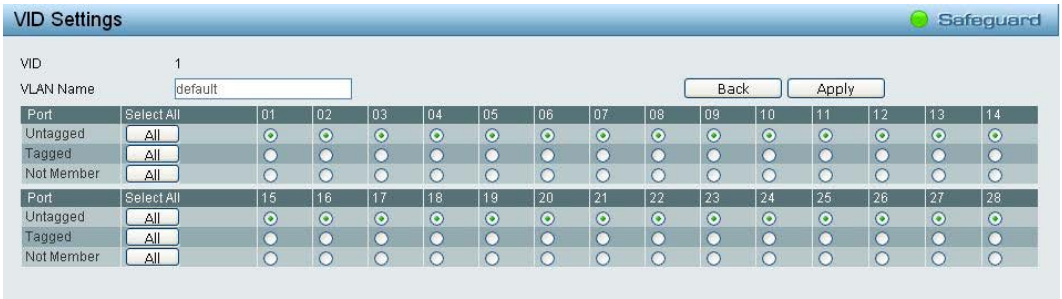


Figure 4.36 – Configuration > 802.1Q VLAN > Add VLAN

VLAN > 802.1Q VLAN PVID

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

Figure 4.37 – Configuration > 802.1Q VLAN PVID

VLAN > 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.

Figure 4.38 – Configuration > 802.1Q Management VLAN

VLAN > Voice VLAN > Voice VLAN Global Settings

Voice VLAN is a feature that allows you to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of

VoIP traffic are guaranteed. If a VoIP packet comes with a VLAN tag, the Voice VLAN function won't replace the original VLAN tag.

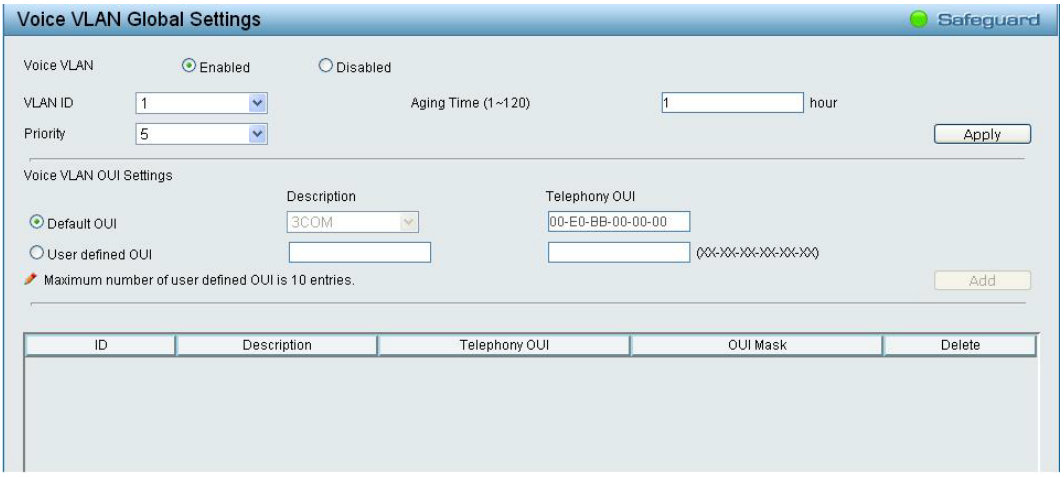


Figure 4.39 – VLAN > Voice VLAN > Voice VLAN Global Settings

Voice VLAN: Select to enable or disable Voice VLAN. The default is *Disabled.* After you enabled Voice VLAN, you can configure the **Voice VLAN Global Settings**.

VLAN ID: The ID of VLAN that you want to assign voice traffic to. You must first create a VLAN from the 802.1Q VLAN page before you can assign a dedicated Voice VLAN. The member port you configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the **Auto Detection** function

Priority: The 802.1p priority levels of the traffic in the Voice VLAN.

Aging Time (1-120): Enter a period of time (in hours) to remove a port from the voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will start. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. Selectable range is from 1 to 120 hours, and default is 1.

Click **Apply** to implement changes made.

Voice VLAN OUI Settings: This allows the user to configure the user-defined voice traffic's OUI. An Organizationally Unique Identifier (OUI) is the first three bytes of the MAC address. This identifier uniquely identifies a vendor, manufacturer, or other organization.

There are some pre-defined OUIs and when the user configures personal OUI, these pre-defined OUIs must be avoided. Below are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3Com	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Default OUI: Pre-defined OUI values, including brand names of 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM, and Avaya.

User defined OUI: You can manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10.

Select the OUI and press **Add** to the lower table to complete the Auto Voice VLAN setting.

Note: Voice VLAN has higher priority than any other features (including QoS). Therefore the voice traffic will be operated according to the Voice VLAN setting and not impacted by the QoS feature.

Note: It is recommended setting the highest priority for Voice VLAN to guarantee the quality of VoIP traffic.

VLAN > Voice VLAN > Voice VLAN Port Settings

The Voice VLAN Port Settings page allows users to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed.

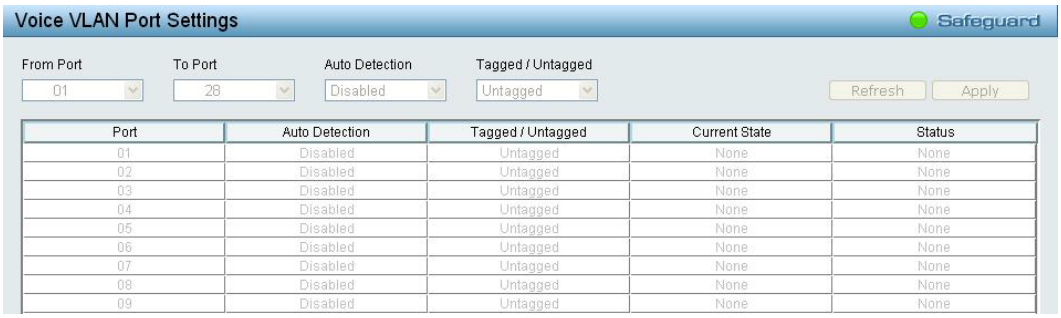


Figure 4.40 – VLAN > Voice VLAN > Voice VLAN Port Settings

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

Auto Detection: Switch will add ports to the voice VLAN automatically if it detects the device OUI matches the Telephony OUI configured in Voice VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is *Disabled*

Tagged / Untagged: tagged or untagged the ports.

Click **Apply** to implement changes made and **Refresh** to refresh the voice vlan table.

Note: Voice VLAN has higher priority than any other features even QoS. Therefore the voice traffic will be operated according to Voice VLAN setting and not impacted by QoS feature.

Note: It is recommended setting the highest priority for Voice VLAN to guarantee the quality of VoIP traffic.

VLAN > Voice VLAN > Voice Device List

The Voice Device List page displays the information of Voice VLAN.

Figure 4.41 – VLAN > Voice VLAN > Voice Device List

Select a port or all ports and click **Search** to display the Voice Device information in the table.

VLAN > Auto Surveillance VLAN Settings

Similar as Voice VLAN, Auto Surveillance VLAN is a feature that allows you to automatically place the video traffic from D-Link IP cameras to an assigned VLAN to enhance the IP surveillance service. With a higher priority and individual VLAN, the quality and the security of surveillance traffic are guaranteed. The Auto Surveillance VLAN function will check the source MAC address / VLAN ID on the incoming packets. If it matches specified MAC address / VLAN ID, the packets will pass through switch with desired priority.

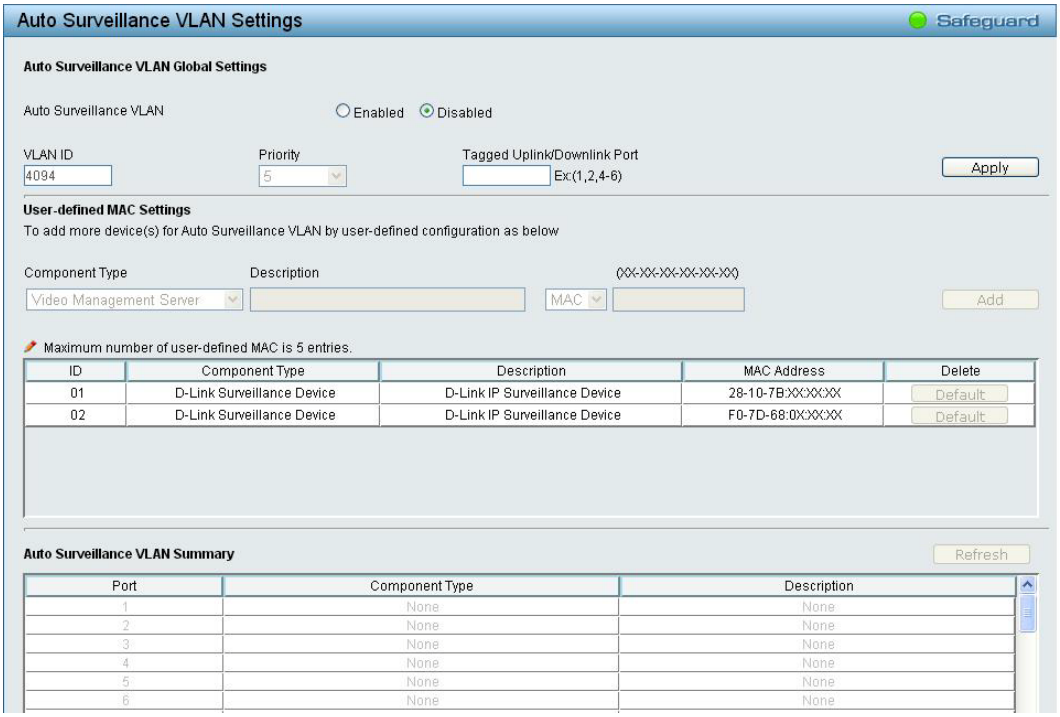


Figure 4.42 – VLAN > Auto Surveillance VLAN

Auto Surveillance VLAN Global Settings:

Auto Surveillance VLAN State: Select to enable or disable Auto Surveillance VLAN. The default is *Disabled.*

VLAN ID: By default, the VLAN ID 4094 was created as Auto Surveillance VLAN. You also can create another Auto Surveillance VLAN by selecting a VLAN ID that you have created a VLAN from the 802.1Q VLAN page. The member port you configured in 802.1Q VLAN setting page will be the static member port of Auto Surveillance VLAN.

Priority: The 802.1p priority levels of the traffic in the Auto Surveillance VLAN. The possible values are *0 to 7*.

Tagged Uplink/Downlink Port: Specifies the ports to be tagged uplink port or downlink port for the Auto Surveillance VLAN.

Click **Apply** to implement changes of Auto Surveillance VLAN global settings.

User-defined MAC Settings:

Component Type: Auto Surveillance VLAN will automatically detect D-Link Surveillance Devices by default. There are another five surveillance components that could be configured to be auto-detected by the Auto Surveillance VLAN. These five components are *Video Management Server (VMS), VMS Client/Remote viewer, Video Encoder, Network Storage* and Other *IP Surveillance Devices*.

Description: Here to input the description for the component type.

MAC/OUI: You can manually create an MAC or OUI address for the surveillance component. The maximum number of user defined MAC address is 5.

Click **Add** to create a new surveillance component and **Refresh** to refresh the Auto Surveillance VLAN summary table.

L2 Functions > Jumbo Frame

D-Link Gigabit Web Smart Switches support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes) of up to 9216 bytes (tagged). Default is disabled, Select **Enabled** then click **Apply** to turn on the jumbo frame support.

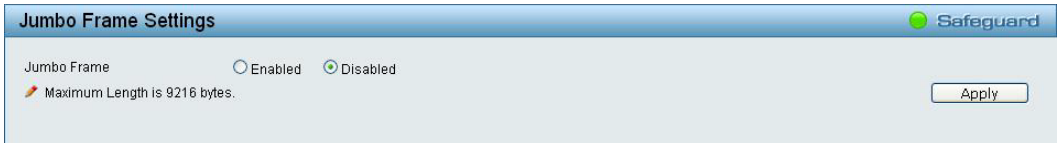


Figure 4.43 – L2 Functions > Jumbo Frame

L2 Functions > 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 4.44 – L2 Functions > 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.

TX/RX (transmit and receive) 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.

L2 Functions > Loopback Detection

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

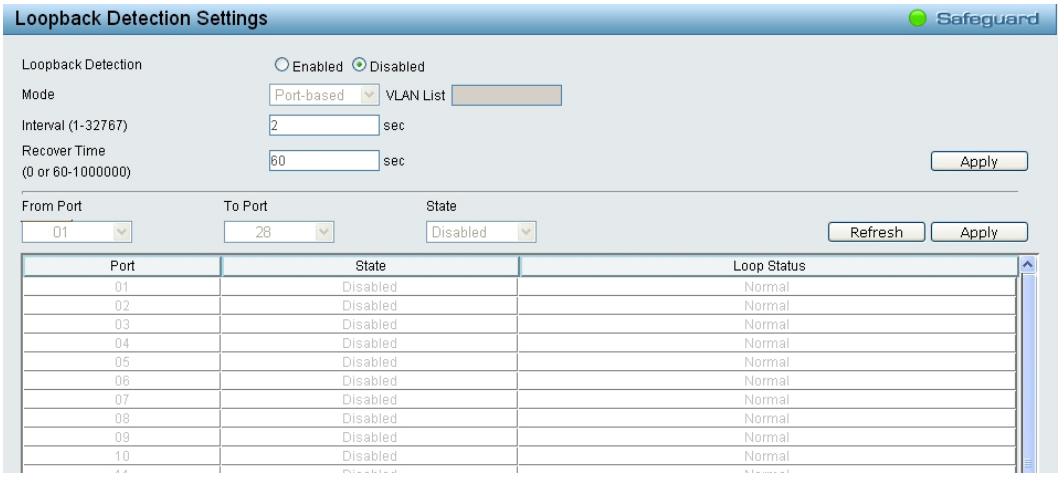


Figure 4.45 – L2 Functions > Loopback Detection

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

Mode: Specifies Port-based or VLAN-based mode. If port-based mode is selected, the loop happening port will be shut down and affect all member VLANs. If VLAN-based mode is selected, only the member port in the loop happening VLAN will be shut down.

VID List: Specifies the VID.

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 or click Refresh to **refresh** the Loopback Detection table.

L2 Functions > MAC Address Table > Static MAC

This feature provides two distinct functions. The **MAC Address** 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 disabled.

Figure 4.46 – L2 Functions > MAC Address Table > Static Mac Address

The **Static MAC Address Lists** table displays the static MAC addresses connected, as well as the VID.

Add Static MAC Address: you need to select the assigned Port number. Enter both the Mac Address and VID, and then Click **Add**. Click **Delete** to remove one entry or click **Delete all** to clear the list.

By disabling MAC Address Auto Learning capability and specifying 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.

L2 Functions > MAC Address Table > Dynamic Forwarding Table

For each port, this table displays the MAC address learned by the Switch. To add a MAC address to the Static Mac Address List, click the **Add** checkbox, and then click **Apply** associated with the identified address.

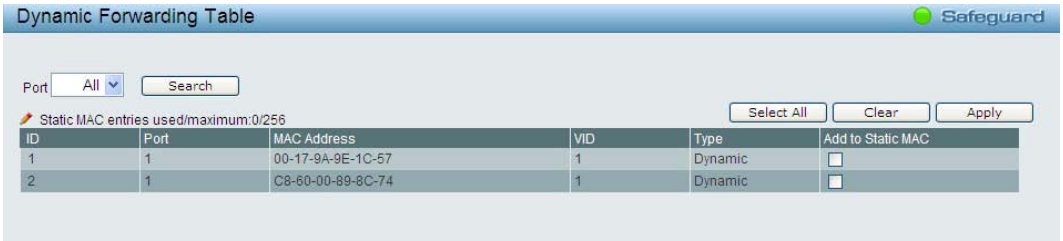


Figure 4.47 – L2 Functions > MAC Address Table > Dynamic Forwarding Table

L2 Functions > Spanning Tree > STP Global Settings

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

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

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

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

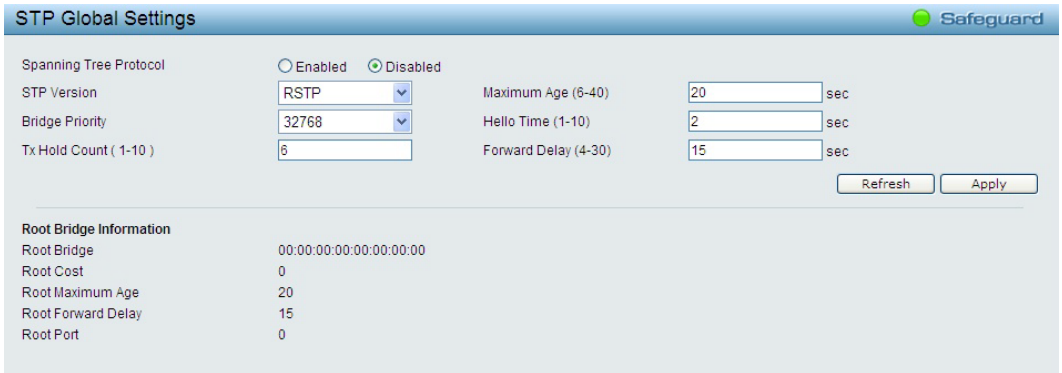


Figure 4.48 – L2 Functions > Spanning Tree > STP Global Settings

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

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

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

Maximum Age (6-40 sec): This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values

consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between 6 and 40 seconds. The default value is 20. (Max Age has to have a value bigger than Hello Time)

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

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

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

Root Cost: Display the cost of the Root Bridge.

Root Maximum Age: Displays the Maximum Age of the Root Bridge.

Root Forward Delay: Displays the Forward Delay of the Root Bridge.

Root port: Displays the root port.

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

L2 Functions > Spanning Tree > STP Port Settings

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

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

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

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

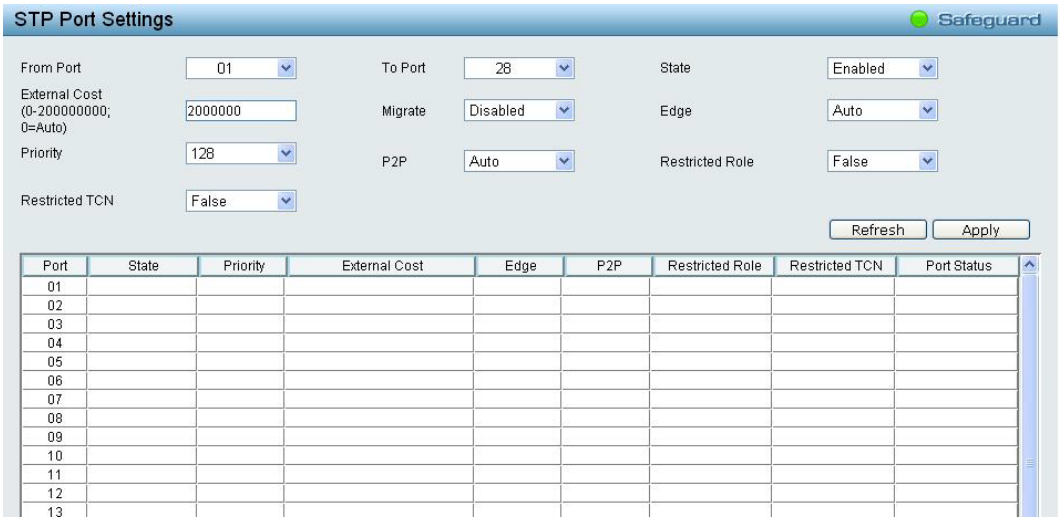


Figure 4.49 – L2 Functions > Spanning Tree > STP Port Settings

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

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

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

> **0 (auto) -** Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.

Value 1-200000000 - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

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

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

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

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

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

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

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

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

L2 Functions > Link Aggregation > Port Trunking

The Trunking function enables the combining of two or more ports together to increase bandwidth. Up to eight Trunk groups may be created, and each group consists up to eight ports. Select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

Static - Static link aggregation.

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

Disable - Remove all members in this trunk group.

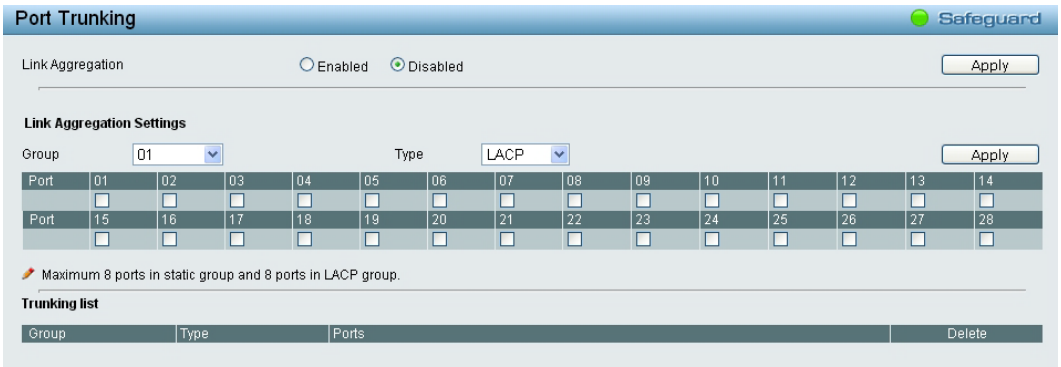


Figure 4.50 – L2 Functions > Link Aggregation > Port Trunking

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

L2 Functions > Link Aggregation > LACP Port Settings

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

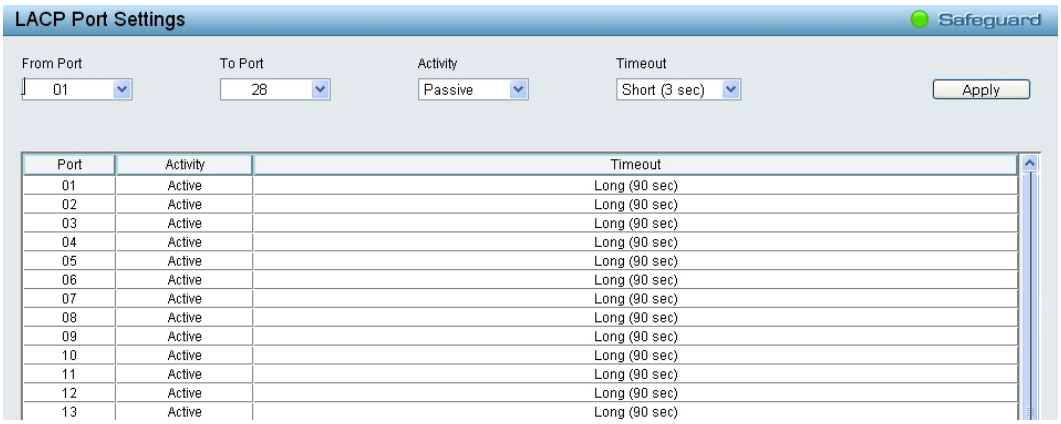


Figure 4.51 – L2 Functions > Link Aggregation > LACP Port Settings

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

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

Activity: There are two different roles of LACP ports:

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

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

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

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

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

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

L2 Functions > Multicast > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the Web Smart Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the Web Smart Switch will forward multicast traffic only to connections that have group members attached.

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

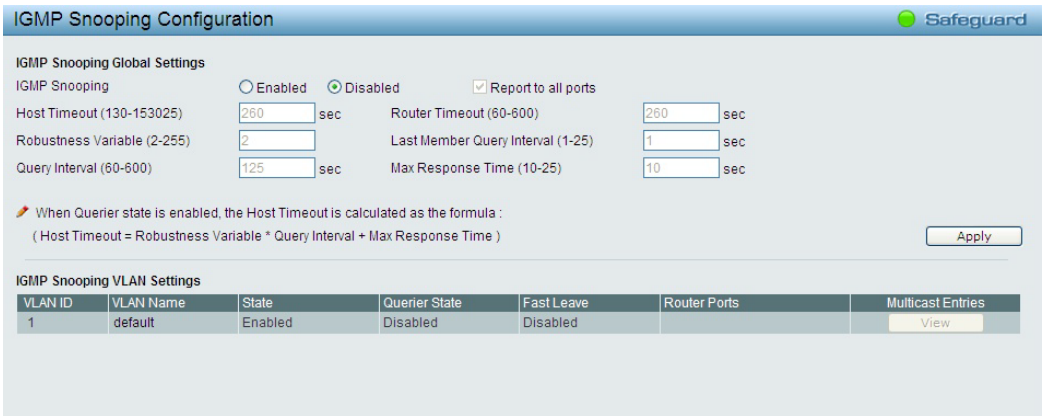


Figure 4.52 – L2 Functions > Multicast > IGMP Snooping

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

It is recommended to keep Report to all ports enable to ensure the functionality of SmartConsole Utility.

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 are 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.

To enable IGMP snooping for a given VLAN, select enable and click on the **Apply** button. Then press the **Edit** button under **Router Port Setting**, and select the ports to be assigned as router ports for IGMP snooping for the VLAN, and press **Apply** for changes to take effect. A router port configured manually is a **Static Router Port**, and a **Dynamic Router Port** is dynamically configured by the Switch when query control message is received.

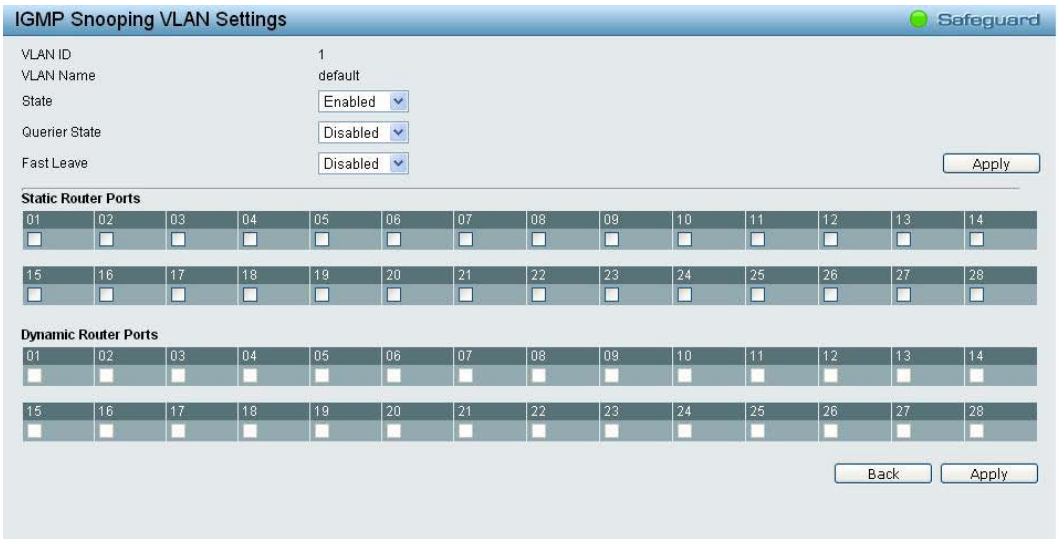


Figure 4.53 – L2 Functions > Multicast > IGMP Snooping VLAN Settings

State : Specify the State to be enabled or disabled.

Querier State: D-Link Smart Switch is able to send out the IGMP Queries to check the status of multicast clients. Default is disabled.

Fast Leave: Specify the Fast Leave feature to be enabled or disabled.

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

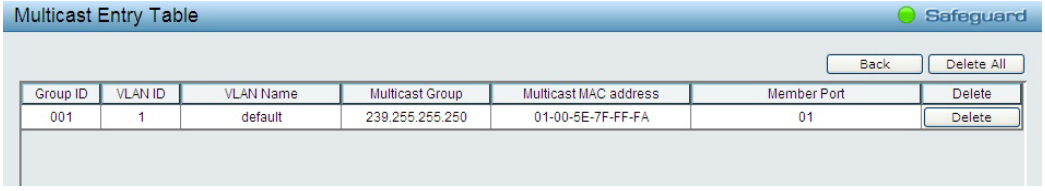


Figure 4.54 – L2 Functions > Multicast > IGMP Multicast Entry Table

Click **Delete** to remove a specified entry or click **Delete All** to remove all entries.

L2 Functions > Multicast > MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

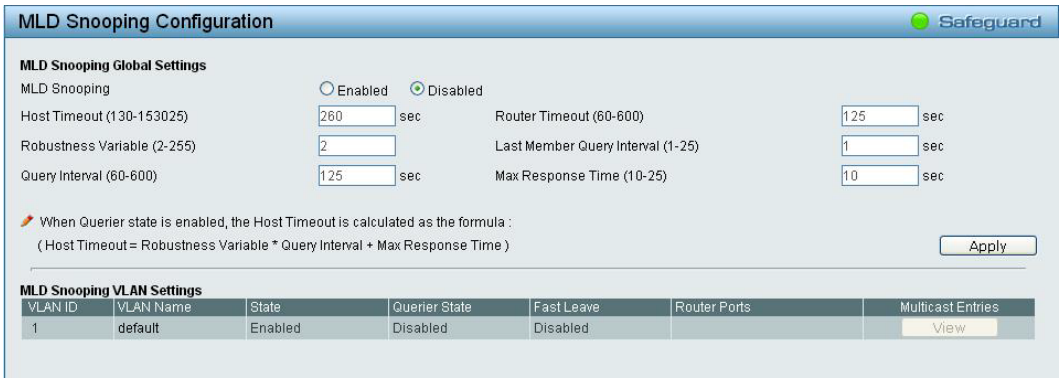


Figure 4.55 – L2 Functions > Multicast > MLD Snooping

MLD Global Settings:

MLD Snooping: Enable or disable the MLD Snooping.

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

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

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

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

default value is 1 second.

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

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

Click **Apply** to implement changes made.

MLD Snooping VLAN Settings List:

Click the number of VLAN ID to modify the settings:

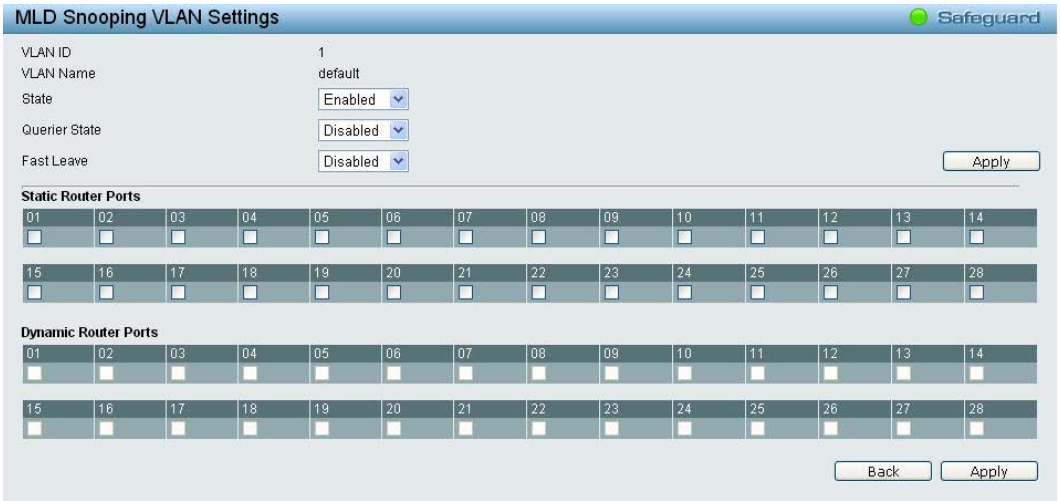


Figure 4.56 – L2 Functions > Multicast > Multicast Forwarding

State: Specify the state of MLD Snooping VLAN to be enabled or disabled.

Querier State: Specify the querier state to be enabled or disabled.

Fast Leave: Specify the fast leave feature to be enabled or disabled.

Click **Apply** to implement changes made.

Static Router Ports: Selects the ports to be static router ports and assigned for MLD snooping for the VLAN.

Dynamic Router Ports: Select the ports to be dynamic router ports and assigned for MLD snooping for the VLAN.

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

L2 Functions > Multicast > Multicast Forwarding

The Multicast Forwarding page displays all of the entries made into the Switch's static multicast forwarding table. To implement the Multicast Forwarding Settings, input **VID**, **Multicast MAC Address** and port settings, then click **Add**.

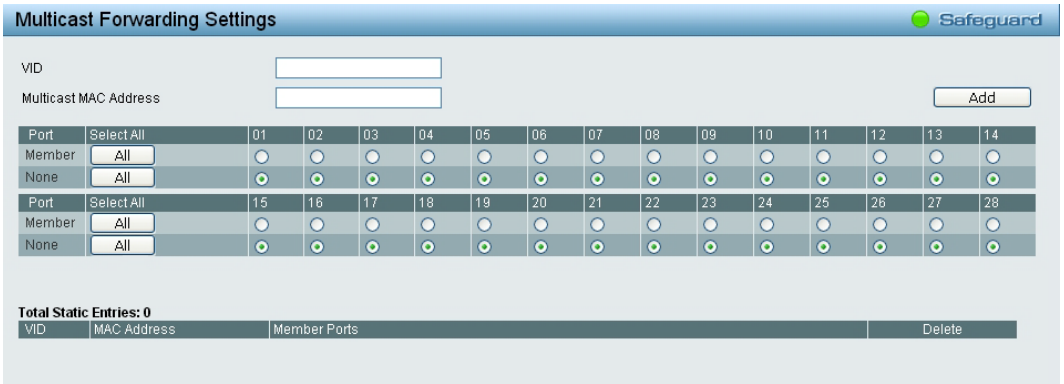


Figure 4.57 – L2 Functions > Multicast > Multicast Forwarding

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.

Member - 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.

L2 Functions > Multicast > Multicast Filtering Mode

The **Multicast Filtering Mode** function allows users to select the filtering mode for IGMP group per VLAN basis.

Figure 4.58 – L2 Functions > Multicast > Multicast Filtering Mode

VLAN ID: Specifies the VLAN ID.

Filtering Mode:

Forward Unregistered Groups: The multicast stream will be forwarded based on the register table in registered group, but it will be flooded to all ports of the VLAN in unregistered group.

Filter Unregistered Groups: The registered group will be forwarded based on the register table and the unregister group will be filtered.

Click **Apply** to make the change effective.

L2 Functions > SNTP > 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.

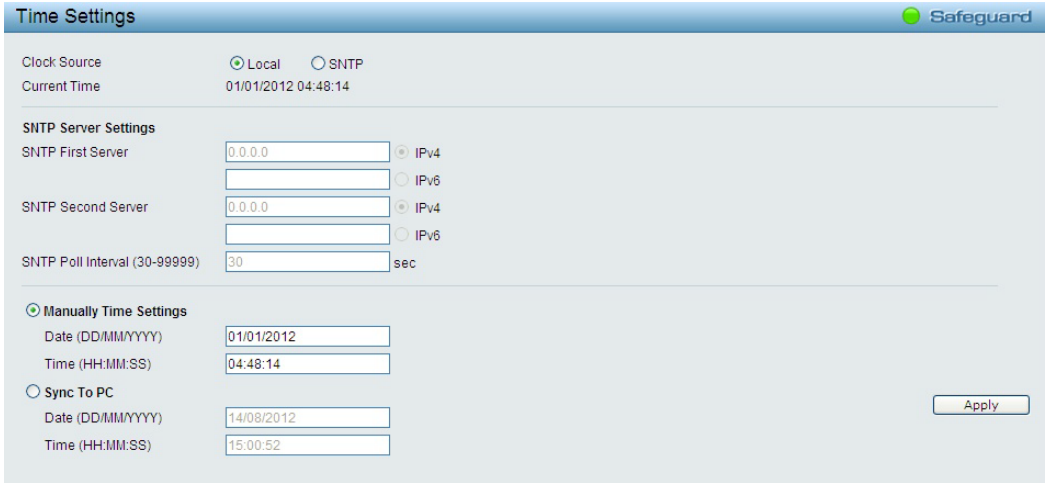


Figure 4.59 – L2 Functions > SNTP > Time Settings

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

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

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

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

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

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

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

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

Click **Apply** to implement changes made.

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

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

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

L2 Functions > SNTP > TimeZone Settings

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

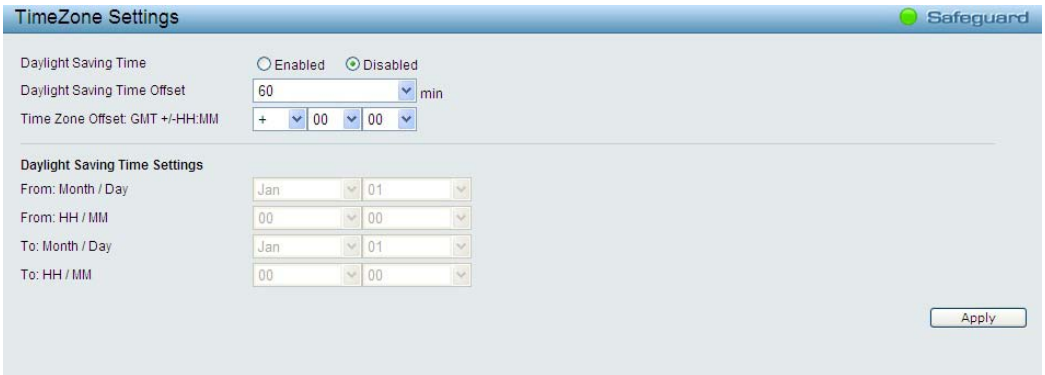


Figure 4.60 – L2 Functions > SNTP > TimeZone Settings

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.

L2 Functions > 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. SNMP utilities can learn the network topology by obtaining the MIB information in each LLDP device. The LLDP function is disabled by default.

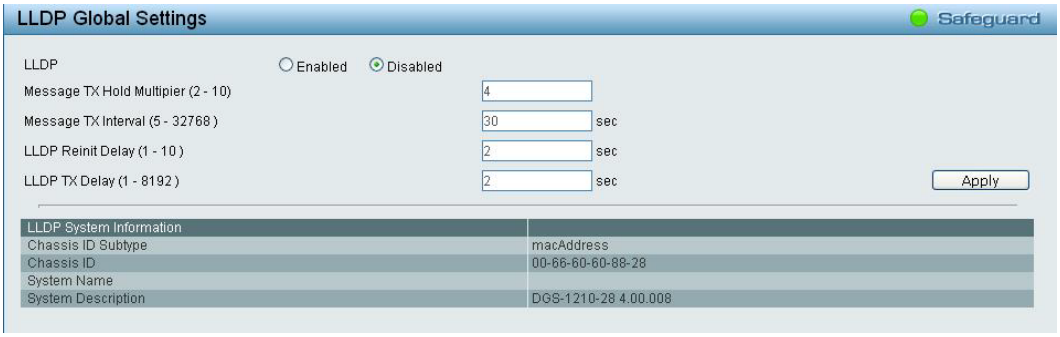


Figure 4.61 – L2 Functions > LLDP > LLDP Global Settings

LLDP: When this function is *Enabled*, the switch can start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

Message TX Hold Multiplier (2-10): This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is **4**.

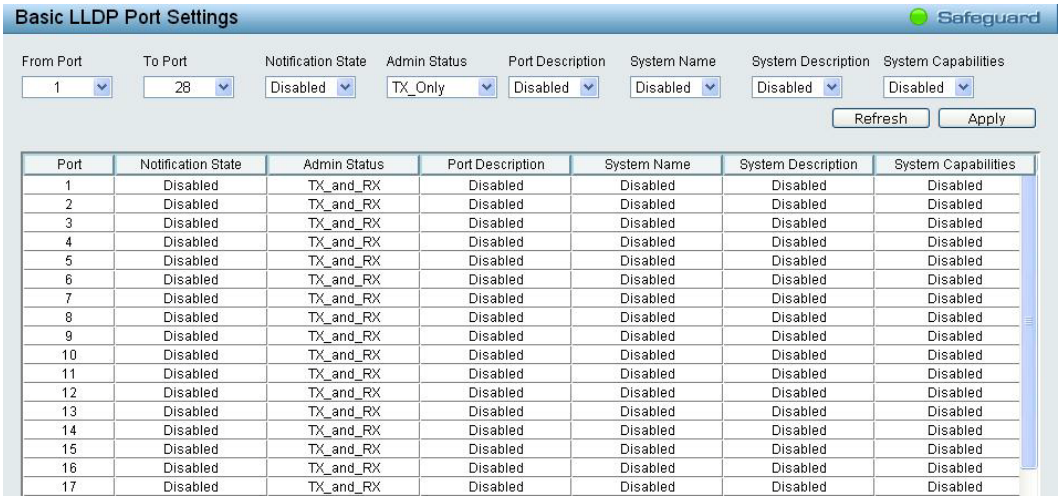
Message TX Interval (5-32768): This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is **30** seconds.

LLDP ReInit Delay (1-10): This parameter indicates the amount of delay from the time adminStatus becomes "disabled" until re-initialization is attempted. The default value is **2** seconds.

LLDP TX Delay (1-8192): This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: 1 < txDelay < (0.25 °— msgTxInterval). The default value is **2** seconds.

L2 Functions > LLDP > LLDP Port Settings

The Basic LLDP Port Settings page displays LLDP port information and contains parameters for configuring LLDP port settings.



Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
2	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
3	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
4	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
5	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
6	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
7	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
8	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
9	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
10	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
11	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
12	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
13	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
14	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
15	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
16	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
17	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled

Figure 4.62 – L2 Functions > LLDP > 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.

L2 Functions > LLDP > 802.1 Extension TLV

This 802.1 Extension TLV page is used to configure the LLDP Port settings.

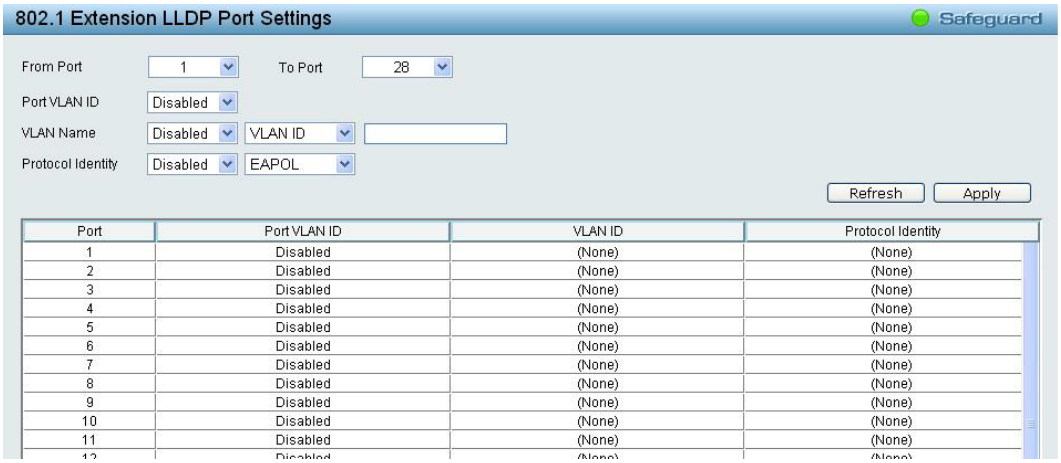


Figure 4.63 – L2 Functions > LLDP > 802.1 Extension TLV Port Settings

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 ID or VLAN Name or all.

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

Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

L2 Functions > LLDP > 802.3 Extension TLV

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.

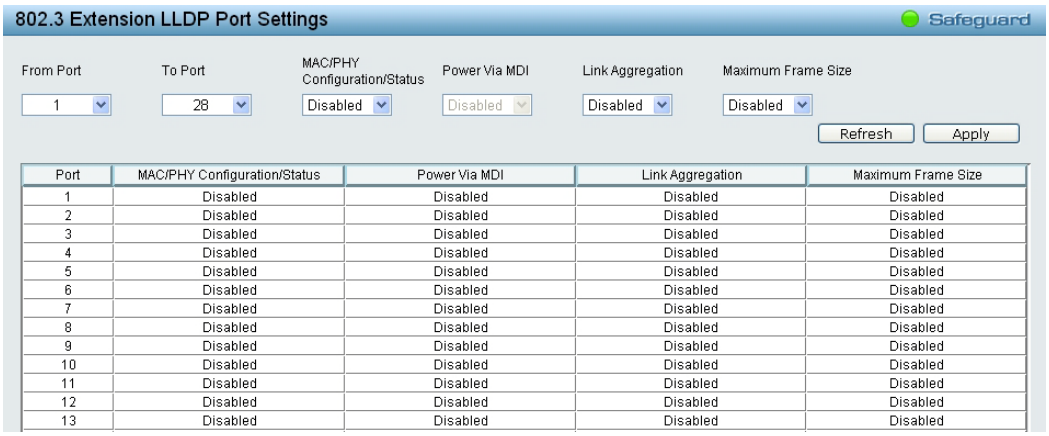


Figure 4.64 – L2 Functions > LLDP > 802.3 Extension TLV

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

MAC/PHY Configuration/Status: Specifies whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are:

Enabled – Enables the MAC/PHY Configuration Status on the port.

Disabled – Disables the MAC/PHY Configuration Status on the port.

Power via MDI: Advertises the Power via MDI implementations supported by the port. The possible field values are:

Enabled – Enables the Power via MDI configured on the port.

Disabled – Disables the Power via MDI configured on the port.

Link Aggregation: Specifies whether the link aggregation is enabled on the port. The possible field values are:

Enabled – Enables the link aggregation configured on the port.

Disabled – Disables the link aggregation configured on the port.

Maximum Frame Size: Specifies whether the Maximum Frame Size is enabled on the port. The possible field values are:

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

Disabled – Disables the Maximum Frame Size configured on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

L2 Functions > LLDP > LLDP Management Address Settings

The LLDP Management Address Settings allows the user to set management address which is included in LLDP information transmitted.

Figure 4.65 – L2 Functions > LLDP > LLDP Management Address Settings

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

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

Address: Specify the address.

Port State: Specify whether the Port State is enabled n the port. The possible field values are:

Enabled – Enables the port state configured on the port.

Disabled – Disables the port state configured on the port.

Click **Apply** to implement changes made.

L2 Functions > LLDP > LLDP Management Address Table

The LLDP Management Address Table page displays the detailed management address information for the entry.

Figure 4.66 – L2 Functions > LLDP > LLDP Management Address Table

Management Address: Select IPv4 or IPv6 address and 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 address or IPv4 address.

Management Address: Displays the IP address.
IF Type: Displays the IF Type.
OID: Displays the SNMP OID.
Advertising Ports: Displays the advertising ports.

L2 Functions > LLDP > LLDP Local Port Table

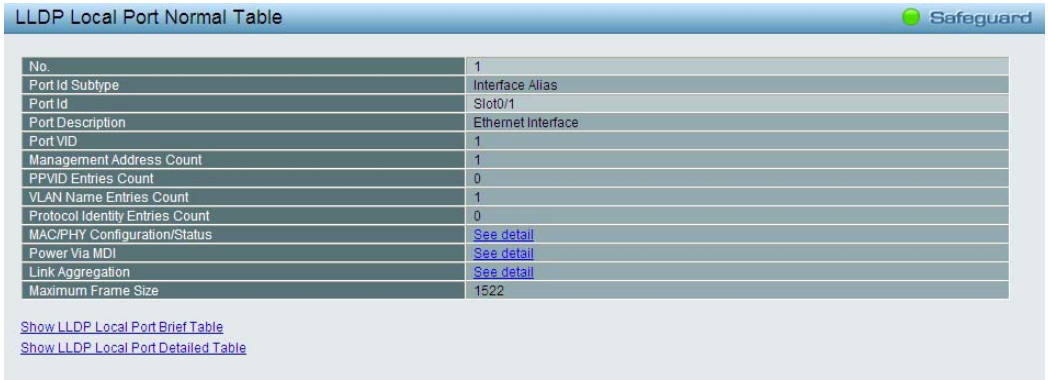
The LLDP Local Port Table page displays LLDP local port information.

Port	Port ID Subtype	Port ID	Port Description	Normal	Detailed
01	Interface Alias	Slot0/1	Ethernet Interface	View	View
02	Interface Alias	Slot0/2	Ethernet Interface	View	View
03	Interface Alias	Slot0/3	Ethernet Interface	View	View
04	Interface Alias	Slot0/4	Ethernet Interface	View	View
05	Interface Alias	Slot0/5	Ethernet Interface	View	View
06	Interface Alias	Slot0/6	Ethernet Interface	View	View
07	Interface Alias	Slot0/7	Ethernet Interface	View	View
08	Interface Alias	Slot0/8	Ethernet Interface	View	View
09	Interface Alias	Slot0/9	Ethernet Interface	View	View
10	Interface Alias	Slot0/10	Ethernet Interface	View	View
11	Interface Alias	Slot0/11	Ethernet Interface	View	View
12	Interface Alias	Slot0/12	Ethernet Interface	View	View
13	Interface Alias	Slot0/13	Ethernet Interface	View	View
14	Interface Alias	Slot0/14	Ethernet Interface	View	View
15	Interface Alias	Slot0/15	Ethernet Interface	View	View
16	Interface Alias	Slot0/16	Ethernet Interface	View	View

Figure 4.67 – L2 Functions > 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	Slot0/1
Port Description	Ethernet Interface
Port VID	1
Management Address Count	1
PPVID Entries Count	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	See detail
Power Via MDI	See detail
Link Aggregation	See detail
Maximum Frame Size	1522

Figure 4.68 – L2 Functions > LLDP > LLDP Local Port Normal Table

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

Figure 4.69 – L2 Functions > LLDP > LLDP Local Port Detailed Table

L2 Functions > LLDP > LLDP Remote Port Table

This LLDP Remote Port Table page is used to display the LLDP Remote Port Brief Table. Select port number and click **Search** to display additional information.

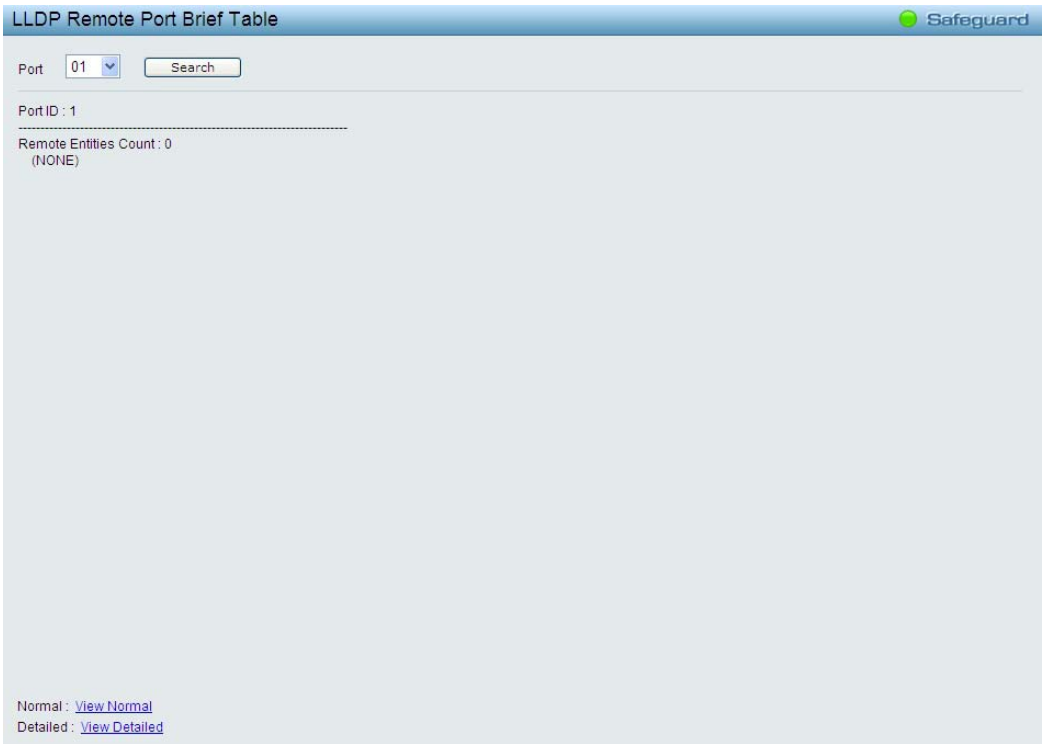


Figure 4.70 – L2 Functions > LLDP > LLDP Remote Port Table

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

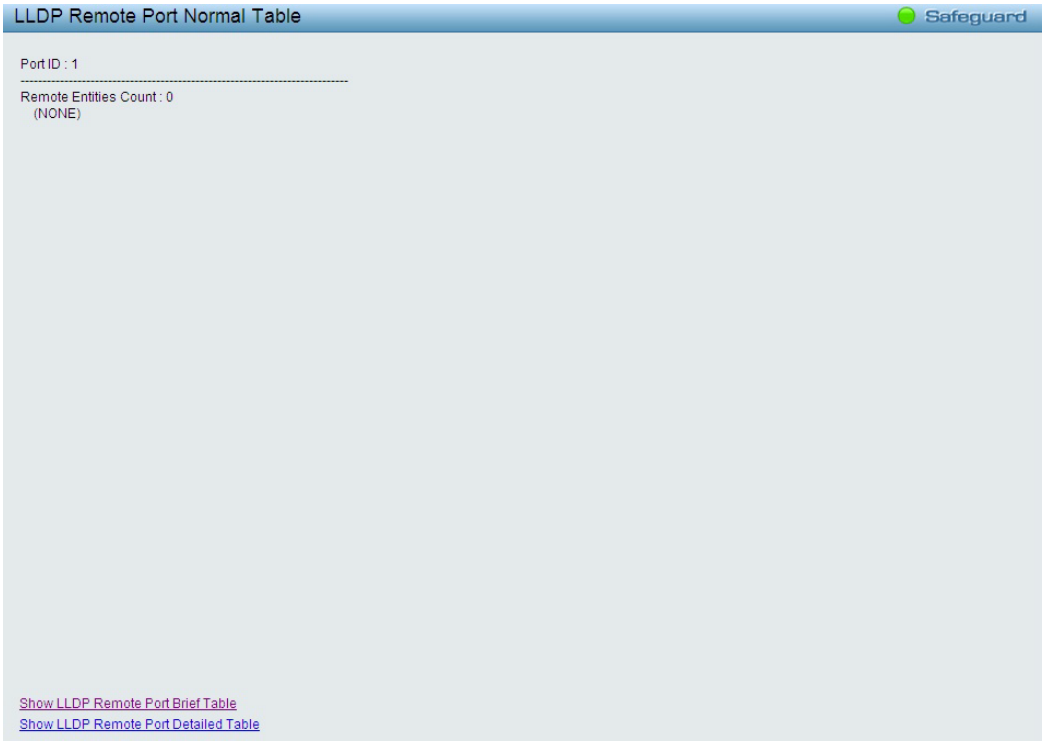


Figure 4.71 – L2 Functions > LLDP > LLDP Remote Port Normal Table

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

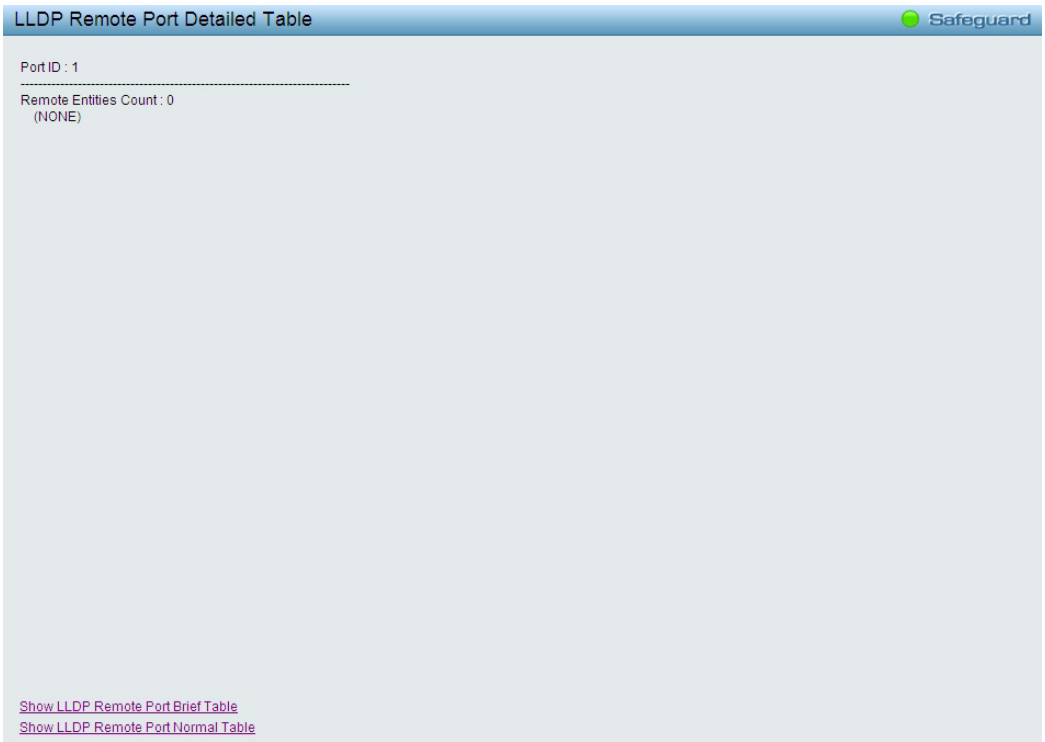


Figure 4.72 – L2 Functions > LLDP > LLDP Remote Port Detailed Table

L2 Functions > LLDP > LLDP Statistics

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

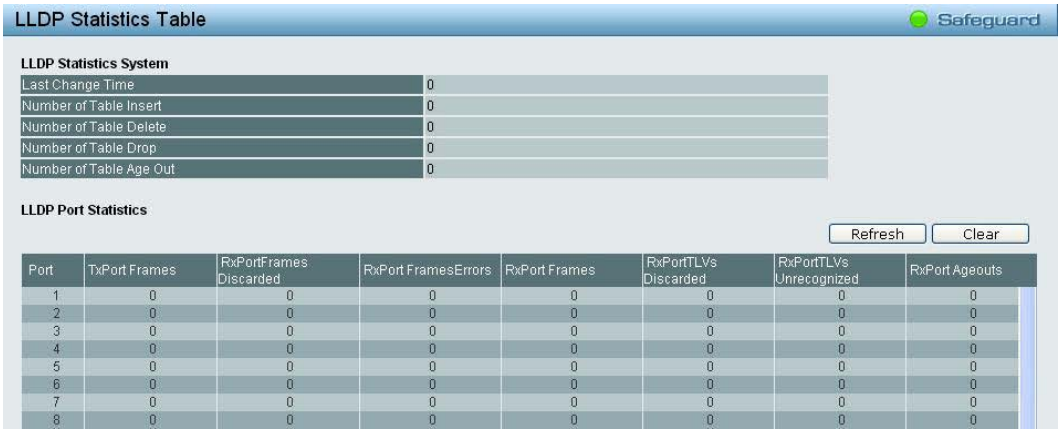


Figure 4.73 – L2 Functions > LLDP > LLDP Statistics

The following information can be viewed:

LLDP Statistics System: Displays the counters that refer to the whole switch.

Last Change Time – Displays the time for when the last change entry was last deleted or added. It is also displays the time elapsed since last change was detected.

Number of Table Insert – Displays the number of new entries inserted since switch reboot.

Number of Table Delete – Displays the number of new entries deleted since switch reboot.

Number of Table Drop – Displays the number of LLDP frames dropped due to that the table was full.

Number of Table Age Out – Displays the number of entries deleted due to Time-To-Live expiring.

LLDP Port Statistics: Displays the counters that refer to the ports.

TxPort FramesTotal – Displays the total number of LLDP frames transmitted on the port.

RxPort FramesDiscarded – Displays the total discarded frame number of LLDP frames received on the port.

RxPort FramesErrors – Displays the Error frame number of LLDP frames received on the port.

RxPort Frames – Displays the total number of LLDP frames received on the port.

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

RxPortTLVsUnrecognized – Displays the number of well-formed TLVs, but with an 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.

Click **Refresh** to renew the page, and click **Clear** to clean out all statistics.

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.

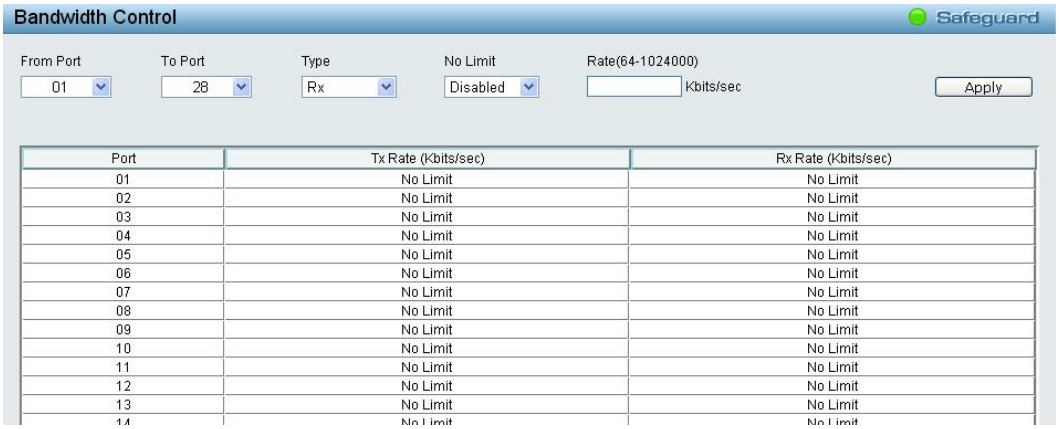


Figure 4.74 – QoS > Bandwidth Control

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

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

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

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

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

QoS > 802.1p/DSCP/ToS

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

The following figure displays the status of Quality of Service priority levels of each port, higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration.

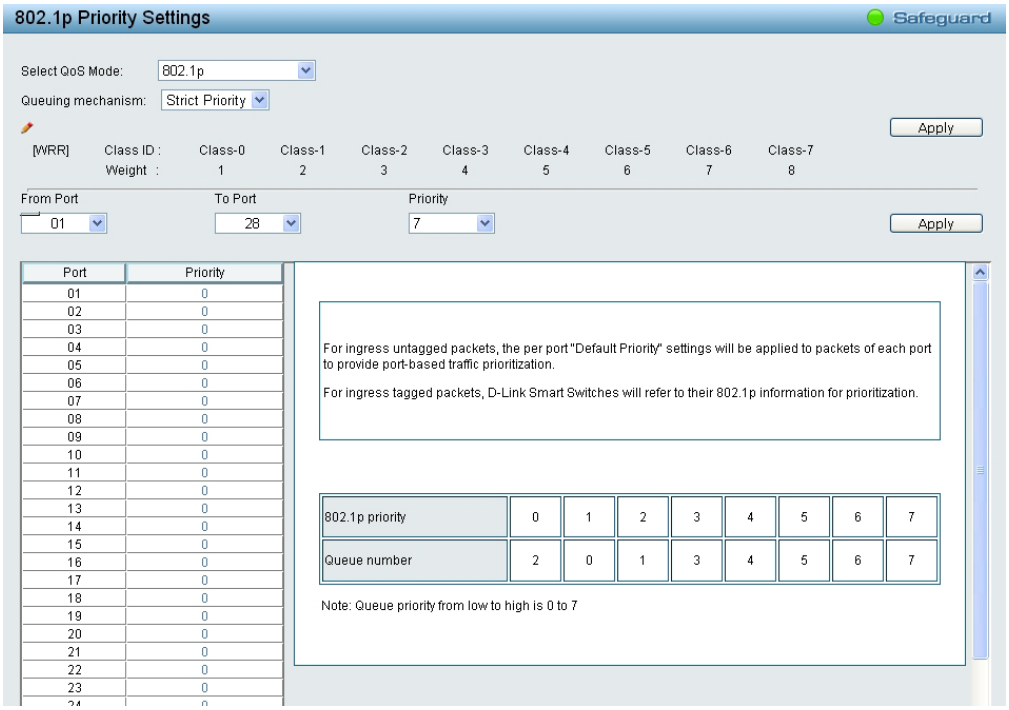


Figure 4.75 – QoS > 802.1p/DSCP/ToS

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

Queuing Mechanism:

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

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

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

From Port / To Port: Defines the port range which the port packet priorities are defined.

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.

Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. You can enter up to ten designated management stations networks by defining the IPv4 Address/Netmask or IPv6 Address/Prefix as seen in the figure below. The first thing after the function is enabled is to add your local host IP address as a trusted host. Otherwise, you may lose the connection.

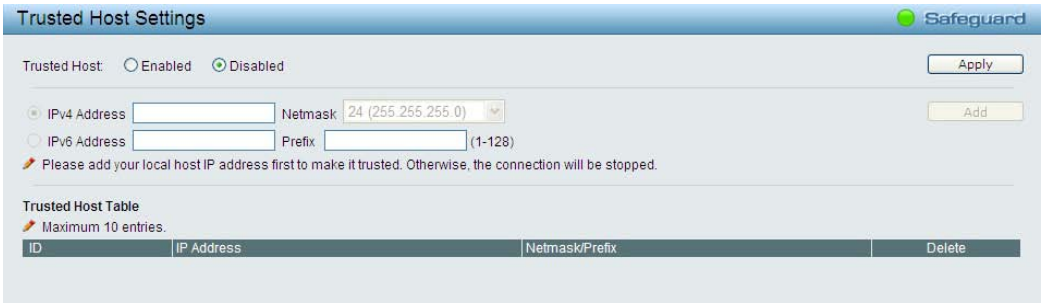


Figure 4.76 Security > Trusted Host

Trusted Host: Specify the Trusted Host to be enabled or disabled. The default is disabled.

To define a management station IP setting, click the **Add** button and type in the IP address and Subnet mask. Click the **Apply** button to save your settings. You may permit only single or a range of IP addresses by different IP mask setting, the format can be either 192.168.1.1/255.255.255.0 or 192.168.0.1/24. Please see the example below for permitting the IP range.

IP Address	Subnet Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

To delete the IP address simply click the **Delete** button, check the unwanted address, and then click **Apply**.

Security > Port Security

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. Using the drop-down menu, change **Admin State** to *Enabled,* input Max Learning Address, and then click **Apply**.

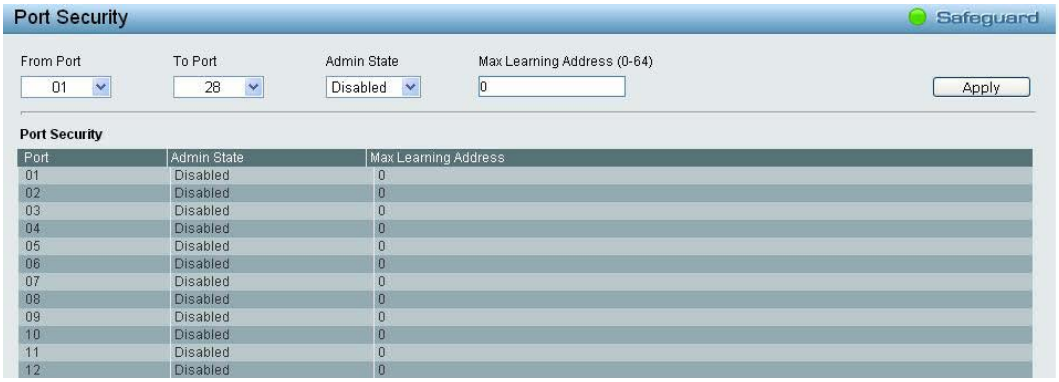


Figure 4.77 – Security > Port Security

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.

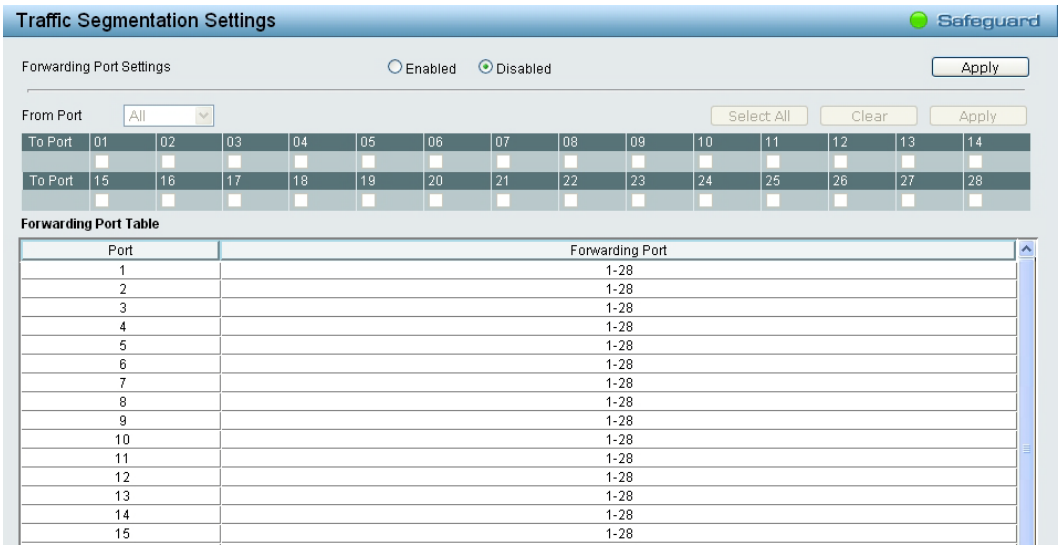


Figure 4.78 – Security > Traffic Segmentation

Click **Apply** to enable or disable this feature.

To configure traffic segmentation specify a port or All ports from the switch, using the **From Port** pull-down menu and select To Port then click **Apply** to enter the settings into the Switch's **Traffic Segmentation** table.

Click **Select All** button to check all ports or click **Clear** button to uncheck all ports.

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 Web-Smart Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.

Figure 4.79 – Security > Safeguard Engine

Security > Storm Control

The Storm 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.

Figure 4.80 – Security > Storm Control

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

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

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

Security > ARP Spoofing Prevention

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network by allowing an attacker to sniff data frames on a LAN, modifying the traffic, or stopping the traffic (known as a Denial of Service – DoS attack). The main idea of ARP spoofing is to send fake or spoofed ARP messages to an Ethernet network. It associates the attacker's or random MAC address with the IP address of another node such as the default gateway. Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one gratuitous ARP to the network claiming to be the gateway, so that the whole network operation is turned down as all packets to the Internet will be directed to the wrong node.

The ARP Spoofing Prevention function can discard the ARP Spoofing Attack in the network by checking the gratuitous ARP packets and filtering those with illegal IP or MAC addresses.

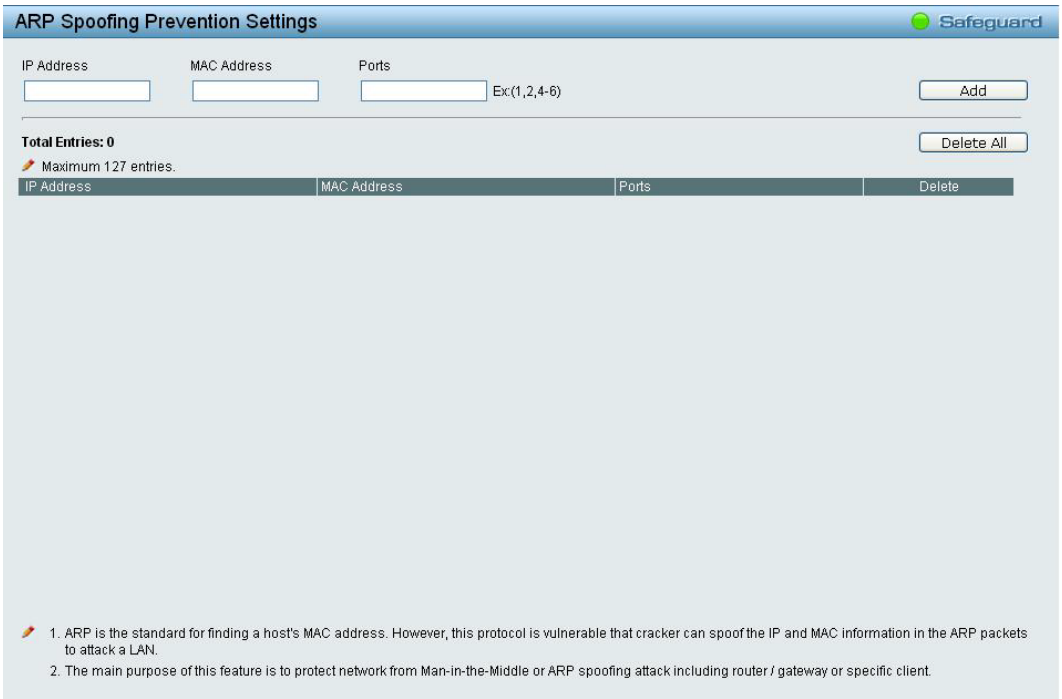


Figure 4.81 – Security > ARP Spoofing Prevention

Enter the **IP Address**, **MAC Address**, **Ports** and then click **Add** to create a checking/filtering rule. Click **Delete** to remove an existing rule and **Delete All** to clear all the entries.

Security > DHCP Server Screening

DHCP Server Screening function allows user to restrict the illegal DHCP server by discarding the DHCP service from distrusted ports. This page allows you to configure the DHCP Server Screening state for each port and designed trusted DHCP server IP address. Select **Ports** and then click **Apply** to enable or disable the function.

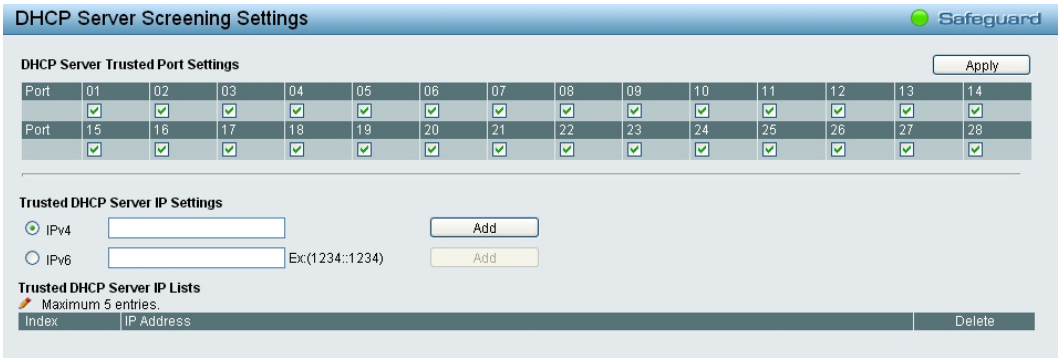


Figure 4.82 – Security > DHCP Server Screening

Trusted DHCP Server IP Settings: Select IPv4 or IPv6 and specify the IP address then click Apply to create Trusted DHCP Server.

Click **Add** to add a DHCP trusted DHCP server.

Security > SSL Settings

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between a Web Management host and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes.

This page allows you to configure the SSL global state and the Ciphersuite settings. Select **Enable** or **Disable** and then click **Apply** to change the SSL state or the Ciphersuite settings of the Switch. By default, SSL is **Disabled** and all Ciphersuites are **Enabled**.

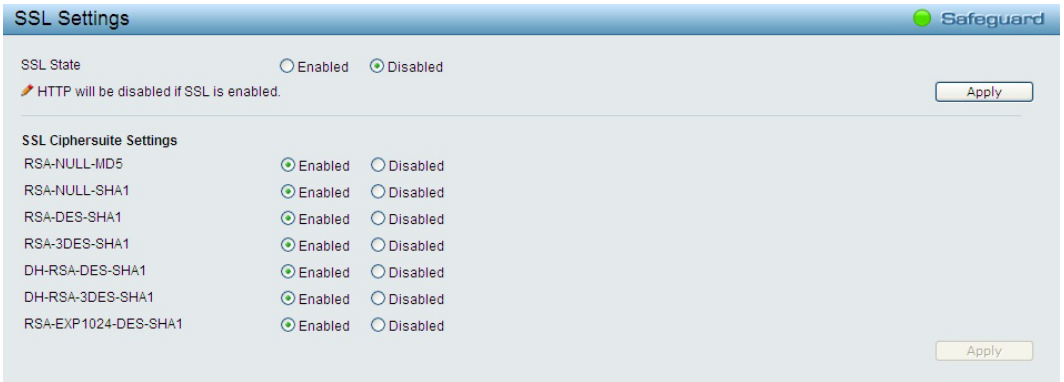


Figure 4.83 – Security > SSL Settings

NOTE: When SSL is enabled, it will take longer time to open a web page due to encryption. After saving configuration, please wait around 10 seconds for the system summery page.

Security > DoS Prevention Settings

The user can enable or disable the prevention of each DoS attacks. As long as user enable DoS Prevention, switch can dtop the packet matching DoS Attack Prevention type listed on below table. The packet matching will be done by hardware.

Figure 4.84 – Security > DoS Prevention Settings

State: Specify the state to be enabled or disabled. Click **Apply** to implement changes made.

Security > SSH > SSH Settings

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

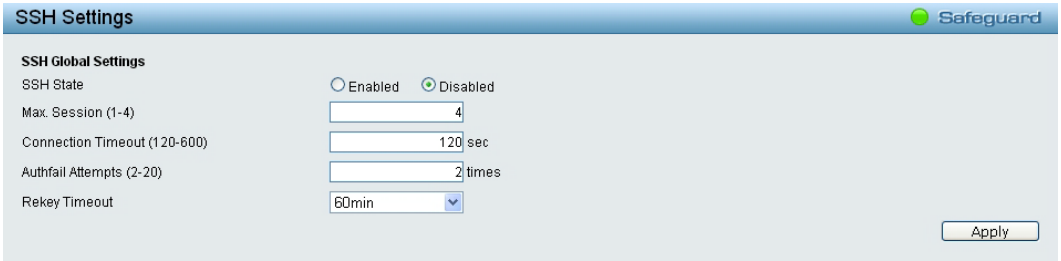


Figure 4.85 – Security > SSH > SSH Settings

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

SSH State: Enabled or Disabled SSH on the Switch. The default is *Disabled*.

Max Session (1 - 4): Enter a value between *1* and 4 to set the number of users that may simultaneously access the Switch. The default setting is *1*.

Connection Timeout (120 - 600): Allows the user to set the connection timeout. The use may set a time between *120* and *600* seconds. The default setting is *120* seconds.

Authfail Attempts (2 - 20): Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between *2* and *20*. The default setting is *2*.

Rekey Timeout: Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min.* The default setting is *60 min.*

Security > SSH > SSH Authmode and Algorithm Settings

The SSH Authentication and Algorithm Settings page allows user to configure the desired types of SSH algorithms used for authentication encryption.

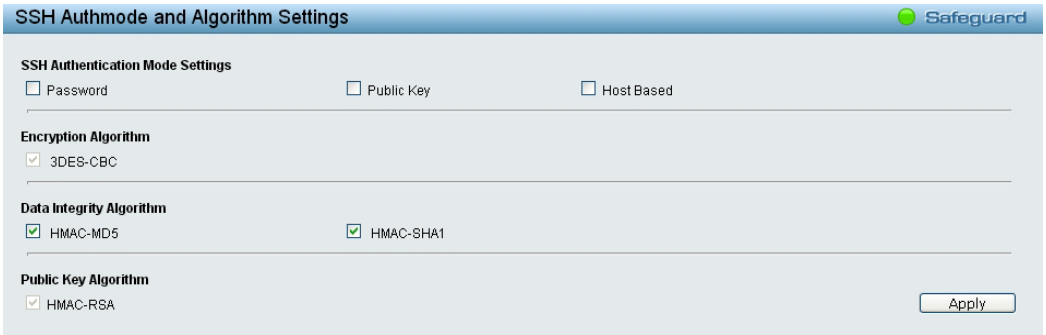


Figure 4.86 – Security > SSH > SSH Settings

SSH Authentication Mode Settings:

Password: Allows user to use a locally configured password for authentication on the Switch.

Public Key: This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch.

Host Based: This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed.

Encryption Algorithm:

3DES-CBC: Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.

Data Integrity Algorithm:

HMAC-MD5: Use the check box to enable the supports of hash for message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism.

HMAC-SHA1: Use the check box to enable the supports of hash for message Authentication Code (HMAC) Secure Hash Algorithm (SHA) mechanism.

Public Key Algorithm:

HMAC-RSA: Use the check box to enable the supports of Hash for Message Authentication Code (HMAC) mechanism utilizing the RSA encryption algorithm.

Click **Apply** to implement changes made.

Security > SSH > SSH User Authentication Lists

The SSH User Authentication Lists page is used to configure parameters for users attempting to access the Switch through SSH.

Figure 4.87 – Security > SSH > SSH User Authentication Lists

The user may view the following parameters:

User Name: A name of no more than *15* characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.

Auth. Mode: The administrator may choose one of the following to set the authorization for users attempting to access the Switch.

> **Host Based –** This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes.

Password – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.

Public Key – This parameter should be chosen if the administrator wishes to use the public key on an SSH server for authentication.

Host Name: Enter an alphanumeric string of no more than *32* characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Host IP: Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Security > Smart Binding > Smart Binding Settings

The primary purpose of Smart Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

The Smart Binding function is port-based, meaning that a user can enable or disable the function on any individual port. Once Smart Binding is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the “IMPB white list”.

Users can enable or disable the **Inspection packets** and **DHCP Snooping** on the Switch.

Figure 4.88 – Security > Smart Binding > Smart Binding Settings

The Smart Binding Settings page contains the following fields:

From Port/ To Port: Select a range of ports to set for IP-MAC-port binding.

State: Use the drop-down menu to enable or disable these ports for Smart Binding.

Enabled –Enable Smart Binding with related configurations to the ports

Disabled –Disable Smart Binding.

Packet Inspection: Specifies *ARP Inspection* or *IP+ARP Inspection* for the IP packets. If ARP inspection is selected, the Switch will inspect incoming ARP packets and compare them with the Switch’s Smart Binding white list entries. If the IP-MAC pair of an ARP packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources. However, it cannot block malicious users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets. If **ARP+ IP Inspection** mode is selected, the Switch will inspect all incoming ARP and IP packets and compare them to the IMPB white list. If the IP-MAC pair find a match in the white list, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the mode examines every ingress ARP and IP packet, it enforces better security.

DHCP Snooping: By enable DHCP Snooping, the switch will snoop the packets sent from DHCP Server and clients, and update information to the White List.

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

Security > Smart Binding > Smart Binding

The Smart Binding Settings page allows users to set IP-MAC-Port Binding entries by manually entering required information, or by scanning all connected devices and clicking to bind.

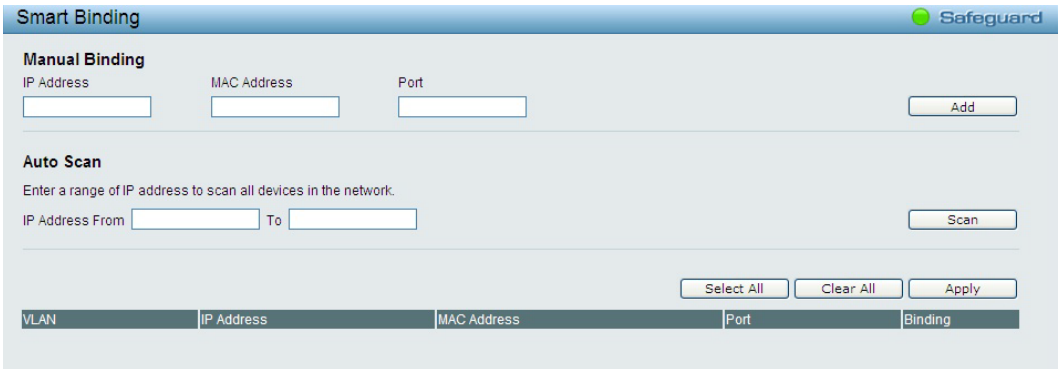


Figure 4.89 – Security > Smart Binding > Smart Binding

The Manual Binding Settings contains the following fields:

IP Address: Specifies the IP address to bind to the MAC address set below.

MAC Address: Specifies the MAC address to bind to the IP address set above.

Port: Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address).

Click **Add** to add a new entry.

Auto Scan: The Auto Scan Setting can list connected devices and easily select to bind. It contains the following fields:

IP Address From/To: Specifies the range of IP Address to find desired devices, or leaves the fields blank to see all connected devices.

Click **Scan** and the search results will be listed in below table.

Binding: check the box to select desired binding devices.

Apply: click **Apply** to set IP-MAC-Port Binding entries."

Select All: to check the boxes of Binding for all found devices.

Clear All: to cancel the box of Binding

Security > Smart Binding > White List

When IP +ARP Inspection Mode is selected, the White List page displays finished IP-MAC-Port Binding entries from page Smart Binding. Only IP packets or ARP packets carrying matched IP-MAC-Port information can access to the switch. You can cancel a device's authorization by deleting it from the table.

Figure 4.90 – Security > Smart Binding > White List

Select the check box of entry then click **Delete** to remove it.

Click **Select All** to select all entries of the table or click **Clean** to select none entries. Please keep at least one management host in the White List.

Security > Smart Binding > Black List

The Black List page shows unauthorized accesses. When ARP Inspection is selected and a device sends out an ARP packet containing unmatched IP-MAC-Port information, the device will be forbidden and listed here.

Figure 4.91 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below and then click **Find** to search for a list of the entry:

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

Port: Enter the port number which the device connects to.

Check a box of Delete column to release an entry from the forbidden list and then click **Apply** to delete an entry from the list.

Click **Select All** to select all entries, or click **Clean** to select none of the entries

AAA > RADIUS Server

The RUAIUS Server of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

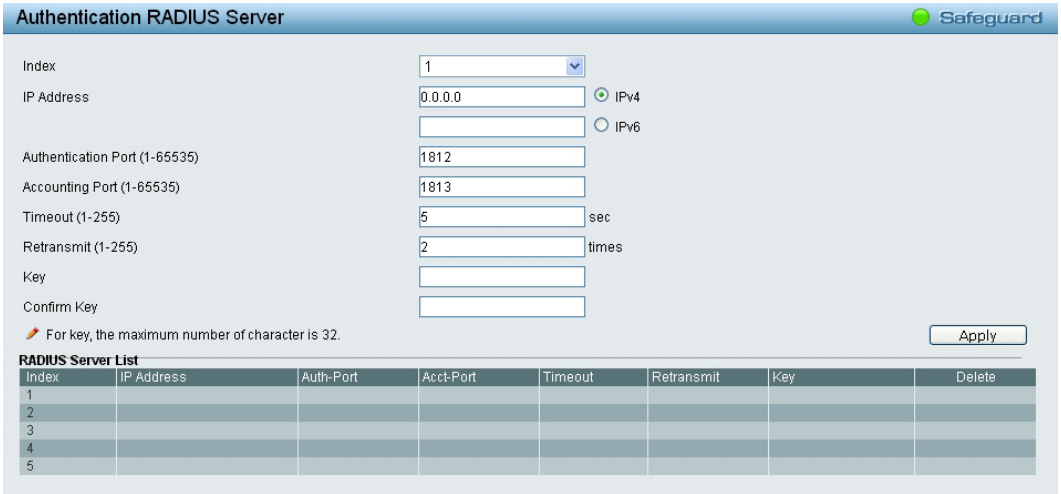


Figure 4.92 – AAA > RADIUS Server

Index: Choose the desired RADIUS server to configure: 1, 2 or 3.

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

Authentication Port (1 - 65535): Set the RADIUS authentic server(s) UDP port. The default port is 1812.

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

Timeout (1 – 255 sec): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *1* and *255* seconds. The default setting is *5* seconds.

Retransmit (1 – 255 times): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *2*.

Key: Set the key the same as that of the RADIUS server.

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

Click **Apply** to implement configuration changes.

AAA > 802.1X > 802.1X Global 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.

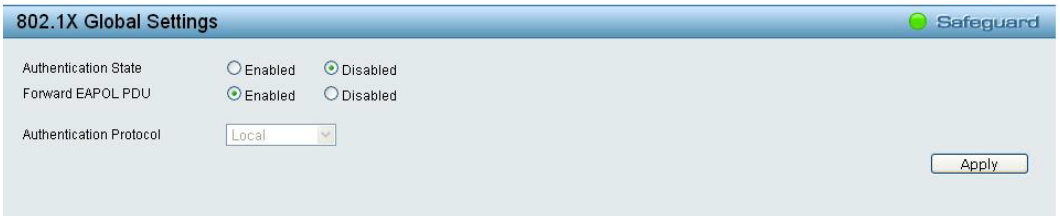


Figure 4.93 – AAA > 802.1x Global Settings

Authentication State: Specify to enable or disable the 802.1X function.

Forward EAPOL PDU: This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.

Authentication Protocol: Indicates the 802.1X Protocol on the device. The possible field values are *Local* and *RADIUS*.

Click **Apply** to implement configuration changes.

AAA > 802.1X > 802.1X Port Settings

To use EAP for security, set the 802.1X Port Settings for the Radius Server and applicable authentication information.

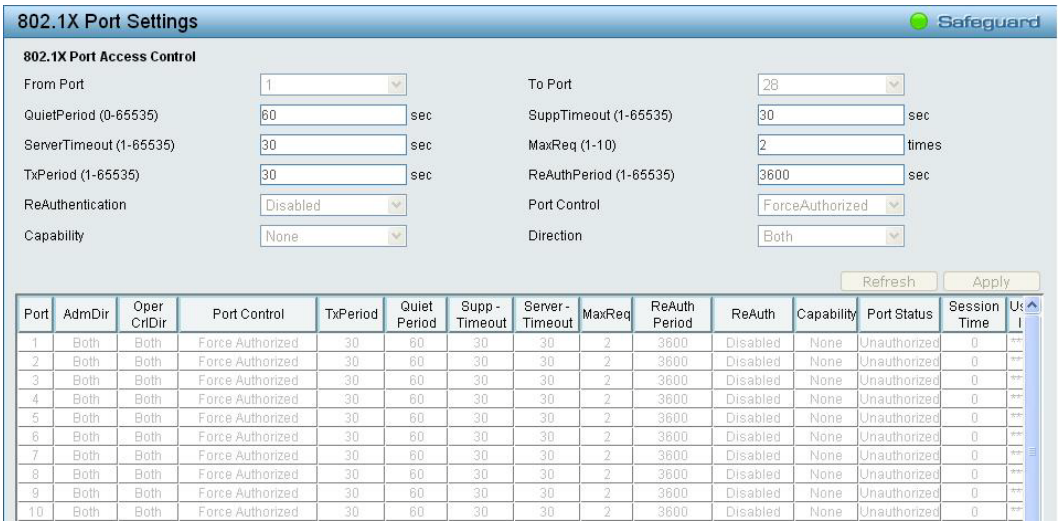


Figure 4.94 – AAA > 802.1X > 802.1X Port Settings

From Port/To Port: Enter the port or ports to be set.

QuietPeriod (0 – 65535 sec): Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is *60* seconds.

ServerTimeout (1 – 65535 sec): Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is *30* seconds.

TxPeriod (1 – 65535 sec): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. Default is *30* seconds.

ReAuthentication: Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.

Capability: Indicates the capability of the 802.1X. The possible field values are:

Authenticator – Specify the Authenticator settings to be applied on a per-port basis.

None – Disable 802.1X functions on the port.

SuppTimeout (1 – 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is *30* seconds.

MaxReq (1 – 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. Default is *2* times.

ReAuthPeriod (1 – 65535 sec): A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.

Port Control: This allows user to control the port authorization state.

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

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

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

The default setting is *Auto***.**

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

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

In – Disables the support in the present firmware release.

Click **Apply** to implement configuration changes.

AAA > 802.1X > 802.1X User

The **802.1X User** page allows user to set different local users on the Switch. Enter a **802.1X User** name, **Password** and **Confirm Password**. Properly configured local users will be displayed in the table.

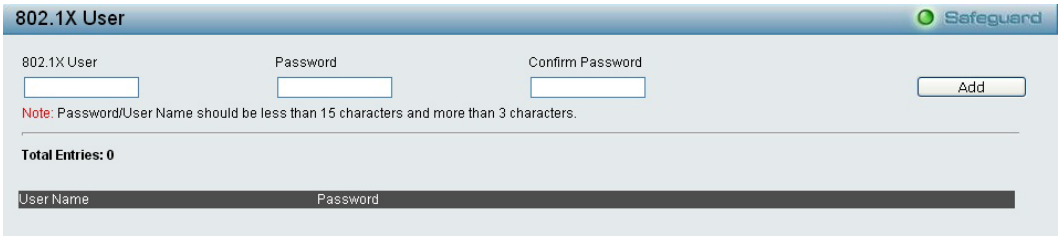


Figure 4.95 - AAA > 802.1X > 802.1X User

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

ACL > ACL Wizard

Access Control List (ACL) allows you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. This criteria can be specified on a basis of the MAC address, or IP address.

The ACL Configuration Wizard will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 200 Rules in total for the switch.

To create a new access rule, select **Create** and enter the **Access-List Name** then click **Next** button.

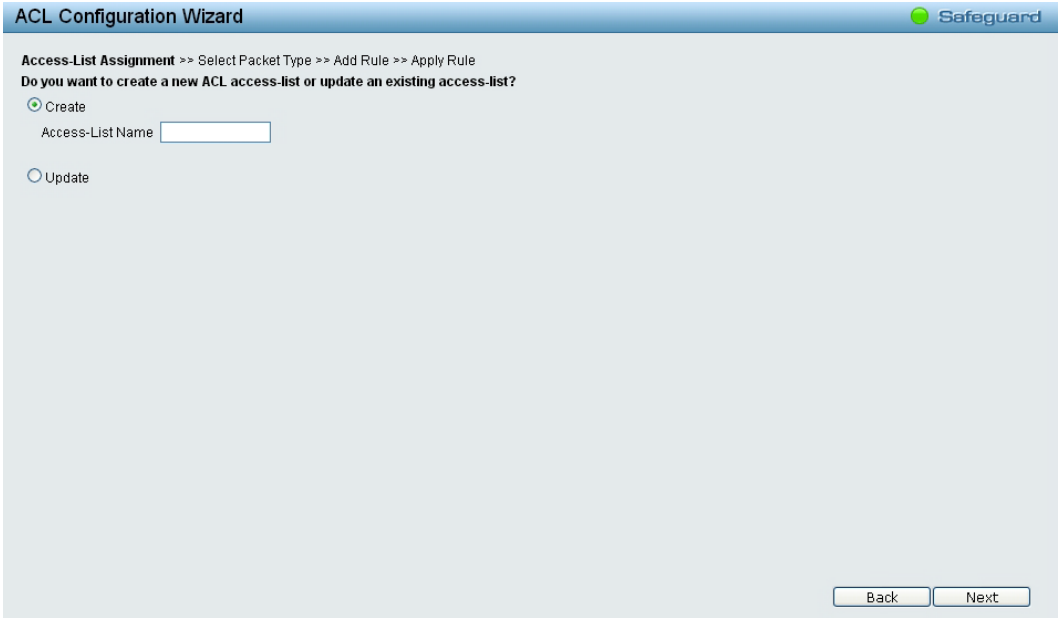


Figure 4.96 - ACL > ACL Wizard – Create Access-List

The steps of adding an access profile are described below:

1) Select the **Packet Type**: **MAC**, **IPv4** or **IPv6**.

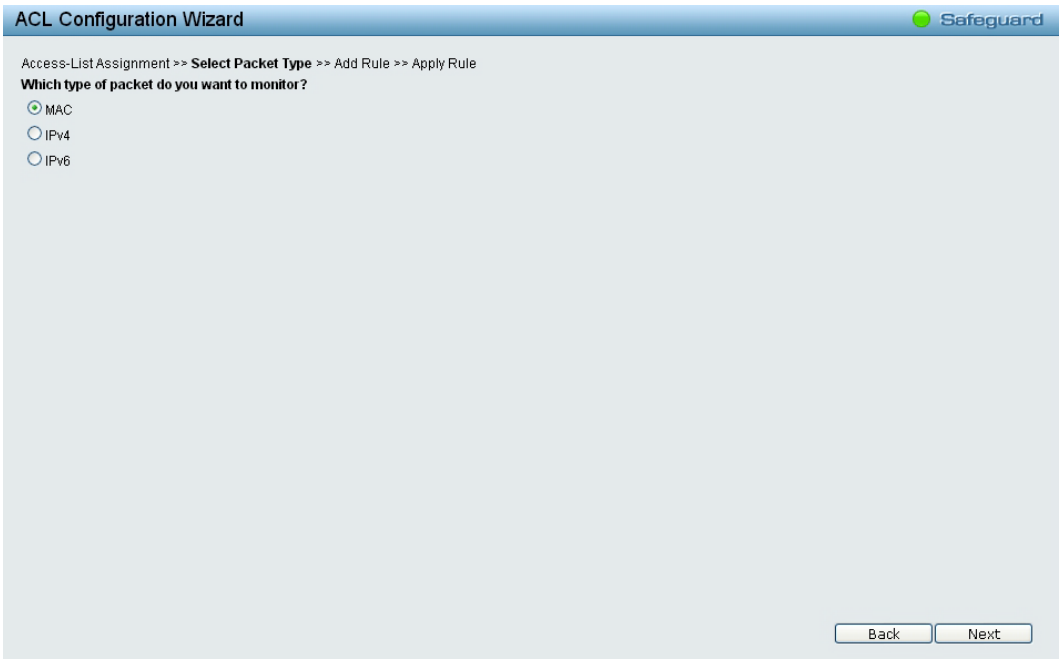


Figure 4.97 - ACL > ACL Wizard – Select Packet Type

Select packet type based on MAC address, IPv4 address, IPv6 address or packet content. This will change the window according to the requirements for the type of profile.

MAC: Defines the ACL profile Layer 2 protocols. Select MAC to monitor MAC address of each packet.

IPv4: Defines the IPv4 ACL profile protocols. Select IPv4 to monitor IPv4 address of each packet.

IPv6: Defines the IPv6 ACL profile protocols. Select IPv6 to monitor IPv6 address of each packet.

To define the MAC ACL Rule: Select **MAC** click **Next** button. The updates to show the follows:

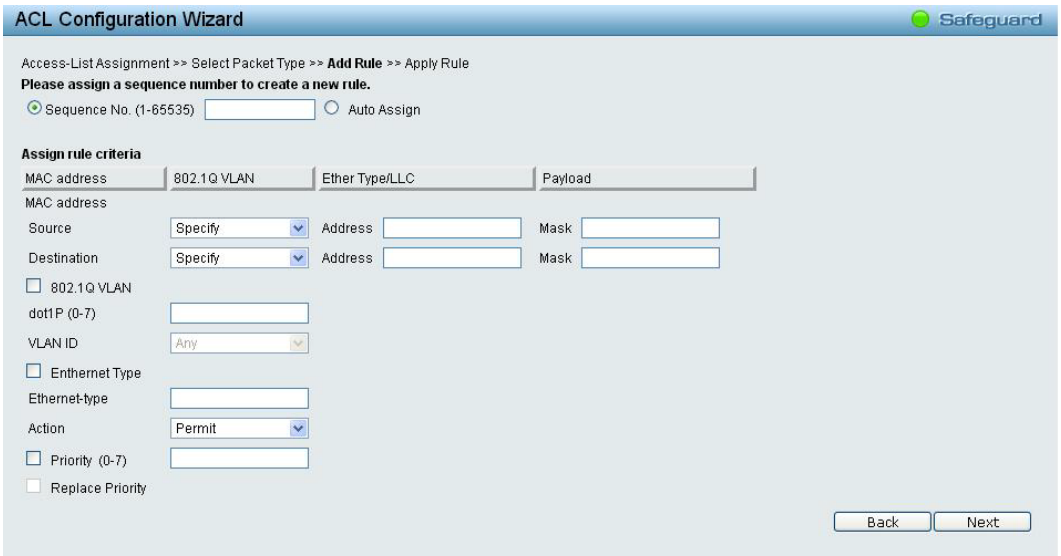


Figure 4.98 – Add Access Rule - MAC

Assign sequence number:

Sequence No. (1-65535): Specify the sequence number. The value is from 1 to 65535.

Auto Assign: Auto assign the sequence number for a new rule.

Assign Rule Criteria: Specify the MAC address settings.

Source: Select the source MAC to be specified or Any. Enter a source MAC address and source MAC mask, e.g. FF-FF-FF-FF-FF-FF.

Destination: Select the destination MAC to be specified or Any. Enter a destination MAC address and destination MAC mask, e.g. FF-FF-FF-FF-FF-FF.

If user selects the **802.1Q VLAN** box, then need to specify the **dot1p** and **VLAN ID**.

Dot1p (0-7): Specify the dot1p priority.

VLAN ID: Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.

If user selects the **Ethernet Type** box, then need to specity the **Ethernet Type** and select the **Action**.

Ethernet Type: Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Action: Specify the ACL forwarding action matching the rule criteria. **Permit** forwards packets if all other ACL criteria are met. **Deny** drops packets if all other ACL criteria is met.

Priority (0-7): Specify the MAC ACL priority whish values are 0-7.

Replace Priority: Check the box to enable the Replace Priority feature.

Click **Next** button then the ACL profile is added.

To define the IPv4 ACL Rule: Select **IPv4** with **ICMP** click **Next** button. The updates to show the follows:

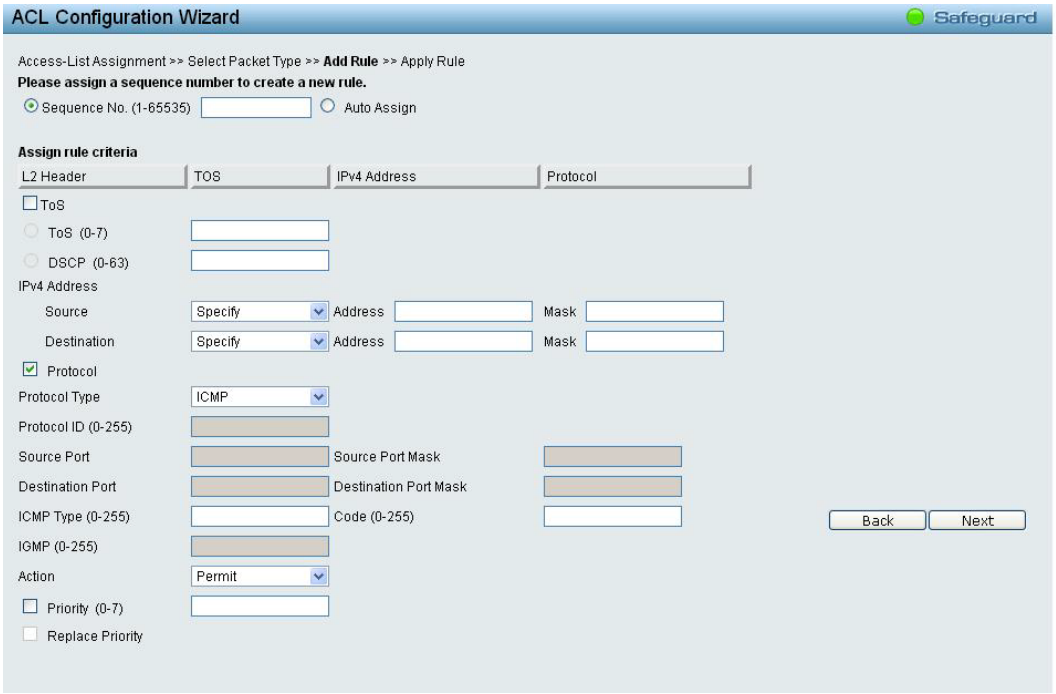


Figure 4.99 - Add Access Rule – IPv4 ICMP

Assign sequence number:

Sequence No. (1-65535): Specify the sequence number. The value is from 1 to 65535.

Auto Assign: Auto assign the sequence number for a new rule.

Assign Rule Criteria: Specify the IPv4 ACL settings.

ToS: Check the box to specify the ToS priority and DSCP value.

ToS (0-7): Specify the ToS value.

DSCP (0-63): Specify the DSCP value. The values are between 0 and 63.

IPv4 Address: Specify the IPv4 Source and destination address.

Source: Select the source IP to be specified or Any relevant to the ACL rules. Enter a source IP address and source IP mask. For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination: Select the destination IP to be specified or Any relevant to the ACL rules. Enter a destination IP address and destination IP mask. For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Protocol: Check **Protocol** to configure the related settings.

Protocol Type: Select the protocol type for IPv4. The possible fields are **ICMP, IGMP, TCP, UDP** and **Protocol ID**.

ICMP Type (0-255): Sets the ICMP Type field as an essential field to match.

Code (0-255): Sets the ICMP code field as an essential field to match.

Select the ports which added into the **Access-List** and click **Next** button then the ACL profile is added.

To define the IPv4 ACL IGMP Rule: Select **IPv4 ACL** with **IGMP** and click **Next** button. The updates to show the follows:

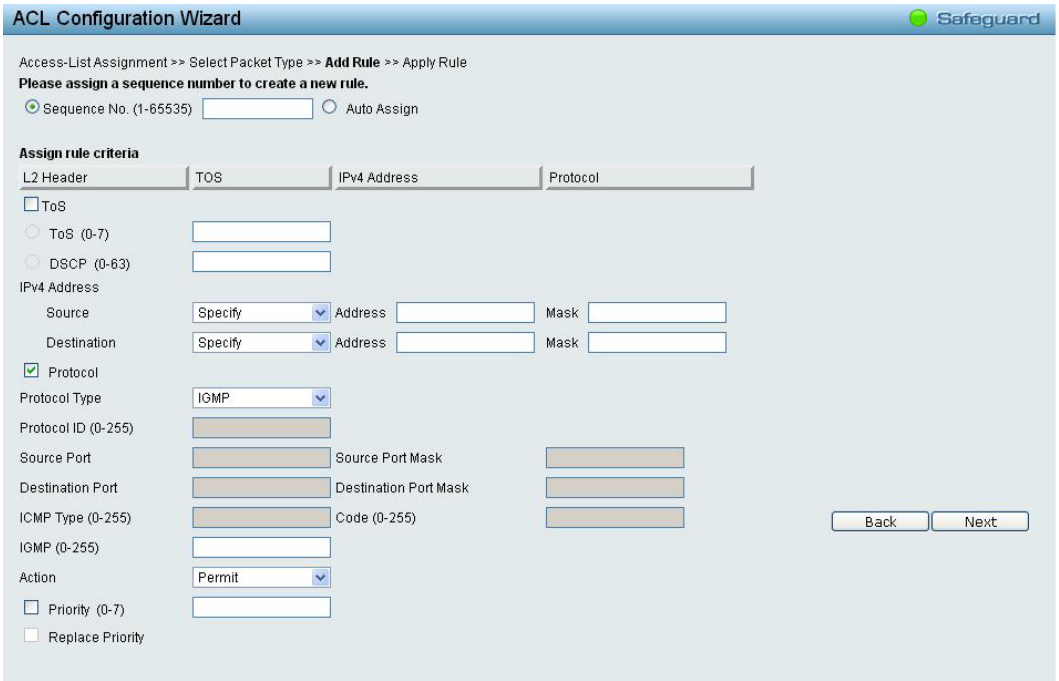


Figure 4.100 - Add Access Rule – IPv4 IGMP

IGMP Type (0-255): Sets the IGMP Type field as an essential field to match.

Click **Next** button then the ACL profile is added.

To define the IPv4 ACL TCP Rule: Select **IPv4 ACL** with **TCP** and click **Next** button. The updates to show the follows:

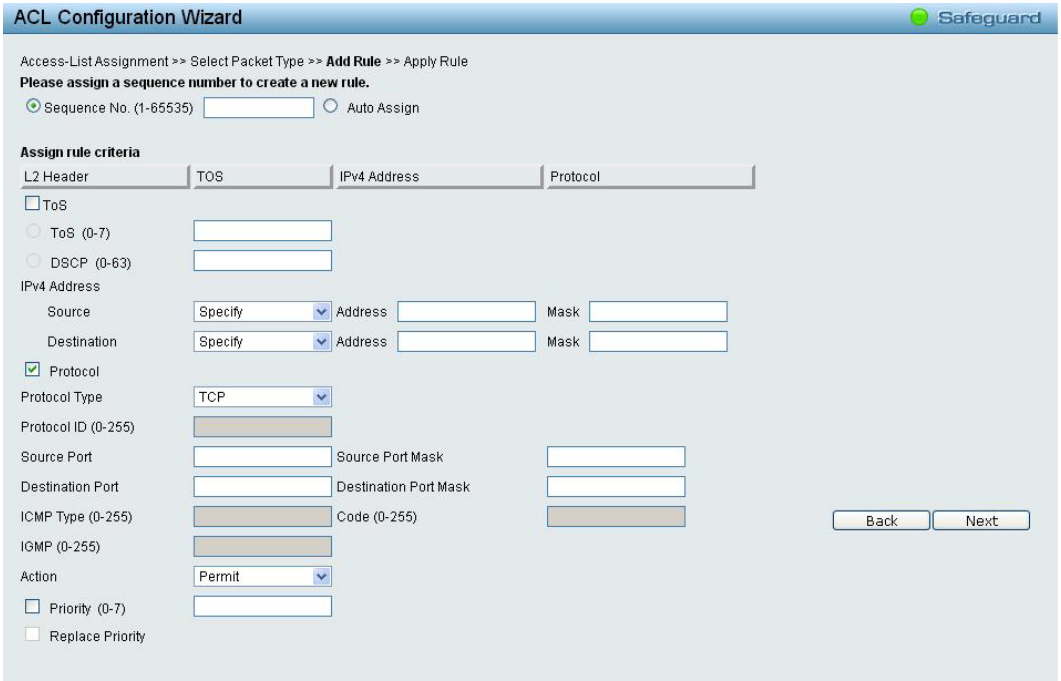


Figure 4.101 - Add Access Rule – IPv4 TCP

IPv4 Address: Defines the range of source Ports relevant to the ACL rules.

Source: Defines the range of source Ports relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

To define the IPv4 ACL UDP Rule: Select **IPv4 ACL** with **UDP** and click **Next** button. The updates to show the follows:

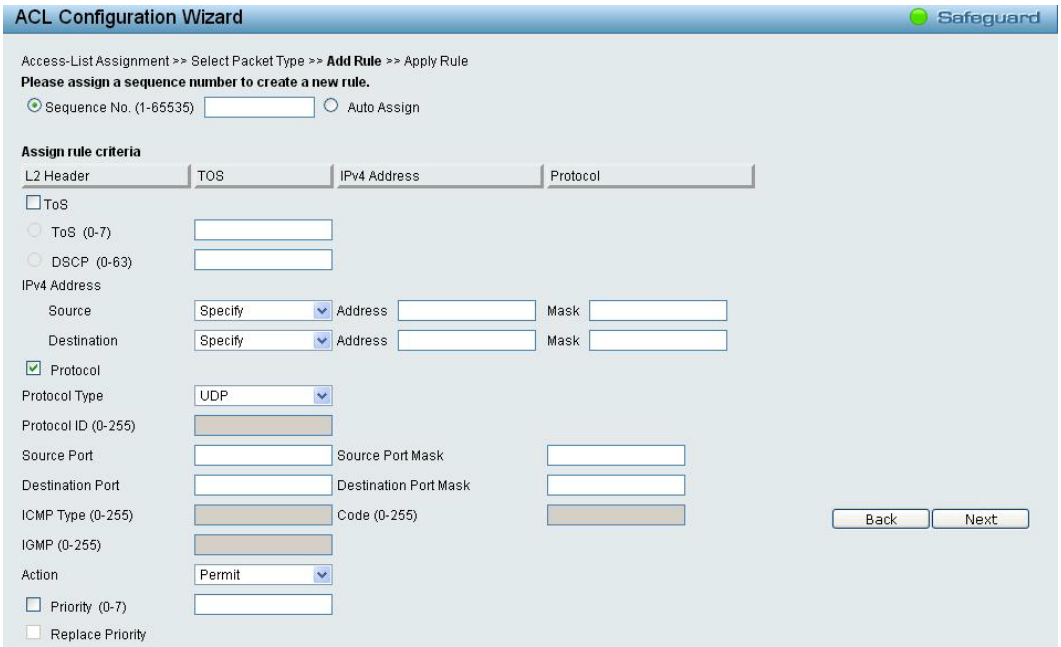


Figure 4.102 - Add Access Rule – IPv4 UDP

IPv4 Address: Defines the range of source Ports relevant to the ACL rules.

Source: Defines the range of source Ports relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

NOTE: A combination of one or several filtering masks can be selected simultaneously. The page updates with the relevant field(s).

To define the IPv6 ACL ICMP rule: Select **IPv6 ACL** with **ICMP** of **Protocol Type** and click **Next** button. The updates to show the follows:

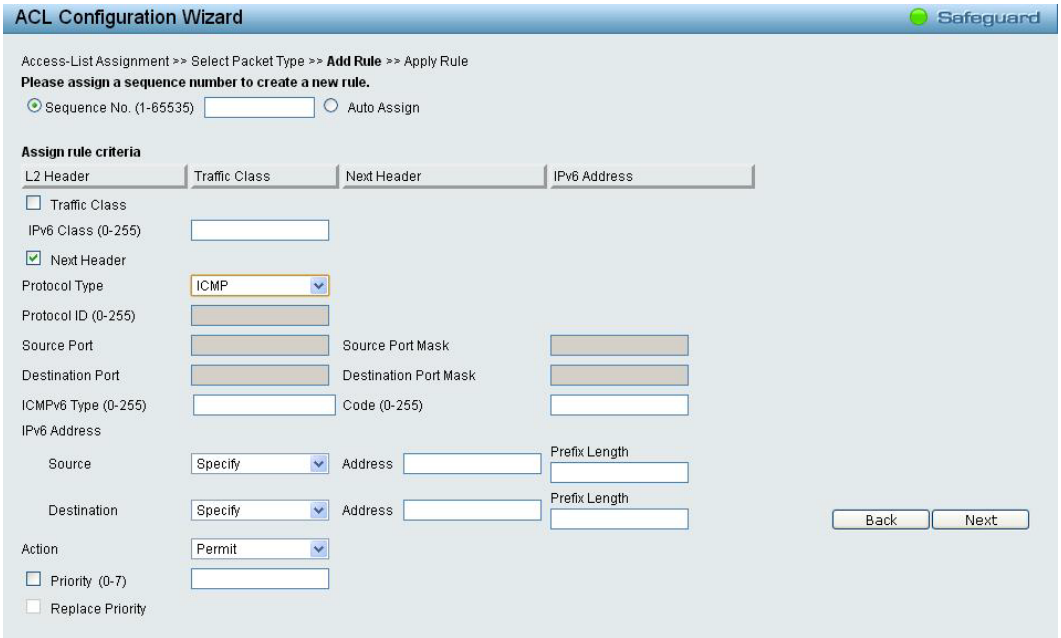


Figure 4.103 - Add Access Rule – IPv6 UDP

IPv6 Class (0-255): Specify the class of access rule. The field range is from 0 to 255.

ICMPv6 Type: Sets the ICMP Type field as an essential field to match.

Code (0-255): Sets the ICMP code field as an essential field to match.

Source IPv6 Address: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 2002:0:0:0:0:0:b0d4:0, use mask 128.

Destination IPv6 Address: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 2002:0:0:0:0:0:bfd4:0, use mask 128.

Action: Specify the ACL forwarding action matching the rule criteria. **Permit** forwards packets if all other ACL criteria are met. **Deny** drops packets if all other ACL criteria is met.

Click **Next** button then the ACL profile is added.

To define the IPv6 ACL TCP profile: Select **IPv6 ACL** with **TCP** of **Protocol Type** and click **Next** button. The updates to show the follows:

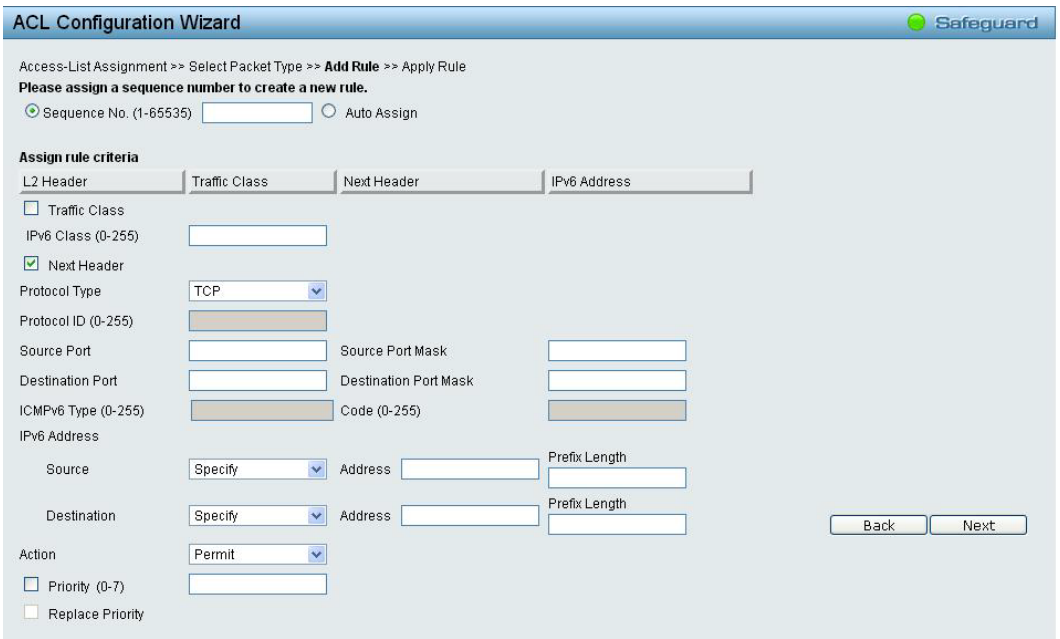


Figure 4.104 - Add Access Rule – IPv6 TCP

Source Port: Specify the source port.

Source Port Mask: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination Port: Specify the destination port.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

To define the IPv6 ACL UDP profile: Select **IPv6 ACL** with **UDP** of **Protocol Type** and click **Next** button. The updates to show the follows:

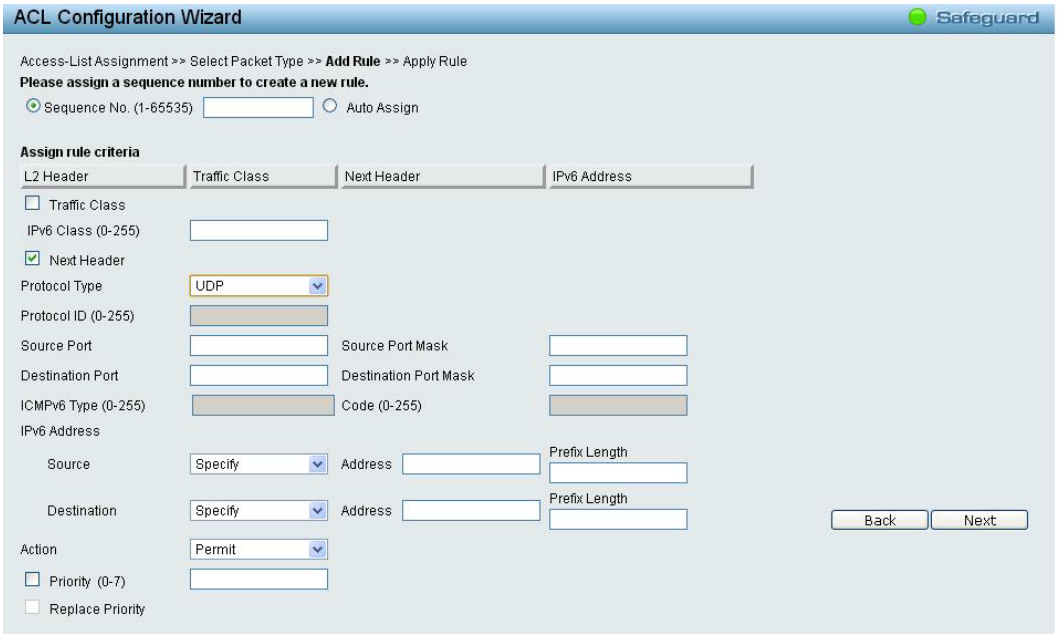


Figure 4.105 - Add Access Rule – IPv6 UDP

Source Port: Specify the source port.

Source Port Mask: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination Port: Specify the destination port.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

2) Selecting the field of interest will display the next page which shows the follows:

Figure 4.106 - Add Access Rule – Ports

Click **Next** button then the ACL profile is added.

3) To modify an existing rule, please select **Update** and the **Access-List Name** hyperlink and click **Next** button.

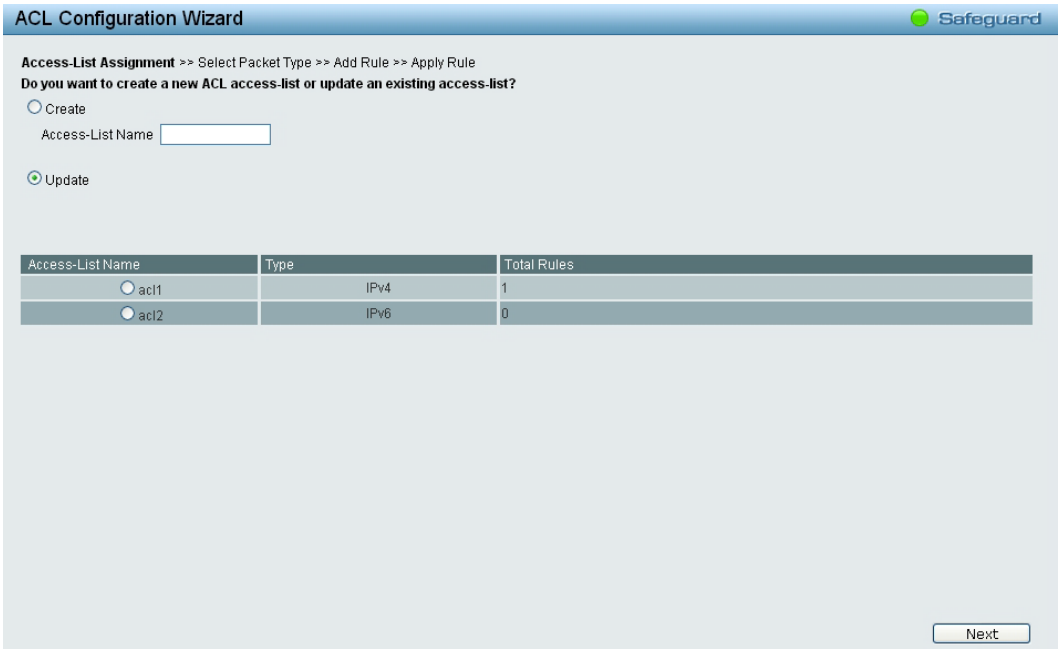


Figure 4.107 - ACL > ACL Wizard – Update ACL List

ACL > ACL Access List

The **ACL Access List** page provides information for configuring ACL Access manually. Click **Edit Rules** button to modify the access profile or click **Delete** button to remove the ACL profile.

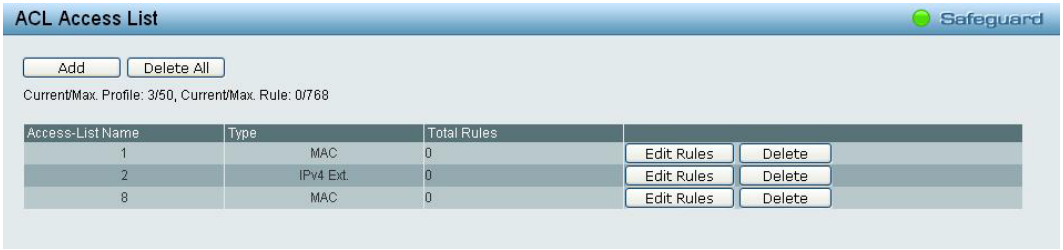


Figure 4.108 - ACL > ACL Access List

To add a new profile, click **Add** button. The updates to show the follows:

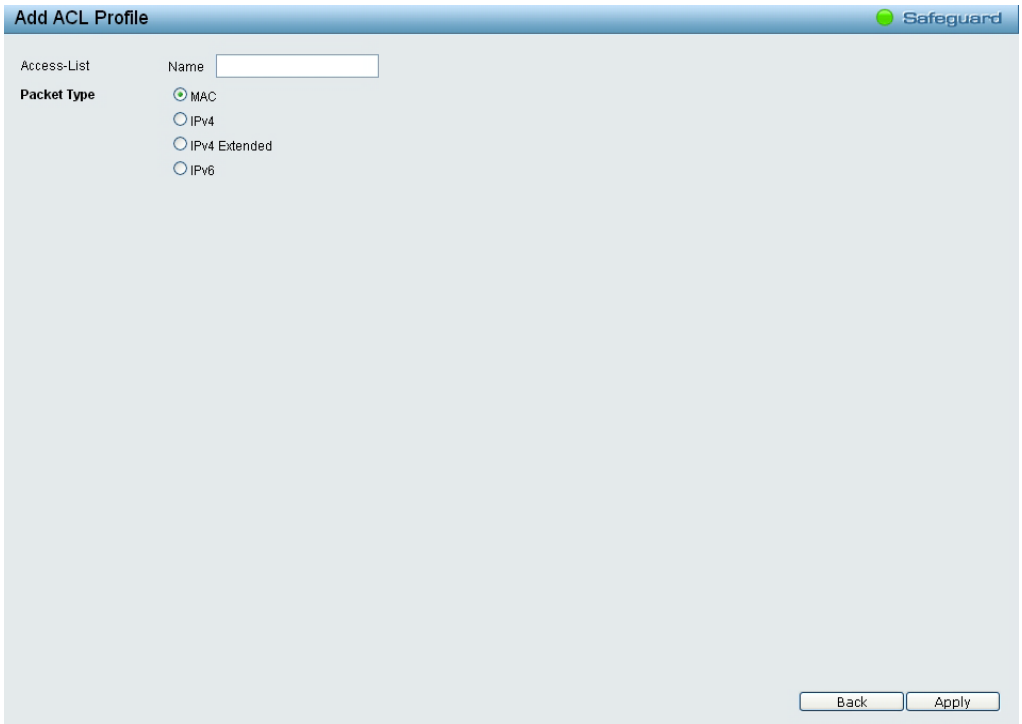


Figure 4.109 - ACL > ACL Access List – Add ACL Profile

Access-List: Specify the access list name for the ACL profile to be added.
Packet Type: Specify the packet type to be **MAC**, **IPv4**, **IPv4 Exdended** or **IPv6** then click **Apply** button.

To modify an existing rule, please click on the Sequence No. hyperlink.

Figure 4.110 - ACL > ACL Access List – Update ACL Profile

ACL > ACL Access Group

The **ACL Access Group** page allows user to configure the ACL access group settings.

Figure 4.111 - ACL > ACL Access Group

Port: Specify the ports to be added in the access list group.
MAC Access-List: Add the specified ports in the MAC access list group.

IPv4 Access-List: Add the specified ports in the IPv4 access list group.
IPv6 Access-List: Add the specified ports in the IPv6 access list group.

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

ACL > ACL Hardware Resource Status

The **ACL Hardware Resource Status** page displays the information of ACL Hardware Resource status.

Hardware Profile ID	Access-List Name	Consumed/Total Entries
1	IMPBV6	2
2	IMPB	1
3		0
4		0
5		0
6		0

Figure 4.112 - ACL > ACL Hardware Resource Status

SNMP > SNMP > SNMP Global Settings

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

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

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

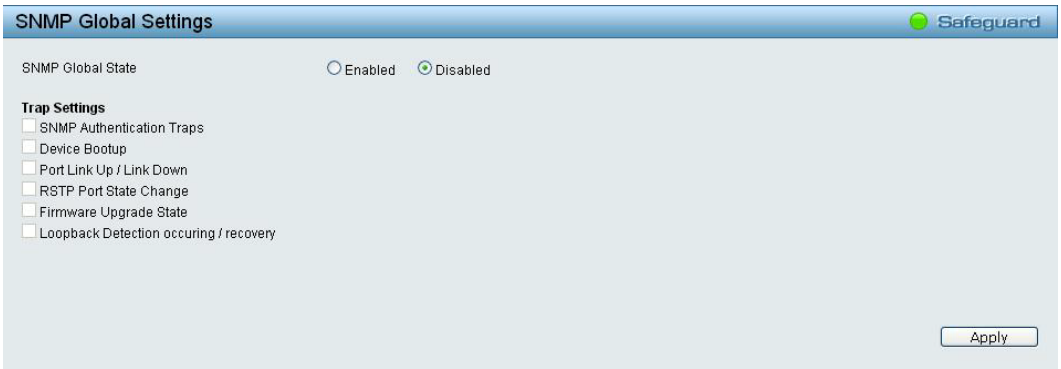


Figure 4.113 – SNMP > SNMP > SNMP Global Settings

Trap Settings: Specifies whether the device can send SNMP notifications.

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

Device Bootup: System boot-up information.

Illegal Login: Events of incorrect password logins, recording the IP of the originating PC.

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

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

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

SNMP > SNMP > SNMP User

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.

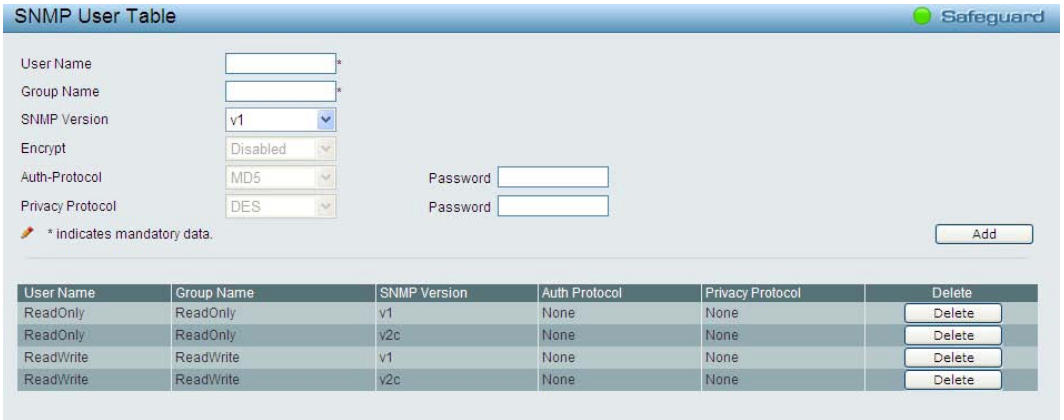


Figure 4.114 – SNMP > SNMP > SNMP User Table

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

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

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

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

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

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

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

SNMP > SNMP > SNMP Group Table

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

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

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

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

Security Model: Select the SNMP security model.

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

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

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

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

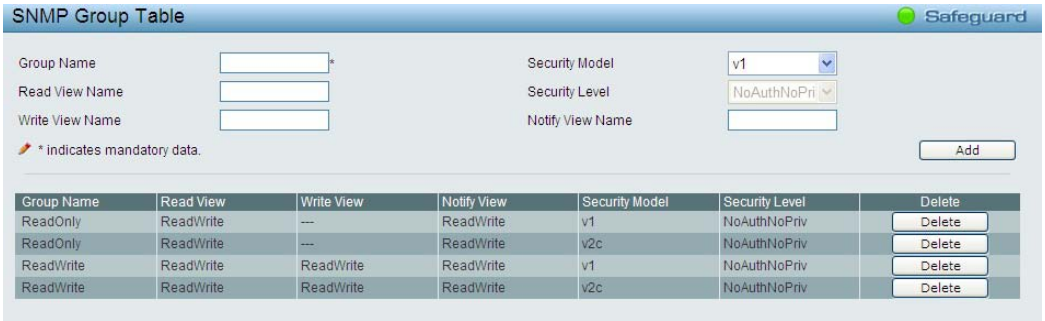


Figure 4.115 – SNMP > SNMP > SNMP Group Table

SNMP > SNMP > SNMP View

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

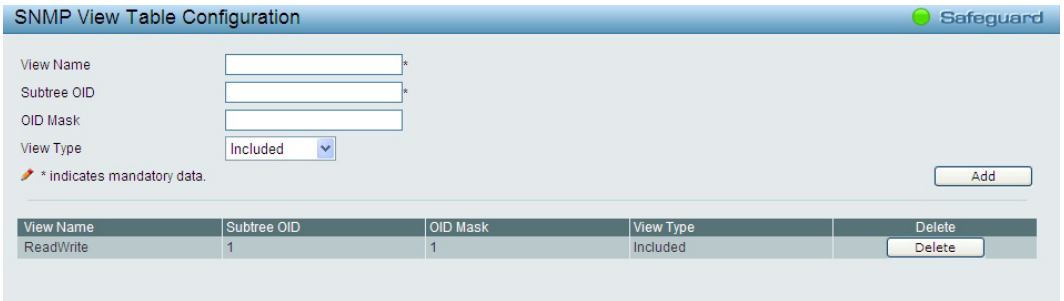


Figure 4.116 – SNMP > SNMP > SNMP View

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

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

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

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

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

SNMP > SNMP > SNMP Community

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

Community Name: Name of the community string

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

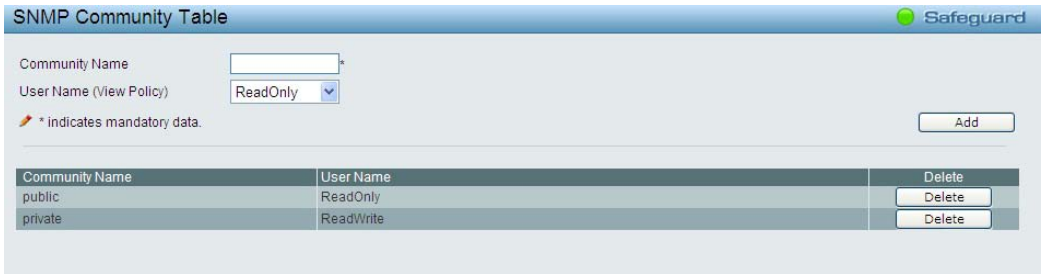


Figure 4.117 –SNMP > SNMP > SNMP Community

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

SNMP > SNMP > SNMP Host

This SNMP Host page is to configure the SNMP trap recipients.

Figure 4.118 – SNMP > SNMP > SNMP Host

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.

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

SNMP > SNMP > SNMP Engine ID

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

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

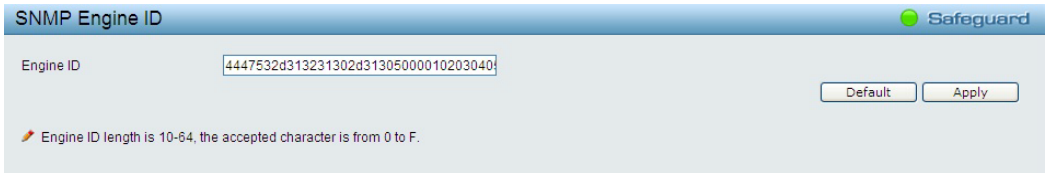


Figure 4.119 – SNMP > SNMP > SNMP Engine ID

SNMP > RMON > RMON Global Settings

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

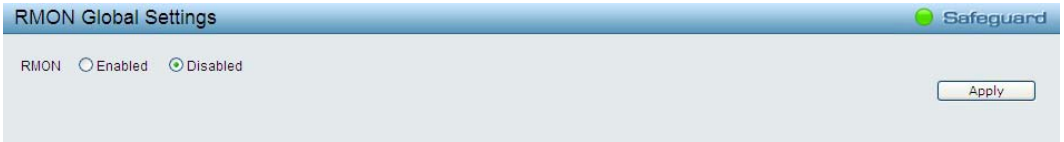


Figure 4.120 - SNMP > RMON > RMON Global Settings

SNMP > RMON > RMON Statistics

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

Figure 4.121 - SNMP > RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:

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

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

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

Click **Add** to make the configurations take effects and click **Refresh** to redisplay the table information.

SNMP > RMON > RMON History

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.

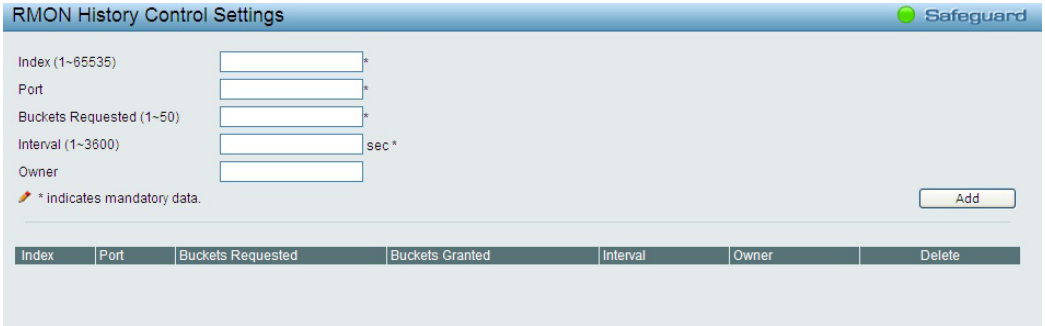


Figure 4.122 - SNMP > RMON > RMON History Control Settings

The History Control Configuration contains the following fields:

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

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

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

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

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

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

SNMP > RMON > RMON Alarm Settings

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

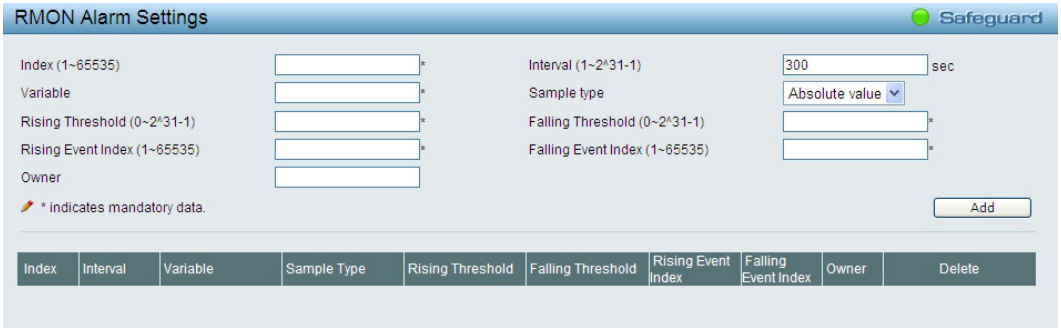


Figure 4.123 - SNMP > RMON > RMON Alarm Settings

The configuration contains the following fields:

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

Variable: Specify the selected MIB variable value.

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

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

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

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

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

Delta value – Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Absolute value – Compares the values directly with the thresholds at the end of the sampling interval.

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

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

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

SNMP > RMON > RMON Event

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

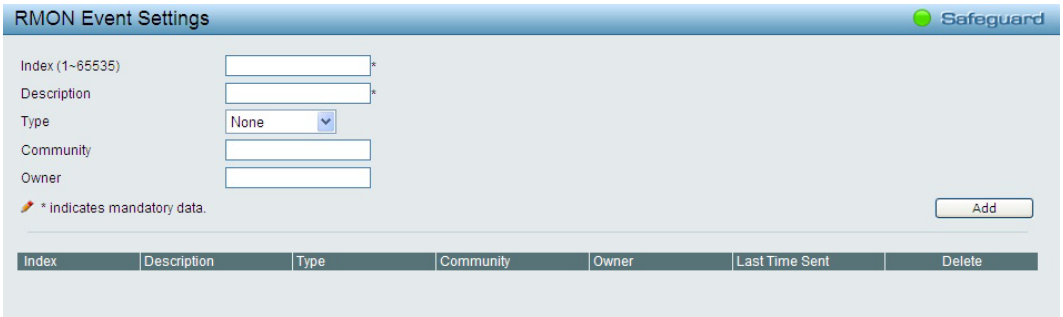


Figure 4.124 - SNMP > RMON > RMON Event Settings

The RMON Events Page contains the following fields:

Index (1~ 65535): Displays the event.

Description: Specifies the user-defined event description.

Type: Specifies the event type. The possible values are:

None – Indicates that no event occurred.

Log – Indicates that the event is a log entry.

SNMP Trap – Indicates that the event is a trap.

Log and Trap – Indicates that the event is both a log entry and a trap.

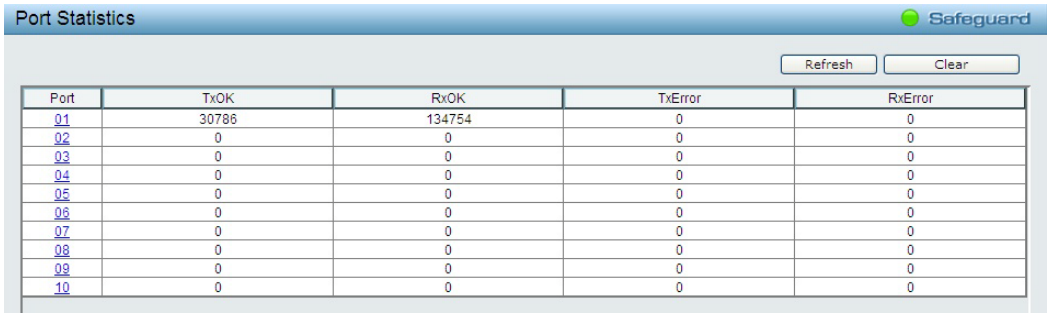
Community: Specifies the community to which the event belongs.

Owner: Specifies the time that the event occurred.

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

Monitoring > Port Statistics

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



Port	TxOK	RxOK	TxError	RxError
01	30786	134754	0	0
02	0	0	0	0
03	0	0	0	0
04	0	0	0	0
05	0	0	0	0
06	0	0	0	0
07	0	0	0	0
08	0	0	0	0
09	0	0	0	0
10	0	0	0	0

Figure 4.125 – Monitoring > Port Statistics

Refresh: Renews the details collected and displayed.

Clear: 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 4.126 – Monitoring > Port Statistics

Back: Go back to the Statistics main page.
Refresh: To renew the details collected and displayed.
Clear: To reset the details displayed.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

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

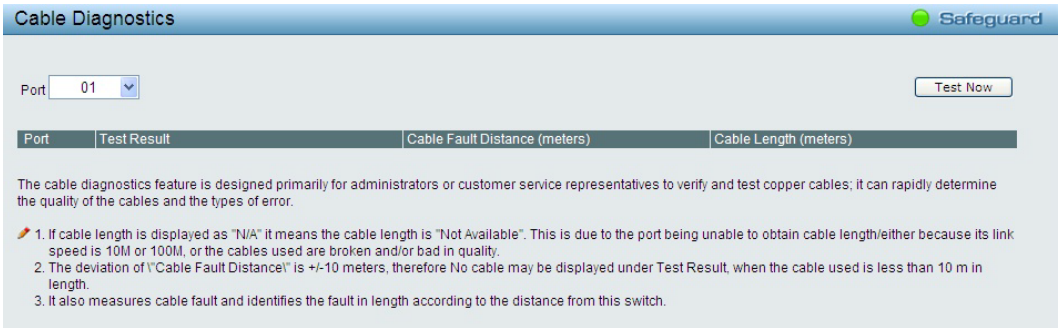


Figure 4.127 – Monitoring > Cable Diagnostic

Test Result: The description of the cable diagnostic results.

- **OK** means the cable is good for the connection.
- **Short in Cable** means the wires of the RJ45 cable may be in contact somewhere.
- **Open in Cable** means the wires of RJ45 cable may be broken, or the other end of the cable is simply disconnected.
- **Test Failed** means some other errors occurred during cable diagnostics. Please select the same port and test again.

Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show “No Cable”.

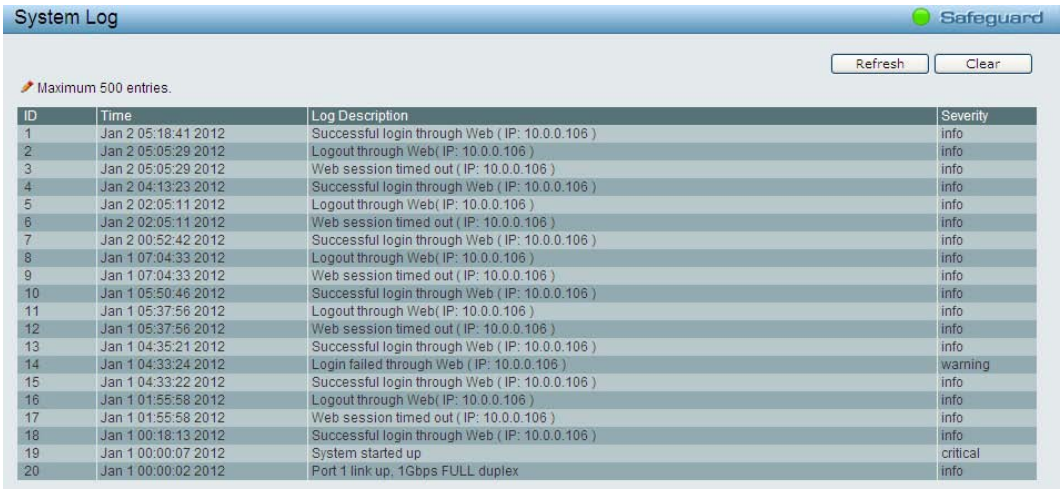
Cable Length (meter): If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and >100 meters.

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

NOTE: Please be sure that Power Saving feature is disabled before enabling Cable Diagnostics function.

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.



ID	Time	Log Description	Severity
1	Jan 2 05:18:41 2012	Successful login through Web (IP: 10.0.0.106)	info
2	Jan 2 05:05:29 2012	Logout through Web(IP: 10.0.0.106)	info
3	Jan 2 05:05:29 2012	Web session timed out (IP: 10.0.0.106)	info
4	Jan 2 04:13:23 2012	Successful login through Web (IP: 10.0.0.106)	info
5	Jan 2 02:05:11 2012	Logout through Web(IP: 10.0.0.106)	info
6	Jan 2 02:05:11 2012	Web session timed out (IP: 10.0.0.106)	info
7	Jan 2 00:52:42 2012	Successful login through Web (IP: 10.0.0.106)	info
8	Jan 1 07:04:33 2012	Logout through Web(IP: 10.0.0.106)	info
9	Jan 1 07:04:33 2012	Web session timed out (IP: 10.0.0.106)	info
10	Jan 1 05:50:46 2012	Successful login through Web (IP: 10.0.0.106)	info
11	Jan 1 05:37:56 2012	Logout through Web(IP: 10.0.0.106)	info
12	Jan 1 05:37:56 2012	Web session timed out (IP: 10.0.0.106)	info
13	Jan 1 04:35:21 2012	Successful login through Web (IP: 10.0.0.106)	info
14	Jan 1 04:33:24 2012	Login failed through Web (IP: 10.0.0.106)	warning
15	Jan 1 04:33:22 2012	Successful login through Web (IP: 10.0.0.106)	info
16	Jan 1 01:55:58 2012	Logout through Web(IP: 10.0.0.106)	info
17	Jan 1 01:55:58 2012	Web session timed out (IP: 10.0.0.106)	info
18	Jan 1 00:18:13 2012	Successful login through Web (IP: 10.0.0.106)	info
19	Jan 1 00:00:07 2012	System started up	critical
20	Jan 1 00:00:02 2012	Port 1 link up, 1Gbps FULL duplex	info

Figure 4.128 – 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 a description event recorded.

Severity: Displays a severity level of the event recorded.

Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.

Command Line Interface

The D-Link Web Smart Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.

To connect a switch via TELNET:

1. Make sure the network connection between the switch and PC is active.
2. To connect, launch any terminal software like ***HyperTerminal*** in Microsoft Windows, or just use the command prompt by typing the command *telnet* followed by the switch IP address, eg. *telnet 10.90.90.90*.
3. The logon prompt will appear.

Logging on to the Command Line Interface:

Enter your User Name and Password to log in. The default user name and password is **admin**. Note that the user name and password are case-sensitive. Press **Enter** in both the Username and Password fields. The command prompt will appear as shown below (**DGS-1210-28>):**

```
DGS-1210-28 login: admin
Password:

DGS-1210-28>
```

Figure 5.1 – Command Prompt

The user session is automatically terminated if idle for the login timeout period. The default login timeout period is 5 minutes. To change the login timeout session, please refer to chapter 5.

CLI Commands:

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
?	
download	{ firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>
Upload	{ firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>
config ipif system	{ ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp | bootp }
config ipif system	{ ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] }
logout	
ping	<ip_addr>
ping6	<ipv6addr>
create iproute	default <ipaddr>
delete iproute	{default}
show iproute	{ <ipaddr> | static }
reboot	
reset config	
show ipif	

Command	Parameter
show switch	
config account admin password	<passwd>
save	
debug info	

Each command is listed in detail, as follows:

?	
Purpose	To display a list of commands.
Syntax	?
Description	The ? command displays a list of commands of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display a list of commands of the switch:

```
DGS-1210-28> ?
USEREXEC commands :
  config account admin password <passwd>
  config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp }
  debug info
  download { firmware_fromTFTP tftp://ip-address/filename | cfg_fromTFTP tftp://ip-address/filename }
  logout
  ping <ip_addr>
  reboot
  reset config
  save
  show ipif
  show switch
  upload { firmware_toTFTP tftp://ip-address/filename | cfg_toTFTP tftp://ip-address/filename }
DGS-1210-28>
```

download	
Purpose	To download and install a firmware, boot, or switch configuration file from a TFTP server.
Syntax	download **{ firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>**

Description	The download command downloads a firmware, boot, or switch configuration file from a TFTP server.
Parameters	*firmware_fromTFTP* − Download and install new firmware on the Switch from a TFTP server. *cfg_fromTFTP* − Download a switch configuration file from a TFTP server. <*ipaddr*> − The IPv4 address of the TFTP server. <*ipv6addr*> − The IPv6 address of the TFTP server. <*path_filename*> − The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server.
Restrictions	None.

Example usage:

To download a firmware file:

```
DGS-1210-28> download firmware_fromTFTP 1.1.1.23 1\dgs_1210-10032.ros

01–Jan–2000 01:19:48 %COPY–I–FILECPY: Files Copy – source URL tftp://1.1.1.23 /1\
dgs_1210—10032.ros destination URL Unit all flash://image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!01–Jan–2000 01:22:49 %COPY–W–TRAP:
The copy operation was completed successfully
!
3920460 bytes copied in 00:03:01 [hh:mm:ss]


DGS-1210-28>
```

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

upload

Purpose	To upload the firmware file or a Switch configuration file to a TFTP server.

Syntax	**upload { firmware_fromTFTP | cfg_fromTFTP } {<ipaddr> | <ipv6addr>} <path_filename>**
Description	The upload command uploads the Switch's current settings to a TFTP server.
Parameters	*firmware_toTFTP* − Upload the firmware on the Switch from a TFTP server. *cfg_toTFTP* − Specifies that the Switch's current settings will be uploaded to the TFTP server. *<ipaddr>* − The IPv4 address of the TFTP server. *<ipv6addr>* − The IPv6 address of the TFTP server. *<path_filename>* − The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server.
Restrictions	None.

Example usage:

To upload a firmware file:

```
DGS-1210-28>upload firmware_toTFTP 1.1.1.23 1\running—config

01-Jan-2000 01:26:11 %COPY-I-FILECPY: Files Copy - source URL
running-config destination URL tftp://1.1.1.23/1\running-config

.....01-Jan-2000 01:26:16 %COPY-W-TRAP: The copy operation was
completed success fully

!

158 bytes copied in 00:00:05 [hh:mm:ss]

DGS-1210-28>
```

config ipif system

Purpose	To configure the System IP interface.
Syntax	**config ipif system { ipaddress <ip-address> <subnet-mask> gateway <gw-address> | dhcp | bootp }**
Description	The config ipif system command configures the System IP interface on the Switch.
Parameters	*ipaddress <ip-address> <subnet-mask>* − The IP address and subnet mask to be created. Users need to specify the address and mask information using the traditional format (for example,10.1.2.3/255.0.0.0) *gateway <gw-address>* − The IP address of the router or gateway. *dhcp* − Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. *bootp* − Allows the selection of the BOOTP to the switch.
Restrictions	None.

Example usage:

To configure the IP interface System:

```
DGS-1210-28> config ipif System ipaddress 10.48.74.122/8
```

```
Success.

DGS-1210-28>
```

config ipif system

Purpose	To configure the System IPv6 interface.
Syntax	**config ipif system { ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] }**
Description	The `config ipif system` command configures the System IPv6 interface on the Switch.
Parameters	*ipv6 ipv6address <ipv6networkaddr>* − Use this parameter to statically assign an IPv6address to this interface. This address should define a host address and a network prefix length. Multiple IPv6 addresses can be configured for a single IP interface. Ex: 3ffe:501:ffff:100::1/64. The /64 represents the prefix length of the IPv6 addresses. *dhcpv6_client [enable | disable]* − Specify the DHCPv6 client to be disabled or enabled.
Restrictions	None.

Example usage:

To configure the IPv6 interface System:

```
DGS-1210-28> config ipif System ipv6 ipv6address 3ffe:501:ffff:100::1/64


Success.

DGS-1210-28>
```

logout

Purpose	To log out a user from the Switch's console.
Syntax	**logout**
Description	The `logout` command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
DGS-1210-28> logout
```

NOTE: Save your configuration changes before logging out.

ping

Purpose	To test the connectivity between network devices.
Syntax	**<ipaddr>**
Description	The ping command checks if another IP address is reachable on the network. You can ping the IP address connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the target IP equipment. By default, Switch sends five pings to the target IP.
Parameters	*<ipaddr>* - The IP address of the host.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.91:

```
DGS-1210-28> ping 10.90.90.91

Reply Received From :10.90.90.91, TimeTaken : 20 msecs
Reply Received From :10.90.90.91, TimeTaken : 20 msecs
Reply Received From :10.90.90.91, TimeTaken : 20 msecs


--- 10.90.90.91 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
DGS-1210-28>
```

ping6

Purpose	To test the connectivity between network devices.
Syntax	**ping6 <ipv6addr>**
Description	The pingv6 command checks if another IP address is reachable on the network. You can ping the IP address connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the target IP equipment. By default, Switch sends five pings to the target IP.
Parameters	*<ipv6addr>* - The IPv6 address of the host.
Restrictions	None.

Example usage:

To ping the IP address 3000::1:

```
DGS-1210-28> ping6 3000 ::1

Reply Received From : 3000 ::1, TimeTaken : 20 msecs
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
Reply Received From : 3000 ::1, TimeTaken : 20 msecs


--- 3000 ::1 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
DGS-1210-28>
```

create iproute

Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	**create iproute default <ipaddr>**
Description	The **create iproute** command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	*default* – Specifies to create a default IP route entry. *<ipaddr>* – The gateway IP address for the next hop router.
Restrictions	Only Administrator, operator and power user-level users can issue this command.

Example usage:

To add the default static address 10.90.90.92 to the routing table:

```
DGS-1210-28> create iproute default 10.90.90.92
Command: create iproute default 10.90.90.92


Success.
DGS-1210-28>
```

delete iproute

Purpose	Used to delete an IP route entry from the Switch's IP routing table.
Syntax	**delete iproute {default}**
Description	The delete iproute command will delete an existing IP route entry from the Switch's IP routing table.
Parameters	{*default*} – Specifies to delete a default IP route entry.
Restrictions	Only Administrator, operator and power user-level users can issue this command.

Example usage:

To delete the default Gateway from the routing table:

```
DGS-1210-28> delete iproute
Command: delete iproute


Success.
DGS-1210-28>
```

show iproute

Purpose	Used to display the Switch's current IP routing table.

Syntax	show iproute {<ipaddr> | static}
Description	The **show iproute** command will display the Switch's current IP routing table.
Parameters	*<ipaddr>* - Enter the IP address used here. *static* – Specifies to display all the static routes.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DGS-1210-28> show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway        Interface    Hops     Protocol
----------------------------  ---------------  --------------  ---------  ---------------

Total Entries  :0
DGS-1210-28>
```

reboot

Purpose	To reboot the Switch. If the Switch is a member of a stack, it may be rebooted individually, without affecting the other members of the stack.
Syntax	reboot
Description	The reboot command reboots the system. All network connections are terminated and the boot code executes.
Parameters	None.
Restrictions	None.

Example usage:

To restart the Switch:

```
DGS-1210-28> reboot
% Device will reboot, please wait a few minutes to re-login.
DGS-1210-28>
```

reset config

Purpose	To reset the Switch to the factory default settings.
Syntax	reset config
Description	All configurations will be reset to the default settings.
Parameters	None.
Restrictions	None.

Example usage:

To restore all of the Switch's parameters to their default values:

```
DGS-1210-28> reset config

% Device will reboot after reset configuration successfully.


DGS-1210-28>
```

show ipif

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	show ipif
Description	The show ipif command displays the current IP address of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings:

```
DGS-1210-28> show ipif

IP Setting Mode              : Static
IP Address                   : 10.90.90.90
Subnet Mask                  : 255.0.0.0
Default Gateway              : 0.0.0.0
DHCPv6 Client State          : Disabled
IPv6 Global Unicast Address:  3ffe:501:ffff:100:100::1/64


DGS-1210-28>
```

show switch

Purpose	To display information about the Switch.
Syntax	show switch
Description	The show switch command displays the status of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the switch information:

```
DGS-1210-28> show switch
System Name              :
System Contact                    :
System Location                   :
System up time                    : 0 days, 6 hrs, 32 min, 17 secs
System Time                       : 02/01/2012 06:32:19
System hardware version           : C1
System firmware version           : 4.00.011
System boot version               : 1.00.005
System Protocol version           : 2.001.004
System serial number              : QBDGS12102800
MAC Address                       : 00-66-60-60-88-28

DGS-1210-28>
```

config account admin password

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	config account admin password <passwd>
Description	The config account admin password command sets the administrator password.
Parameters	*<passwd>* – The new password of the administrator.
Restrictions	None.

Example usage:

To configure the account admin password:

```
DGS-1210-28> config account admin password 1234

DGS-1210-28>
```

save

Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	save
Description	The save command saves the configuration changes to the memory.
Parameters	None.
Restrictions	None.

Example usage:

To save the Switch's current configuration to non-volatile RAM:

```
DGS-1210-28> save
Building configuration ...
[OK]

DGS-1210-28>
```

debug info

Purpose	To display the ARP table and MAC FDB information of the Switch.
Syntax	debug info
Description	The debut info command displays the ARP table and MAC FDB of the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP table and MAC FDB information of the Switch:

```
DGS-1210-28> debug info
% segmentation fault log file:

File doesn't exist !!!
% ARP table :

Address          Hardware Address    Type    Interface    Mapping
------- ------   ----------- ----------------  ------   -------------  -------------
10.90.90.90      00:18:8b:bf:75:30    ARPA    vlan1       Static
10.90.90.98      00:19:5b:14:3d:c4    ARPA    vlan1       Dynamic
10.255.255.255   ff:ff:ff:ff:ff:ff    ARPA    vlan1       Static

% MAC table :

Vlan    Mac Address         Type      Ports
------   -------------------      --------    -------
1        00:00:00:00:00:26   Learnt   Gi0/7

Total Mac Addresses displayed: 1

DGS-1210-28>
```

Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link Web Smart Switch and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, and management objects, but with a tenfold increase in theoretical throughput of over 100-Mbps Fast Ethernet and a hundredfold increase over 10-Mbps Ethernet. Since it is compatible with all 10-Mbps and 100-Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting existing investments in hardware, software, or trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential in solving network bottlenecks, which frequently develops as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology, can greatly improve network response times as well as significantly speed up the traffic between subnets.

Gigabit Ethernet enables fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. With expected advances in the coming years in silicon technology and digital signal processing, which will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, a flexible foundation for the next generation of network technology products will be created. This will outfit your network with a powerful 1000-Mbps-capable backbone/server connection.

Fast Ethernet Technology

The growing importance of LANs, and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments, which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

Appendix B - Technical Specifications

Hardware Specifications

Key Components / Performance

- Switching Capacity: 56Gbps
- Max. Forwarding Rate: 41.7Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory: 1.5MBytes
- DDRIII for CPU: 128M Bytes
- Flash Memory: 16M Bytes

Port Functions

- 10/100/1000Base-T ports compliant with the following standards:
  - IEEE 802.3
  - IEEE 802.3u
  - IEEE 802.3ab
  - IEEE 802.3az Energy Efficient Ethernet
  - Supports Half/Full-Duplex operations
  - IEEE 802.3x Flow Control support for Full-Duplex mode
  - Auto MDI/MDIX
- SFP ports compliant with the following standards:
  - IEEE 802.3z
  - Supports Full-Duplex operations
- SFP transceivers supported
  - DGS-712 (1000Base-T)
  - DEM-310GT (1000BASE-LX, 10km)
  - DEM-311GT (1000BASE-SX, 550m)
  - DEM-314GT (1000BASE-LH, 50km)
  - DEM-315GT (1000BASE-ZX, 80km)
  - DEM-312GT2 (1000BASE-SX, 2km)

  WDM Transceivers Supported:
  - DEM-330T (1000Base-BX,TX-1550/RX-1310nm, 10km)
  - DEM-330R (1000Base-BX,TX-1310/RX-1550nm, 10km)
  - DEM-331T (1000Base-BX,TX-1550/RX-1310nm, 40km)
  - DEM-331R (1000Base-BX,TX-1310/RX-1550nm, 40km)

Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value: 0dB (Fan-less)
- Operation Temperature: 5~50°C
- Storage Temperature -20~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A
- IC Class A

Safety Certifications

- cUL, LVD, CE

Features

L2 Features

- Supports up to 16K MAC address
- Supports 256 static MAC
- Jumbo frame: Supports up to 9,216 bytes
- IGMP snooping v1/v2/v3 awareness:
  - Supports 256 multicast groups
  - Supports at least 64 static multicast groups
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- Loopback Detection
- 802.3ad Link Aggregation: Supports max 14 groups per device and 8 ports per group

  Port mirroring
- SNTP
- LLDP/LLDP-MED
- IPv6 neighbor Discovery (ND)
- L2 Multicast Filtering

VLAN

- 802.1Q VLAN standard (VLAN Tagging)
- Up to 256 static VLAN groups
- Asymmetric VLAN
- Management VLAN
- Auto Voice VLAN
- Auto Surveillance VLAN

QoS (Quality of Service)

- Priority queue mapping by :
  - 802.1p
  - DSCP
  - ToS
  - TCP/UDP port number
  - IPv6 traffic class
- Up to 4 queues per port
- Supports Strict in queue handling
- Bandwidth Control

AAA

- 802.1X port-based access control
- Support RADIUS server

ACL

- Max 50 ingress ACL access-list

- Ingress ACL rules: 768 rules (each rule can be associated to a single port or multiple ports)
- Support different ACL policy packet contents:
  - 802.1p priority
  - VLAN
  - MAC address
  - Ethernet Type
  - IPv4/IPv6 address
  - DSCP
  - Protocol type
  - TCP/UDP port number
  - IPv6 Traffic class

Security

- Trusted Host
- Port Security: Support 64 MAC addresses per port
- Traffic Segmentation
- D-Link Safeguard Engine
- Broadcast Storm Control
- ARP Spoofing Prevention: Supports max 127 entries
- DHCP Server Screening: Able to conFigure 4 IP addresses for DHCP server.
- SSL: Support v1/v2/v3
- Smart Binding
  - Support manual configuration and scanning for binding.
  - Supports ARP packet inspection as default, ARP and IP packet inspection as an option.
  - Supports DHCP Snooping

OAM

- Cable Diagnostics
- Reset button (reset to factory default)

Management

- Web-based GUI or D-Link Network Assistant (DNA)
- D-Link CLI style
- SNMP support
- DHCP client
- Trap setting for destination IP, system events, fiber port events, twisted-pair port events
- Password access control
- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade using D-Link Network Assistant (DNA) & Web-based management
- Reset, Reboot

D-Link Green Technology

- Power Saving: Enabled by default to save power:
  - By Link Status: Drastically save power when the switch port link is down. For example, no PC connection or the connected PC is powered off.
  - By LED Shut-Off: LEDs can be turned on/off by port or system through schedule.
  - By Port Shut-Off: Each port on the system can be turned on/off by schedule.
  - By System Hibernation: System enters hibernation by schedule. In this mode, switches save most power since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

Appendix C – Rack mount Instructions

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

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

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

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

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

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

D-Link®

Building Networks for People