D-Link®
Building Networks for People

DGS-1210-08P/16/24/24P/48

Web UI Reference Guide
Web Smart Switch

Ver. 4.10

IPv6 READY

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

SFP (Mini-GBIC), XENPAK, and XFP Regulatory Compliance

Networks pluggable optical modules meet the following regulatory requirements:

UL recognized Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

EN60825-1:2007 2nd Ed. or later, European standard.

FCC 21 CFR Chapter 1, Subchapter J in accordance with FDA & CDRH requirements.

47 CFR Part 15, Class A.

Application of CE Mark in accordance with 2004/108/EEC EMC Directive and the 2006/95/EC Low Voltage Directives.

Table of Contents

Intended Readers

This guide provides instructions to install the D-Link Gigabit Web Smart Switch DGS-1210-08P/16/24/24P/48, how 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 three parts:

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

Terms/Usage

In this guide, the term "Switch" (first letter capitalized) refers to 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 **NOTICE** indicates either potential damage to hardware or loss of data and tells how to avoid the problem.

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

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from

potential damage. Throughout this safety section, the caution icon (⚠) is used to indicate cautions and precautions that need to be reviewed and followed.

> **CAUTION**: Only trained and qualified service personnel should install, replace or perform maintenance on D-Link switches.

To reduce the risk of bodily injury, electrical shock, fire, or damage to the equipment, observe the following precautions.

- Observe and follow service markings.
    - o   Do not service any product except as explained in your system documentation.
    - o   Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
    - o   Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
    - o   The power cable, extension cable, or plug is damaged.

- An object has fallen into the product.
  - o The product has been exposed to water.
  - o The product has been dropped or damaged.
  - o The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage on the power supply is set to match the power available at your location:
  - o 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - o 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
  - o 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  - o Install the power supply before connecting the power cable to the power supply.
  - o Unplug the power cable before removing the power supply.
  - o If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also, refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

- Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.

- Always load the rack from the bottom up, and load the heaviest item in the rack first.

- Make sure that the rack is level and stable before extending a component from the rack.

- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.

- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.

- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.

- Ensure that proper airflow is provided to components in the rack.

- Do not step on or stand on any component when servicing other components in a rack.

⚠️ **CAUTION:** Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

⚠️ **CAUTION:** The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. A qualified electrical inspector must inspect completed power and safety ground wiring. An energy hazard will exist if the safety ground cable is omitted or disconnected.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.

2. When transporting a sensitive component, first place it in an antistatic container or packaging.

3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

1 *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 series is the new generation of Web Smart series. It provides a variety of port counts- 8, 16 or 24 10/100/1000Mbps ports plus 2/4 SFP ports, or 44 10/100/1000Mbps ports plus 4 Combo Copper/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 series 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 video 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 a Web-Based management interface that allows administrators to remotely control their network down to the port level. The **D-Link Network Assistant (DNA)** is a program that allows administrators to quickly discover all D-Link smart switches and D-Link Discover Protocol (DDP) supported devices that are in the same subnet as the PC, collect traps and log messages, and provide quick access to basic configurations of the switch.

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

DGS-1210-08P

8-Port 10/100/1000Mbps PoE plus 2 SFP Slot Web Smart Switch.

Front Panel

Figure 1.1 – DGS-1210-08P Front Panel

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

Port Link/Act/Speed LED (1-10): 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.

PoE LED: The PoE LED illuminates green when power is supplied to PoE devices plugged into the ports. It illuminates amber when an error condition is met and will be off when no power is supplied.

> ⚠️ **CAUTION:** The Mini-GBIC ports should use UL recognized Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

Reset: By pressing the Reset button for 5 seconds, the Switch will change back to the default configuration and all changes will be lost.
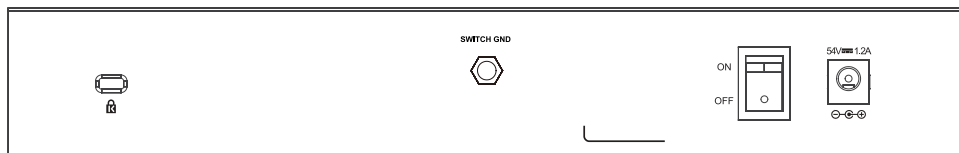
Rear Panel

Figure 1.2 – DGS-1210-08P Rear Panel

Power: The power port is where to connect the external power adapter.

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

Power Switch: Toggle this switch to turn the switch's power on or off.

DGS-1210-16

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

Front Panel

Figure 1.3 – DGS-1210-16 Front Panel

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

Port Link/Act/Speed LED (1-20): 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.

> ⚠️ **CAUTION:** The Mini-GBIC ports should use UL recognized Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

Reset: By pressing the Reset button for 5 seconds, the Switch will change back to the default configuration and all changes will be lost.
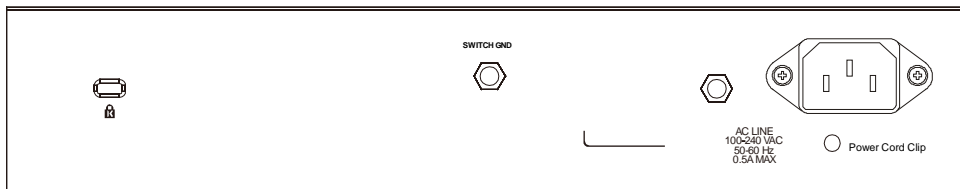
Rear Panel

Figure 1.4 – DGS-1210-16 Rear Panel

Power: The power port is where to connect the AC power cord.

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

DGS-1210-24

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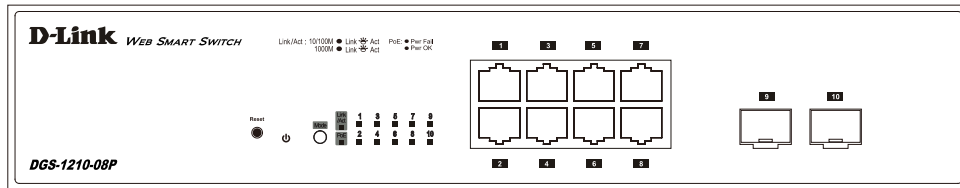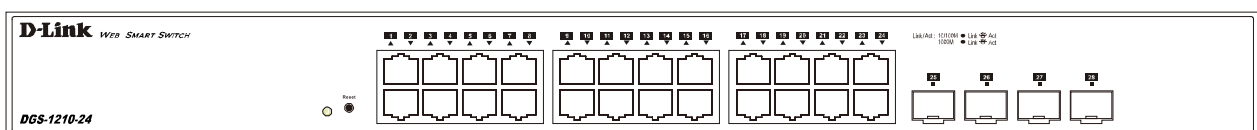
Front Panel

Figure 1.5 – DGS-1210-24 Front Panel

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

Port Link/Act/Speed LED (1-28): 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.

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 recognized Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

Rear Panel

Figure 1.6 DGS-1210-24 Rear Panel

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

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

DGS-1210-24P

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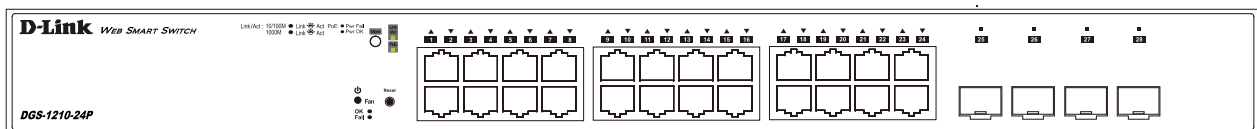
Front Panel

Figure 1.7 – DGS-1210-24P Front Panel

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

Port Link/Act/Speed LED (1-28): 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.

PoE LED: The PoE LED illuminates green when power is supplied to PoE devices plugged into the ports. It illuminates amber when an error condition is met and will be off when no power is supplied.

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

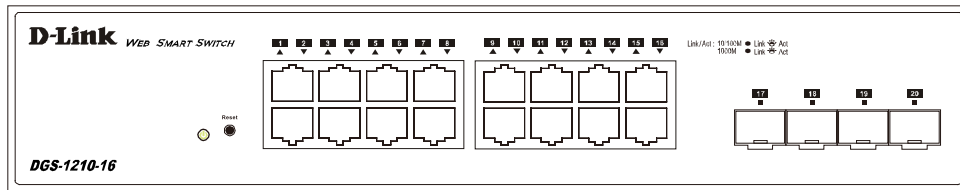> ⚠️ **CAUTION:** The MiniGBIC ports should use UL recognized Optical Transceiver product, Rated Laser Class I. 3.3Vdc.
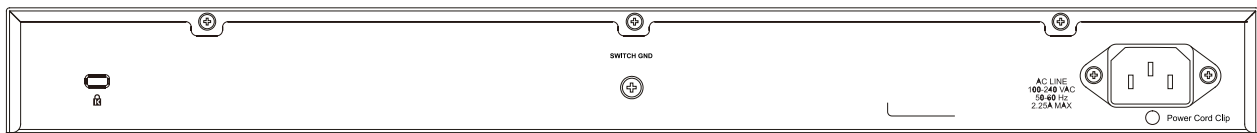
Rear Panel

Figure 1.8 DGS-1210-24P Rear Panel

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

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

DGS-1210-48

44-Port 10/100/1000Mbps plus 4-Port Combo Copper/SFP Web Smart Switch.

Front Panel
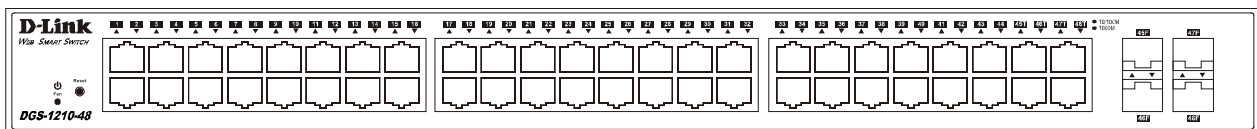
Figure 1.9 – DGS-1210-48 Front Panel

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

Port Link/Act/Speed LED (1-48): 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.

Fan: The Fan LED lights green when the fan work well, and lights red when the fan fail.

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 recognized Optical Transceiver product, Rated Laser Class I. 3.3Vdc.
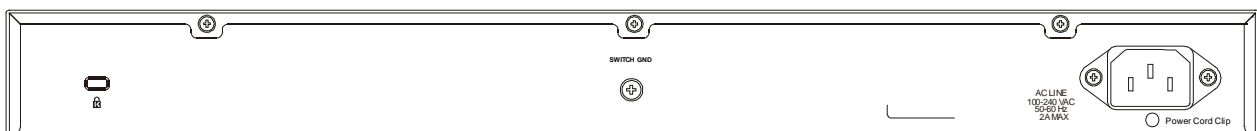
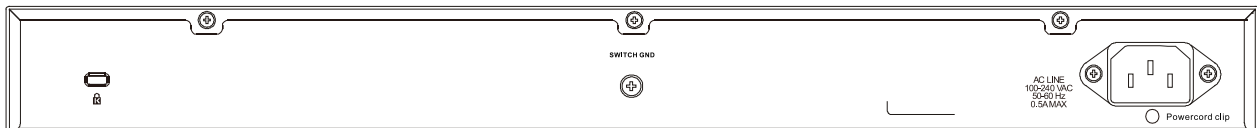### Rear Panel

Figure 1.10 – DGS-1210-48 Rear Panel

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

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

2 *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.

> One D-Link Web-Smart Switch
> One AC power cord
> One set of Power Cord Clip
> Four rubber feet
> Screws and two mounting brackets
> One Multi-lingual Getting Started Guide
> One CD with Web UI Reference Guide, Getting Started Guide, D-Link Network Assistant User Guide, Language Pack Files, 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.
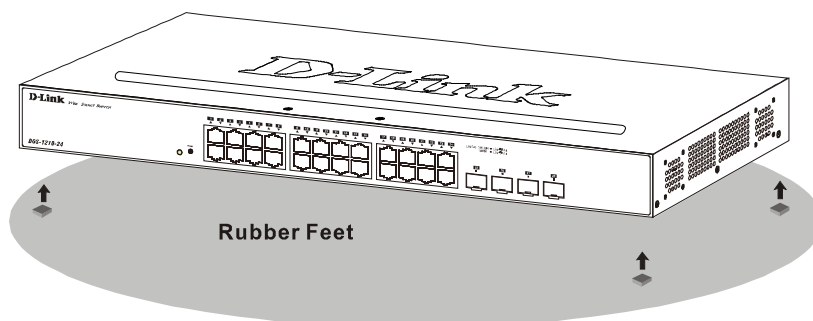
Figure 2.1 – Attach the adhesive rubber pads to the bottom

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).
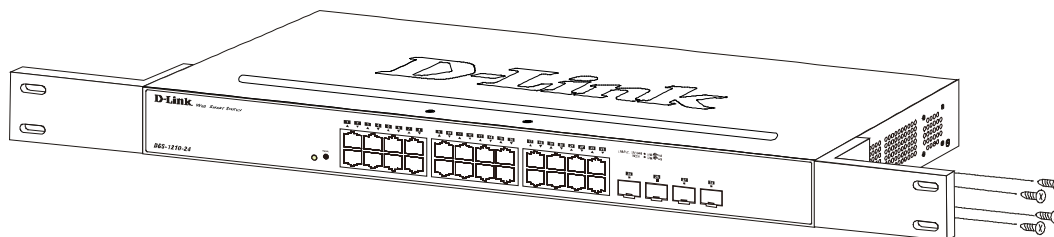
Figure 2.2 – Attach the mounting brackets to the Switch

Then, use the screws provided with the equipment rack to mount the switch in the rack.
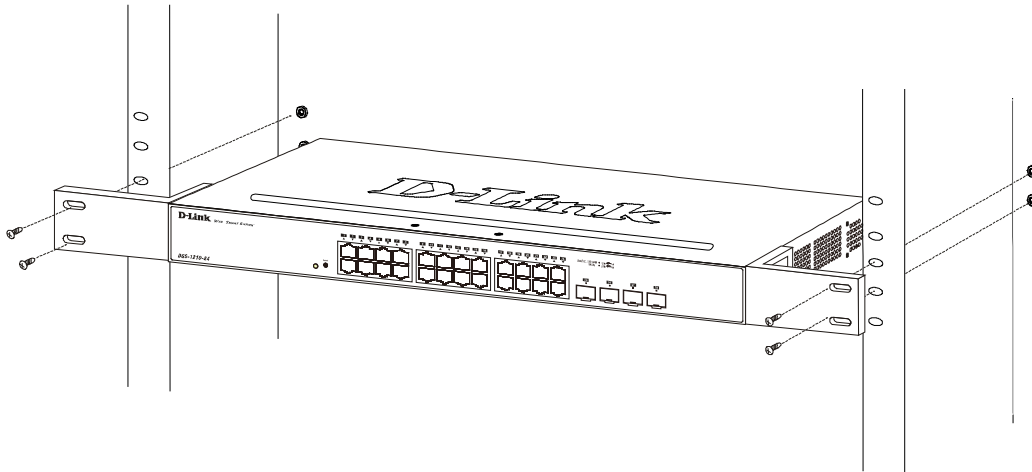
Figure 2.3 – Mount the Switch in the rack or chassis

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.
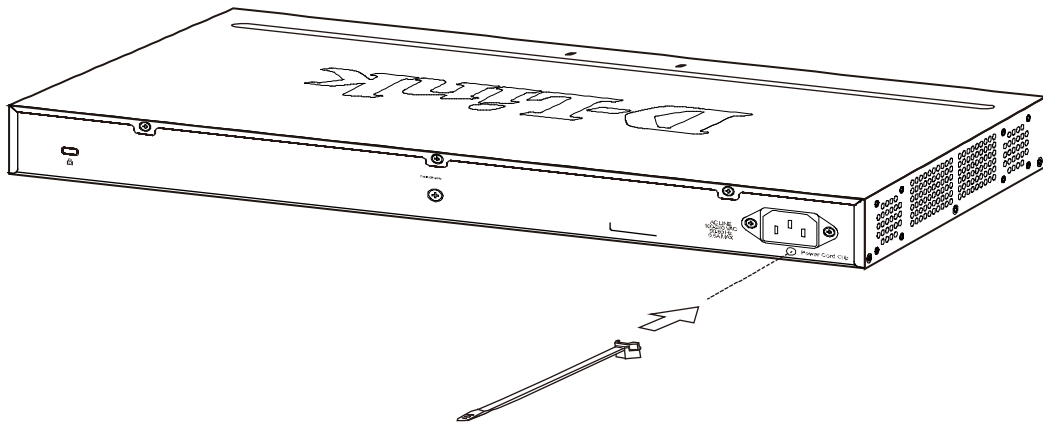
Figure 2.4 – Insert Tie Wrap to the Switch

B) Plug the AC power cord into the power socket of the Switch.
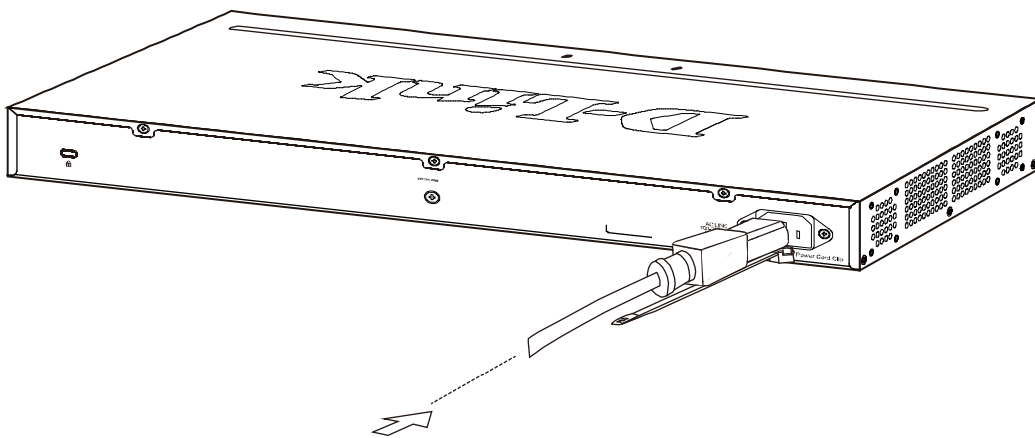
Figure 2.5 – Connect the power cord to the Switch

C) Slide the Retainer through the Tie Wrap until the end of the cord.
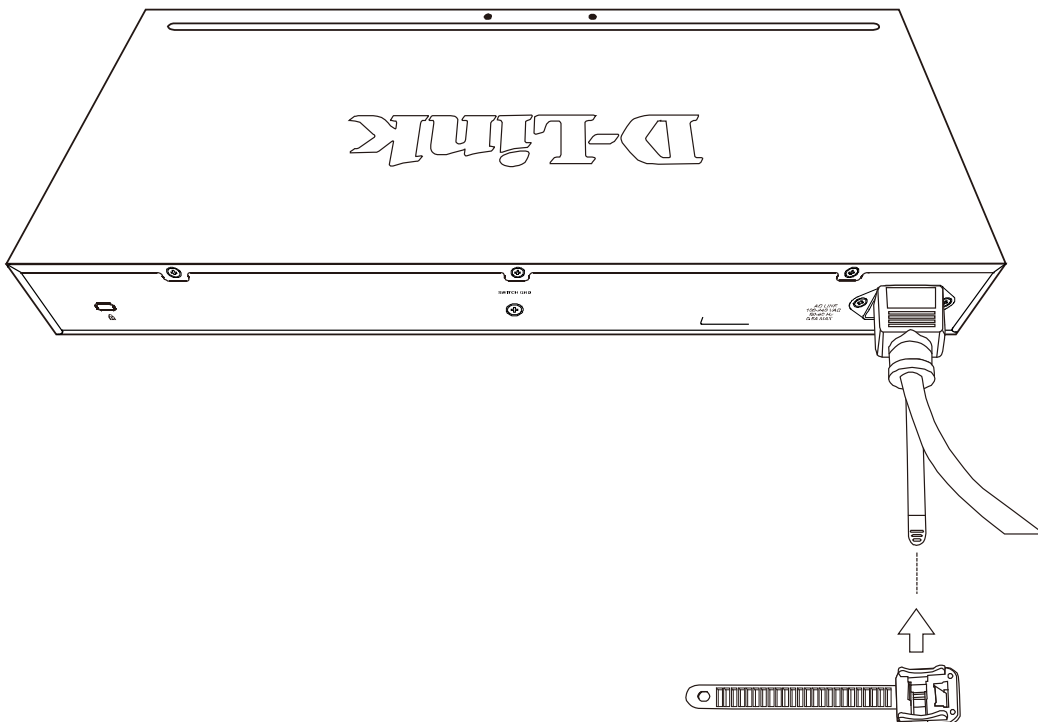
Figure 2.6 – Slide the Retainer through the Tie Wrap

D) Circle the tie of the Retainer around the power cord and into the locker of the Retainer.
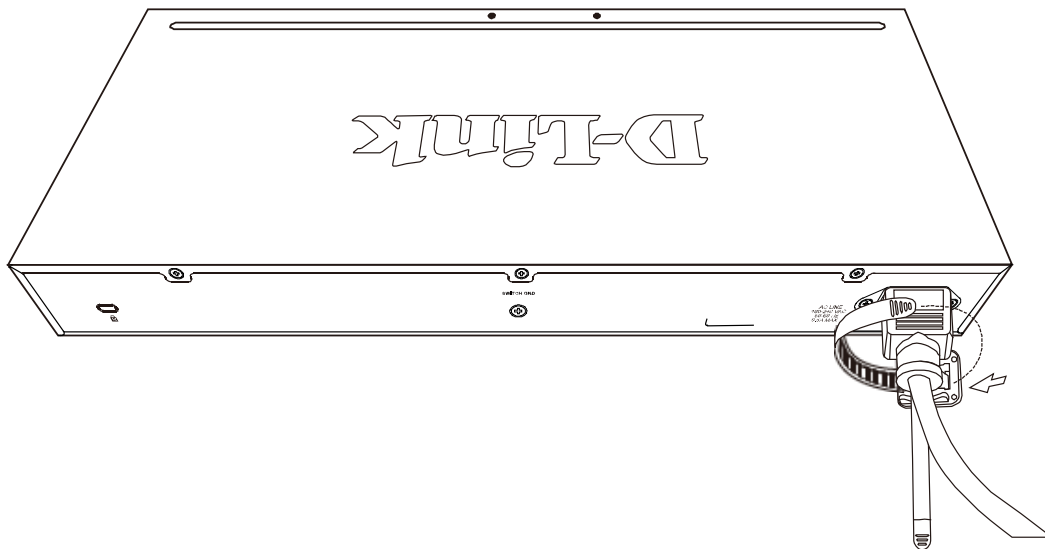
Figure 2.7 – Circle around the power cord

E) Fasten the tie of the Retainer until the power cord is secured.
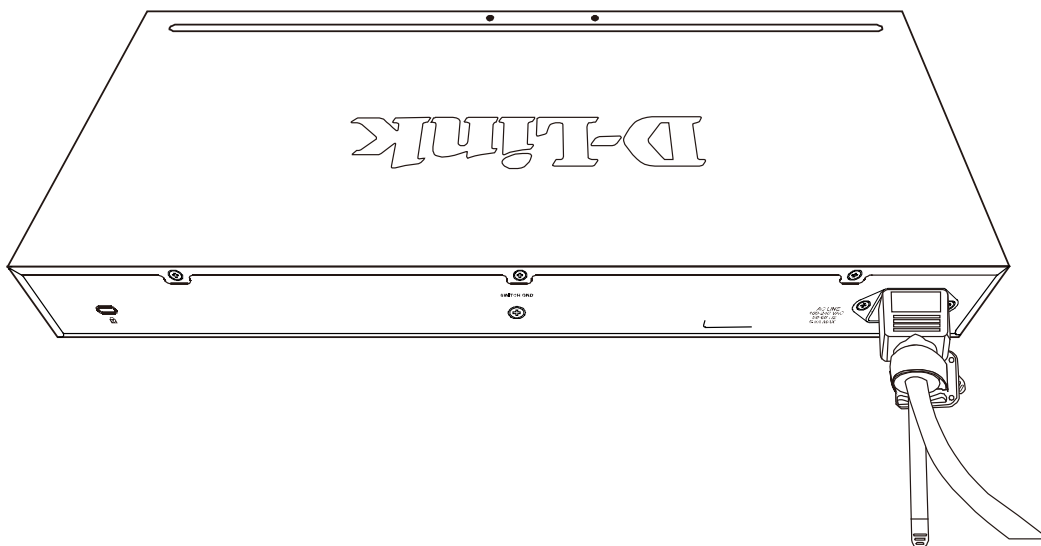
Figure 2.8 – Secure the power cord

F) Users may now connect the AC power cord to an electrical outlet (preferably one that is grounded and surge protected).
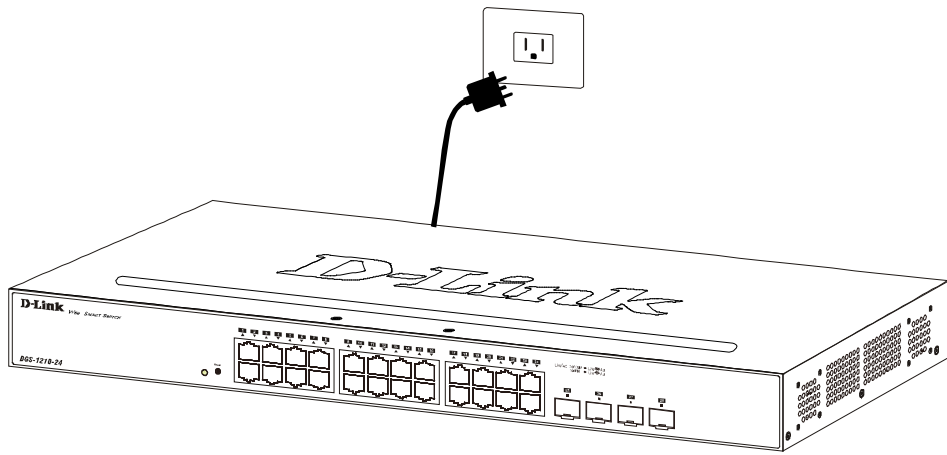
Figure 2.9 – Plugging the switch into an outlet

<u>**Power Failure**</u>

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

3 *Getting Started*

This chapter introduces the management interface of D-Link 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.

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

Please refer to the following installation instructions for the Web-based Management 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
- Firefox 3.0 or later version
- Chrome 5.0 or later version
- Safari 4.0 or later version
- Opera 10 or later version

Connecting to the Switch

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

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

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.
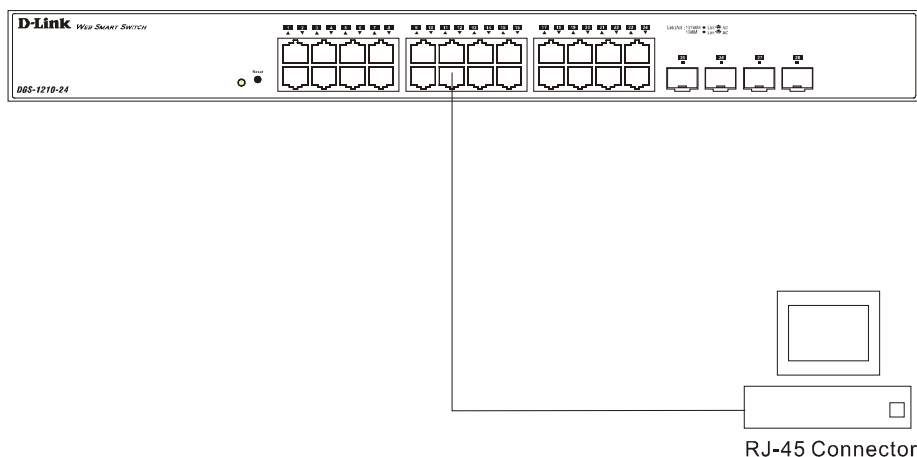
Figure 3.1 – Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. Open the web browser and enter **10.90.90.90** (the factory-default IP address) in the address bar. Then press <Enter>.
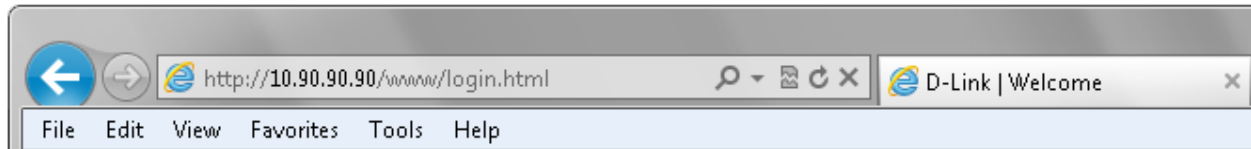
Figure 3.2 – Enter the IP address 10.90.90.90 in the web browser

> **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.

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**. For more information about language packs, refer to **Language Management**.
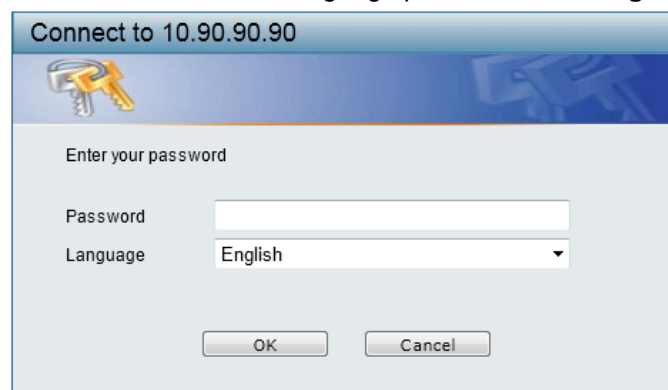
Figure 3.3 – Logon Dialog Box

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 5 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.*

4 *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. If you are not changing the settings, click the **Exit** button to go to the main page of Web-based Management. You can also tick **Ignore the wizard next time** check box 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.

<u>**Password**</u>

Type the desired new password in the **Password** field and again in the **Confirm Password** field, then click the **Next** button to the **SNMP** setting page.
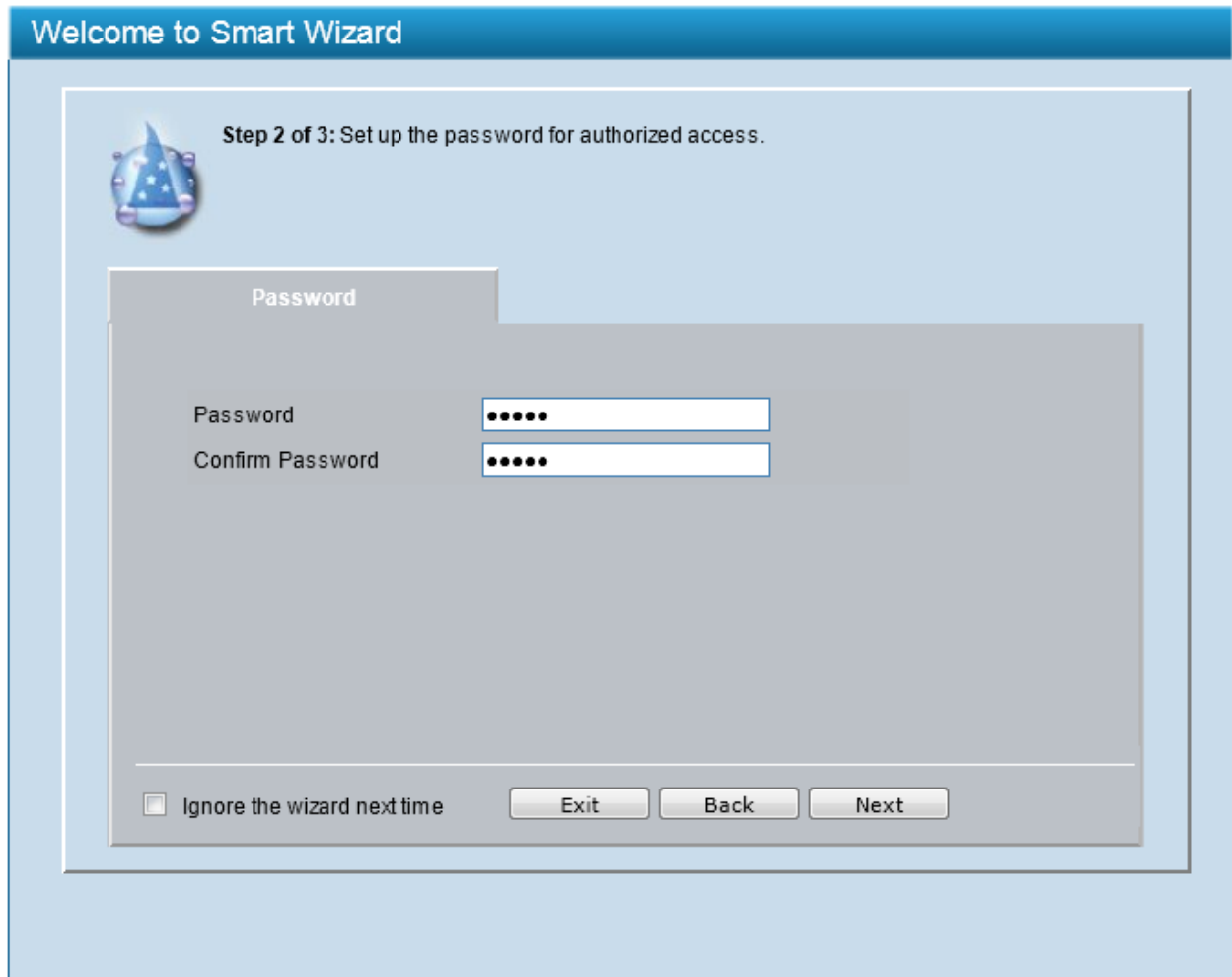
<p align="center">**Figure 4.2 – Password in Smart Wizard**</p>

SNMP

The SNMP Setting allows you to quickly enable or disable the SNMP function. The default SNMP Setting is *Disabled*. Click **Enabled** and then click **Apply** to make it effective.
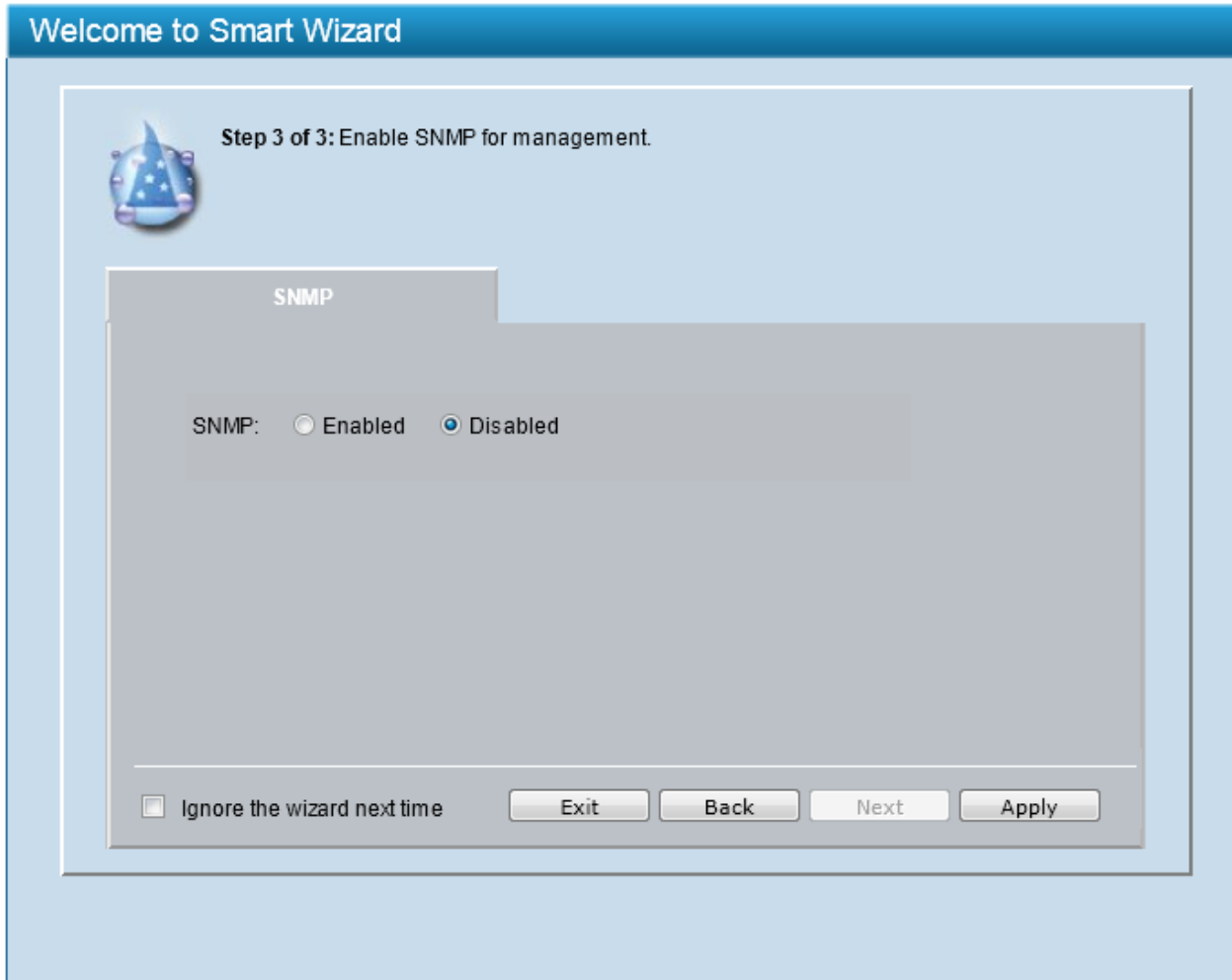
Figure 4.3 – SNMP in Smart Wizard

> **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.

When **IP Address** in Step 1 is changed, the following dialog box appears. Click **OK** to confirm all settings in the Wizard, and start a new web browser.
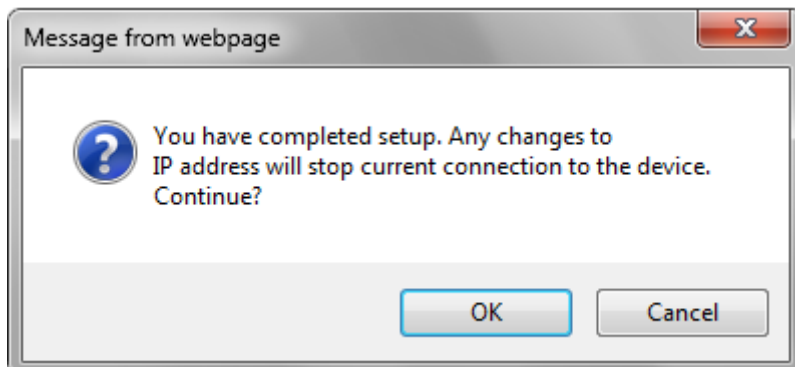
Figure 4.4 – Confirm the changes of IP address in Smart Wizard

Web-based Management

After clicking the **Exit** button in Smart Wizard, you will see the screen below:
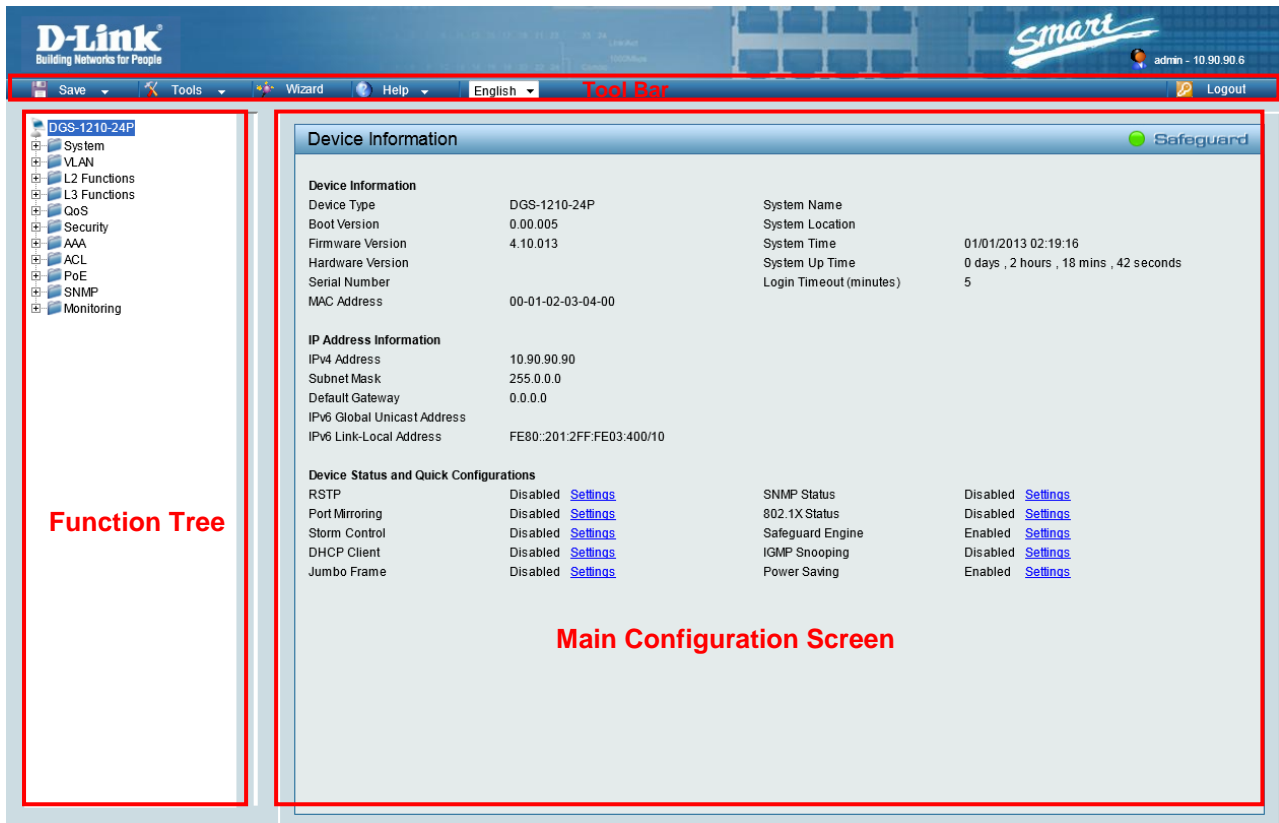
<div align="center">**Figure 4.5 – Web-based Management**</div>

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.
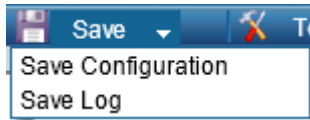
Figure 4.6 – Save Menu

Save Configuration

Select to save the entire configuration changes you have made to the device to switch's non-volatile RAM.
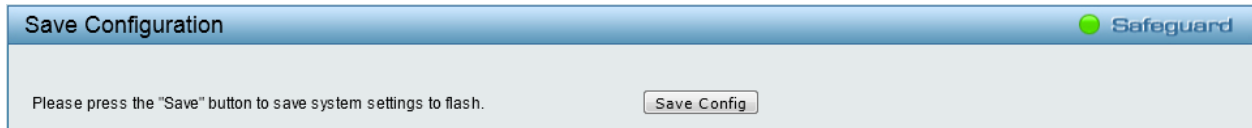
Figure 4.7 – Save Configuration

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).
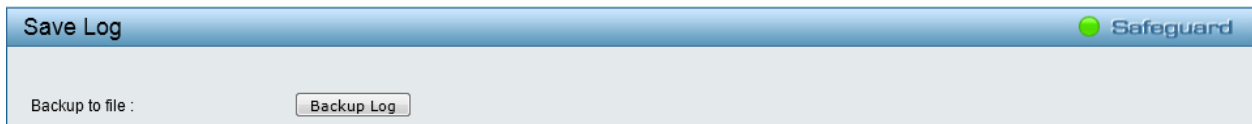
Figure 4.8 – Save Log

Tool Bar > Tools Menu

The Tools Menu offers global function controls Reset, Reset System, Reboot Device, Configuration Backup & Restore, Firmware Backup & Upgrade, and Language Management.
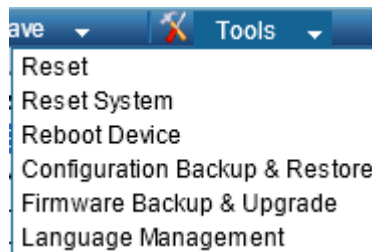
Figure 4.9 – Tools Menu

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.
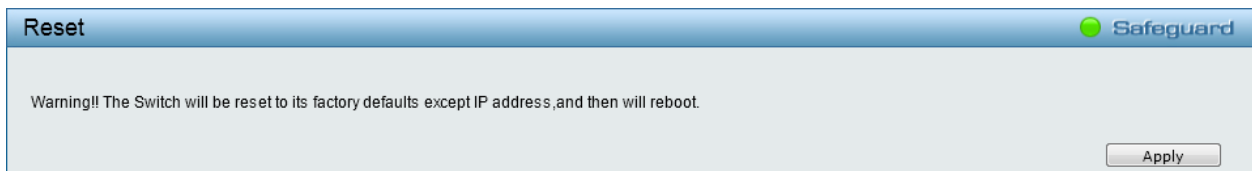
Figure 4.10 – Tools Menu > Reset

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.
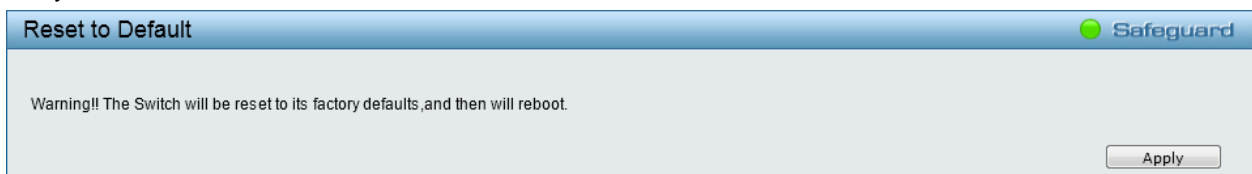
Figure 4.11 – Tools Menu > Reset System

Reboot Device

Provide a safe way to reboot the system. Click **Apply** to restart the Switch.
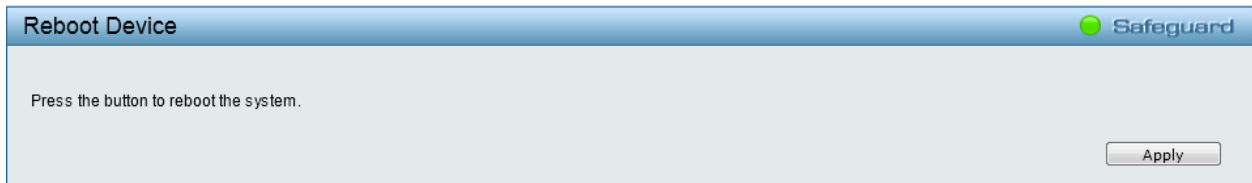
<p align="center">**Figure 4.12 – Tools Menu > Reboot Device**</p>

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 the configuration settings from this file. Two methods can be selected: **HTTP** or **TFTP**.
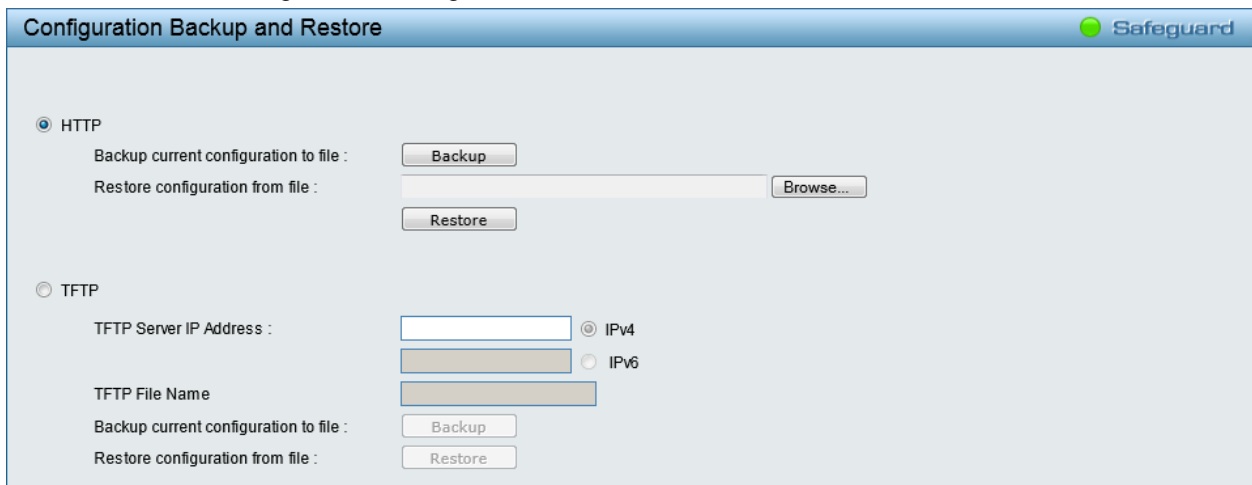
<p align="center">**Figure 4.13 – Tools Menu > Configure Backup and Restore**</p>

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 or 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:** The 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**.
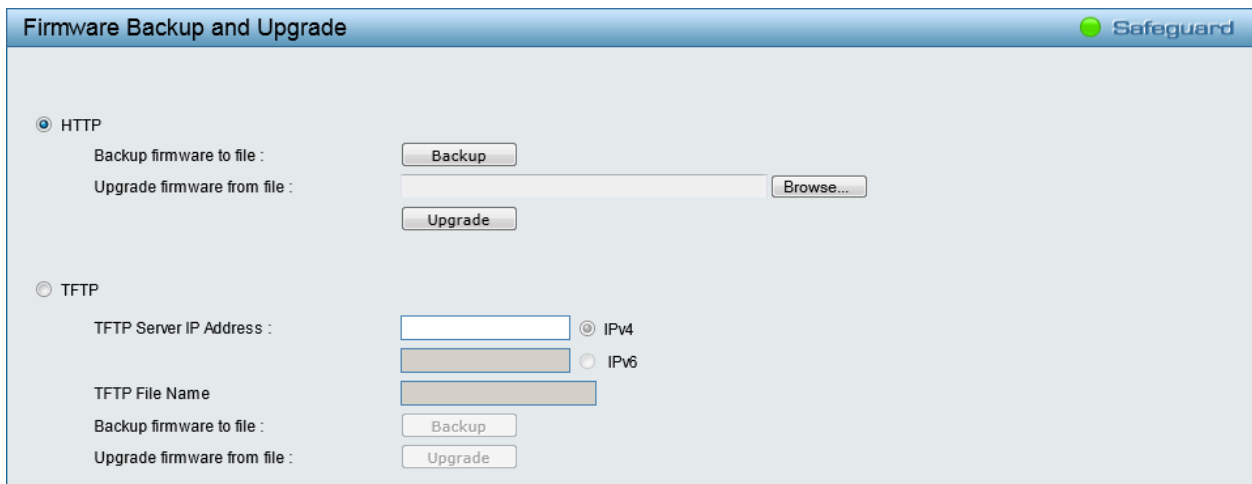
Figure 4.14 – Tools Menu > Firmware Backup and Upgrade

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

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

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

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

TFTP: Backup or upgrade the firmware to or from a remote TFTP server. Specify **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the firmware file you want to save to or 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 the Switch until the upgrade completes. The Switch may crash if the firmware upgrade is incomplete.

Language Management

Allow to select different language packages for the Switch. Two methods can be selected: **HTTP** or **TFTP**.
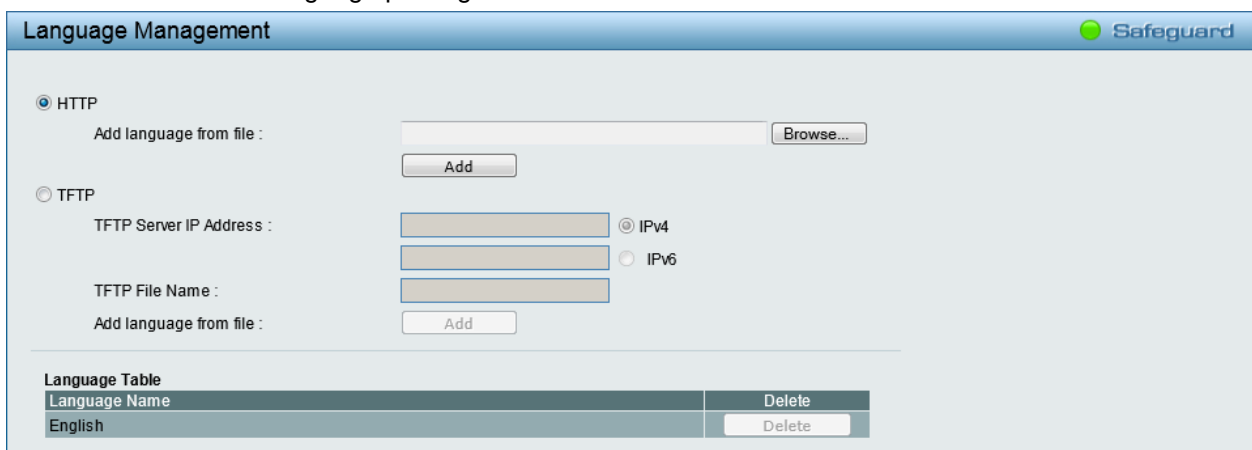
Figure 4.15 – Tools Menu > Language Management

HTTP: Install the language pack from your local PC drive.

Click **Browse** to find the file in your PC.

Click **Add** after selecting the language pack you want to install.

TFTP: Install the language pack from a remote TFTP server. Specify **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the language file you want to install.

Click **Add** after selecting the language pack file you want to install.

> **NOTE:** Language pack files are included on the CD in the Language Package folder.

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.
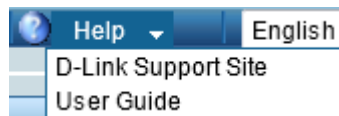
Figure 4.16 – Online Help

Function Tree

All configuration options on the Switch are accessed through the Function Tree. Click the setup item that you want to configure. The following sections provide more detailed description of each feature and function.
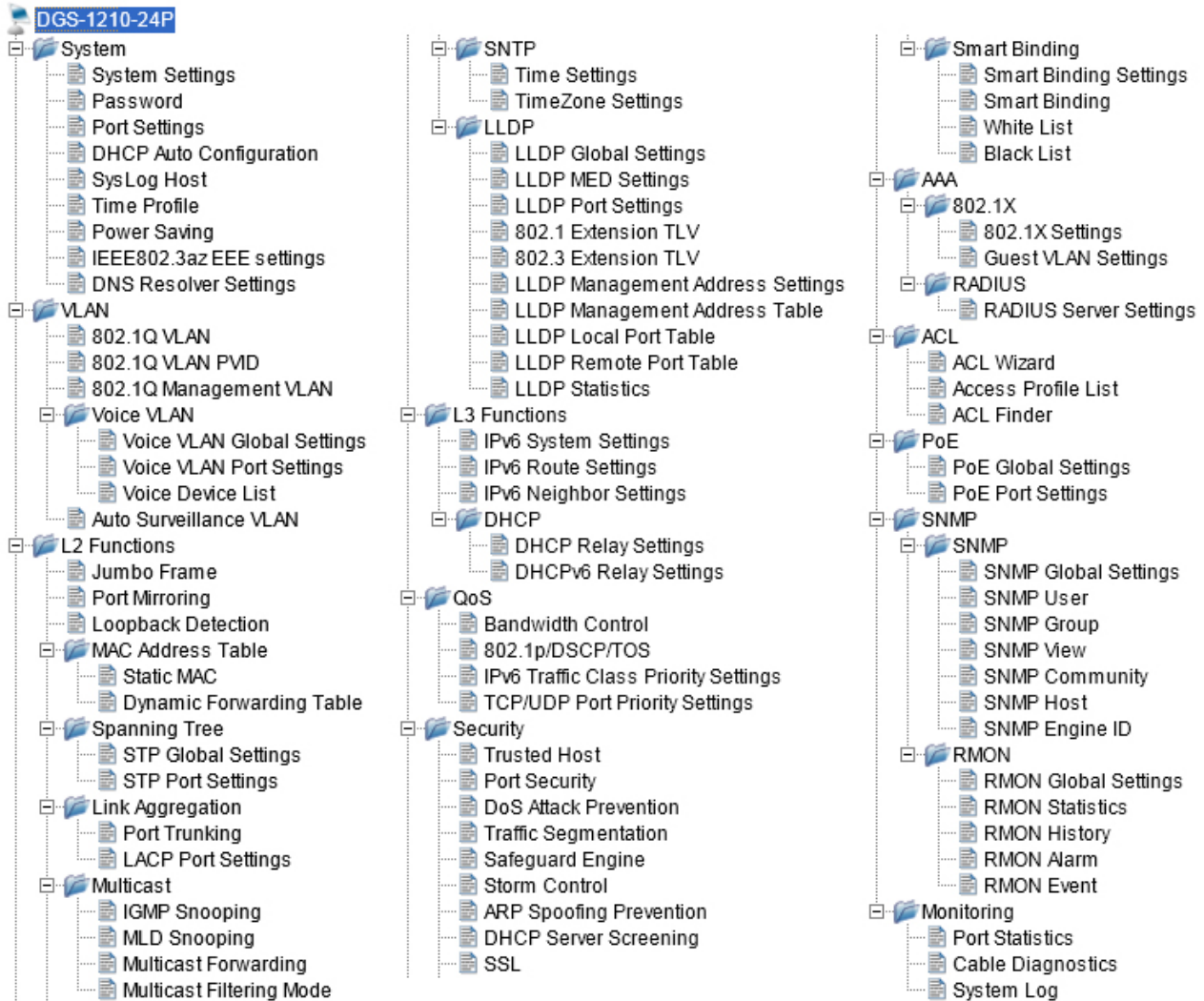
Figure 4.17 – Available settings in the Function Tree

Device Information

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

Figure 4.18 – Device Information

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 enabled.

<u>**System > System Settings**</u>

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

Figure 4.19 – 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 the static mode, the **IP Address**, **Subnet Mask** and **Gateway** can be manually configured. When using the 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 the static mode with IP address is **10.90.90.90** and subnet mask is **255.0.0.0**.

System Information: By entering a **System Name** and **System Location**.

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 > Password

Setting a password is a critical tool for managers to secure the Switch. After entering the **Old Password** and the new password in **New Password** and **Confirm Password**, click **Apply** for the changes to take effect.
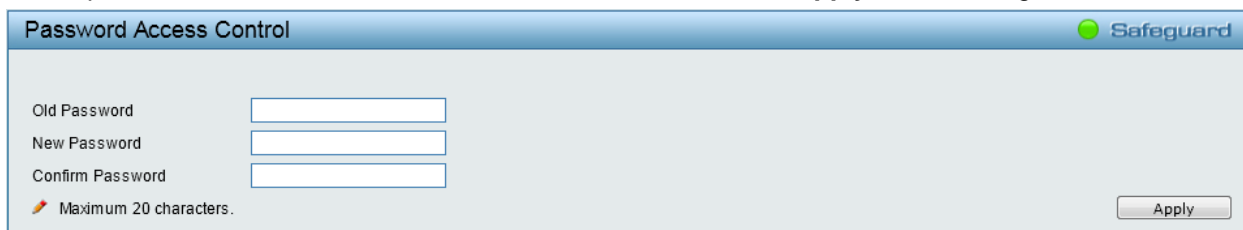
<p align="center">Figure 4.20 – System > Password Access Control</p>

System > Port Settings

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

Figure 4.21 – System > Port Settings

Speed: Gigabit Fiber connections can operate in **1000M Full**, **Auto** or **Disabled**. Copper connections can operate in Forced Mode settings (**1000M Full**, **100M Full**, **100M Half**, **10M Full**, **10M Half**), **Auto**, or **Disabled**. 100M Fiber connections support **100M Full**, or **Disabled**. Only the DGS-1210-48 switch's combo ports cannot be forced to 10M/100M Full/Half Mode. The default setting for all ports is *Auto*.

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

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

This Switch provides a configurable **MDI/MDIX** function for users. The Switch 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*.

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*.

Medium Type: If configuring the Combo ports, this defines the type of transport medium to be used. This is only for DGS-1210-48.

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

System > DHCP Auto Configuration

This window 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.
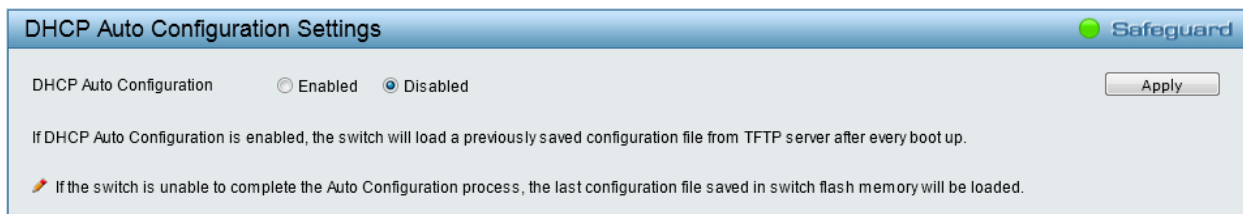
Figure 4.22 – System > DHCP Auto Configuration

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 **Enabled** to configure the related settings of the remote system log server, and click **Apply** for the changes to take effect.
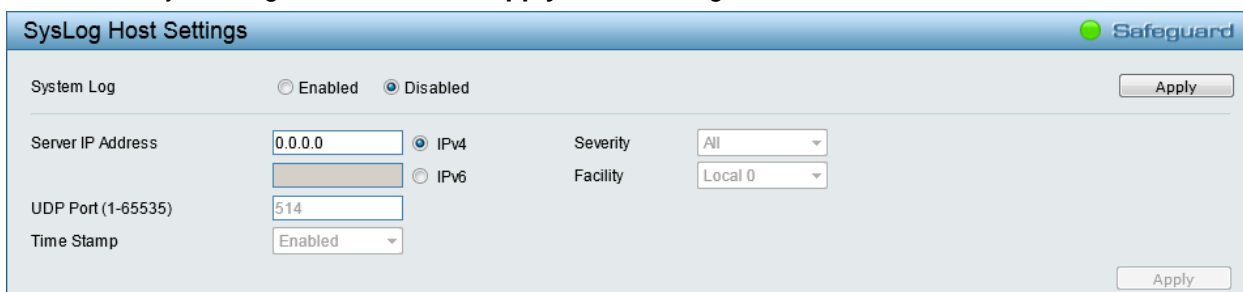
Figure 4.23 – System > SysLog Host Settings

Server IP Address: Specifies the IPv4 or IPv6 address of the system log server.

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

Time Stamp: Select **Enabled** 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 to Local 7).

System > Time Profile

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

Figure 4.24 – System > Time Profile

Profile Name: Specifies the profile name.

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

Weekdays: Specifies the week days.

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.

<u>**System > Power Saving**</u>

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

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

Figure 4.25 – System > Power Saving

Advanced Power Saving Settings:

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

> **LED Shut-off -** The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means when the **State** is **Disabled**, the LED cannot be turned on after Time Profile time is up. On the contrary, if the LED is enabled, the Time Profile function will work.

Port Shut-off - The Port Shut-off state has high priority (the priority rule is the same as LED.) Therefore, if the Port Shut-off sate is already disabled, the Time Profile function will not take effect.

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

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

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

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

Port: Select 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 the 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 802.3az EEE function is *Disabled*.
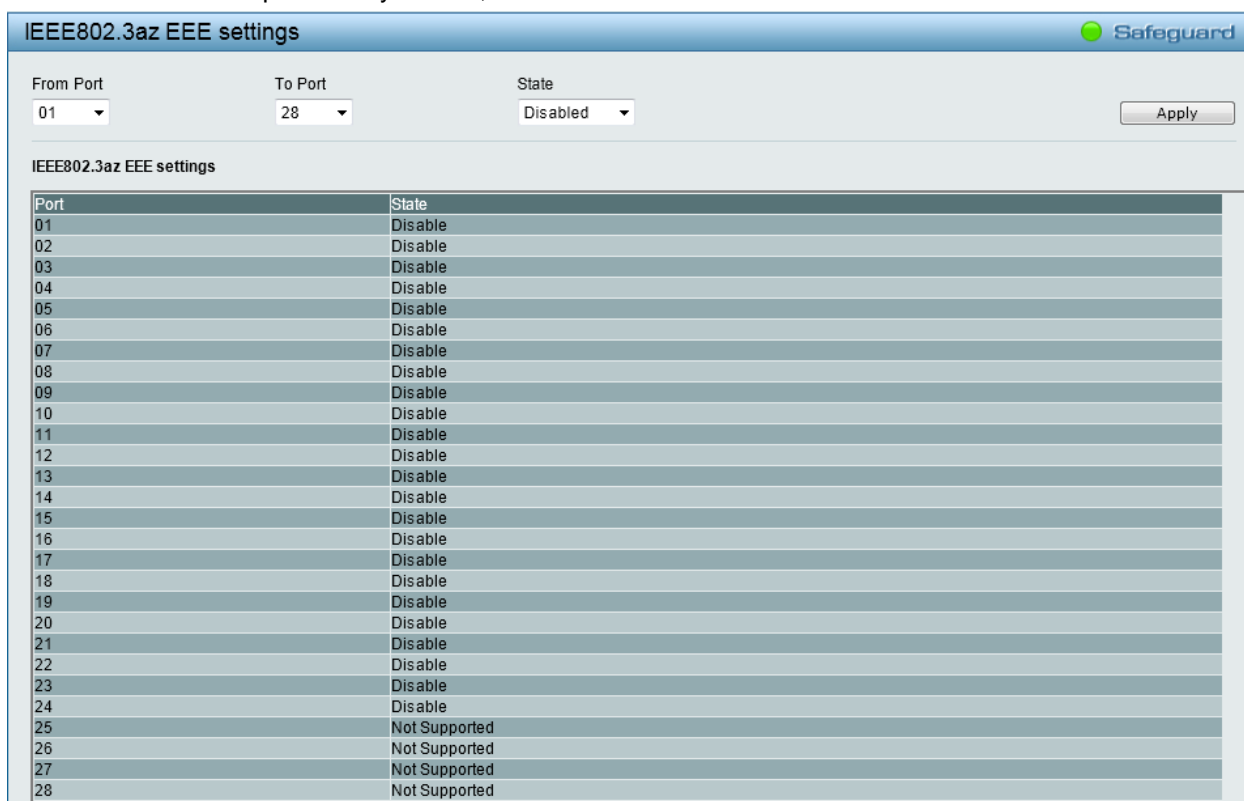
Figure 4.26 – System > IEEE802.3az EEE Settings

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 the 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 > DNS Resolver Settings

This window allows configuring Domain Name Server (DNS) resolver. The **DNS Resolver State** is *Disabled* by default. Click **Enabled** to enable DNS resolver. Click **Apply** for the changes to take effect.

Figure 4.27 – System >DNS Resolver Settings

Name Server Timeout: The maximum time waiting for a response from a specified name server.

Server IP Address: Enter a DNS Resolver name server's IPv4 address. Tick the **Primary** check box to set the name server as a primary name server.

Click **Add** to create a name server or click **Delete** to delete an entry from the table.

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 Settings window provides powerful VID management functions. The original settings have the VID as 1, VLAN Name as default, and all ports as Untagged.
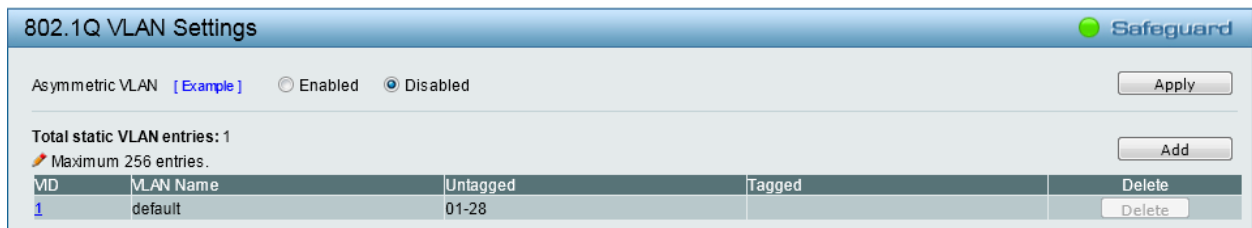
Figure 4.28 – Configuration > 802.1Q VLAN

Asymmetric VLAN: Select to enable or disable Asymmetric VLAN. The default is *Disabled*. Click **Example** to see a setup example about asymmetric VLAN.

Click **Apply** for the changes to take effect. Click **Add** to view the following window to create a VLAN. Click **Delete** to remove an entry from the table. Click the VLAN ID in VID to modify the corresponding VLAN settings. The window is similar to the following window, but cannot modify the VID.

Figure 4.29 – Configuration > 802.1Q VLAN > Add VLAN

VID: Enter a VLAN ID.

VLAN Name: Enter a name of VLAN.

Port: Click to assign ports as **Untag**, **Tag**, or **Not Member**. A port can be untagged in only one VID.

To save the VID group, click **Apply**. Click **Back** to go to the previous window.

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

VLAN > 802.1Q VLAN PVID

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

Figure 4.30 – 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 4.31 – 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.
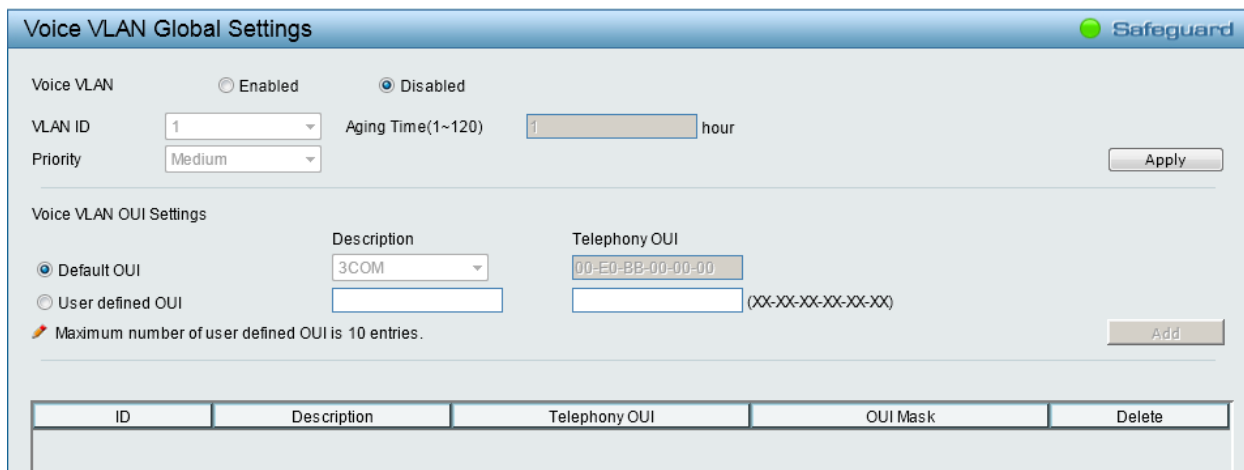
Figure 4.32 – VLAN > Voice VLAN > Voice VLAN Global Settings

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 window before you can assign a dedicated Voice VLAN. The member port configured in 802.1Q VLAN will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, enable the **Auto Detection** function in the Voice VLAN Port Settings window.

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 the 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, Huawei-3COM, and Avaya.

User defined OUI: You can manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10. It will occupy one ACL rule when selecting a user defined OUI by default, and to configure one user-defined OUI will take extra one ACL rule. System will auto generate an ACL profile (Profile ID: 51) for all the Voice VLAN rules.

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.

Port	Auto Detection	Tagged / Untagged	Current State	Status
01	Disabled	UnTagged	None	None
02	Disabled	UnTagged	None	Static
03	Disabled	UnTagged	None	None
04	Disabled	UnTagged	None	Static
05	Disabled	UnTagged	None	None
06	Disabled	UnTagged	None	None
07	Disabled	UnTagged	None	None
08	Disabled	UnTagged	None	None
09	Disabled	UnTagged	None	None
10	Disabled	UnTagged	None	None
11	Disabled	UnTagged	None	None
12	Disabled	UnTagged	None	None
13	Disabled	UnTagged	None	None
14	Disabled	UnTagged	None	None
15	Disabled	UnTagged	None	None
16	Disabled	UnTagged	None	None
17	Disabled	UnTagged	None	None
18	Disabled	UnTagged	None	None
19	Disabled	UnTagged	None	None
20	Disabled	UnTagged	None	None
21	Disabled	UnTagged	None	None
22	Disabled	UnTagged	None	None
23	Disabled	UnTagged	None	None
24	Disabled	UnTagged	None	None
25	Disabled	UnTagged	None	None
26	Disabled	UnTagged	None	None
27	Disabled	UnTagged	None	None
28	Disabled	UnTagged	None	None

Figure 4.33 – 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 the changes made. Click **Refresh** to renew the 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.
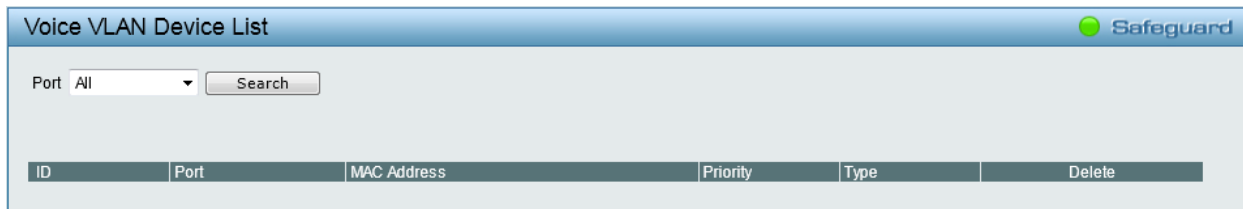
Figure 4.34 – VLAN > Voice VLAN > Voice Device List

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

VLAN > Auto Surveillance VLAN

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 on the incoming packets. If it matches specified MAC address, the packets will pass through switch with desired priority.
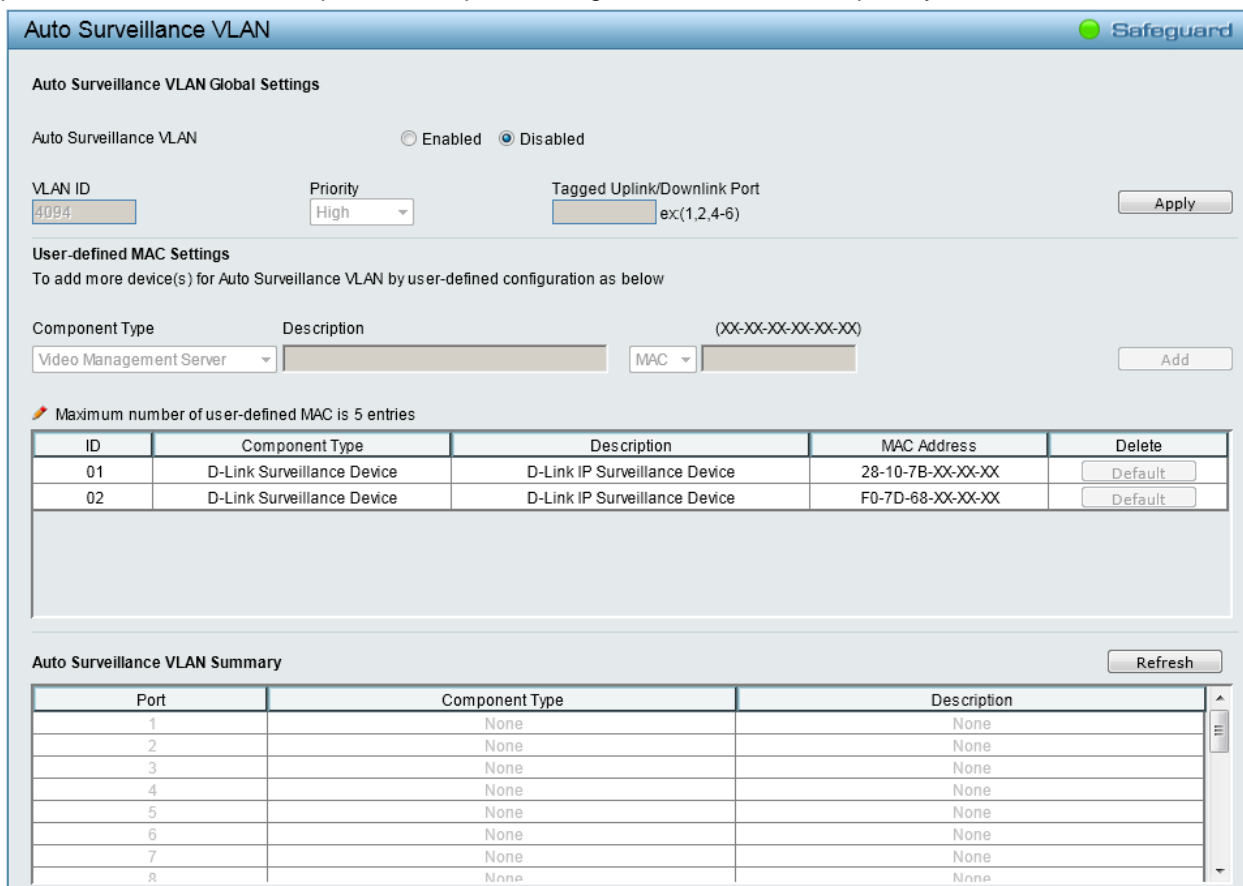
Figure 4.35 – VLAN > Auto Surveillance VLAN

Auto Surveillance VLAN Global Settings:

Auto Surveillance VLAN: 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 after **Enabled** is selected in **Auto Surveillance VLAN**.

Priority: The 802.1p priority levels of the traffic in the Auto Surveillance VLAN. The possible values are **Highest**, **High**, **Medium** and **Low**.

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

Click **Apply** to implement the changes.

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. System will auto generate an ACL profile (Profile ID: 53) for all the Auto Surveillance VLAN rules.

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 13,004 bytes (tagged). Default is *Disabled.* Click **Enabled**, and then **Apply** to turn on the jumbo frame support.
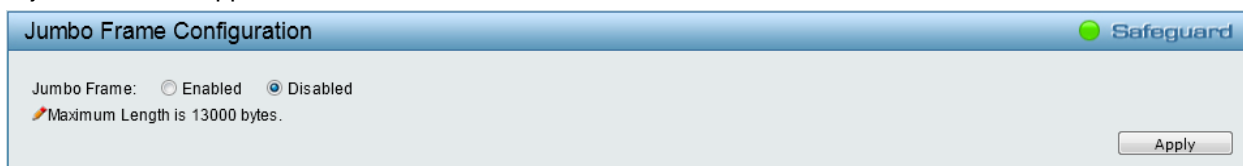
<p align="center">**Figure 4.36 – L2 Functions > Jumbo Frame**</p>

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. The function is *Disabled* by default. Click **Enabled** to enable the function.
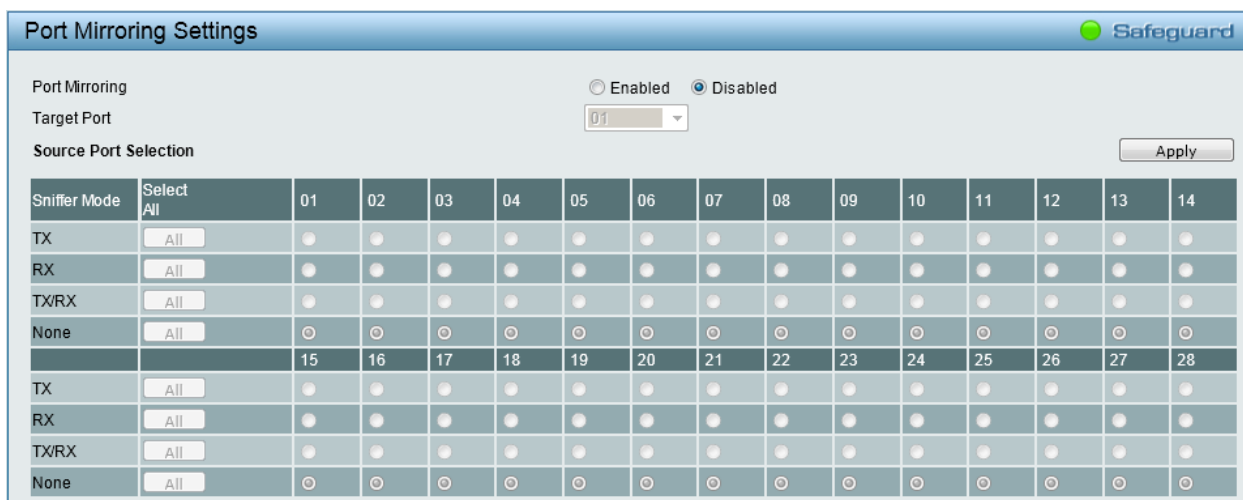
<p align="center">**Figure 4.37 – L2 Functions > Port Mirroring**</p>

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.

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

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 shut down the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection **Recover Time** times out. The Loopback Detection function can be implemented on a range of ports at the same time.
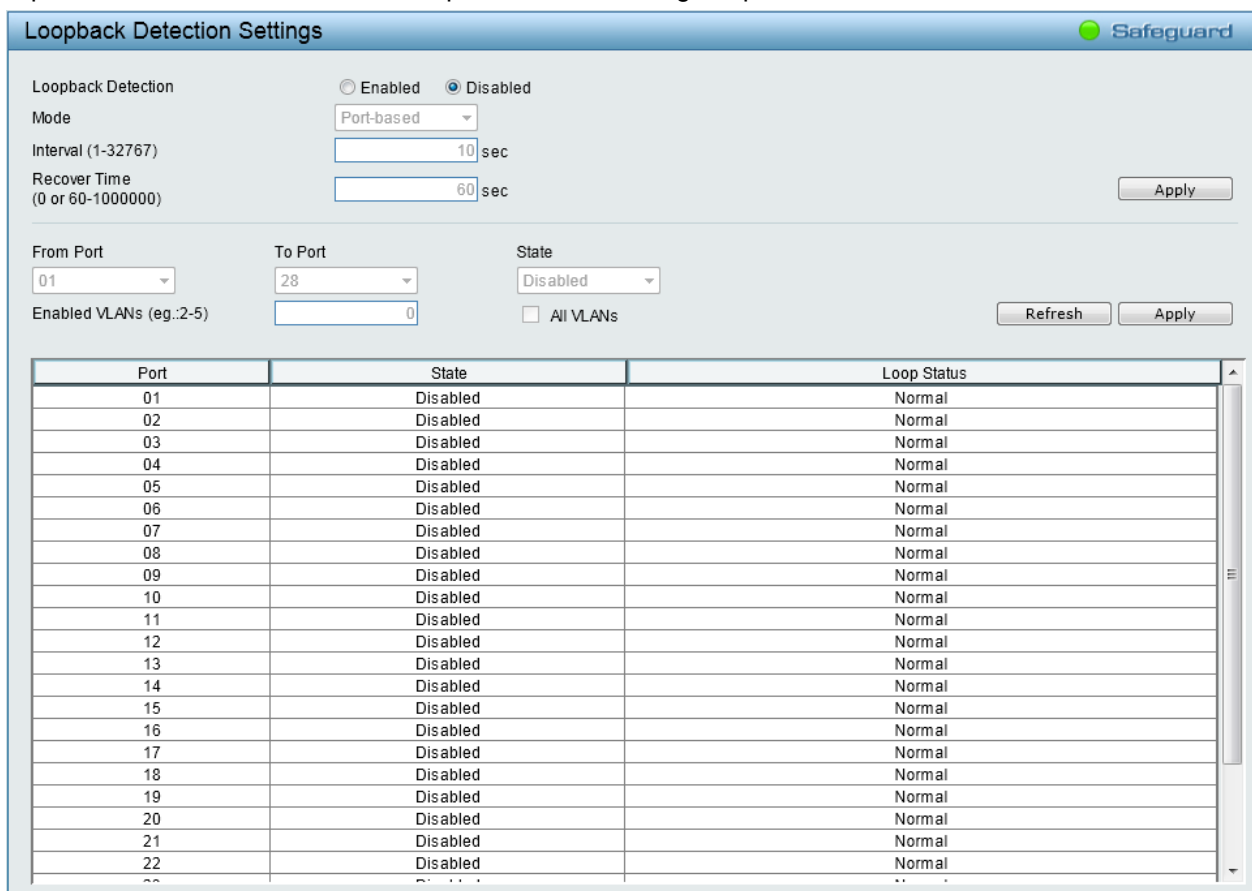
<p align="center">**Figure 4.38 – L2 Functions > Loopback Detection**</p>

Loopback Detection: Click to enable or disable loopback detection. The default is *Disabled*.

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

Interval (1-32767): Set a Loop detection Interval between 1 and 32767 seconds. The default is *10* 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 / To Port: 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*.

Enabled VLANs: This is used to configure the loopback detection function for the VLANs on VLAN-based mode. Enter the list of VLAN used for this configuration. Tick the **All VLANs** check box to enable this option on all the VLANs configured on the Switch.

Click **Apply** to implement the changes made. 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** allows turning on or off the function of learning MAC address automatically, if a port is not specified as an uplink port (for example, connects to a DHCP Server or Gateway). By default, this feature is *Disabled* (off).
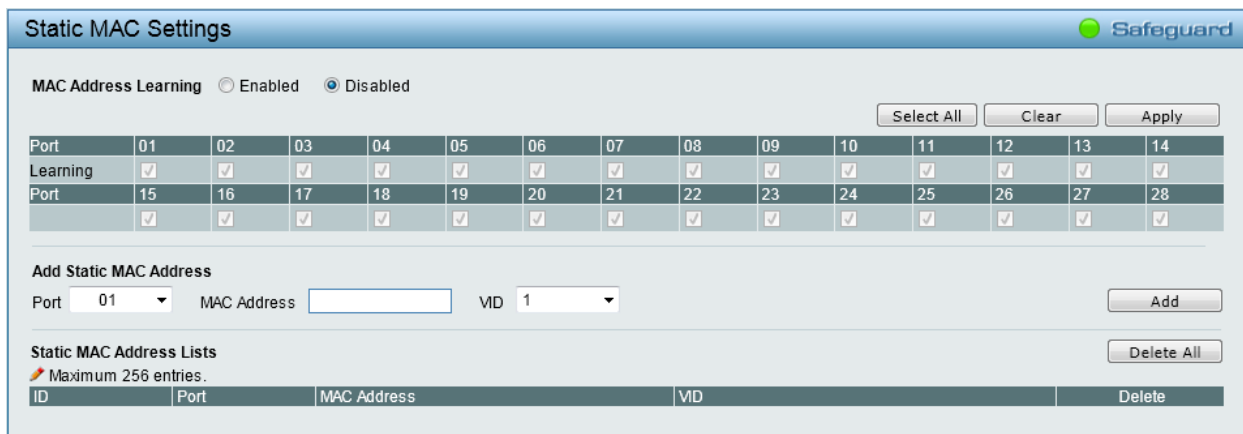
<p align="center">**Figure 4.39 – L2 Functions > MAC Address Table > Static Mac Address**</p>

To initiate the removal of auto-learning for any of the uplink ports, click **Enabled** to enable this feature, and then select the port(s) for auto learning to be enabled.

The **Static MAC Address Lists** table displays the static MAC addresses connected, as well as the VID. To add a new 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 the corresponding entry, or click **Delete all** to remove all entries.

By disabling 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 List, tick the checkbox in **Add to Static MAC**, and then click **Apply** associated with the identified address. Click **Select** to tick the entries in the list. Click **Clear** to deselect all entries.
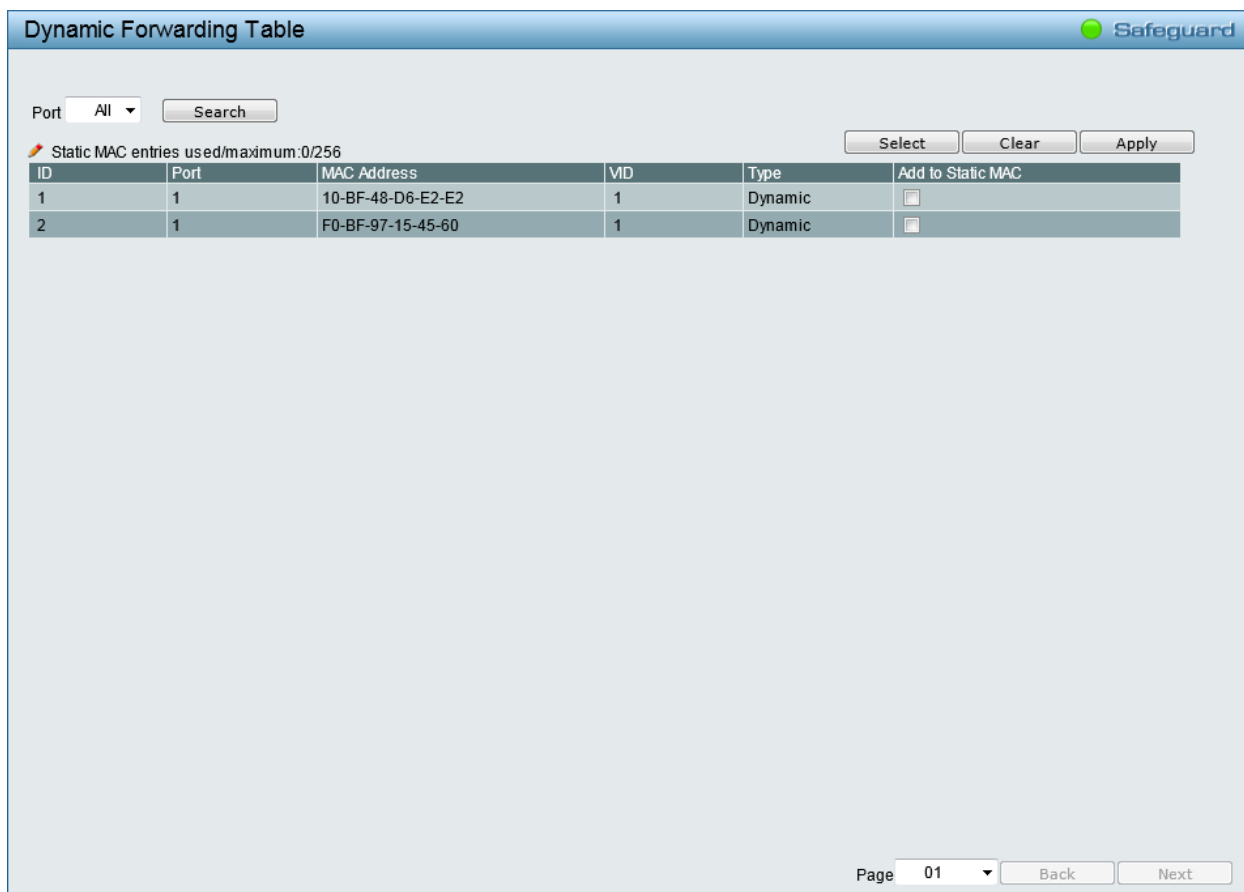
Figure 4.40 – L2 Functions > MAC Address Table > Dynamic Forwarding Table

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 802.1D-2004 specification and a version compatible with the IEEE 802.1D-98 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-98, however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-98 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, Spanning Tree Protocol 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:
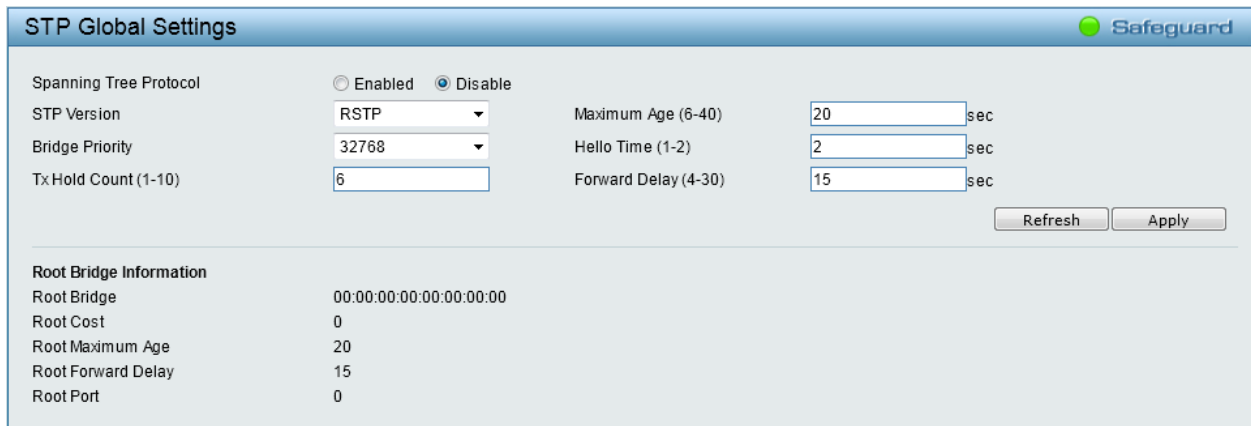
Figure 4.41 – L2 Functions > Spanning Tree > STP Global Settings

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

Bridge Priority: This value, between 0 and 61440, specifies the priority for forwarding packets. The lower the value, the higher the priority. The default is *32768*.

TX Hold Count (1-10): Specifies 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): 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*. (Maximum Age must have a value larger than Hello Time)

Hello Time (1-2): 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): 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

This window allows the user to configure STP parameters for individual ports or a range of ports. 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 recommended to define an STP Group to correspond to a VLAN group of ports.
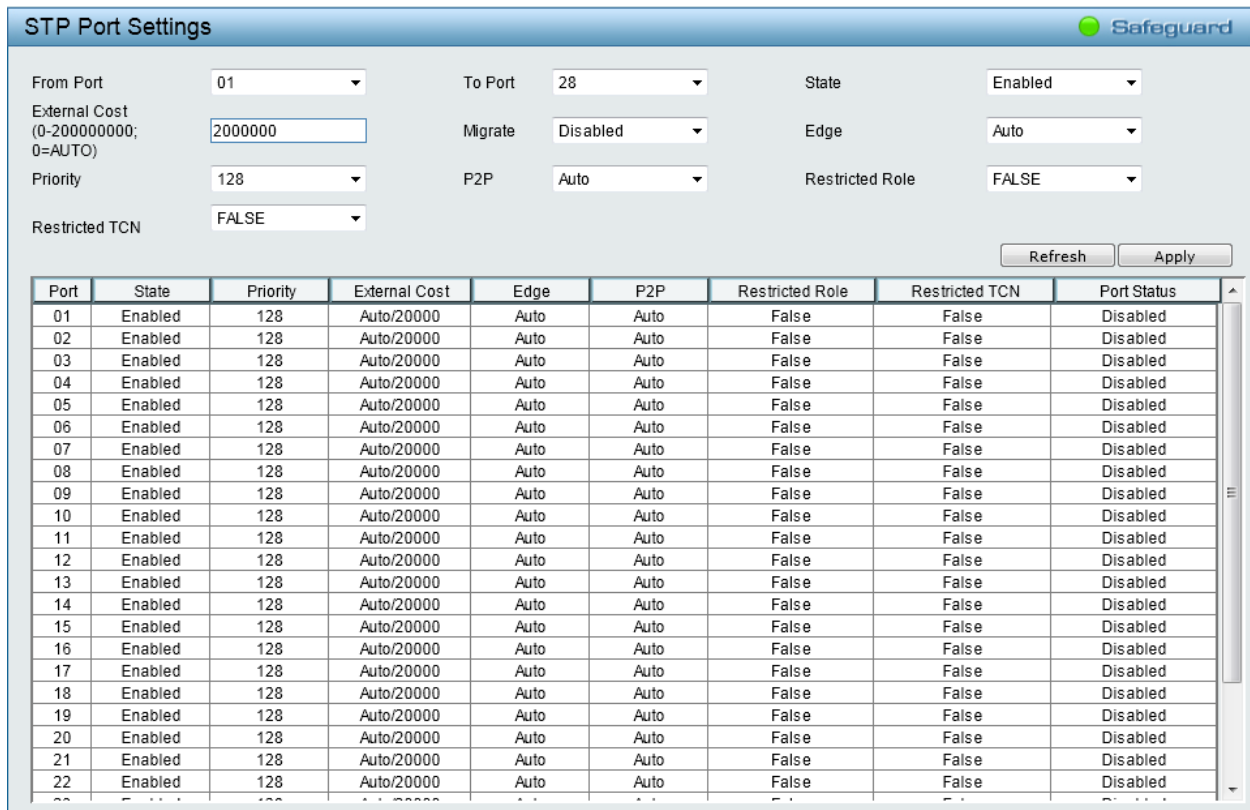
Figure 4.42 – L2 Functions > Spanning Tree > STP Port Settings

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 packets to 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 **Enabled** 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-98 STP to 802.1D-2004 RSTP. Migration should be set as enabled on ports connected to network stations or segments that are capable of being upgraded to 802.1D-2004 RSTP on all or some portion of the segment.

Edge: Select **True** to designate 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. Select **False** to indicate that the port does not have edge port status. Select **Auto** to indicate 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: Select **Force True** to indicate 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 **Force 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 **Force False**. The default setting 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.
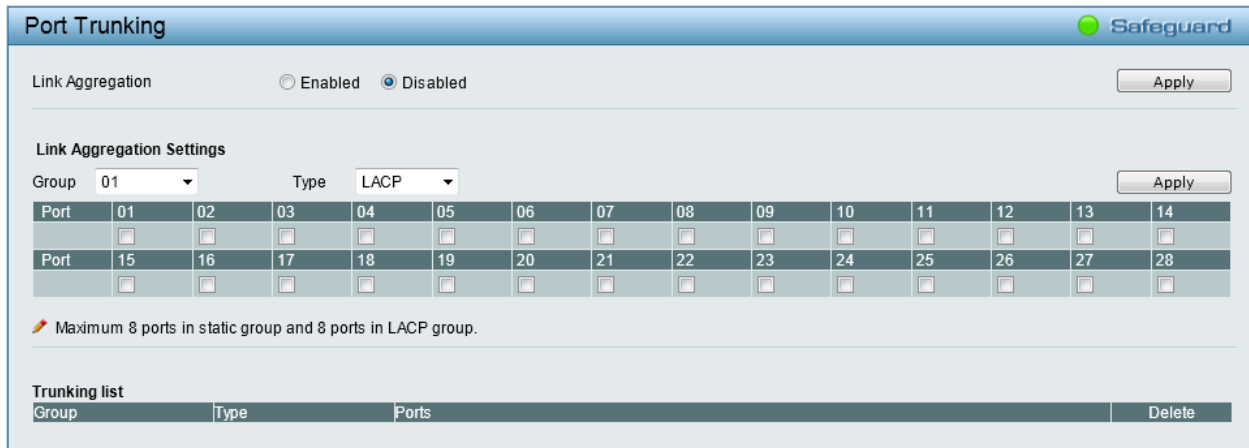
Figure 4.43 – L2 Functions > Link Aggregation > Port Trunking

Link Aggregation: Click to enable or disable link aggregation.

Group: Use the drop-down menu to select a trunk group.

Type: 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.

Select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups.

> **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 4.44 – L2 Functions > Link Aggregation > LACP Port Settings

From Port / To Port: 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: Specifies 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.
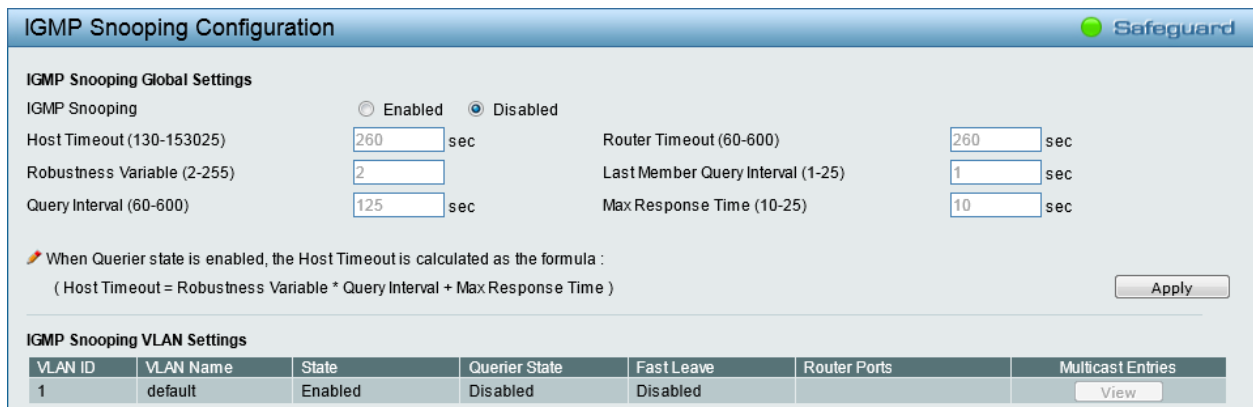
Figure 4.45 – L2 Functions > Multicast > IGMP Snooping

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

Host Timeout (130-153025): 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): 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. The default value is *2*.

Query Interval (60-600): 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): 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): 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): 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 Enabled and click the **Apply** button. Then, click the VLAN ID hyperlink to see the following window. Select the ports to be assigned as router ports for IGMP snooping for the VLAN, and click **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.
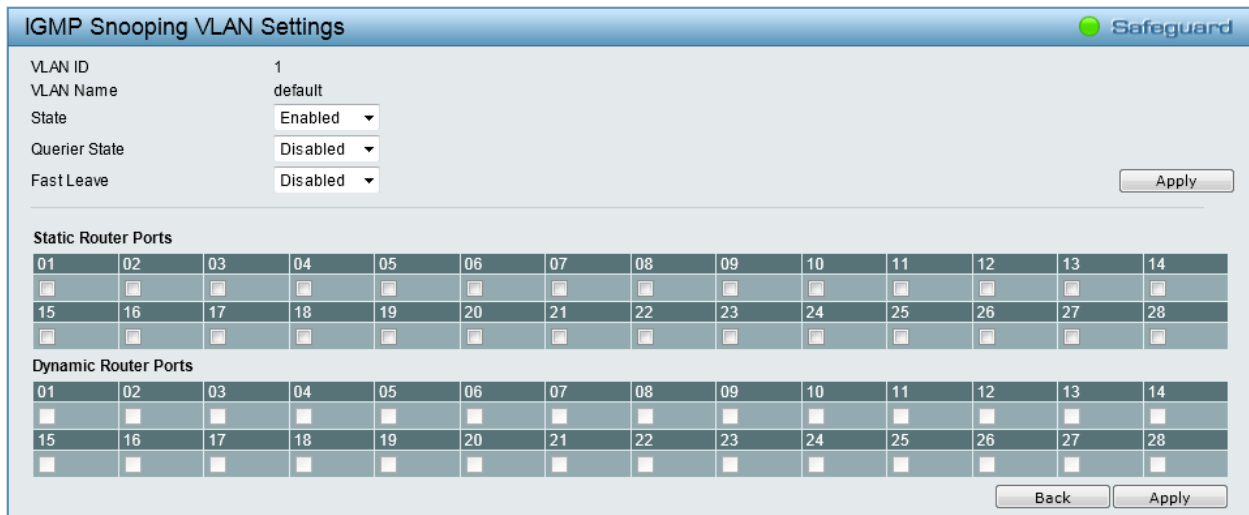
Figure 4.46 – L2 Functions > Multicast > IGMP Snooping VLAN Settings

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. The default state is *Disabled*.

Fast Leave: Specify the Fast Leave feature to be enabled or disabled. The default state is *Disabled*.

To view the Multicast Entry Table for a given VLAN, press the **View** button.
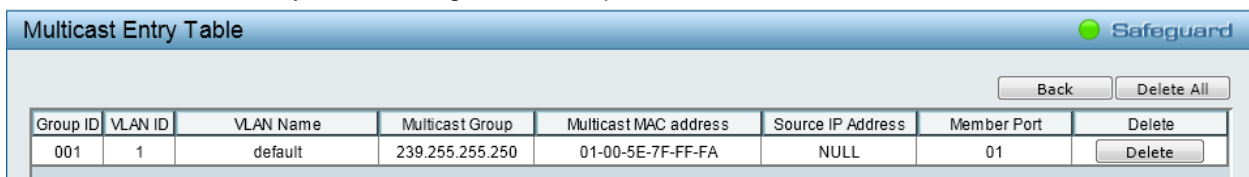
Figure 4.47 – L2 Functions > Multicast > IGMP Multicast Entry Table

Click **Delete** to remove the corresponding entry. Click **Delete All** to remove all entries. Click **Back** to go back to the previous window.

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.
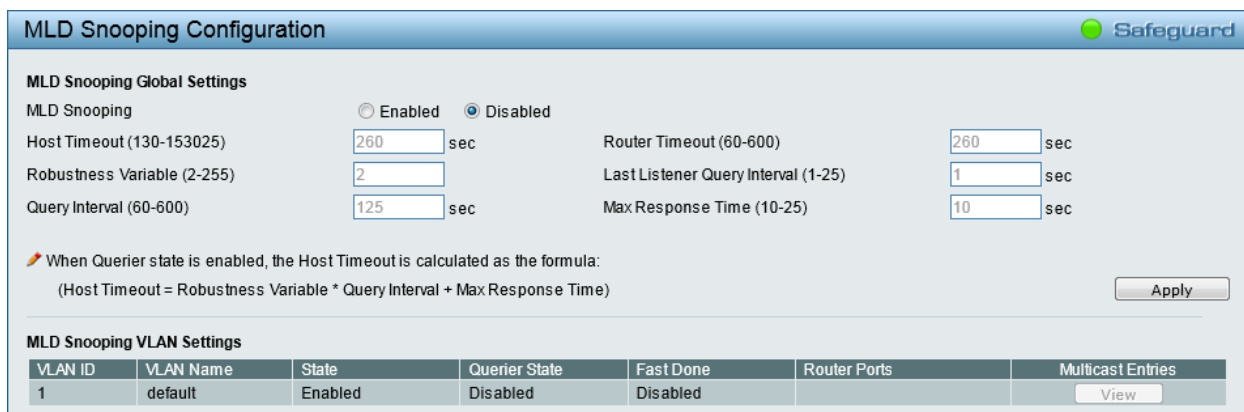
By default, MLD is *Disabled*. If enabled, the MLD Global Settings will need to be entered:

Host Timeout (130-153025): 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): 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. The default value is *2*.

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

Router Timeout (60-600): 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 Listener Query Interval (1-25): The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group. The default is *1* second.

Max Response Time (10-25): 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 MLD traffic on a subnet. Default is *10* seconds.

To enable MLD snooping for a given VLAN, select Enabled and click the **Apply** button. Then, click the VLAN ID hyperlink to see the following window. Select the ports to be assigned as router ports for MLD snooping for the VLAN, and click **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.
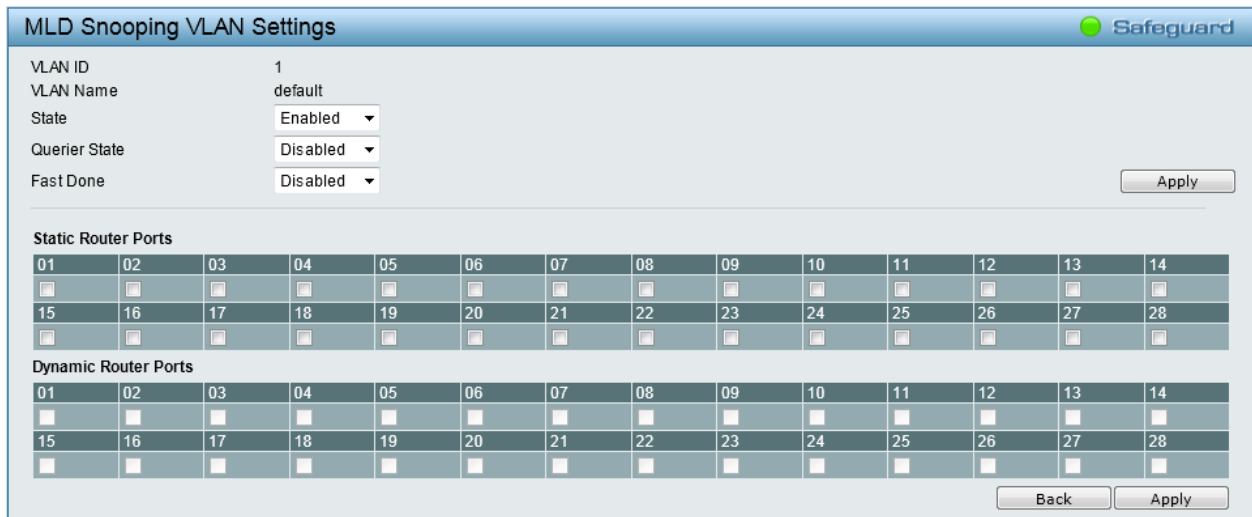
Figure 4.49 – L2 Functions > Multicast > MLD Snooping VLAN Settings

State: Specify the State to be enabled or disabled.

Querier State: D-Link Smart Switch is able to send out the MLD Queries to check the status of multicast clients. The default state is *Disabled*.

Fast Done: Specify the Fast Done feature to be enabled or disabled. The default state is *Disabled*.

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

Figure 4.50 – L2 Functions > Multicast > MLD Multicast Entry Table

Click **Delete** to remove the corresponding entry. Click **Delete All** to remove all entries. Click **Back** to go back to the previous window.

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**.
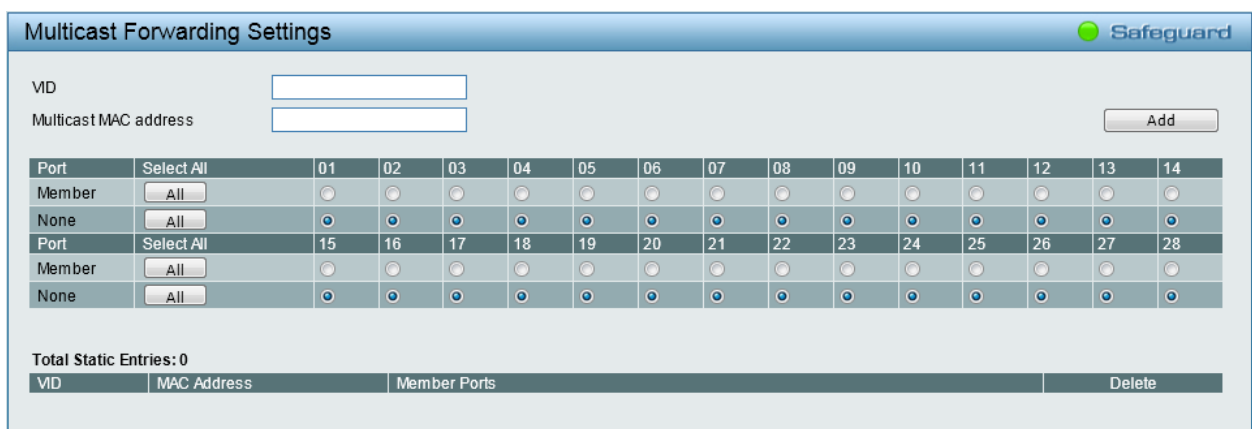
Figure 4.51 – L2 Functions > Multicast > Multicast Forwarding

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: Allows the selection of ports that will be members of the static multicast group.
    Member - The port is a static member of the multicast group.
    None - When **None** is selected, 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.
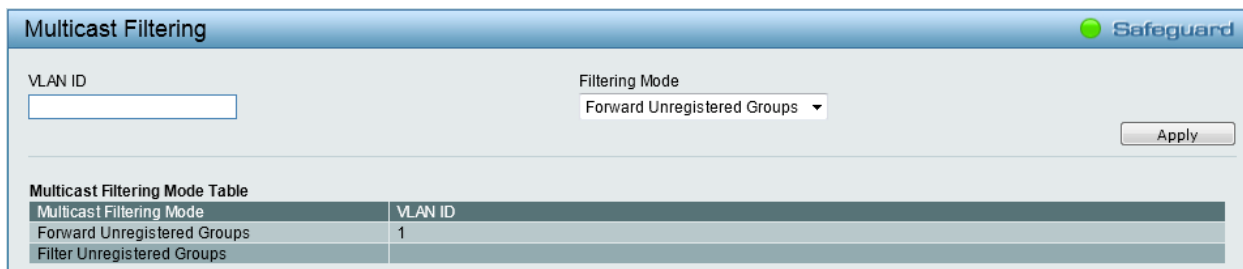
VLAN ID: Specifies the VLAN ID.
Filtering Mode:
    Forward Unregistered Groups - The multicast stream will be forwarded based on the register table in registered group, but it will be flooded to all ports of the VLAN in unregistered group.
    Filter Unregistered Groups - The registered group will be forwarded based on the register table and the unregister group will be filtered.

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

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 window.

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: Specifies the IPv4 or IPv6 address of the primary SNTP server from which the system time is retrieved.
SNTP Second Server: Specifies the IPv4 or IPv6 address of the secondary SNTP server from which the system time is retrieved.
SNTP Poll Interval (30-99999): Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is *720* seconds.

When selecting **Local** for the clock source, users can select from one of two options:
Manually Time Settings: Users input the system time manually.
Sync To PC: The system time will be synchronized from the local computer.

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

L2 Functions > SNTP > Time Zone Settings
The Time Zone Setting window is used to configure time zones and Daylight Savings time settings for SNTP.

<div align="center">
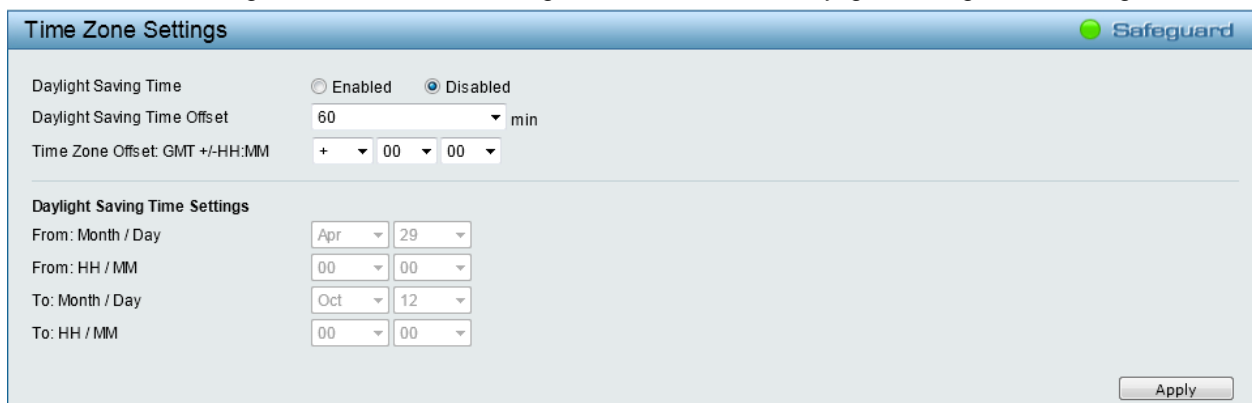
Figure 4.54 – L2 Functions > SNTP > Time Zone Settings

</div>

Daylight Saving Time: 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.
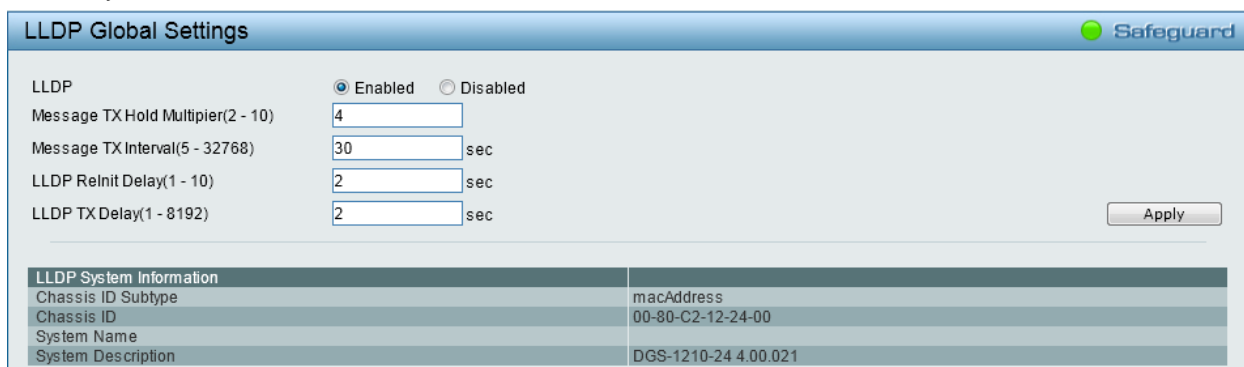
Click **Apply** to implement the changes made.

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 enabled by default.

Figure 4.55 – 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.

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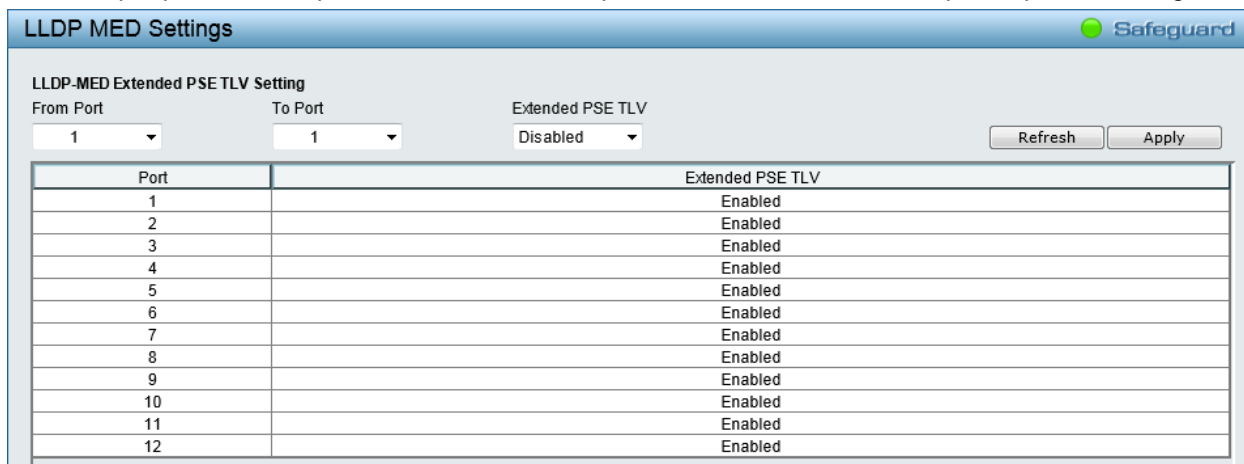
LLDP ReInit Delay (1-10): This parameter indicates the amount of delay from the time adminStatus becomes disabled until re-initialization is attempted. The default value is *2* seconds.

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: $1 < txDelay \leq 0.25 * (Message\ TX\ Interval)$. The default value is *2* seconds.

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

L2 Functions > LLDP > LLDP MED Settings (DGS-1210-24P only)

By selecting a range of ports (**From Port** and **To Port**), the power PSE TLV type can be enabled for all selected ports to indicate the power source equipment (PSE) switch to transmit high power (15.4 to 30 Watts) to the pre-standard of 802.3at power devices via LLDP MDI TLV. Through this feature, the PSE can provide precise output power to the pre-standard of 802.3at power devices and achieve optimal power management.

Figure 4.56 – L2 Functions > LLDP > LLDP MED Settings

From Port/ To Port: A consecutive group of ports may be configured starting with the selected port.
Extended PSE TLV: Select to enable or disable the extended PSE TLV option.

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

L2 Functions > LLDP > LLDP Port Settings
The Basic LLDP Port Settings page displays LLDP port information and contains parameters for configuring LLDP port settings.
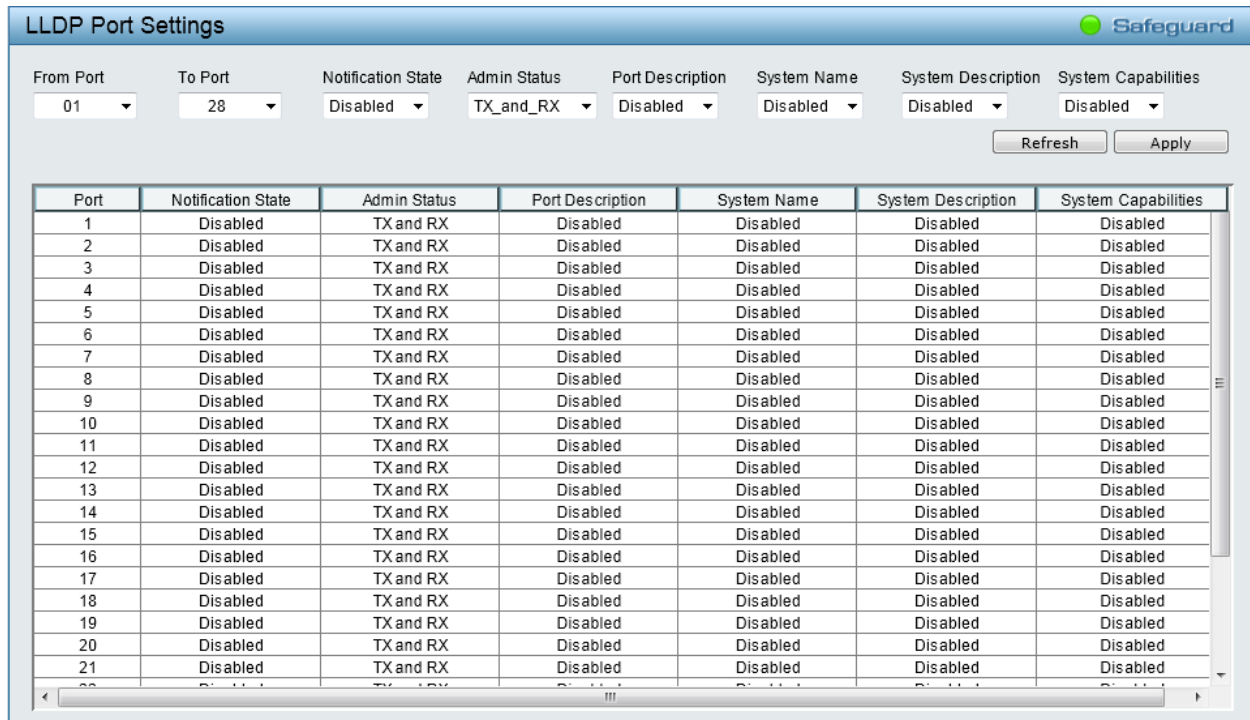
<div align="center">Figure 4.57 – L2 Functions > LLDP > LLDP Port Settings</div>

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 default is *Disabled*.

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.
System Name: Specifies whether the System Name TLV is enabled on the port.
System Description: Specifies whether the System Description TLV is enabled on the port.
System Capabilities: Specifies whether the System Capabilities TLV is enabled on the port.

Click **Apply** to implement the changes made. 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.
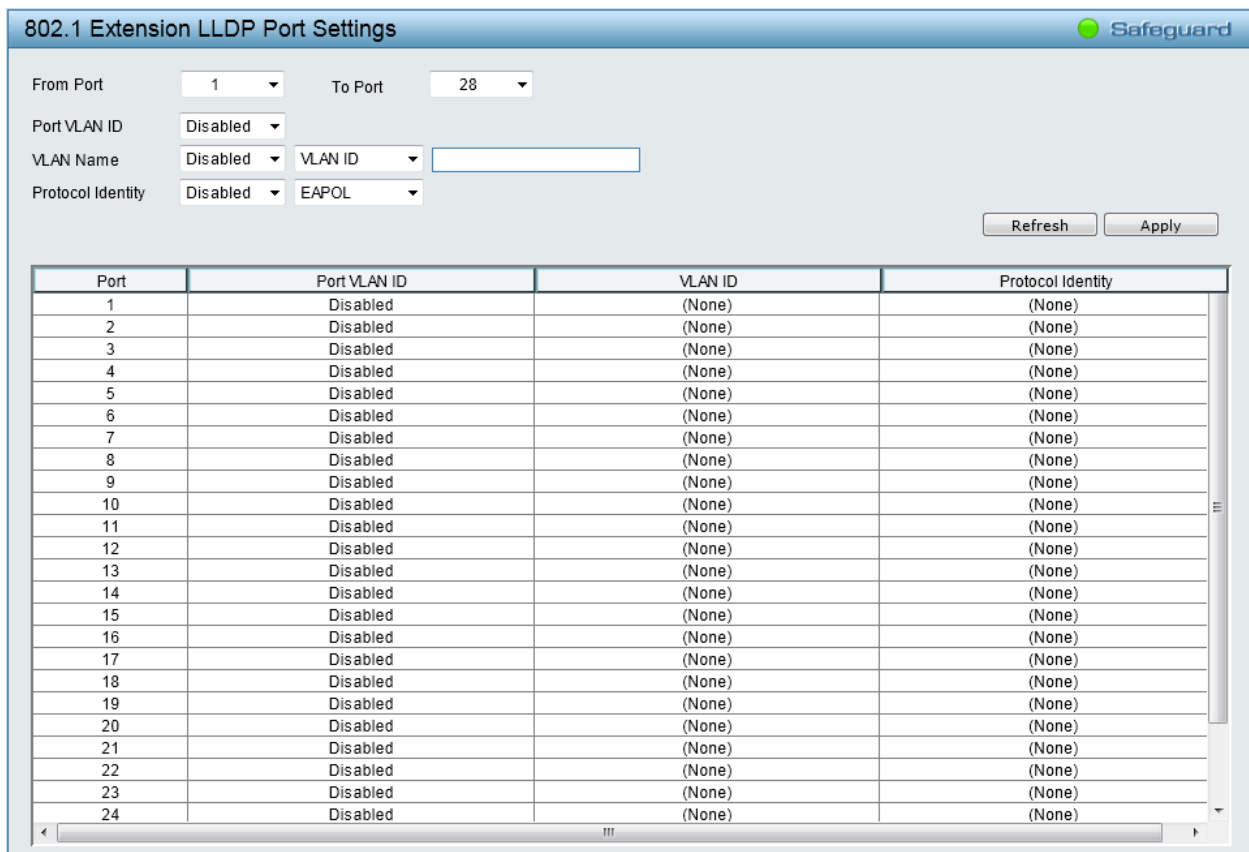
Figure 4.58 – L2 Functions > LLDP > 802.1 Extension TLV Port Settings

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 TLV to be enabled or disabled.

VLAN Name: Specifies the VLAN name TLV to be enabled or disabled in the LLDP port. If enabled, users can specify the content of **VLAN ID**, **VLAN Name** or **All**.

Protocol Identity: Specifies the Protocol Identity TLV to be enabled or disabled in the LLDP port. If enabled, users can specify the **EAPOL**, **LACP**, **GVRP**, **STP** or **All**.

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

L2 Functions > LLDP > 802.3 Extension TLV

The 802.3 Extension LLDP Port Settings window displays 802.3 Extension LLDP port information and contains parameters for configuring 802.3 Extension LLDP port settings.

Figure 4.59 – L2 Functions > LLDP > 802.3 Extension TLV Port Settings

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

MAC/PHY Configuration/Status: Specifies that the LLDP agent should transmit the MAC/PHY configuration/status TLV. This indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, whether it has auto-negotiated advertised capability, and what is the operational MAU type. The default state is *Disabled*.

Power Via MDI: Specifies whether LLDP agent should transmit Power via MDI TLV. Three IEEE 802.3 PMD implementations (10BASE-T, 100 BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN stations. The default state is *Enabled* in PoE ports which support 802.3af.

Link Aggregation: The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is *Disabled*.

Maximum Frame Size: Specifies whether the maximum frame size TLV is enabled on the port. The default state is *Disabled*.

Click **Apply** to implement the changes made. 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.
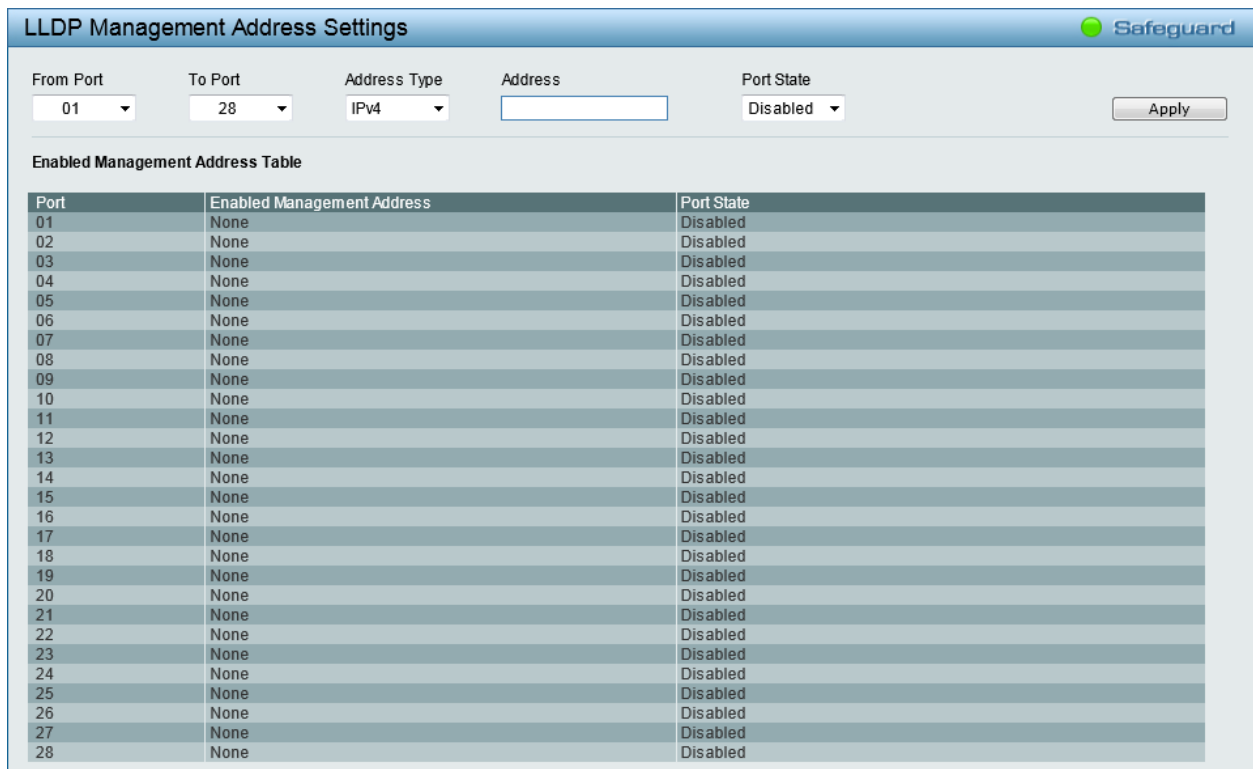
Figure 4.60 – L2 Functions > LLDP > LLDP Management Address Settings

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

Address Type: Select the IP address type here. Options to choose from are *IPv4* and *IPv6.*

Address: Enter the management IPv4 or IPv6 address.

Port State: Specify whether the Port State is enabled on the port.

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

L2 Functions > LLDP > LLDP Management Address Table

The LLDP Management Address Table page displays the detailed management address information for the entry.
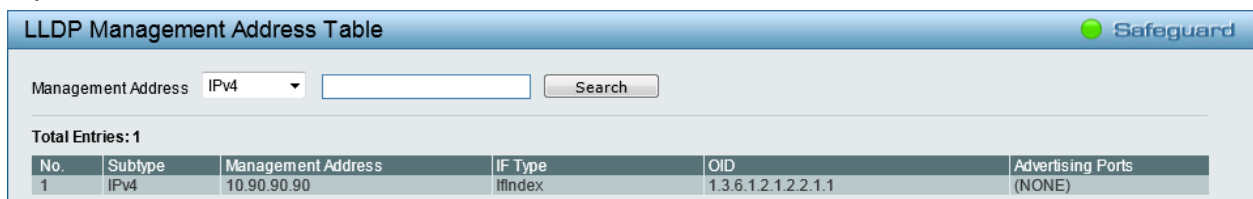
Figure 4.61 – L2 Functions > LLDP > LLDP Management Address Table

Management Address: Select *IPv4* or *IPv6*, from the drop-down menu, and enter the IPv4 or IPv6 address in the textbox. 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 window displays LLDP local port information.

Port	Port ID Subtype	Port ID	Port Description	Normal	Detailed
01	MAC Address	00-80-C2-12-24-01	D-Link DGS-1210-24 R4.10.007 Port 1	View	View
02	MAC Address	00-80-C2-12-24-02	D-Link DGS-1210-24 R4.10.007 Port 2	View	View
03	MAC Address	00-80-C2-12-24-03	D-Link DGS-1210-24 R4.10.007 Port 3	View	View
04	MAC Address	00-80-C2-12-24-04	D-Link DGS-1210-24 R4.10.007 Port 4	View	View
05	MAC Address	00-80-C2-12-24-05	D-Link DGS-1210-24 R4.10.007 Port 5	View	View
06	MAC Address	00-80-C2-12-24-06	D-Link DGS-1210-24 R4.10.007 Port 6	View	View
07	MAC Address	00-80-C2-12-24-07	D-Link DGS-1210-24 R4.10.007 Port 7	View	View
08	MAC Address	00-80-C2-12-24-08	D-Link DGS-1210-24 R4.10.007 Port 8	View	View
09	MAC Address	00-80-C2-12-24-09	D-Link DGS-1210-24 R4.10.007 Port 9	View	View
10	MAC Address	00-80-C2-12-24-0A	D-Link DGS-1210-24 R4.10.007 Port 10	View	View
11	MAC Address	00-80-C2-12-24-0B	D-Link DGS-1210-24 R4.10.007 Port 11	View	View
12	MAC Address	00-80-C2-12-24-0C	D-Link DGS-1210-24 R4.10.007 Port 12	View	View
13	MAC Address	00-80-C2-12-24-0D	D-Link DGS-1210-24 R4.10.007 Port 13	View	View
14	MAC Address	00-80-C2-12-24-0E	D-Link DGS-1210-24 R4.10.007 Port 14	View	View
15	MAC Address	00-80-C2-12-24-0F	D-Link DGS-1210-24 R4.10.007 Port 15	View	View
16	MAC Address	00-80-C2-12-24-10	D-Link DGS-1210-24 R4.10.007 Port 16	View	View
17	MAC Address	00-80-C2-12-24-11	D-Link DGS-1210-24 R4.10.007 Port 17	View	View
18	MAC Address	00-80-C2-12-24-12	D-Link DGS-1210-24 R4.10.007 Port 18	View	View
19	MAC Address	00-80-C2-12-24-13	D-Link DGS-1210-24 R4.10.007 Port 19	View	View
20	MAC Address	00-80-C2-12-24-14	D-Link DGS-1210-24 R4.10.007 Port 20	View	View
21	MAC Address	00-80-C2-12-24-15	D-Link DGS-1210-24 R4.10.007 Port 21	View	View
22	MAC Address	00-80-C2-12-24-16	D-Link DGS-1210-24 R4.10.007 Port 22	View	View
23	MAC Address	00-80-C2-12-24-17	D-Link DGS-1210-24 R4.10.007 Port 23	View	View
24	MAC Address	00-80-C2-12-24-18	D-Link DGS-1210-24 R4.10.007 Port 24	View	View
25	MAC Address	00-80-C2-12-24-19	D-Link DGS-1210-24 R4.10.007 Port 25	View	View
26	MAC Address	00-80-C2-12-24-1A	D-Link DGS-1210-24 R4.10.007 Port 26	View	View
27	MAC Address	00-80-C2-12-24-1B	D-Link DGS-1210-24 R4.10.007 Port 27	View	View
28	MAC Address	00-80-C2-12-24-1C	D-Link DGS-1210-24 R4.10.007 Port 28	View	View

Figure 4.62 – L2 Functions > LLDP > LLDP Local Port Brief Table

Port: Displays the port number.

Port ID Subtype: Displays the port ID subtype.

Port ID: Displays the port ID.

Port Description: Displays the port description.

Click **View** in the Normal column to display more information.

No.	1
Port ID Subtype	MAC Address
Port Id	00-80-C2-12-24-01
Port Description	D-Link DGS-1210-24 R4.10.007 Port 1
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	1536

Show LLDP Local Port Brief Table

Show LLDP Local Port Detailed Table

Figure 4.63 – L2 Functions > LLDP > LLDP Local Port Normal Table

Click **View** in the Detailed column to display detail information.
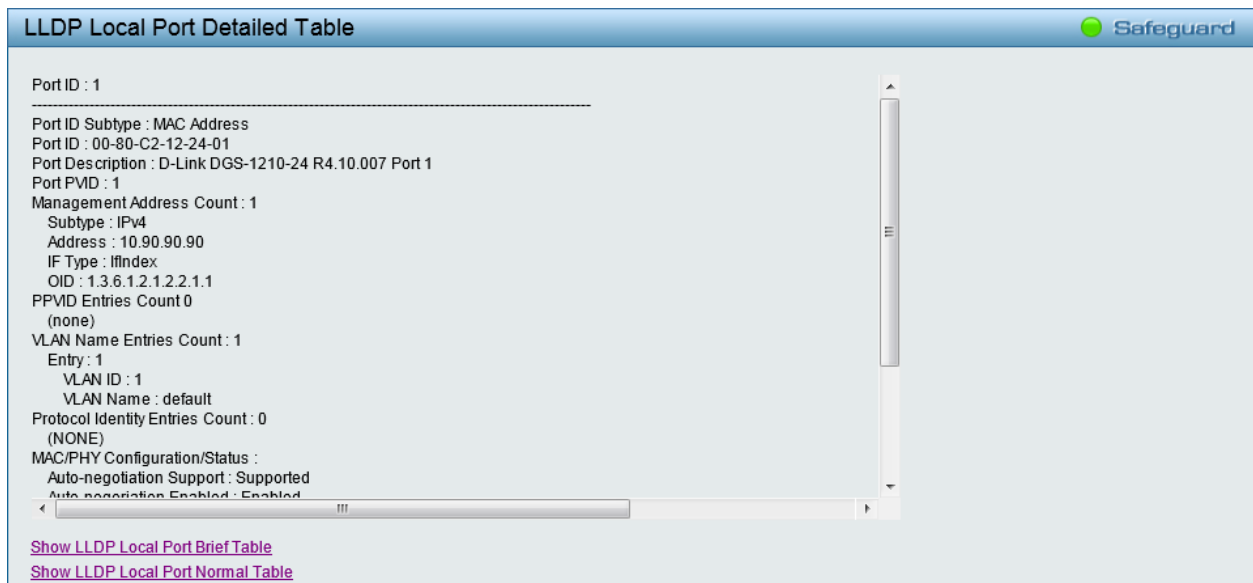
Figure 4.64 – L2 Functions > LLDP > LLDP Local Port Detailed Table

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 the detail information of the port.
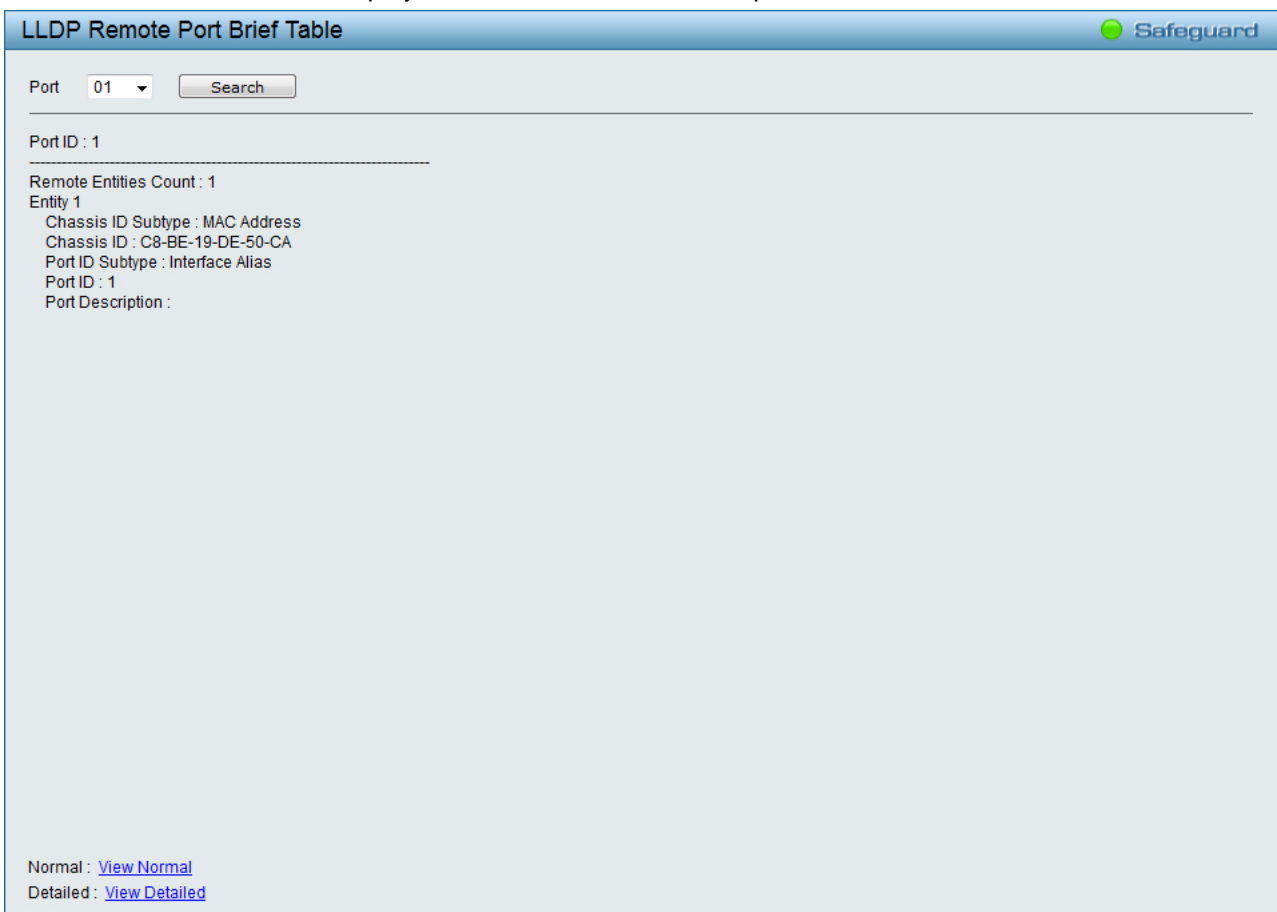
Figure 4.65 – L2 Functions > LLDP > LLDP Remote Port Brief Table

To view the more information for a remote port, click the View Normal hyperlink and the following window displays.

LLDP Remote Port Normal Table   ● Safeguard

Port ID : 1

Remote Entities Count : 1
Entity 1
   Chassis ID Subtype : MAC Address
   Chassis ID : C8-BE-19-DE-50-CA
   Port ID Subtype : Interface Alias
   Port ID : 1
   Port Description :
   System Name :
   System Description :
   System Capabilities :
   Management Address Count : 0
   Port PVID : 0
   PPVID Entries Count : 0
   VLAN Name Entries Count : 0
   Protocol Identity Entries Count : 0
   MAC/PHY Configuration/Status : See detail
   Power Via MDI : See detail
   Link Aggregation : See detail
   Maximum Frame Size : 0
   Unknown TLVs Count : 0

Show LLDP Remote Port Brief Table
Show LLDP Remote Port Detailed Table

Figure 4.66 – L2 Functions > LLDP > LLDP Remote Port Normal Table

To view the detailed information for a remote port, click View Detailed and the following page displays.

Figure 4.67 – L2 Functions > LLDP > LLDP Remote Port Detailed Table

L2 Functions > LLDP > LLDP Statistics

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

Figure 4.68 – 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 Frames –** Displays the total number of LLDP frames transmitted on the port.

> **RxPortFrames Discarded –** Displays the total discarded frame number of LLDP frames received on the port.

> **RxPort Frames Errors –** 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.

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

> **RxPortTLVs Unrecognized –** 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 table. Click **Clear** to clean out all LLDP port statistics.

L3 Functions > IPv6 System Settings
The IPv6 System Settings window allows users to configure the IPv6 system settings for this Switch.

Figure 4.69 – L3 Functions > IPv6 System Settings

IPv6 System Settings:
Interface Name: Displays the IPv6 interface name.
IPv6 State: Select to enable or disable the IPv6 interface state.
DHCPv6 Client: Select to enable or disable the DHCPv6 client feature.
IPv6 Network Address: Enter the IPv6 network address for this interface here.

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

NS Retransmit Time Settings:
NS Retransmit Time: Enter the neighbor solicitation retransmit time value here. This value must be between 1 and 3600 seconds.

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

Automatic Link Local State Settings:
Automatic Link Local Address: Select to enable or disable the automatic link local address feature.

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

L3 Functions > IPv6 Route Settings
The IPv6 Route Settings window allows users to configure the IPv6 route settings for this Switch.

Figure 4.70 – L3 Functions > IPv6 Route Settings

IPv6 Default Gateway:
IP Interface: Enter the IPv6 interface name here.

Default Gateway: Enter the IPv6 default gateway address here.

Metric: Enter the metric value for this route here.

Click **Create** to create a new IPv6 route. Click **Delete** to remove the corresponding route.

L3 Functions > IPv6 Neighbor Settings

The IPv6 Neighbor Settings window allows users to configure the IPv6 neighbor settings for this Switch.

Figure 4.71 – L3 Functions > IPv6 Neighbor Settings

Interface Name: Enter the neighbor IPv6 interface name here.

Neighbor IPv6 Address: Enter the neighbor IPv6 address here.

VID: Enter the neighbor IPv6 VLAN ID here.

Link Layer MAC Address: Enter the neighbor IPv6 link layer MAC address here.

Click **Add** to create a new IPv6 neighbor entry.

Interface Name: Enter the neighbor IPv6 interface name here.

State: Select and enter the neighbor IPv6 state here. Options to choose from are *All*, *Address*, *Static*, and *Dynamic*.

Click **Find** to locate the IPv6 neighbor.

Click **Clear** to remove the entries displayed in the table.

L3 Functions > DHCP > DHCP Relay Settings

This window contains two main parts, DHCP Relay Global Settings and DHCP Relay Interface Settings.

In DHCP Relay Global Settings, users can enable and configure DHCP Relay Global Settings. The relay hops count limit allows the maximum number of hops (routers) that the DHCP messages can be relayed through to be set. The DHCP packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds' field of the packet is less than the relay time threshold, the packet will be dropped.

In DHCP Relay Interface Settings, users can set up a server, by IP address, for relaying DHCP information to the Switch. Properly configured settings will be displayed in the DHCP Relay Interface Table at the bottom of the window, once the user clicks the **Add** button. The user can only add one server IP for the System interface on the Switch. Entries may be deleted by clicking the corresponding **Delete** button.
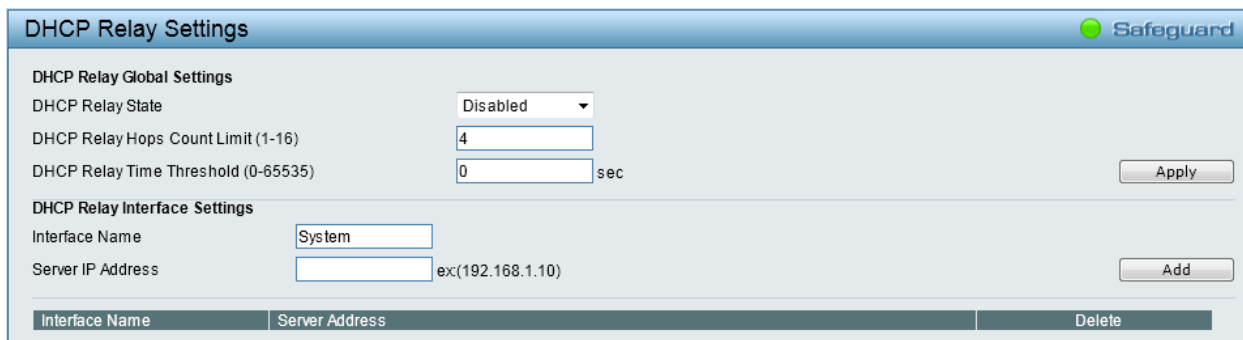
Figure 4.72 – L3 Functions > DHCP > DHCP Relay Settings

DHCP Relay Global Settings:

DHCP Relay State: Use the drop-down menu to toggle between **Enabled** and **Disabled**. It is used to enable or disable the DHCP Relay service on the Switch. The default is *Disabled*.

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

DHCP Relay Time Threshold (0-65535): Allows an entry between 0 and 65535 seconds, and defines the minimum time limit for routing a DHCP packet.

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

DHCP Relay Interface Settings:

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

Server IP Address: Enter the IP address of the DHCP server.

Click **Add** to create the information and display the information in the table below. Click **Delete** to remove the corresponding entry.

L3 Functions > DHCP > DHCPv6 Relay Settings

This window contains two main parts, DHCPv6 Relay Global Settings and DHCPv6 Relay Interface Settings.

In DHCPv6 Relay Global Settings, users can enable and configure DHCPv6 Relay Global Settings. The relay hops count limit allows the maximum number of hops (routers) that the DHCPv6 messages can be relayed through to be set. The DHCPv6 packet will be dropped when the relay hop count in the received packet is equal to or greater than this setting.

In DHCPv6 Relay Interface Settings, users can set up a server, by IPv6 address, for relaying DHCPv6 information to the Switch. Properly configured settings will be displayed in the DHCPv6 Relay Interface Table at the bottom of the window, once the user clicks the **Add** button. Entries may be deleted by clicking the corresponding **Delete** button.
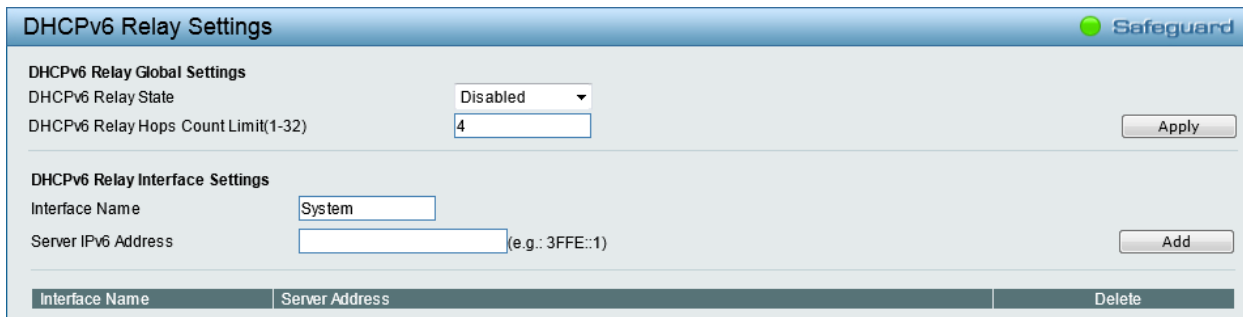
Figure 4.73 – L3 Functions > DHCP > DHCPv6 Relay Settings

DHCPv6 Relay Global Settings:

DHCPv6 Relay State: Use the drop-down menu to toggle between **Enabled** and **Disabled**. It is used to enable or disable the DHCPv6 Relay service on the Switch. The default is *Disabled*.

DHCPv6 Relay Hops Count Limit (1-32): This field allows an entry between 1 and 32. If the message received by the relay agent is a Relay-forward message and the hop-count in the message is greater than or equal to the Relay Hops Count Limit, the relay agent discards the received message. The default hop count is 4.

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

DHCPv6 Relay Interface Settings:

Interface Name: The IPv6 interface on the Switch that will be connected directly to the client.

Server IPv6 Address: Enter the IPv6 address of the DHCPv6 server.

Click **Add** to create the information and display the information in the table below. Click **Delete** to remove the corresponding entry.

QoS > Bandwidth Control

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

Port	TX Rate (Kbit/sec)	RX Rate (Kbit/sec)
1	No Limit	No Limit
2	No Limit	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit
22	No Limit	No Limit
23	No Limit	No Limit
24	No Limit	No Limit
25	No Limit	No Limit
26	No Limit	No Limit
27	No Limit	No Limit
28	No Limit	No Limit

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 (15-1024000): 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 15 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.
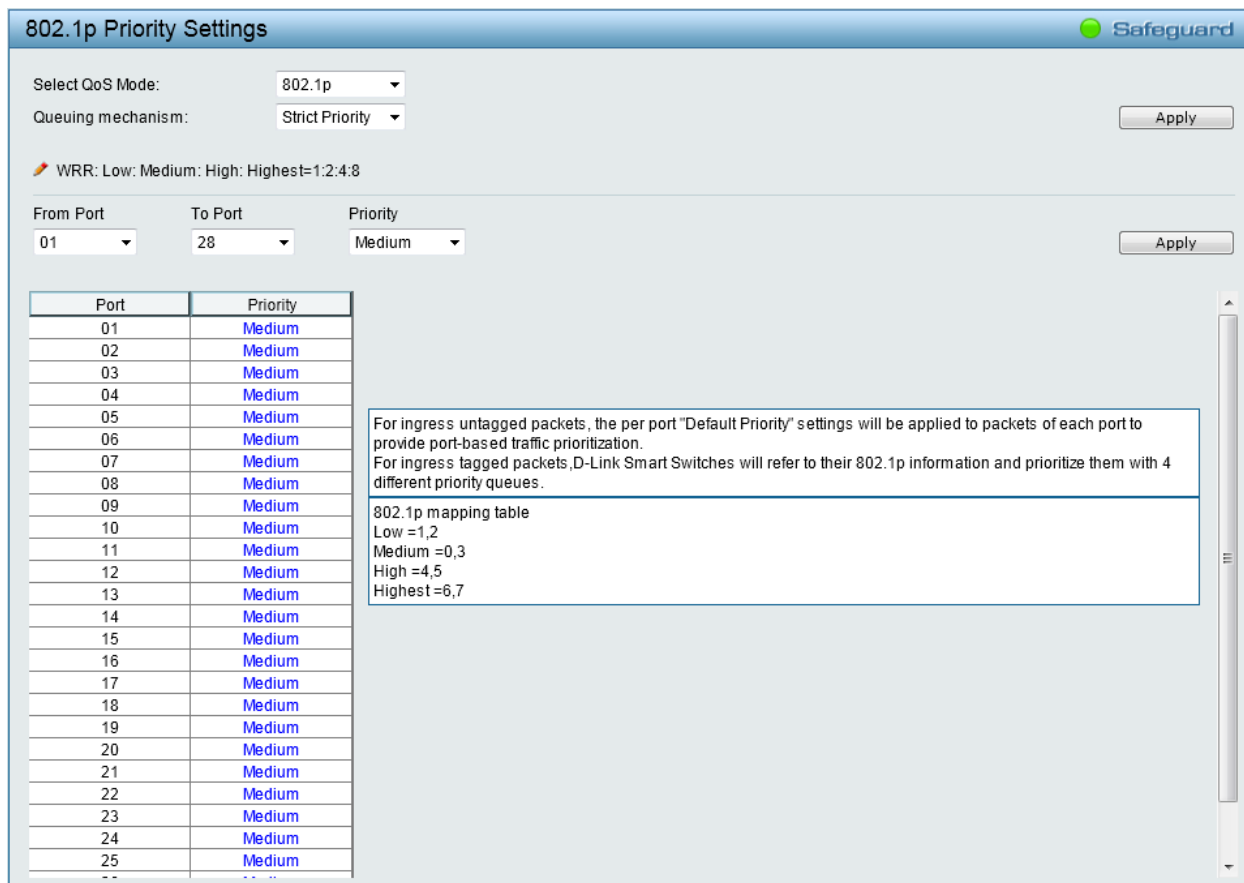
Figure 4.75 – QoS > 802.1p/DSCP/ToS

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.

When **802.1p** is selected in **Select QoS Mode**, the following selections appear.

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

Priority: Defines the priority assigned to the port. The priorities are **Highest**, **High**, **Medium** and **Low**.

When **DSCP** is selected in **Select QoS Mode**, the following selections appear.

From DSCP value / To DSCP value: Select a consecutive DSCP value.

Priority: Defines the priority assigned to the port. The priorities are **Highest**, **High**, **Medium** and **Low**.

When **ToS** is selected in **Select QoS Mode**, the following selections appear.

From ToS / To ToS: Select a consecutive ToS.

Priority: Defines the priority assigned to the port. The priorities are **Highest**, **High**, **Medium** and **Low**.

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

<u>**QoS > IPv6 Traffic Class Priority Settings**</u>

The IPv6 Traffic Class Priority Settings window allows users to configure the IPv6 traffic class priority settings.
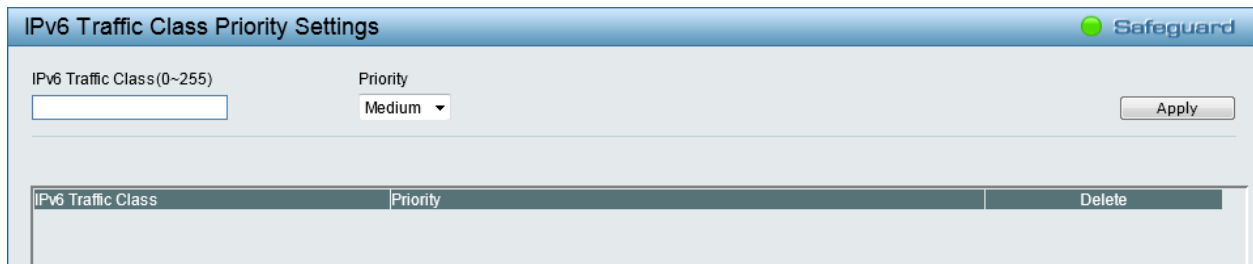
Figure 4.76 – QoS > IPv6 Traffic Class Priority Settings

IPv6 Traffic Class: Enter the IPv6 traffic class value here. This value must be between 0 and 255.

Priority: Defines the priority assigned to the class. The priorities are **Highest**, **High**, **Medium** and **Low**.

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

<u>**QoS > TCP/UDP Port Priority Settings**</u>

The TCP/UDP Port Priority Settings window allows user to configure the port priority.
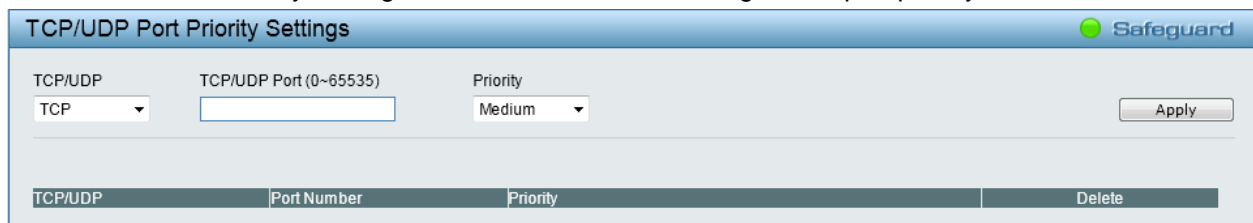
Figure 4.77 – QoS > TCP/UDP Port Priority Settings

TCP/UDP: Specify port priority of TCP or UDP to be configured.

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

Priority: Defines the priority assigned to the port. The priorities are **Highest**, **High**, **Medium** and **Low**.

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

<u>**Security > Trusted Host**</u>

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 the 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.
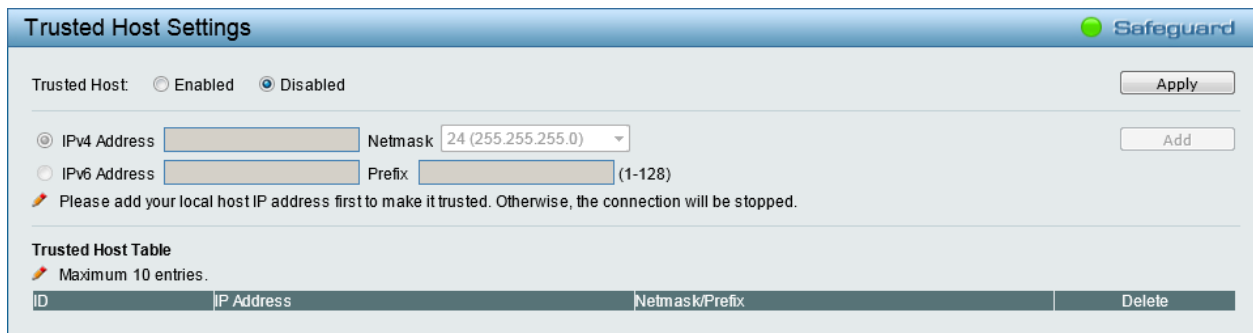
Figure 4.78 – Security > Trusted Host

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 IPv4 address and Subnet mask or IPv6 address and Prefix value. Click the **Apply** button to save your settings. You may permit only single or a range of IPv4 addresses by different IPv4 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 IPv4 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

Click **Delete** to remove the IP address.

Security > Port Security

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

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port lock is enabled.

Figure 4.79 – Security > Port Security

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

Admin State: Use the drop-down menu to enable or disable Port Security (locked MAC address table for the selected ports).

Max Learning Address (1-64): Specifies the maximum value of port security entries that can be learned on this port.

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

Security > DoS Attack Prevention

The user can configure the prevention of each DoS attacks. The packet matching will be done by hardware. For a specific type of attack, the content of the packet will be matched against a specific pattern.
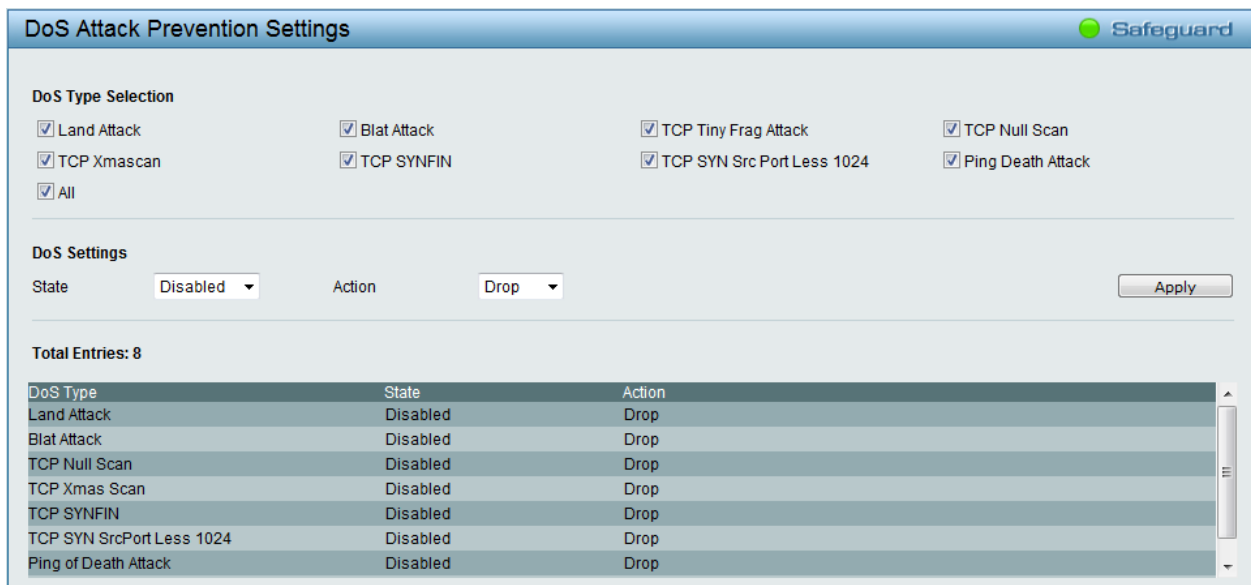
<p align="center">Figure 4.80 – Security > DoS Attack Prevention</p>

DoS Type Selection:

  Land Attack - Specifies that the DoS attack prevention type will be set to prevent LAND attacks.

  Blat Attack -- Specifies that the DoS attack prevention type will be set to prevent BLAT attacks.

  TCP Tiny Frag Attack - Specifies that the DoS attack prevention type will be set to prevent TCP Tiny Frag attacks.

  TCP Null Scan - Specifies that the DoS attack prevention type will be set to prevent TCP Null Scan attacks.

  TCP Xmascan - Specifies that the DoS attack prevention type will be set to prevent TCP Xmas Scan attacks.

  TCP SYNFIN -- Specifies that the DoS attack prevention type will be set to prevent TCP SYN FIN attacks.

  TCP SYN Src Port Less 1024 - Specifies that the DoS attack prevention type will be set to prevent TCP SYN Source Port Less 1024 attacks.

  Ping Death Attack - Specifies that the DoS attack prevention type will be set to prevent Ping of Death attacks.

  All - Specifies that the DoS attack prevention type will be set to prevent all attacks.

State: Use the drop-down menu to enable or disable the DoS Attack Prevention state

Action: Select the action that the DoS Prevention function will take.

  Drop - Select to drop all matched DoS attack packets.

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

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.
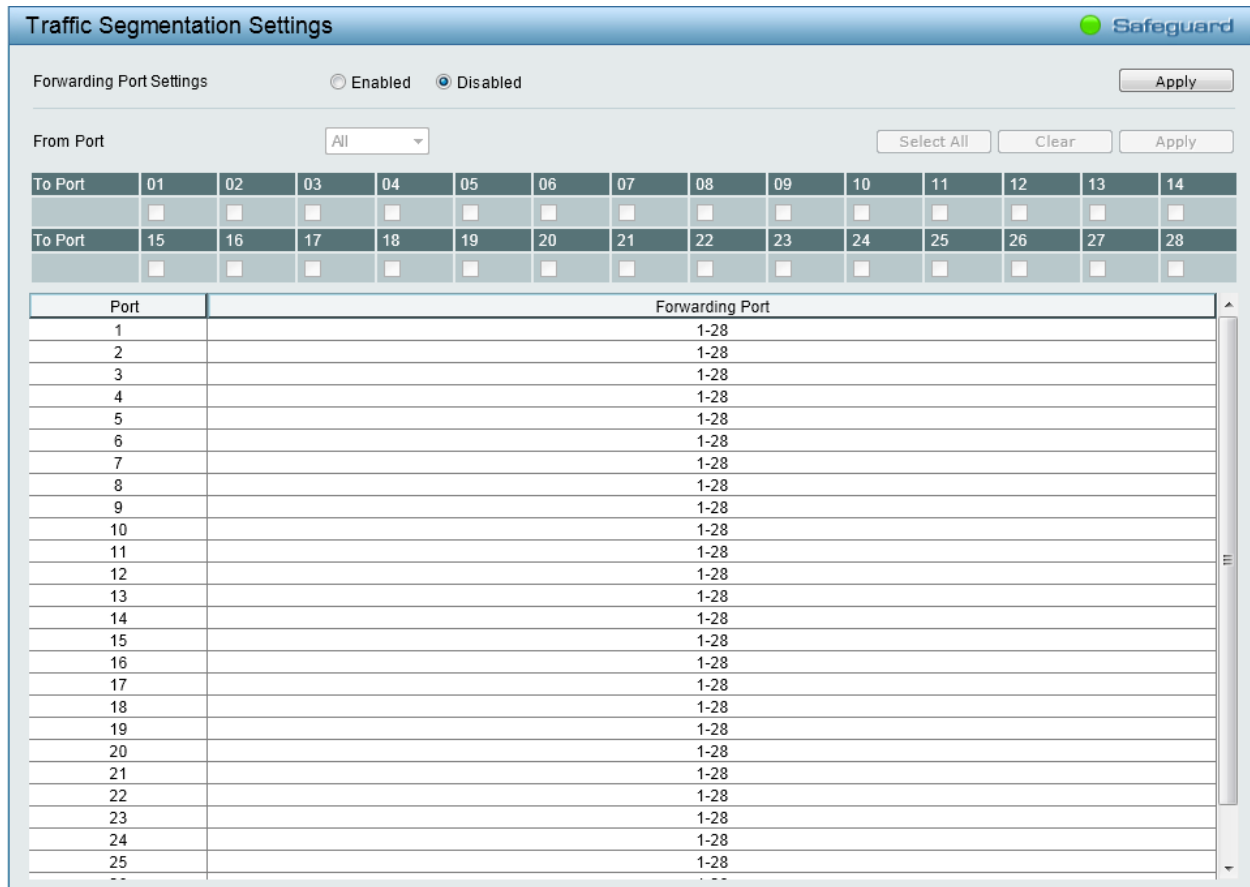
<p align="center">Figure 4.81 – Security > Traffic Segmentation</p>

Forwarding Port Settings: Click to enable or disable the function.

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

Use the **From Port** drop-down menu to specify a port or all ports from the Switch, tick the ports under **To Port**, and click **Apply** to implement the changes made and display the settings at the table below.

Click **Select All** button to check all ports. Click **Clear** 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.
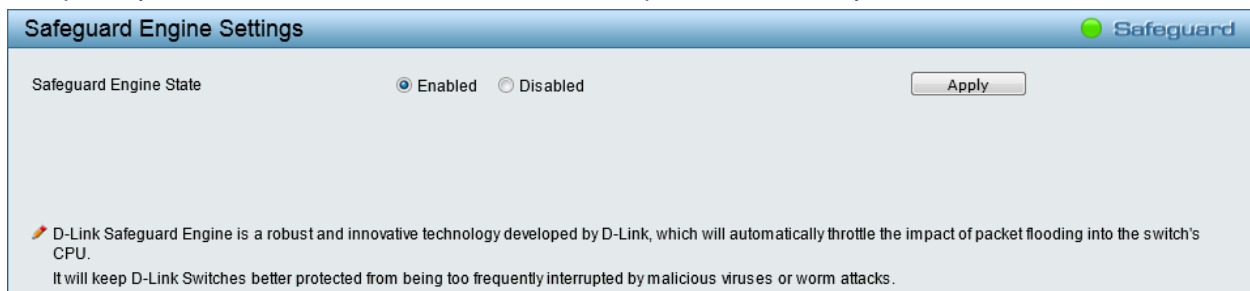
<p align="center">Figure 4.82 – Security > Safeguard Engine</p>

<p align="center">69</p>

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.

Storm Control Settings

Storm Control	○ Enabled ● Disabled
Traffic Control Type	Multicast & Broadcast & Unknown Unicast ▼
	N = (1 ~ 68266)
Threshold (15Kbps * N)	15Kbps * [0] = 0 Kbps
	Apply
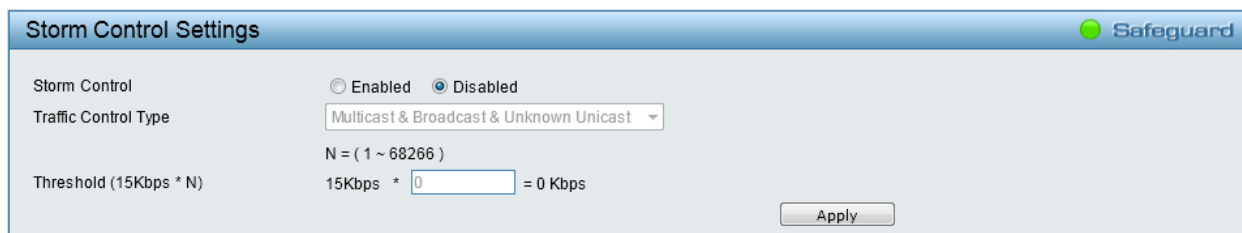
Figure 4.83 – Security > Storm Control

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

Threshold (15Kbps * N): If storm control is enabled (default is disabled), the threshold is from of 15 to 1,024,000 Kbit per second, with steps (N) of 15Kbps. N can be from 1 to 68266.

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.
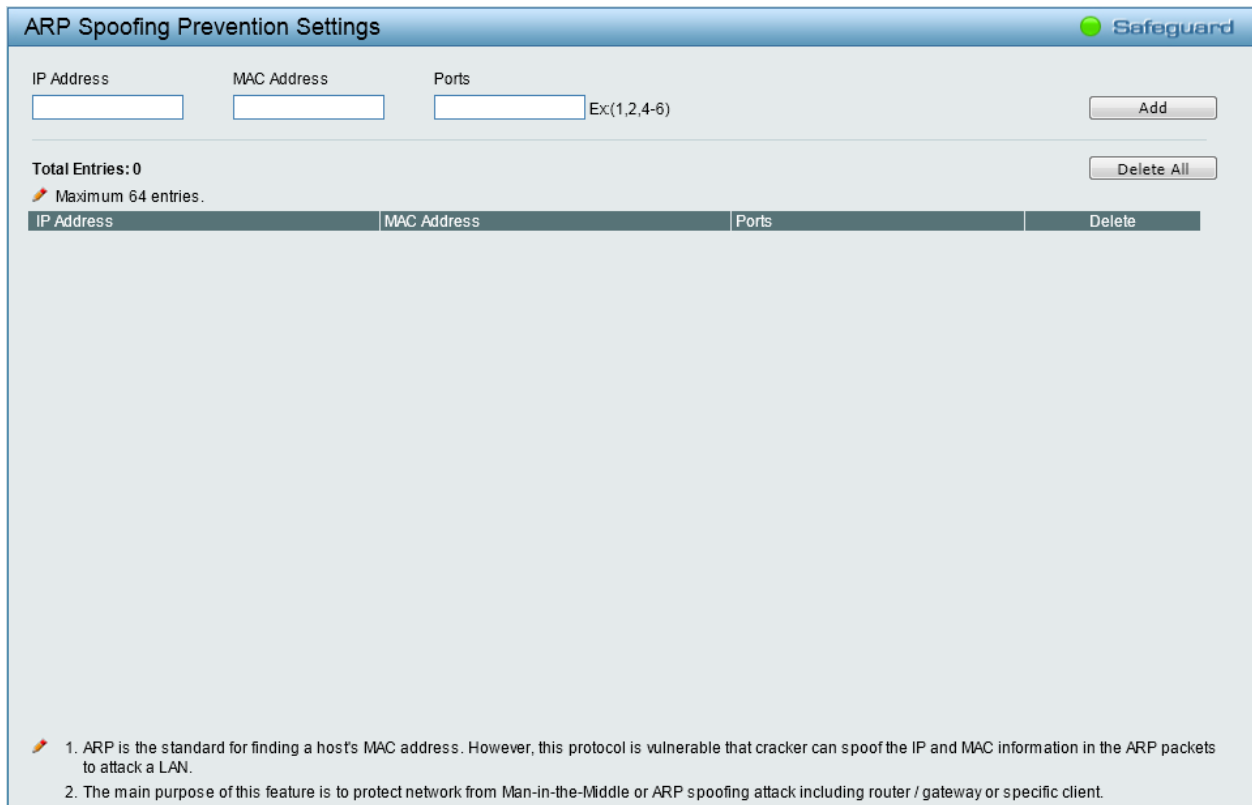
Figure 4.84 – Security > ARP Spoofing Prevention

Enter the **IP Address**, **MAC Address**, **Ports** and then click **Add** to create a checking/filtering rule. Click **Delete** to remove the corresponding rule. Click **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 window is used 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.
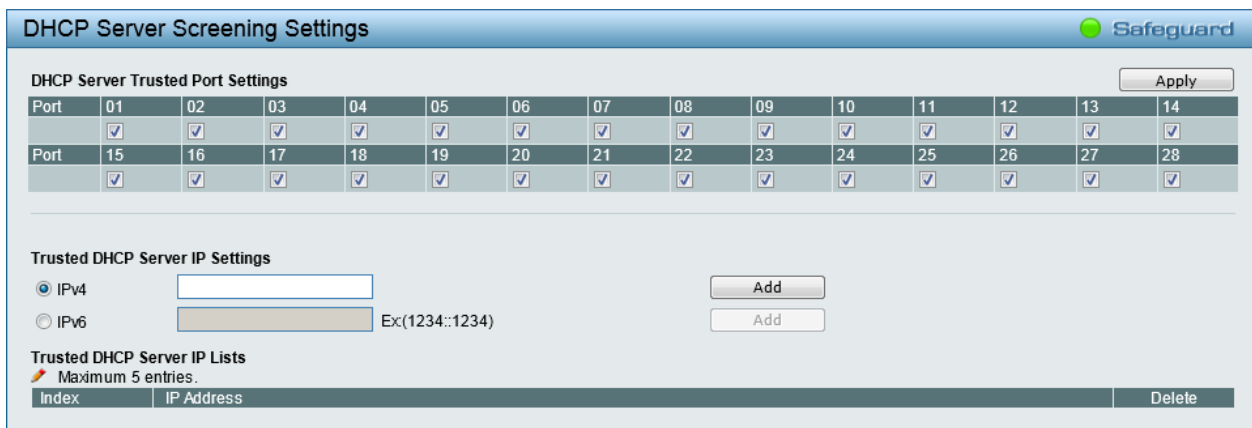
Figure 4.85 – Security > DHCP Server Screening

Trusted DHCP Server IP Settings: Click **IPv4** or **IPv6** and enter the IPv4 or IPv6 address of the DHCP server.
Click **Add** to add a trusted DHCP server.

Security > SSL

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**.
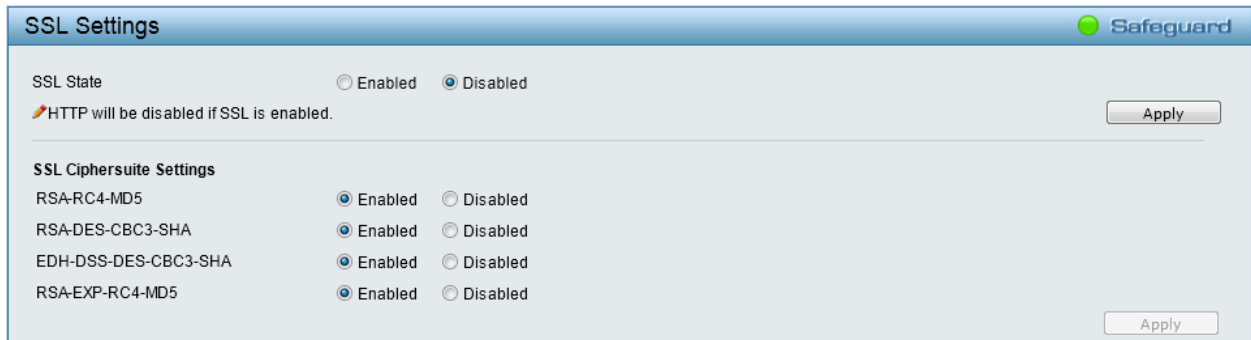
Figure 4.86 – Security > SSL Settings

> **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 > 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.
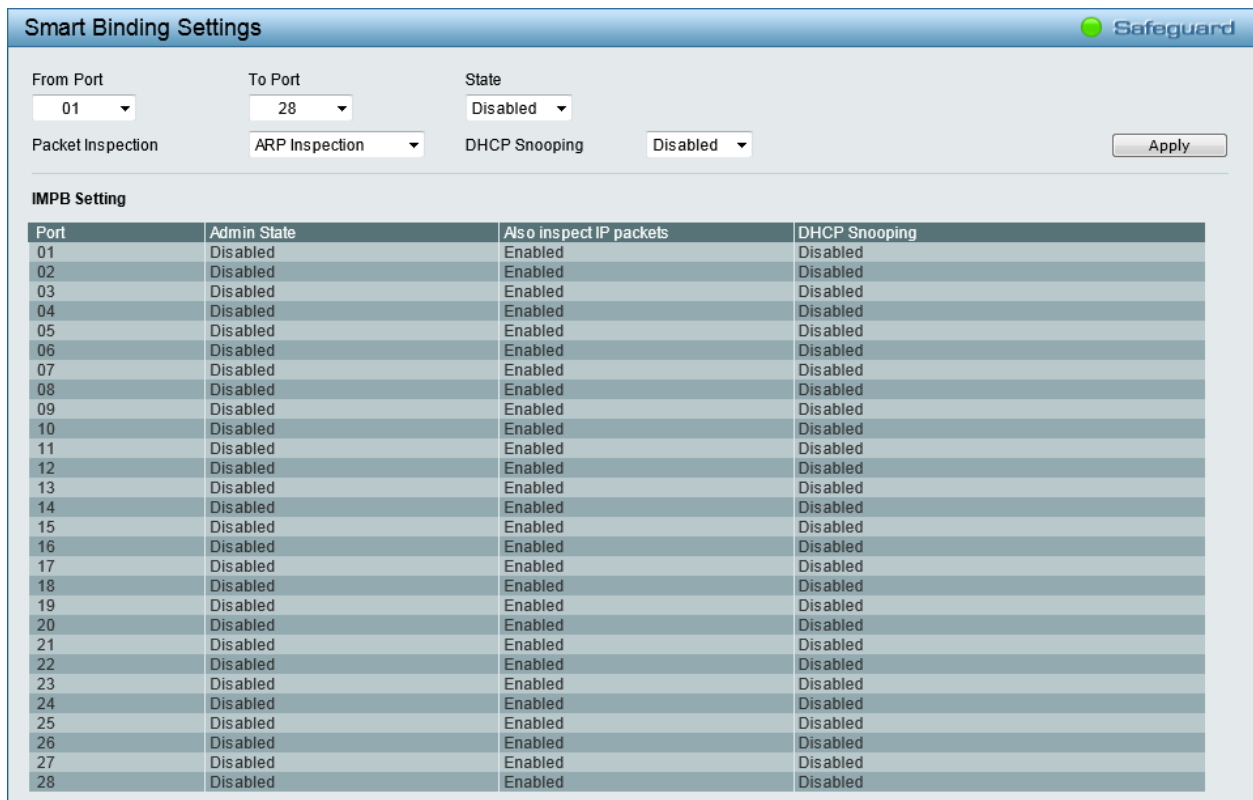
Figure 4.87 – Security > Smart Binding > Smart Binding Settings

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.

> **Enable:** Select this option to enable the smart binding feature with related configurations to the ports.

> **Disable:** Select this option to disable the smart binding feature.

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. 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** for the settings to take effect.

Security > Smart Binding > Smart Binding

The Smart Binding page allows users to set IP-MAC-Port Binding entries by manually entering the required information or by scanning all connected devices and then binding them to the respective MAC addresses.
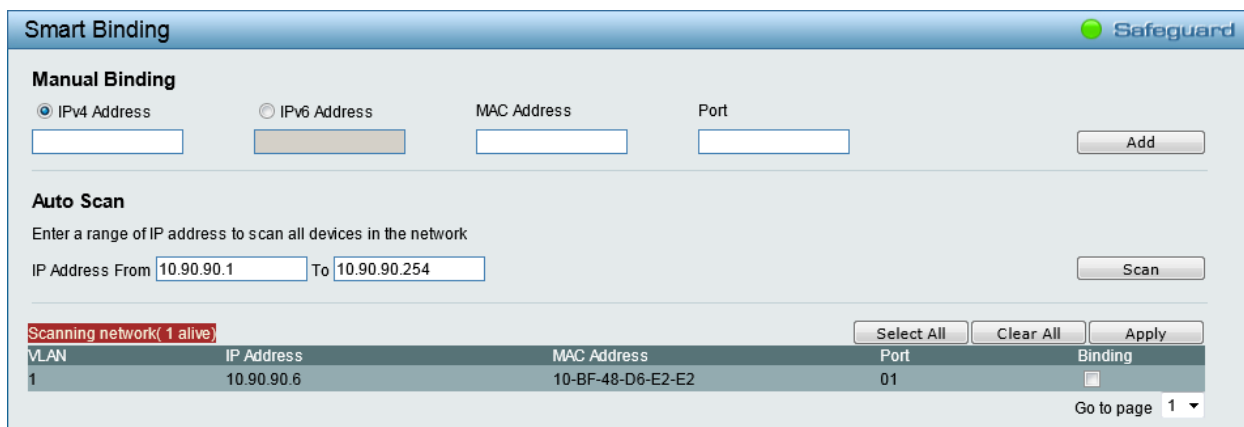
Figure 4.88 – Security > Smart Binding > Smart Binding

Manual Binding:

IPv4 Address: Specifies the IPv4 address to bind to the MAC address set below.

IPv6 Address: Specifies the IPv6 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: This setting will list connected devices that can easily be selected to bind.

IP Address From/To: Specifies the range of IP address that will be scanned.

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

Binding: Tick this option to bind the IP address of the entry to the MAC address.

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

Click **Select All** to select all the entries found.

Click **Clear All** to unselect all the entries found.

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.
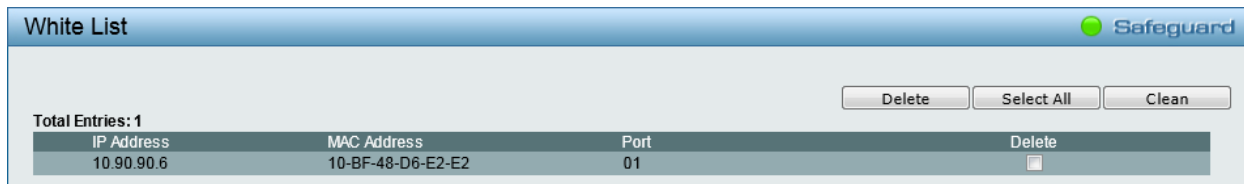
Figure 4.89 – Security > Smart Binding > White List

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.
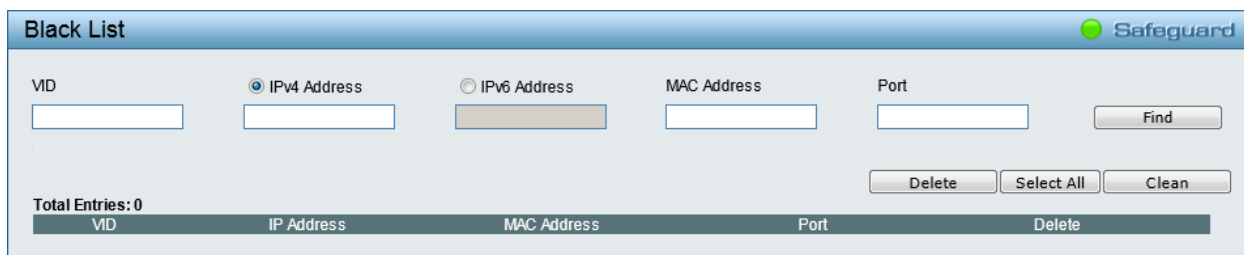
Figure 4.90 – Security > Smart Binding > Black List

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.

IPv4 Address: Enter the IPv4 address of the device.

IPv6 Address: Enter the IPv6 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 the 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 > 802.1X > 802.1X Settings

Network switches provide easy and open access to resources, by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

You can configure the RADIUS configuration in the **AAA > 802.1X > RADIUS > RADIUS Server Settings** window.
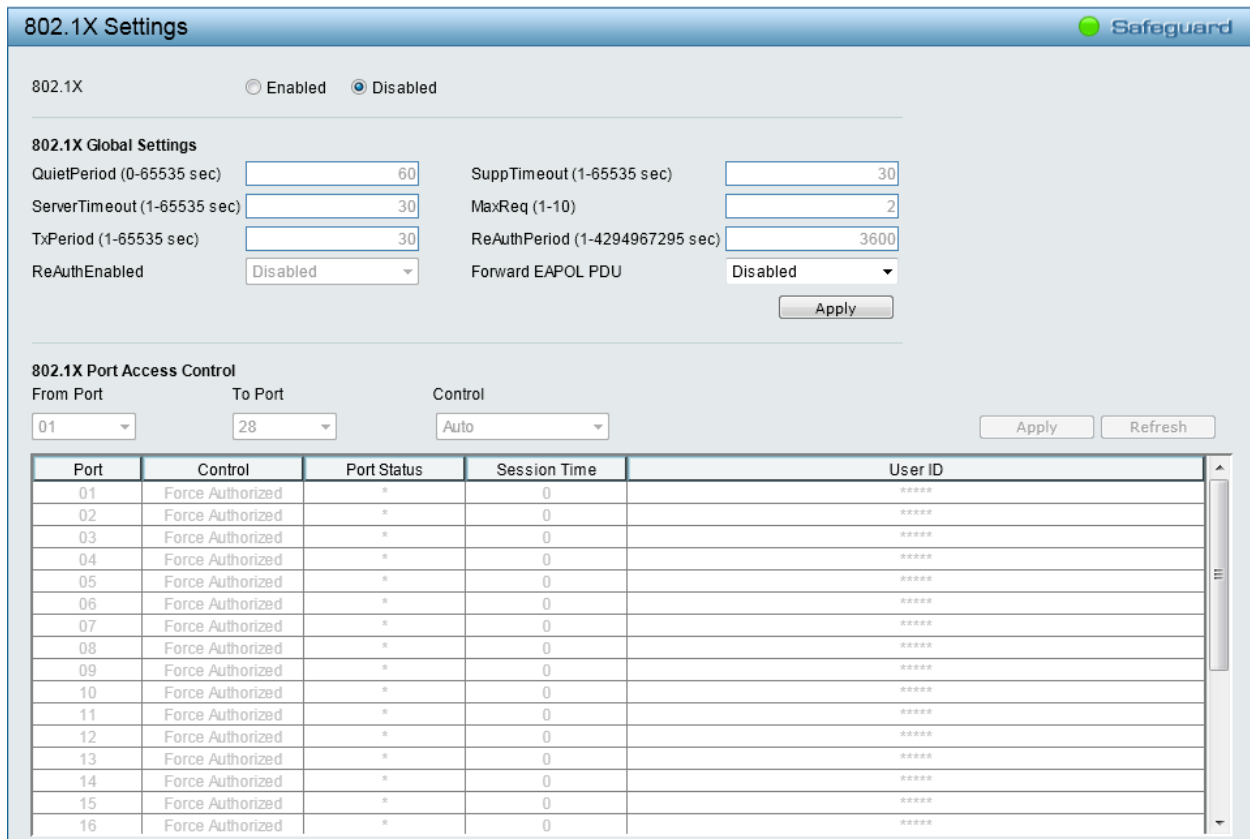
Figure 4.91 – AAA > 802.1X > 802.1X Settings

802.1X: By default, 802.1X is disabled. To use EAP for security, click **Enabled** and set the 802.1X Global Settings. To establish 802.1X port-specific assignments, click **Enabled** and configure 802.1X Port Access Control.

802.1X Global Settings:

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.

ReAuthEnabled: This function is to determine whether regular re-authentication will take place on this port(s). When the 802.1X function is enabled, the switch sends an EAP-request/identity packet to client. The ReAuthEnabled function is disabled by default.

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 – 4294967295 sec): This command affects the behavior of the switch only if periodic re-authentication is enabled. Default is *3600.*

Forward EAPOL PDU: This is a global setting to control the forwarding of EAPOL PDU. The default state is *Disabled*.

802.1X Port Access Control:

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

Control: Three type of Port Access Control State can be **Force Authorized**, **Auto** and **Force UnAuthorized**.

> **Force Authorized** - Select 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. This is the default setting.

Auto - 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.

Force Unauthorized - If **Force Unauthorized** 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.

AAA > 802.1X > Guest VLAN Settings

On 802.1X security-enabled networks, there is a need for non-802.1X supported devices to gain limited access to the network, due to lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or older operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements 802.1X Guest VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To set an 802.1X guest VLAN, the user must first configure a normal VLAN, which can be enabled here for guest VLAN status. Only one VLAN may be assigned as the 802.1X guest VLAN.
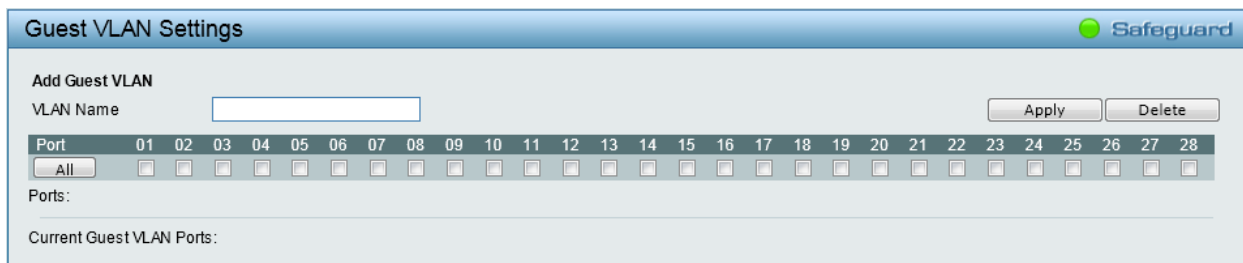
Figure 4.92 – AAA > 802.1X > Guest VLAN Settings

VLAN Name: Enter the pre-configured VLAN name to create as an 802.1X guest VLAN.

Port: Set the ports to be enabled for the 802.1X guest VLAN. Click **All** to select all the ports.

Click **Apply** to implement the changes made. Click **Delete** to remove the specific entry based on the information entered.

AAA > 802.1X > RADIUS > RADIUS Server Settings

The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.
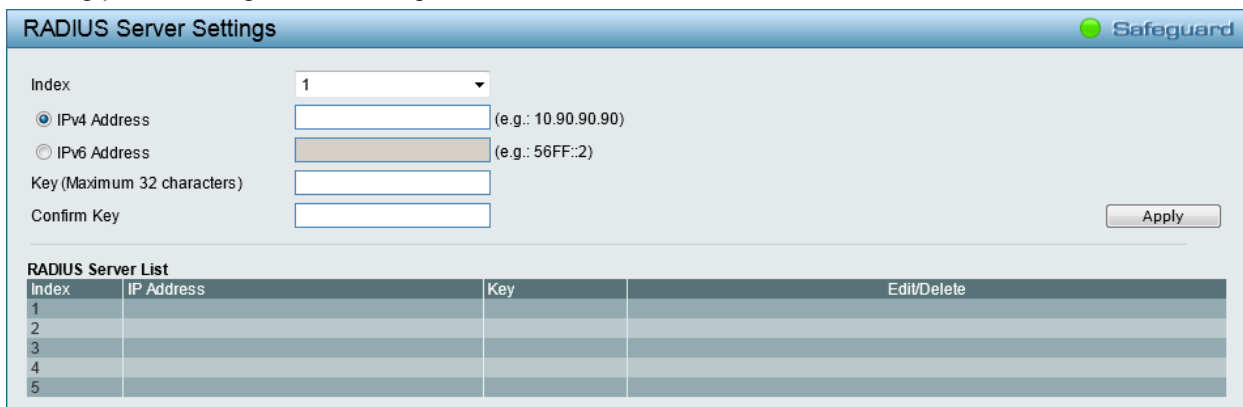
Figure 4.93 – AAA > 802.1X > RADIUS > RADIUS Server Settings

Index: Select the desired RADIUS server to configure.

IPv4 Address: Enter the IPv4 address of the RADIUS Server.

IPv6 Address: Enter the IPv6 address of the RADIUS Server.

Key: Enter the key which is the same as that of the RADIUS server.

Confirm Key: Re-type the key which is the same as that of the RADIUS server.

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

ACL > ACL Wizard

Access Control List (ACL) allows you to establish criterion to determine whether or not the Switch will forward packets based on the information contained in each packet's header. This criterion 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 profiles are 50 and with 200 Rules in total for the Switch.
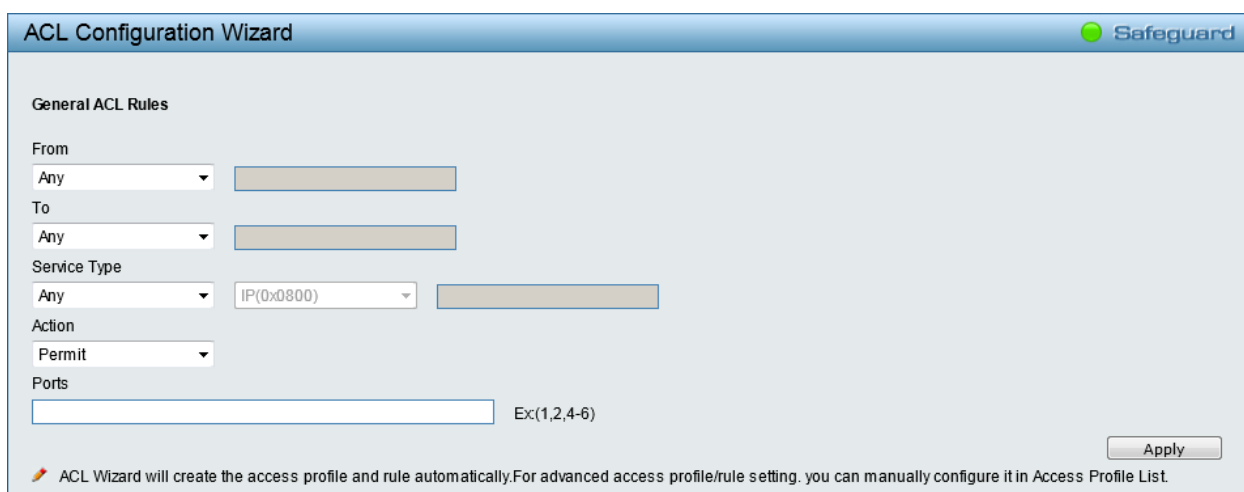
Figure 4.94 – ACL > ACL Wizard

From / To: The rule can be created to apply to different categories:

> **Any –** Select this to include any starting category to this rule.
>
> **MAC Addresses –** Select this to enter the source and destination of MAC addresses for this rule.
>
> **IPv4 Addresses –** Select this to enter the source and destination of IPv4 addresses for this rule.
>
> **IPv6 Addresses –** Select this to enter the source and destination of IPv6 addresses for this rule.

Service Type: Specify the Type of Service to match. The possible values are:

> **Any –** Indicates any service type of packets are examined.
>
> **Ether type –** Select Ethernet type and IP, ARP or User Define value for filtering packets.
>
> **LLC –** Select the IEEE 802.2 Logic Link Control Layer (LLC) header, including SSAP, DSAP and Control fields, for filtering packets.
>
> **ICMP All –** Indicates all ICMP packets are examined.
>
> **IGMP –** IGMP packets can be filtered by IGMP message type.
>
> **TCP All –** Indicates all TCP packets are examined.
>
> **TCP Source Port –**- Specify packets from the TCP source port.
>
> **TCP Destination Port –** Matches the packet to the TCP Destination Port.
>
> **UDP All –** Indicates all UDP packets are examined.
>
> **UDP Source Port –** Specify packets from the UDP source port.
>
> **UDP Destination Port –** Matches the packet to the UDP Destination Port.

Action: Specify the forwarding action for packets matching the ACL rule.

> **Permit –** Specifies that the packets that match the access profile are forwarded by the Switch.
>
> **Deny –** Specifies to drop packets if all conditions are met.

Ports: Enter a port number or a port range to be configured.

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

>
> **NOTE:** Once the ACL rules conflict, rules with the smaller rule ID will take higher priority.

>
> **NOTE:** Be careful on ACL configuration. Inappropriate design may lead to management access failure.

ACL > Access Profile List

The ACL Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

<p align="center">**Figure 4.95 – ACL > ACL Profile List**</p>

The contents of Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are 1 to 50, and any profile ID after 50 is reserved for functional ACL.

Type: The owner type of ACL profile; it can be normal ACL or functional ACL.

Profile Summary: Displays the profile summary.

Click **Show** to see the corresponding ACL's profile details. The ACL profile details are displayed below the ACL table. Click **Show Rules** to see the access rules of the corresponding profile. Click **Edit / New Rules** to edit or create an access rule in this profile. To add a new rule, please see **Access Rule List** in the next section. Click **Delete**, in the corresponding rule's line, to remove an access profile. Click **Delete**, at the top of the page, to remove all normal ACL entries.

To manually add a profile, click **Add**:
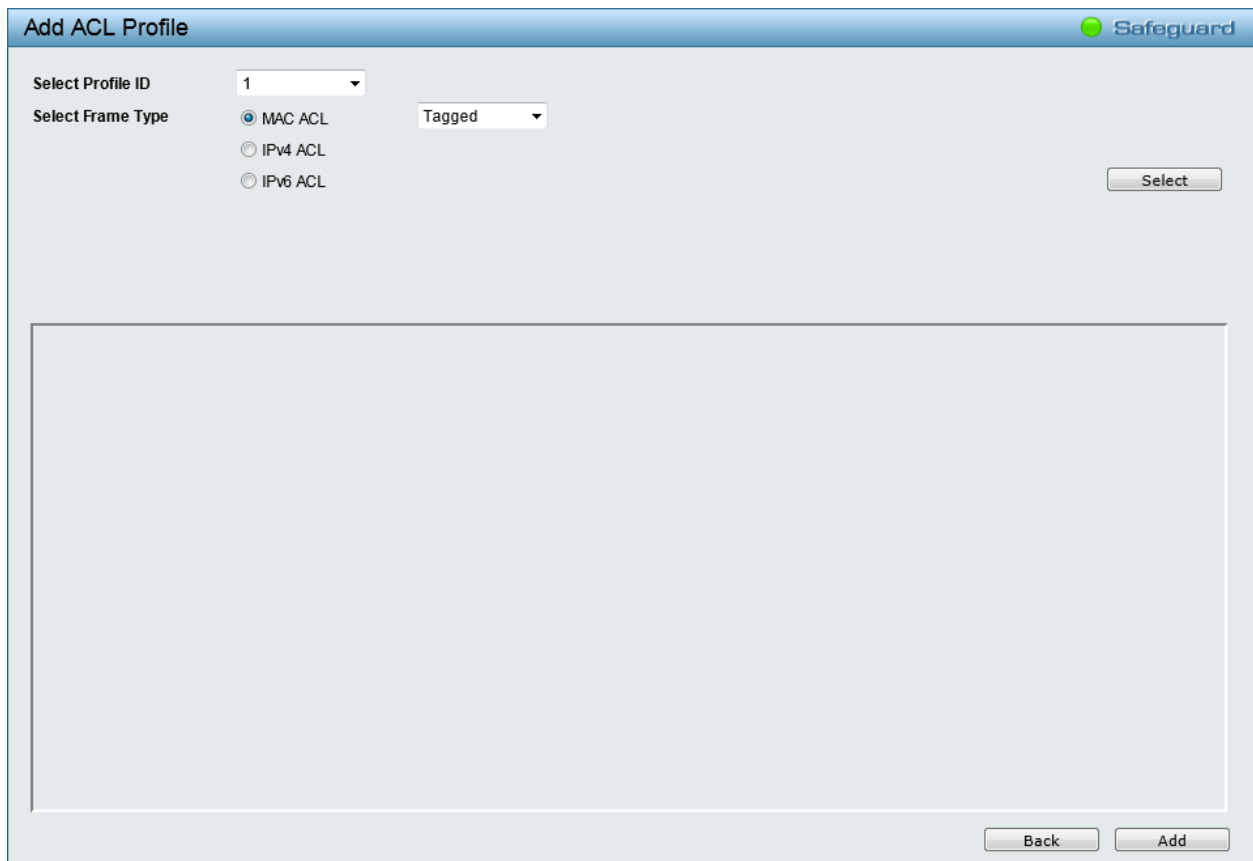
Figure 4.96 – Add Access Profile

The steps of adding an access profile are described below:

1) After selecting the **Select Profile ID** and **Select Frame Type** (**MAC ACL**, **IPv4 ACL**, or **IPv6 ACL**), specify attributes like Untagged/Tagged (for MAC), ICMP/IGMP/TCP/UDP/Protocol-ID (for IPv4), or ICMP/TCP/UDP (for IPv6). Click **Select** and a simplified frame diagram will be displayed.
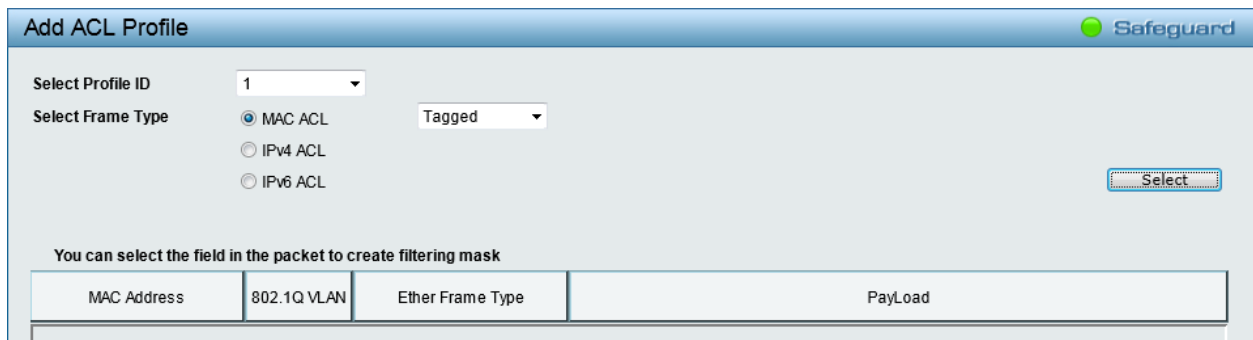
Figure 4.97 – ACL > Access Profile List > Add ACL Profile

The Add ACL Profile window contains the following fields:

Select Profile ID: Select a unique identifier number for this profile set. This value is from 1 to 50.

Select Frame Type: Select frame type based on MAC address, IPv4 address, or IPv6 address. This will change the window according to the requirements for the type of profile.

> **MAC ACL –** Select to instruct the Switch to examine the layer 2 part of each packet header.

>> **Tagged:** Defines the profile Layer 2 to match 802.1Q fields in the Layer 2 header.

>> **Untagged:** Defines the profile Layer 2 to check the Layer 2 header without the 802.1Q fields.

> **IPv4 ACL –** Select to instruct the Switch to examine the IPv4 address in each frame's header.

>> **ICMP:** Specifies ICMP as the Layer 3 protocol that the access profile checks.

>> **IGMP:** Specifies IGMP as the Layer 3 protocol that the access profile checks.

>> **TCP:** Specifies TCP as the Layer 3 protocol that the access profile checks.

>> **UDP:** Specifies UDP as the Layer 3 protocol that the access profile checks.
>> **Protocol ID:** Specifies Protocol ID as the Layer 3 protocol that the access profile checks.
> **IPv6 ACL –** Select to instruct the Switch to examine the IPv6 address in each frame's header.
>> **ICMP:** Specifies ICMP as the Layer 3 protocol that the access profile checks.
>> **TCP:** Specifies TCP as the Layer 3 protocol that the access profile checks.
>> **UDP:** Specifies UDP as the Layer 3 protocol that the access profile checks.

To define the MAC ACL profile, select **MAC ACL** with **Tagged** and click **Select** button. The following window displays:
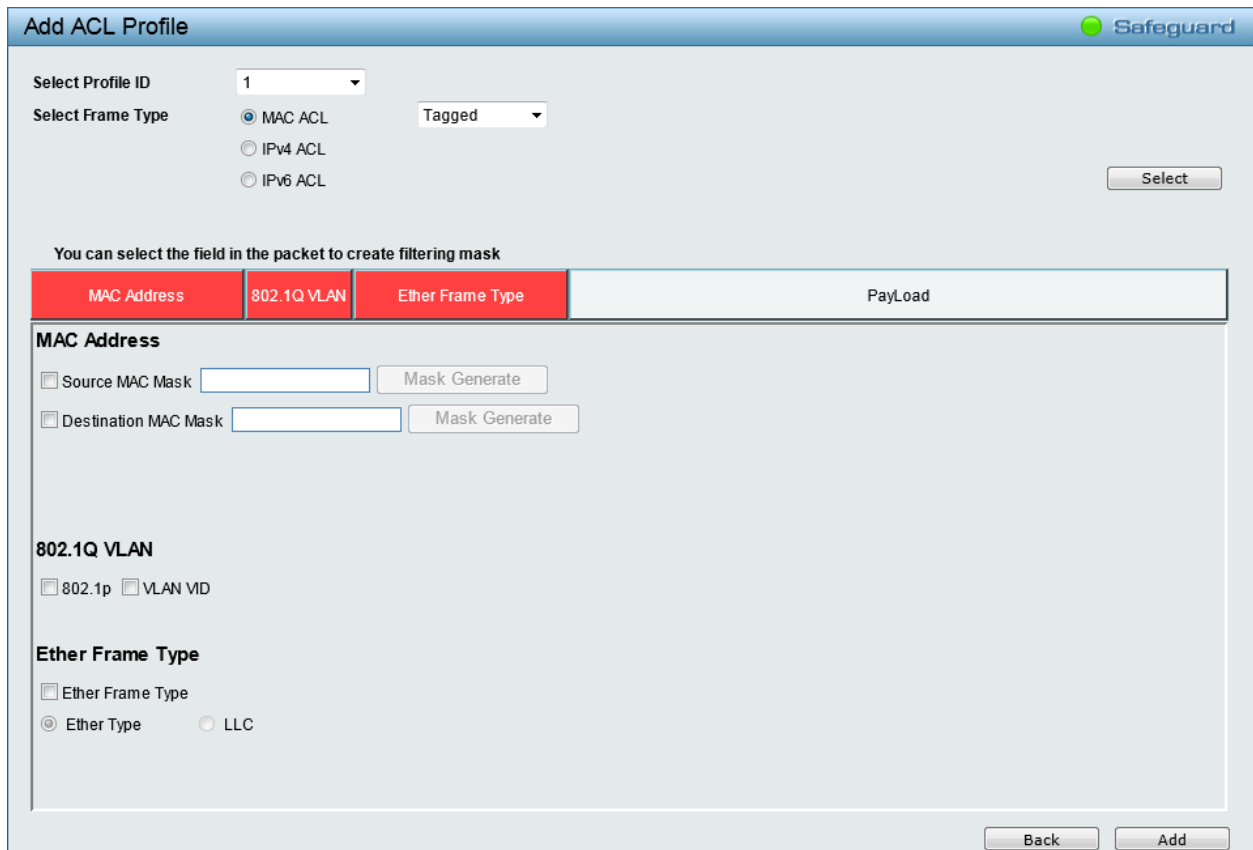
Figure 4.98 – ACL > Access Profile List > Add ACL Profile (MAC ACL)

The Add ACL Profile MAC ACL contains the following fields:

Source MAC Mask: Enter a MAC address mask for the source MAC address, e.g. FF-FF-FF-FF-FF-FF.

Destination MAC Mask: Enter a MAC address mask for the destination MAC address, e.g. FF-FF-FF-FF-FF-FF.

802.1p: Select to examine the 802.1p priority of each packet header and use this as the full or partial criterion for forwarding.

VLAN ID: Select to examine the 802.1Q VLAN of each packet header and use this as the full or partial of the criterion for forwarding.

Ether Type: Select to examine the Ethernet type value in each frame's header.

LLC: Select to examine the SSAP, DSAP or Control value of each frame's header.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv4 ACL ICMP profile, Select **IPv4 ACL** with **ICMP** and click **Select** button. The following window displays:

Figure 4.99 – ACL > Access Profile List > Add ACL Profile (IPv4 ACL ICMP)

The Add ACL Profile IPv4 ACL ICMP address window contains the following fields:

IPv4 TOS: Select this option to include IPv4 type of service parameters in this profile.

> **DSCP –** Select this option to use the DSCP field for IPv4 TOS.

> **TOS –** Select this option to use the type of service (TOS) field for IPv4 TOS.

> **Precedence –** Select this option to use the precedence field for IPv4 TOS.

Source IP Mask: Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination IP Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

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

ICMP Code: Sets the ICMP code field as an essential field to match.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv4 ACL IGMP profile, Select **IPv4 ACL** with **IGMP** and click **Select** button. The following window displays:

Figure 4.100 – ACL > Access Profile List > Add ACL Profile (IPv4 ACL IGMP)

The Add ACL Profile IPv4 ACL IGMP address window contains the following fields:

IPv4 TOS: Select this option to include IPv4 type of service parameters in this profile.

> **DSCP –** Select this option to use the DSCP field for IPv4 TOS.

> **TOS –** Select this option to use the type of service (TOS) field for IPv4 TOS.

> **Precedence –** Select this option to use the precedence field for IPv4 TOS.

Source IP Mask: Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination IP Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Type: Sets the IGMP Type field as an essential field to match.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv4 ACL TCP profile, Select **IPv4 ACL** with **TCP** and click **Select** button. The following window displays:

<p align="center">**Figure 4.101 – ACL > Access Profile List > Add ACL Profile (IPv4 ACL TCP)**</p>

The Add ACL Profile IPv4 ACL TCP port window contains the following fields:

IPv4 TOS: Select this option to include IPv4 type of service parameters in this profile.

    DSCP – Select this option to use the DSCP field for IPv4 TOS.

    TOS – Select this option to use the type of service (TOS) field for IPv4 TOS.

    Precedence – Select this option to use the precedence field for IPv4 TOS.

Source IP Mask: Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination IP Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Source Port Mask: Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv4 ACL UDP profile, Select **IPv4 ACL** with **UDP** and click **Select** button. The following window displays:

Figure 5.92 – ACL > Access Profile List > Add ACL Profile (IPv4 ACL UDP)

The Add ACL Profile IPv4 ACL UDP port window contains the following fields:

IPv4 TOS: Select this option to include IPv4 type of service parameters in this profile.

      DSCP – Select this option to use the DSCP field for IPv4 TOS.

      TOS – Select this option to use the type of service (TOS) field for IPv4 TOS.

      Precedence – Select this option to use the precedence field for IPv4 TOS.

Source IP Mask: Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination IP Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Source Port Mask: Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv4 ACL Protocol ID profile, Select **IPv4 ACL** with **Protocol-ID** and click **Select** button. The following window displays:

Figure 4.102 – ACL > Access Profile List > Add ACL Profile (IPv4 ACL Protocol ID)

The Add ACL Profile IPv4 Protocol ID contains the following fields:

IPv4 TOS: Select this option to include IPv4 type of service parameters in this profile.

> **DSCP –** Select this option to use the DSCP field for IPv4 TOS.

> **TOS –** Select this option to use the type of service (TOS) field for IPv4 TOS.

> **Precedence –** Select this option to use the precedence field for IPv4 TOS.

Source IP Mask: Defines the range of source IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination IP Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv6 ACL ICMP profile, Select **IPv6 ACL** with **ICMP** and click **Select** button. The following window displays:
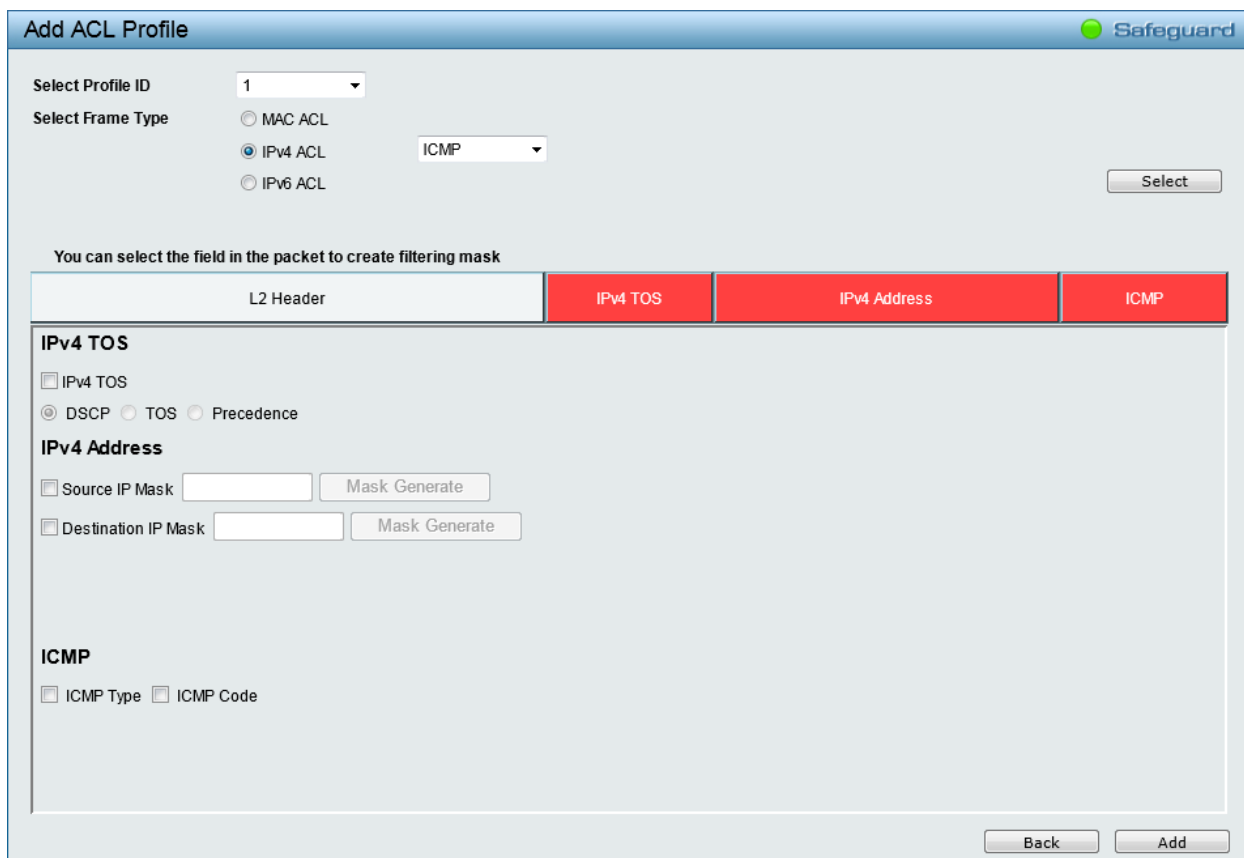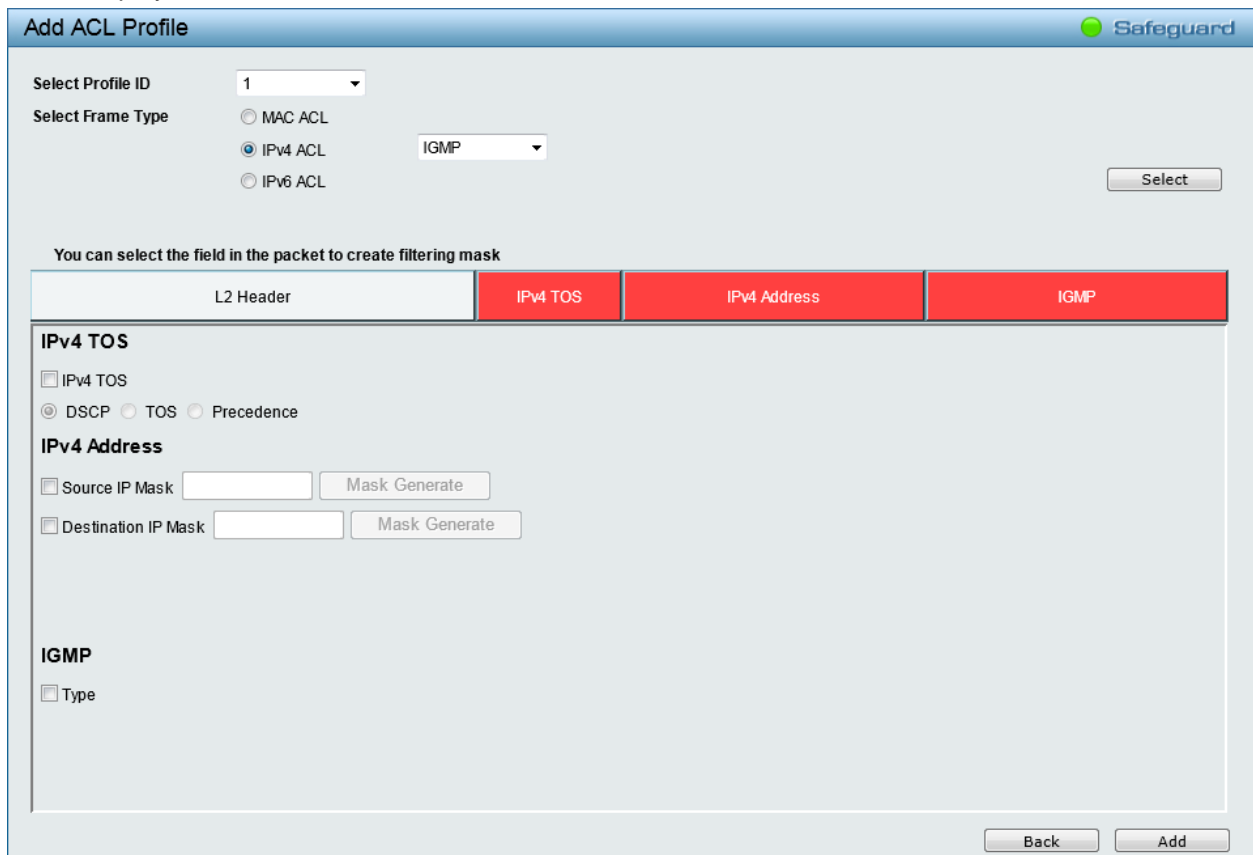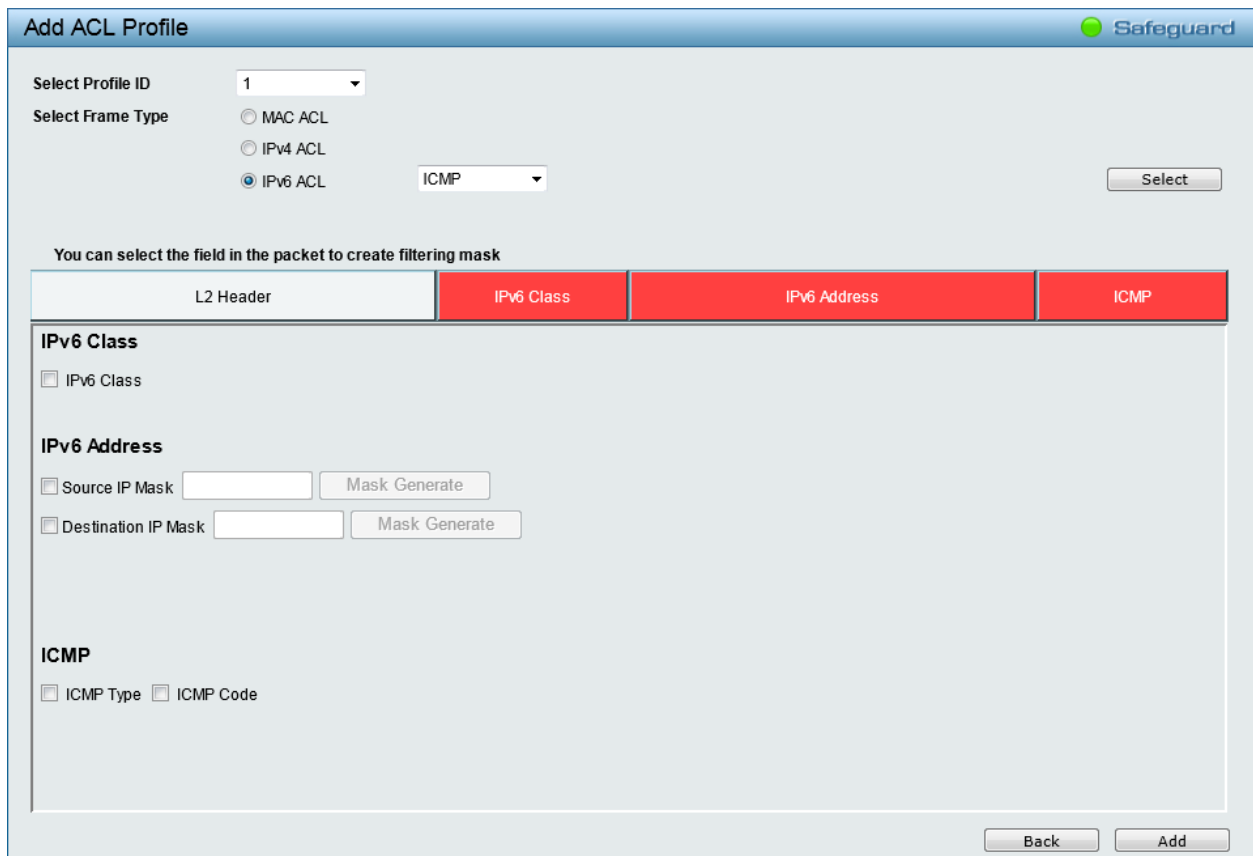
Figure 4.103 – ACL > Access Profile List > Add ACL Profile (IPv6 ACL ICMP)

The Add ACL Profile IPv6 ACL ICMP address window contains the following fields:

IPv6 Class: Tick this option to include the IPv6 class field.

Source IP Mask: Defines the range of source IPv6 addresses, relevant to the ACL rules. (0=ignore, 1=check).

Destination IP Mask: Defines the range of destination IPv6 addresses, relevant to the ACL rules. (0=ignore, 1=check).

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

ICMP Code: Sets the ICMP code field as an essential field to match.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv6 ACL TCP profile, Select **IPv6 ACL** with **TCP** and click **Select** button. The following window displays:

Figure 4.104 – ACL > Access Profile List > Add ACL Profile (IPv6 ACL TCP)

The Add ACL Profile IPv6 ACL TCP port window contains the following fields:

IPv6 Class: Tick this option to include the IPv6 class field.

Source IP Mask: Defines the range of source IPv6 addresses, relevant to the ACL rules. (0=ignore, 1=check).

Destination IP Mask: Defines the range of destination IPv6 addresses, relevant to the ACL rules. (0=ignore, 1=check).

Source Port Mask: Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

To define the IPv6 ACL UDP profile, Select **IPv6 ACL** with **UDP** and click **Select** button. The following window displays:
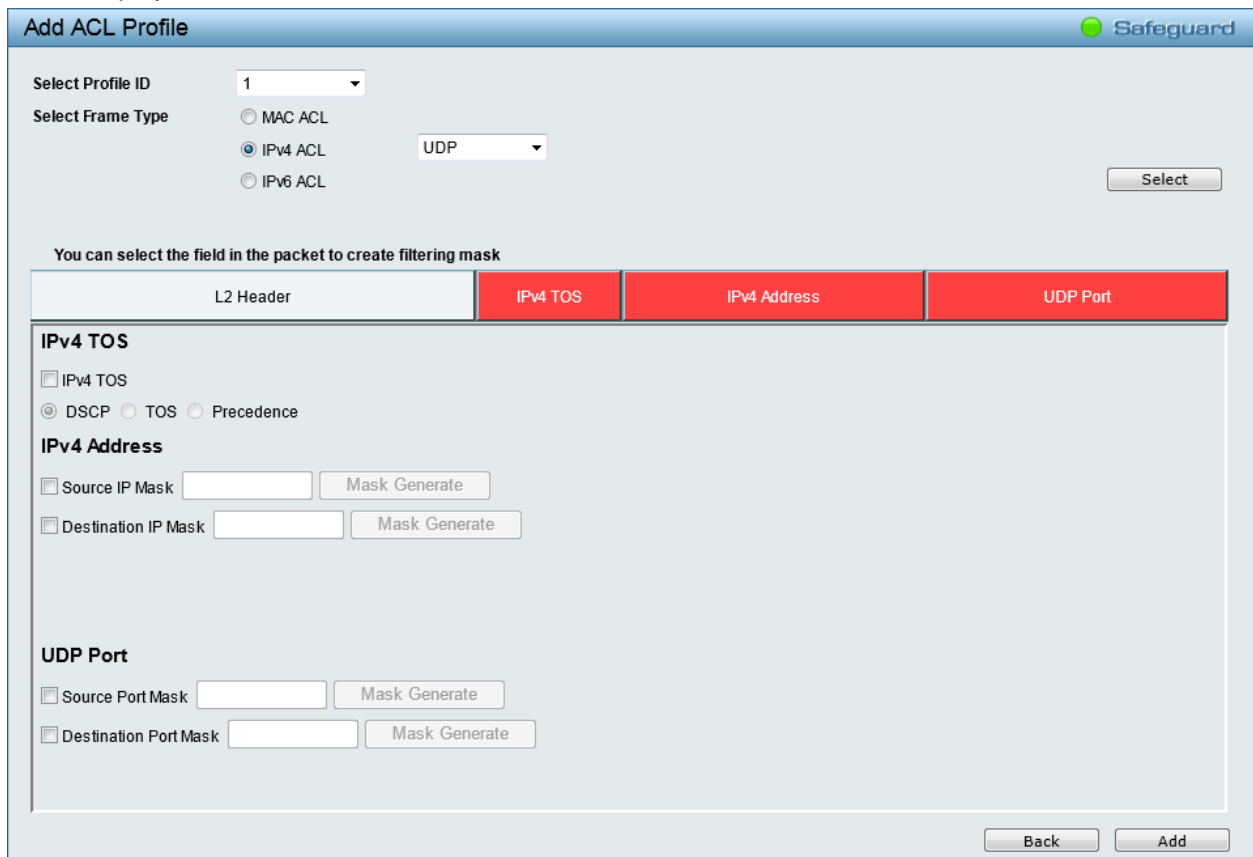
The Add ACL Profile IPv4 ACL UDP port window contains the following fields:

IPv6 Class: Tick this option to include the IPv6 class field.

Source IP Mask: Defines the range of source IPv6 addresses, relevant to the ACL rules. (0=ignore, 1=check).

Destination IP Mask: Defines the range of destination IPv6 addresses, relevant to the ACL rules. (0=ignore, 1=check).

Source Port Mask: Defines the range of source Ports relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. (0=ignore, 1=check). For example, to set 0 – 15, set mask of FFF0.

Click **Add** button to add the ACL profile. Click **Back** to go back to the previous window.

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

2) Selecting the field of interest will display the related columns in the lower part of the page. Enter the filtering mask and click **Apply** when done. A filtering mask is to specify the digit that you want to check. For example, if you want to check a network of 192.168.1.0/24, then you should enter the IP mask as 255.255.255.0.
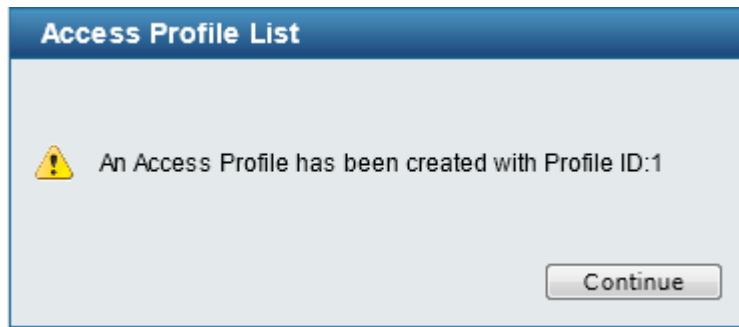
Figure 4.105 – Confirmation of Creating Access Profile List

> **NOTE:** You cannot select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, click **Continue** to go back to the main Access Profile List window. Click the **Edit / New Rules** button to enter the **Access Rule List** window.
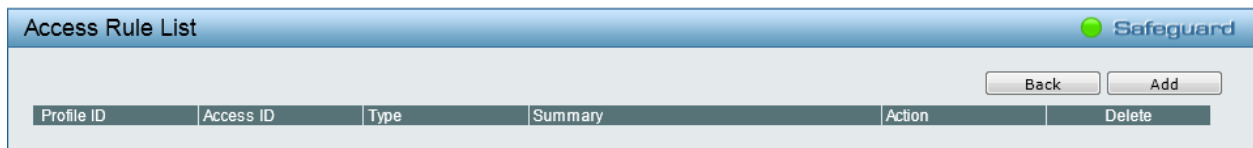
Figure 5.97 – ACL > Access Profile List > Access Rule List

Profile ID: Indicates the corresponding access profile Identification number.

Access ID: Indicates the access rule Identification number.

Type: Displays the profile type.

Summary: Displays the access rule summary.

Action: Displays the access rule action.

Click Add to create a new rule. Click **Back** to go back to the previous page. Click **Delete** to remove the corresponding entry.

Click **Add** to see the following window.
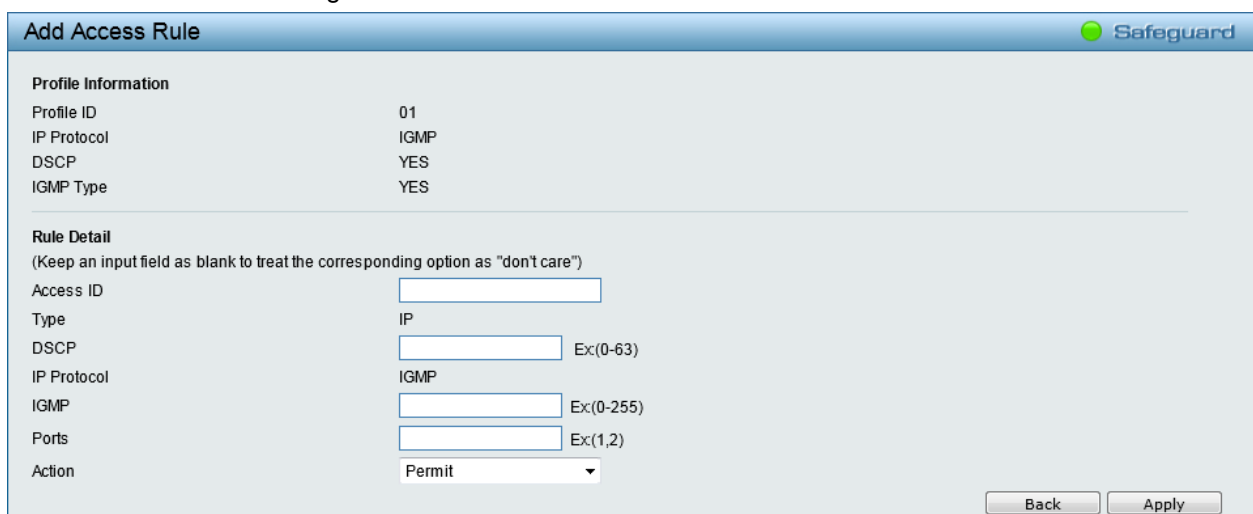
Figure 4.106 – ACL > Access Profile List > Add Access Rule

Profile Information: Displays the information about this rule.

Rule Detail: Specifies the detail of the rule.

    Access ID – Specifies the Access ID (1-65535).

Type – Displays the type of rule. MAC, or IP.

VLAN ID – Specifies the VLAN ID.

Destination MAC Address - Enter a destination MAC address.

Source MAC Address - Enter a source MAC address.

Destination IP Address - Enter a destination IP address.

Source IP Address - Enter a source IP address.

802.1p – Specifies the 802.1p value.

DSAP – Specifies the DSAP field in LLC header.

SSAP – Specifies the SSAP field in LLC header.

Control – Specifies the Control field in LLC header.

DSCP – Specifies the DSCP value for this rule. This value must be between 0 and 63.

TOS – Specifies the TOS value for this rule. This value must be between 0 and 15.

Precedence - Specifies the precedence value for this rule. This value must be between 0 and 7.

IP Protocol – Displays the IP protocol of access rule.

IGMP – Specifies the IGMP value for this rule. This value must be between 0 and 255.

Type – Specifies the type. The possible value is from 0 to 255.

Code – Specifies the code of access rule. The field range is from 0 to 255.

Source Port – Specifies the source port number of the access rule. This value must be between 0 and 65535.

Destination Port – Specifies the destination port number of the access rule. This value must be between 0 and 65535.

Protocol ID – Specifies the protocol ID between 0 and 255.

Ports – Specifies the switch ports that you want to implement the access rule to.

Action – Specifies 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 **Apply** to make it effective.

> **NOTE:** The switch begins the access rule with the smallest access ID, so be careful in assigning the ID for the expected results.

To modify an existing rule, please click on the Access ID hyperlink.

Figure 4.107 – ACL > Access Profile List > Access Rule List

ACL > ACL Finder

This page is used to help find a previously configured ACL entry. To search for an entry, enter the profile ID from the drop-down menu, select a port that you wish to view, define the state and click **Search**. The table on the lower half of the screen will display the entries. To delete an entry, click the corresponding **Delete** button.

Figure 4.108 – ACL > ACL Finder

PoE > PoE Global Settings (DGS-1210-08P/24P only)

This page will display the PoE status including System Budget Power, Support Total Power, Remainder Power, and The ratio of system power supply.
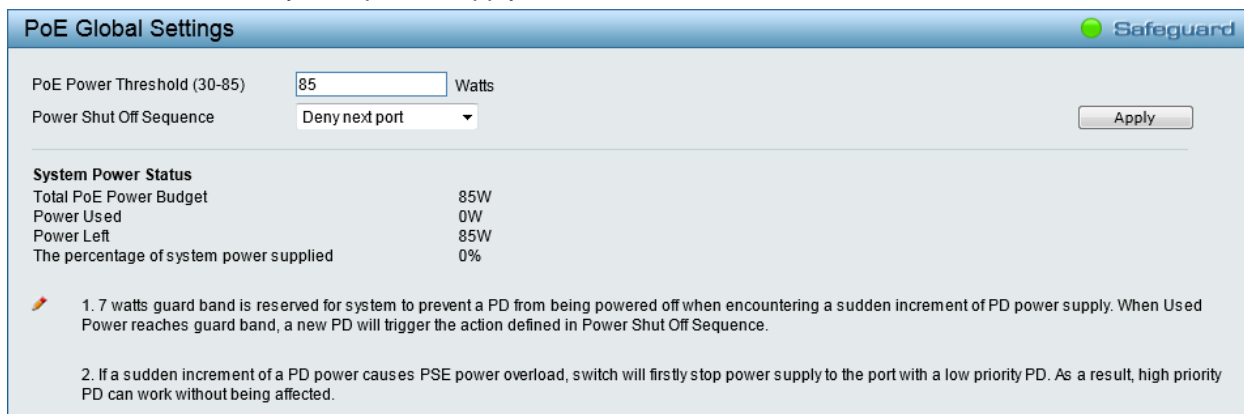
Figure 4.109 – PoE > PoE Global Settings

PoE Power Threshold: Manually configure the system's power budget.

Power Shut Off Sequence: Defines the method used to deny power to a port once the threshold is reached. The possible fields are:

   Deny next port: When the power budget is exceeded, the next port attempting to power up is denied, regardless of the port priority.

   Deny low priority port: The port with the lower priority will be shut down to allow the higher priority port to power up.

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

System Power Status: Displays the system power status of device.

   Total PoE Power Budget: Displays the total PoE power budget of this switch.

   Power Used: Displays the current used power of the switch.

   Power Left: Displays the spare power of the switch.

   The percentage of system power supplied: Displays the percentage of power supplied by the PoE.

PoE > PoE Port Settings (DGS-1210-08P/24P only)

The DGS-1210-24P supplies power to PD devices up to 30 Watt for ports 1 to 12, meeting IEEE 802.3af and 802.3at standards. The DGS-1210-08P supplies power to PD devices up to 15.4 Watt for ports 1 to 8.

The DGS-1210-24P works with all D-Link 802.3af or 802.3at capable devices. The DGS-1210-08P works with all D-Link 802.3af devices.

IEEE 802.3at defined that the PSE provides power according to the following classification:

Class	Usage	Output power limit by PSE
0	Default	15.4W
1	Optional	4.0W
2	Optional	7.0W
3	Optional	15.4W
4	Reserved	30W

The PoE port table will display the PoE status including, Port Enable, Power Limit, Power (W), Voltage (V), Current (mA), Classification, Port Status. You can select **From Port** / **To Port** to control the PoE functions of

a port. DGS-1210-08P/24P will auto disable the ports if port current is over 375mA in 802.3af mode or 625mA in pre-802.3at mode.

Note: The PoE Status information of Power current, Power Voltage, and Current is the power usage information of the connected PD; please "Refresh" to renew the information.

Figure 4.110 – PoE > PoE Port Setting

From Port/To Port: Specifies the PoE function of a port or ports.

State: Select "Enabled" or "Disabled" to configure PoE function for designated port(s). Default is **Enabled**.

Time Range: Select the PoE time profile configured from Time Range Settings to enable the time-based PoE function on designated port(s). Default setting is **N/A**.

Priority: Configure the power supply priority as "Low", "Normal", or "High" on designated port(s). Default is **Normal**.

Power Limit: This function allows you to manually set the port power current limitation to be given to the PD. To protect the DGS-1210-08P/24P and the connected devices, the power limit function will disable the PoE function of the port when the power is overloaded. Select from "**Class 1**", "**Class 2**", "**Class 3**", "**Class 4**" (DGS-1210-24P only) and "**Auto**" for the power limit. "**Auto**" will negotiate and follow the classification from the PD power current based on the 802.3at standard.

User Define: Check the box and input the power budget (from 1 to 30W for the DGS-1210-24P or 1 to 15.4W for the DGS-1210-08P) to manually assign an upper limit of port power budget on designated port(s).

Click **Apply** to make the configurations take effects or click **Refresh** to redisplay the table.

Note: For the PoE Port Settings table, if the classification was shown as "Legacy PD", it will be classified to non-AF PD or Legacy PD.

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 **Enabled** and click **Apply** to enable the SNMP function.

Figure 4.111 – 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.

Port Link Up / Link Down: Port connection information.

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

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

Loopback occurring and recovery: The port status of Loopback Detection.

PoE Power On / Off: The PSE port is delivering power to the PD or not.

PoE Power Error: PoE power status error.

PoE over max power budget: PoE power over budget.

SNMP > SNMP > SNMP User

This window 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.
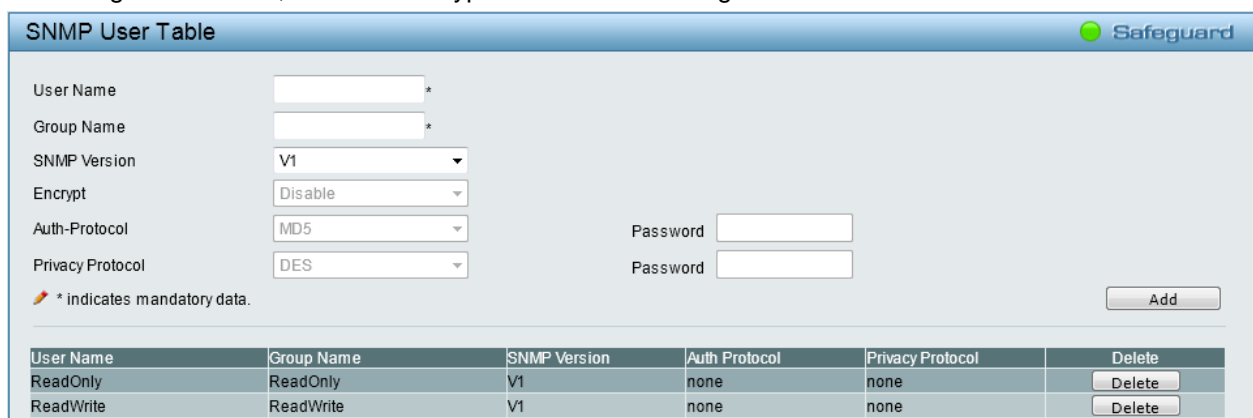
Figure 4.112 – SNMP > SNMP > SNMP User Table

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 **MD5** or **SHA** to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column.

Privacy Protocol/Password: Specify either **none** or **DES** and then enter a password for SNMPv3 encryption in the right column.

Click **Add** to create a new SNMP user account. Click **Delete** to remove the corresponding entry.

SNMP > SNMP > SNMP Group

This window 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.

SNMP Group Table

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Delete
public	ReadWrit...	---	ReadWrit...	v1	NoAuthNoPriv	Delete
public	ReadWrit...	---	ReadWrit...	v2c	NoAuthNoPriv	Delete
private	ReadWrit...	ReadWrit...	ReadWrit...	v1	NoAuthNoPriv	Delete
private	ReadWrit...	ReadWrit...	ReadWrit...	v2c	NoAuthNoPriv	Delete
ReadOnly	ReadWrit...	---	ReadWrit...	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrit...	---	ReadWrit...	v2c	NoAuthNoPriv	Delete
ReadWrit...	ReadWrit...	ReadWrit...	ReadWrit...	v1	NoAuthNoPriv	Delete
ReadWrit...	ReadWrit...	ReadWrit...	ReadWrit...	v2c	NoAuthNoPriv	Delete

Figure 4.113 – SNMP > SNMP > SNMP Group

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

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

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

Security Model: Select the SNMP security model.

> **v1 –** SNMPv1 does not support the security features.

> **v2c –** SNMPv2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.

> **v3 –** 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 view name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.

Click **Add** to create a new SNMP group name. Click **Delete** to remove the corresponding entry.

SNMP > SNMP > SNMP View

This window allows you to maintain SNMP views to community strings or user name that define which MIB objects can be accessed by a remote SNMP manager.

Figure 4.114 – 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 SNMP view name. Click **Delete** to remove the corresponding entry.

SNMP > SNMP > SNMP Community

This window 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.

Figure 4.115 –SNMP > SNMP > SNMP Community
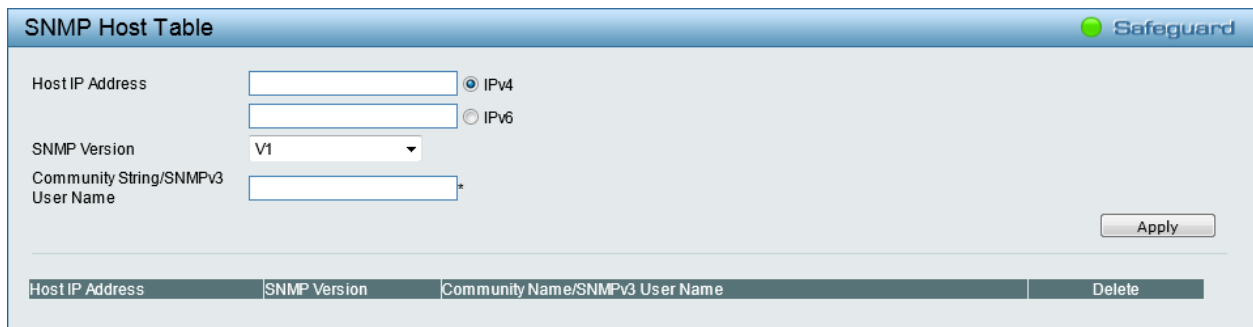
Community Name: Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.

User Name (View Policy): Specifies that the SNMP community string will be created with privileges that can either be **ReadOnly** or **ReadWrite**. Alternatively, an existed user name can be selected that will be used together with the community string. The privileges will depend on the SNMP user that was created.

Click **Add** to create a new SNMP community. Click **Delete** to remove the corresponding entry.

SNMP > SNMP > SNMP Host

This SNMP Host window is used to configure the SNMP trap recipients.

Figure 4.116 – SNMP > SNMP > SNMP Host

Host IP Address: Specifies the IPv4 or IPv6 address of the SNMP management host.

SNMP Version: Select the SNMP version to be used to the management host.
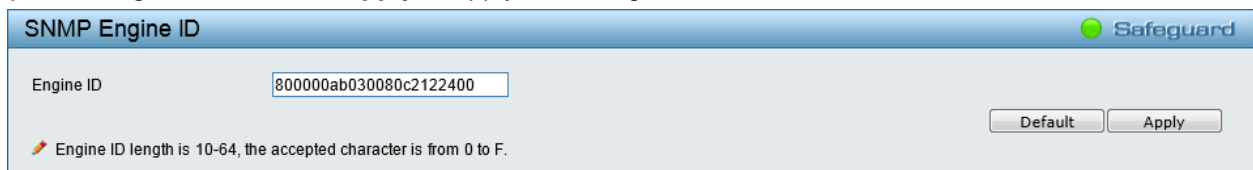
Community String/SNMPv3 User Name: Specifies the community string or SNMPv3 user name for the management host.

Click **Add** to create a new SNMP host. Click **Delete** to remove the corresponding entry.

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.
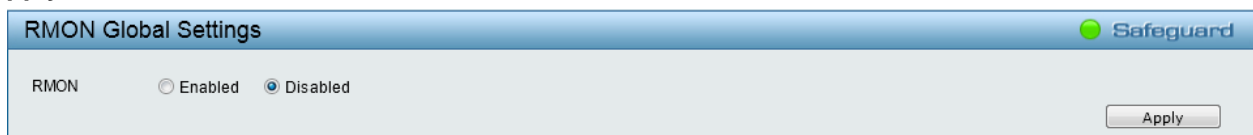
Figure 4.117 – SNMP > SNMP > SNMP Engine ID

SNMP > RMON > RMON Global Settings

Users can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch. Click **Apply** to make effects.

Figure 4.118 – SNMP > RMON > RMON Global Settings

SNMP > RMON > RMON Statistics

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

Figure 4.119 – 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 create a new entry. Click **Refresh** to renew the table information. Click **Delete** to remove the corresponding entry.

SNMP > RMON > RMON History

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

Figure 4.120 – 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*.

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

Click **Add** to create a new entry. Click **Delete** to remove the corresponding entry.

SNMP > RMON > RMON Alarm

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

Figure 4.121 – SNMP > RMON > RMON Alarm Settings

The configuration contains the following fields:

Index (1 ~ 65535): Indicates the RMON alarm entry number.

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 create a new entry. Click **Delete** to remove the corresponding entry.

SNMP > RMON > RMON Event

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

Figure 4.122 – SNMP > RMON > RMON Event Settings

The RMON Events Page contains the following fields:

Index (1~ 65535): Indicates the RMON event entry number.

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: When **SNMP Trap** or **Log and Trap** is selected in Type, enter the community name that has been configured in SNMP Host.

Owner: Specifies the device or the user that defined the event.

Click **Add** to create a new entry. Click **Delete** to remove the corresponding entry.

Monitoring > Port Statistics

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

Figure 4.123 – Monitoring > Port Statistics

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.

Click **Refresh** to renew the information. Click **Clear** to reset the details.

To view the statistics of individual ports, click one of the linked port numbers for details.
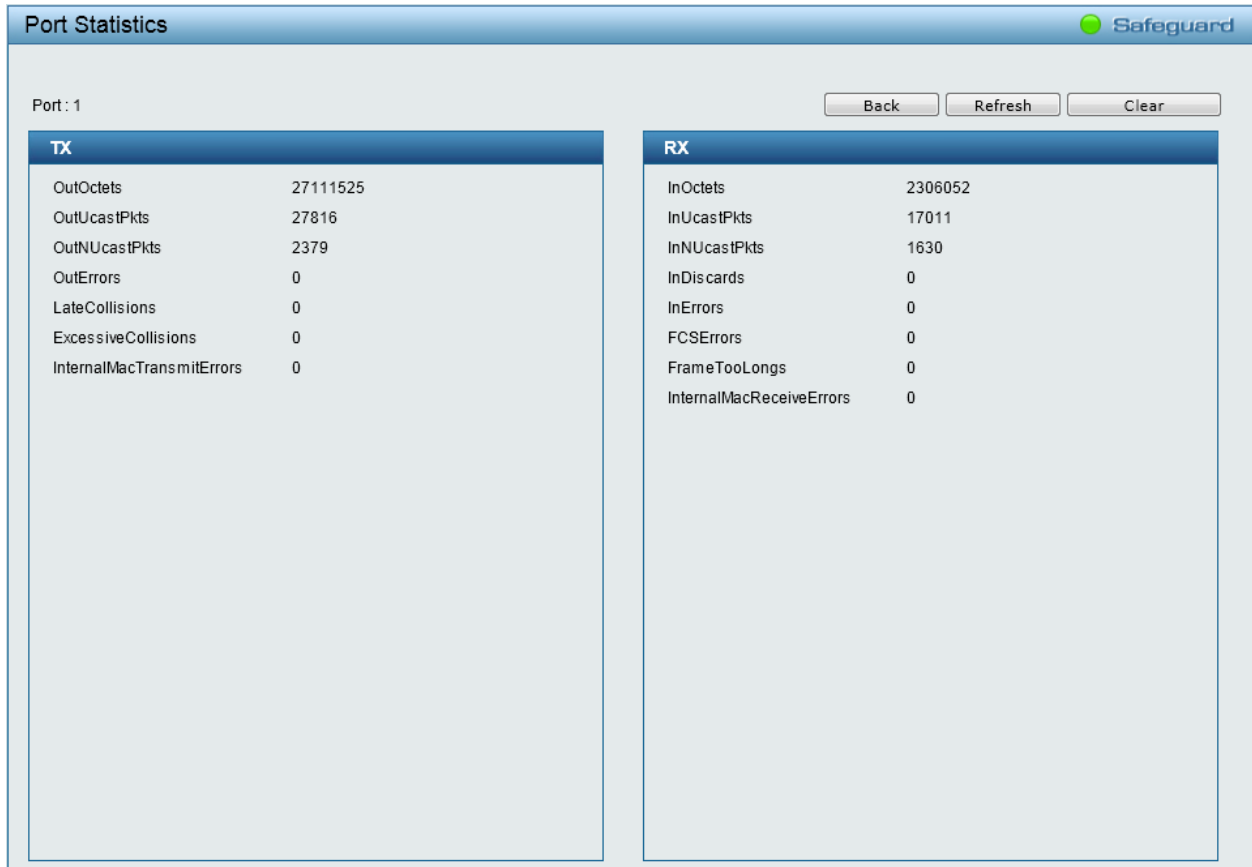
Figure 4.124 – Monitoring > Port Statistics

Click **Back** to go back to the previous page. Click **Refresh** to renew the information. Click **Clear** to reset the details.

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.
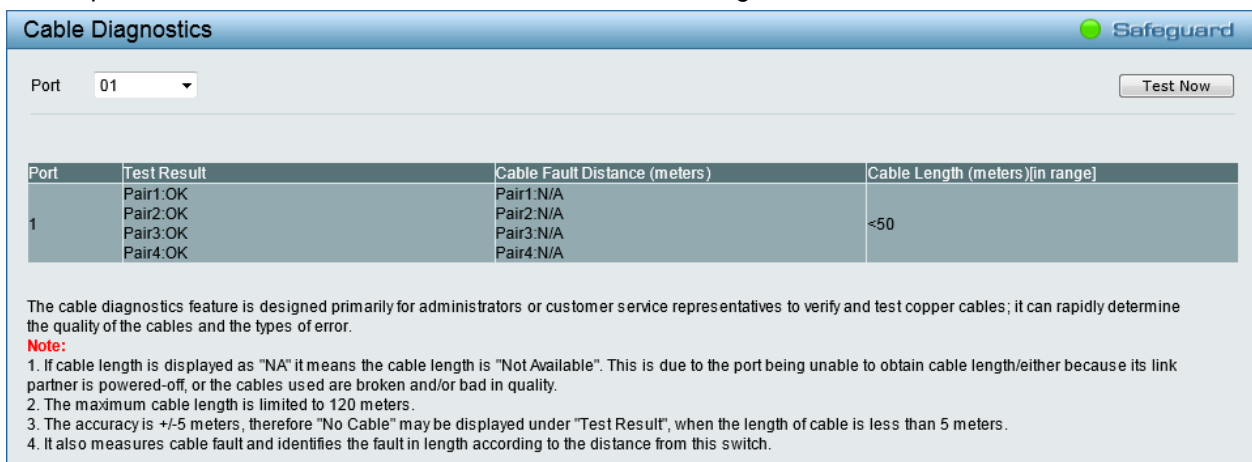
Figure 4.125 – Monitoring > Cable Diagnostic

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 window 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	2013-04-01 13:38:07	Successful login through Web (IP: 10.90.90.6)	INFO(6)
2	2013-04-01 12:07:58	Logout through Web (IP: 10.90.90.6)	INFO(6)
3	2013-04-01 12:07:58	Web session timed out (IP: 10.90.90.6)	INFO(6)
4	2013-04-01 11:32:36	Successful login through Web (IP: 10.90.90.6)	INFO(6)
5	2013-04-01 11:26:58	Logout through Web (IP: 10.90.90.6)	INFO(6)
6	2013-04-01 11:26:58	Web session timed out (IP: 10.90.90.6)	INFO(6)
7	2013-01-01 00:01:07	Successful login through Web (IP: 10.90.90.6)	INFO(6)
8	2013-01-01 00:00:51	Port 1 link up, 1Gbps FULL duplex	INFO(6)
9	2013-01-01 00:00:45	System started up	CRIT(2)

Figure 5.119 – Monitoring > System Log

ID: Displays an incremented counter of the System Log entry. The Maximum entries are 500.

Time: Displays the time in years, months, days, hours, minutes, and seconds 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.

5 *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 the TELNET or SSH 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.

To connect a switch via SSH:

1. Make sure the network connection between the switch and PC is active.

2. To connect, launch any SSH client tool like PuTTY, SecureCRT to access device.

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 (**DGS-1210-24:admin#**) will appear as shown below:

```
                    DGS-1210-24 Gigabit Ethernet Switch
                          Command Line Interface

                        Firmware: Build 4.10.007
           Copyright(C) 2013 D-Link Corporation. All rights reserved.

UserName:admin
PassWord:*****

DGS-1210-24:admin#
```

Figure 6.1 – Command Prompt

The user session is automatically terminated if idle for the login timeout period. The default login timeout period for TELENET is 5 minutes, and for SSH is 120 seconds.

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 [<ipaddr>	<ipv6addr>] <path_filename 64>	cfg_fromTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>]
upload	[cfg_toTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>	firmware_toTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>]
config ipif System	[ipaddress <ip-address> <subnet-mask> gateway <gw-address>	dhcp	bootp	ipv6 ipv6address <ipv6networkaddr>	dhcpv6_client {enable	disable}]

Command	Parameter
logout	
ping	[<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99>}
ping6	<ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99>}
reboot	
reset config	
show ipif	
show switch	
config account admin password	<password>
save	
debug info	

Each command is listed in detail, as follows:

?	
Purpose	This command is used 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-1210-24:admin#?

USEREXEC commands :
config account admin password <password>
config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-
address>|
dhcp | bootp}
config ipif System { ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client {enable
| disable}}
debug info
download  {  firmware_fromTFTP  |  cfg_fromTFTP}  {<ipaddr>|<ipv6addr>}
<path_filenam
e 64>
logout
ping <ipaddr>
ping6 <ipv6addr>
reboot
reset config
save
show ipif
show switch
upload { firmware_toTFTP | cfg_toTFTP} {<ipaddr>|<ipv6addr>} <path_filename>

DGS-1210-24:admin#
```

download

Purpose	This command is used to download and install a firmware file, boot file, or switch configuration file from a TFTP server.
Syntax	**download [firmware_fromTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>	cfg_fromTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>]**
Description	The **download** command downloads a firmware file, boot file, or switch configuration file from a TFTP server.
Parameters	*firmware_fromTFTP* – Specifies to download and install new firmware on the Switch from a TFTP server.
	<ipaddr> − Enter the IPv4 address of the TFTP server.
	<ipv6addr> − Enter the IPv6 address of the TFTP server.
	<path_filename 64> − Enter the filename of the firmware file or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not in the root directory of the TFTP server.
	cfg_fromTFTP – Specifies to download a switch configuration file from a TFTP server.
	<ipaddr> − Enter the IPv4 address of the TFTP server.
	<ipv6addr> − Enter the IPv6 address of the TFTP server.
	<path_filename 64> − Enter the filename of the firmware file or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not in the root directory of the TFTP server.

Restrictions	None.

Example usage:

To download a firmware file:

```
DGS-1210-24:admin#download firmware_fromTFTP 10.90.90.10 RUNTIME


 Connecting to server................... Done.
 Download firmware...................... Done. Do not power off!
 Please wait, programming flash......... Done.


 DGS-1210-24:admin#
```

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

upload	
Purpose	This command is used to upload the firmware file or a Switch configuration file to a TFTP server.
Syntax	**upload [cfg_toTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>	firmware_toTFTP [<ipaddr>	<ipv6addr>] <path_filename 64>]**
Description	The **upload** command uploads the Switch's current settings to a TFTP server.
Parameters	*cfg_toTFTP* − Specifies that the Switch's current settings will be uploaded to the TFTP server.
	<ipaddr> − Enter the IPv4 address of the TFTP server.
	<ipv6addr> − Enter the IPv6 address of the TFTP server.
	<path_filename> − Enter the filename of the firmware or switch configuration file to be saved on the TFTP server. You need to specify the DOS path if the file is not to be saved in the root directory of the TFTP server.
	firmware_toTFTP – Specifies to upload the firmware on the Switch to a TFTP server.
	<ipaddr> − Enter the IPv4 address of the TFTP server.
	<ipv6addr> − Enter the IPv6 address of the TFTP server.
	<path_filename> − Enter the filename of the firmware or switch configuration file to be saved on the TFTP server. You need to specify the DOS path if the file is not to be saved in the root directory of the TFTP server.
Restrictions	None.

Example usage:

To upload a firmware file:

```
DGS-1210-24:admin#upload firmware_toTFTP 10.90.90.10 RUNTIME

 Connecting to server................... Done.
 Upload firmware....................... Done.

DGS-1210-24:admin#
```

config ipif System

Purpose	This command is used to configure the System IP interface.
Syntax	**config ipif System [ipaddress <ip-address> <subnet-mask> gateway <gw-address>	dhcp	bootp	ipv6 ipv6address <ipv6networkaddr>	dhcpv6_client {enable	disable}]**
Description	The **config ipif System** command configures the System IP interface on the Switch.
Parameters	*ipaddress <ip-address> <subnet-mask>* − Specifies the IPv4 address and subnet mask to be created. Users need to specify the IPv4 address and subnet mask information using the traditional format (For example, 10.1.2.3/255.0.0.0). *gateway <gw-address>* − Specifies 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. *ipv6 ipv6address <ipv6networkaddr>* - Specifies the IPv6 address and network address to be created. *dhcpv6_client {enable	disable}* – Specifies to enable or disable the DHCPv6 client feature.
Restrictions	None.

Example usage:

To configure the IP interface System:

```
DGS-1210-24:admin#config ipif System ipaddress 10.90.90.2 255.0.0.0 gateway
10.90.90.1

Success.

DGS-1210-24:admin#
```

logout

Purpose	This command is used to logout a user from the Switch's Command Line Interface.
Syntax	**logout**
Description	The **logout** command terminates the current user's session from the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
DGS-1210-24:admin#logout




**********

* Logout *
**********
```

> ✏️ **NOTE:** Save your configuration changes before logging out.

ping

Purpose	This command is used to test the connectivity between the Switch and other network devices.
Syntax	**ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99>}**
Description	The **ping** command checks if another IPv4 address is reachable on the network. You can ping the IPv4 address through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the Switch and the target IPv4 equipment. By default, the Switch sends five pings to the target IPv4 address.
Parameters	*<ipaddr>* - Enter the IPv4 address of the host. *<domain_name 255>* - Enter the domain name here. This name can be up to 255 characters long. *times <value 1-255>* - Enter the ping times value here. This value must be between 1 and 255. *timeout <sec 1-99>* - Enter the ping timeout value here. This value must be between 1 and 99 seconds.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.6:

```
DGS-1210-24:admin#ping 10.90.90.6


Reply Received From :10.90.90.6, TimeTaken : 1 msecs
Reply Received From :10.90.90.6, TimeTaken : 1 msecs
Reply Received From :10.90.90.6, TimeTaken : 1 msecs
Reply Received From :10.90.90.6, TimeTaken : 1 msecs
Reply Received From :10.90.90.6, TimeTaken : 1 msecs


--- 10.90.90.6 Ping Statistics ---
5 Packets Transmitted, 5 Packets Received, 0% Packets Loss


DGS-1210-24:admin#
```

ping6

Purpose	This command is used to test the IPv6 connectivity between the Switch and other network devices.
Syntax	**ping6 <ipv6addr> {times <value 1-255> | size <value 1-6000> | timeout <sec 1-99>}**
Description	The **ping6** command checks if another IPv6 address is reachable on the network. You can ping the IPv6 address through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the Switch and the target IPv6 equipment. By default, the Switch sends five pings to the target IPv6 address.
Parameters	*<ipv6addr>* - Enter the IPv6 address of the host.
	times <value 1-255> - Enter the ping times value here. This value must be between 1 and 255.
	size <value 1-6000> - Enter the ping size value here. This value must be between 1 and 6000.
	timeout <sec 1-99> -Enter the ping timeout value here. This value must be between 1 and 99 seconds.
Restrictions	None.

Example usage:

To ping the IP address 3FFE:2::D04D:7878:66D:E5BC:

```
DGS-1210-24:admin#ping6 3FFE:2::D04D:7878:66D:E5BC

Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000, time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000, time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000, time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000, time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000, time<10 ms
 Ping Statistics for 3FFE:2::D04D:7878:66D:E5BC
 Packets: Sent =5, Received =5, Lost =0

DGS-1210-24:admin#
```

reboot

Purpose	This command is used 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 Switch. All network connections are terminated and the boot code executes.
Parameters	None.
Restrictions	None.

Example usage:

To reboot the Switch:

DGS-1210-24:admin#reboot

Are you sure you want to proceed with the system reboot?(y/n) y
% Device will reboot, please wait a few minutes to re-login.
Success.

DGS-1210-24:admin#

reset config

Purpose	This command is used to reset the Switch's configuration to the factory default settings.
Syntax	**reset config**
Description	All the Switch's configurations will be reset to the default settings.
Parameters	None.
Restrictions	None.

Example usage:

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

DGS-1210-24:admin#reset config

% Device will reboot after reset configuration successfully.

DGS-1210-24:admin#

show ipif

Purpose	This command is used to display the configuration of the IP interface on the Switch.
Syntax	**show ipif**
Description	The **show ipif** command displays the current IP interface configuration of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the IP interface settings:

```
DGS-1210-24:admin#show ipif


IP Setting Mode          : Static
IP Address            : 10.90.90.90
Subnet Mask           : 255.0.0.0
Default Gateway         : 10.90.90.1
DHCPv6 Client State       : Disabled
IPv6 Link-Local Address    : FE80::280:C2FF:FE12:2400/128


DGS-1210-24:admin#
```

show switch

Purpose	This command is used to display information about the Switch.
Syntax	**show switch**
Description	The **show switch** command displays information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's information:

```
DGS-1210-24:admin#show switch


System Name         :
System Location      :
System Contact       :
System up time       : 0 days, 4 hrs, 0 min, 51 secs
System Time        : 4/1/2013  15:05:49
System hardware version   :
System firmware version   : 4.10.007
System boot version     : 0.00.005
System serial number    :
MAC Address        : 00-80-C2-12-24-00


DGS-1210-24:admin#
```

config account admin password

Purpose	This command is used to configure the administrator user account password used on the Switch.
Syntax	**config account admin password <password>**
Description	The **config account admin password** command configures the administrator user account password used on the Switch.
Parameters	*<password>* − Enter the new password for the administrator account.
Restrictions	None.

111

Example usage:

To configure the administrator user account password used on the Switch:

DGS-1210-24:admin#config account admin password 1234
DGS-1210-24:admin#

save
Purpose	This command is used to save changes made in the Switch's configuration to the 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 the non-volatile RAM:

DGS-1210-24:admin#save
Building configuration ...
[OK]
DGS-1210-24:admin#

debug info
Purpose	This command is used 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-1210-24:admin#debug info

% segmentation fault log file :

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

Address         Hardware Address   Type  Interface  Mapping
-------         ---------------- ---- --------- -------
10.0.0.0        FF-FF-FF-FF-FF-FF  ARPA  System     Local/Broadcast
10.90.90.6      10-BF-48-D6-E2-E2  ARPA  System     Dynamic
10.90.90.90     00-80-C2-12-24-00  ARPA  System     Local
10.255.255.255  FF-FF-FF-FF-FF-FF  ARPA  System     Local/Broadcast

% MAC table :

Vlan   Mac Address      Type     Ports
----   -----------     ----    -----
1      10-BF-48-D6-E2-E2   Learnt      1

Total Entries: 1


DGS-1210-24:admin#
```

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 100Mbps Fast Ethernet and a hundredfold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps 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 1000Mbps capable backbone/server connection.

Fast Ethernet Technology

The growing importance of LAN 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-TX (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:
  - DGS-1210-08P: 20Gbps
  - DGS-1210-16: 40Gbps
  - DGS-1210-24: 56Gbps
  - DGS-1210-24P: 56Gbps
  - DGS-1210-48: 96Gbps
- Max. Forwarding Rate
  - DGS-1210-08P: 14.88Mpps
  - DGS-1210-16: 29.80Mpps
  - DGS-1210-24: 41.70Mpps
  - DGS-1210-24P: 41.70Mpps
  - DGS-1210-48: 71.43Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory:
  - DGS-1210-08P: 6Mbits
  - DGS-1210-16: 6Mbits
  - DGS-1210-24: 6Mbits
  - DGS-1210-24P: 6Mbits
  - DGS-1210-48: 6Mbits
- DDRIII for CPU: At least 128MBytes
- Flash Memory: At least 16Mbytes (SPI Flash)

Port Functions

- 10BASE-T/100BASE-TX/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
  - IEEE 802.3af Power over Ethernet (Only DGS-1210-08P and DGS-1210-24P)
  - IEEE 802.3at Power over Ethernet plus (Only DGS-1210-24P)
- 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, SM, 10km)
  - DEM-311GT (1000BASE-SX, MM, 550m)
  - DEM-312GT2 (1000BASE-SX, MM, 2km)
  - DEM-314GT (1000BASE-LH, SM, 50km)
  - DEM-315GT (1000BASE-ZX, SM, 80km)
- WDM Transceivers Supported:
  - DEM-330T/R (1000BASE-BX, TX-1550/RX-1310nm, SM, 10km)
  - DEM-331T/R (1000BASE-BX, TX-1550/RX-1310nm, SM, 40km)

Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:
  - DGS-1210-08P/16/24: 0dB (Fanless)
  - DGS-1210-24P: max. 48dB (Two Smart Fans)
  - DGS-1210-48: max. 46.7dB (One Smart Fan)
- Operation Temperature:
  - DGS-1210-08P: 0~40°C
  - DGS-1210-16/24/24P/48: -5~50°C
- Storage Temperature -20~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- CE Class A
- C-Tick Class A

Safety Certifications

- UL, CB Report

Features

L2 Features

- Supports up to 16K MAC address
- Supports 256 static MAC
- Jumbo frame: Supports up to 13,000 bytes
- IGMP snooping v1/v2 (v3 awareness):
  - Supports 256 IGMP snooping groups
  - Supports at least 64 static multicast groups
- MLD snooping v1 (v2 awareness):
  - Supports 256 MLD snooping groups
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- Loopback Detection
- 802.3ad Link Aggregation:
  - Supports maximum of 8 groups per device and 8 ports per group
- Port mirroring
- SNTP
- LLDP/LLDP-MED
- L2 Multicast Filtering

L3 Features
- DHCP Relay
- IPv6

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

QoS (Quality of Service)
- Priority queue mapping by :
  - 802.1p
  - DSCP
  - ToS
  - TCP/UDP port number
  - IPv6 traffic class
- Up to 8 queues per port
- Supports Strict / WRR mode in queue handling
- Bandwidth Control

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

ACL
- Max 50 ingress ACL profiles
- Ingress ACL rules:

  - Total 200 rules (each rule can be associated to a single port or multiple ports)
- Support different ACL policy packet contents:
  - MAC address
  - Ethernet Type
  - IPv4/IPv6 address
  - ICMP
  - IGMP
  - TCP/UDP port number
  - Protocol ID
  - IPv6 Traffic Class

Security
- Trusted Host
- Port Security: Support 64 MAC addresses per port
- DoS Attack Prevention
- Traffic Segmentation
- D-Link Safeguard Engine
- Broadcast Storm Control
- ARP Spoofing Prevention: Supports max 64 entries

- DHCP Server Screening: Able to configure 5 IP addresses for DHCP server.
- SSL: Support v1/v2/v3

Smart Binding
- Supports 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 Graphical User Interface
- Limited Command Line Interface (via Telnet)
- D-Link Network Assistant (DNA)
- SNMP support
- DHCP client
- DHCP Auto Configuration
- 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 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 Cable Length: Detects the length of connected RJ-45 cables and adjusts power usage accordingly without affecting performance. Once the RJ-45 connection is less than 20 meters, the switch will reduce the power instead of full power, which is only needed for 100 meters cables.

  - 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 Port Standby: Each port on the system enters sleep state 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.

- Power saving by Time-based PoE: PoE ports can be turned on/off by port or system through schedules. (DGS-1210-08P and DGS-1210-24P only)