DGS-1248T

48-Port 10/100/1000 Mbps with 4 Combo Mini GBIC Gigabit Smart Switch

User Manual

V1.00

TABLE OF CONTENTS

About This Guide 1
Purpose 1
Terms/Usage 1
Introduction 2
Gigabit Ethernet Technology 2
Fast Ethernet Technology 3
Switching Technology 3
Features 4
Technical Specifications 5
Unpacking and Installation 9
Unpacking 9
Installation 9
Rack Mounting 10
Connecting Network Cable 11
AC Power 12
Identifying External Components 13
Front Panel 13
Rear Panel 14
Understanding LED Indicators 15
Power and System LEDs 15
Configuration 18
Supported web browsers 18
Installing the SmartConsole Utility 18

SmartConsole Utility Features 19
Menu Toolbar 19
Discovery List 21
Monitor List 22
Device Setting 24
Web-based Utility 26
Login 26
Tool Menu 28
Setup Menu 29
System > System Setting 30
System > Trap Setting 31
System > Port Setting 32
System > SNMP Setting 34
System > Password Access Control 36
Configuration > 802.1Q VLAN 36
Configuration > Trunking 39
Configuration > IGMP Snooping 40
Configuration > 802.1D Spanning Tree 44
Configuration > Port Mirroring 46
QoS > 802.1p Default Priority 47
Security > Safeguard Engine 48
Security > Broadcast Storm Control 48
Security > 802.1X Setting 48
Security > Mac Address Table > Static MAC 51
Security > Mac Address Table > Dynamic Forwarding Table 52

Monitoring > Statistics..... 53

ABOUT THIS GUIDE

Thank you and congratulations on your purchase of the DGS-1248T 48-Port 10/100/1000 Mbps with 4 Combo Mini GBIC Gigabit Smart Switch. This device integrates 1000Mbps Gigabit Ethernet, 100Mbps Fast Ethernet and 10Mbps Ethernet network capabilities in a highly flexible package.

Purpose

This guide will show you how to install and use the configuration functions of the DGS-1248T Web-Smart Switch step-by-step.

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to the DGS-1248T 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.

INTRODUCTION

This chapter will describe the features of the DGS-1248T and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

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

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential to help solving network bottlenecks that frequently develop 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. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, outfitting your network with a powerful 1000-Mbps-capable backbone/server connection which will create a flexible foundation for the next generation of network technology products.

Fast Ethernet Technology

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

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.

Features

- Address Table: Supports up to 8K MAC address per device
- Supports a packet buffer of up to 1024K Bytes
- IGMP Snooping support
- IEEE802.1D Spanning Tree
- Support static Port Trunk
- Port Mirroring support
- IEEE802.1Q VLAN
- IEEE802.1p Priority Queues
- IEEE802.1X Port-based Access Control
- Supports Broadcast Storm Control

- Supports Static MAC setting
- D-Link Safeguard Engine support
- Supports Simple Network Management Protocol(SNMP)
- MIB support for: RFC1213 MIB II, Private MIB
- Supports DHCP client
- Supports Port setting for Speed, Duplex Mode
- Easy configuration via Web Browser
- Easy setting via SmartConsole Utility
- Firmware backup and upload via Web GUI
- System reboot via Web GUI
- Provides parallel LED display for port status such as link/act, speed, etc.
- Reset configuration (hardware and Web GUI)

Technical Specifications

Key Components / Performance	
Switching Capacity	96Gbps
Max. Forwarding Rate	10M: 14,880 pps 100M: 148,809 pps 1G: 1,488,095 pps
Forwarding Mode	Store and Forward
Packet Buffer memory	1024K Bytes

SDRAM for CPU	8M Bytes
Flash Memory	Prom 2M Bytes
Port Functions	
LAN	- 48 x 10/100/1000BaseT ports - Compliant with the following standards: 1. IEEE 802.3 compliance 2. IEEE 802.3u compliance 3. IEEE 802.3ab compliance 4. Support Full Duplex at 10/100Mbps and 1000Mbps only for SFP ports
Combo ports in the front panel	- 4 SFP Combo Ports (port 45~48) - SFP Transceivers Supported: 1. DEM-310GT (1000BASE-LX), up to 10km 2. DEM-311GT (1000BASE-SX), up to 550m 3. DEM-314GT (1000BASE-LH), up to 50km 4. DEM-315GT (1000BASE-ZX), up to 80km 5. DEM-312GT2 (1000BASE-SX), up to 2km -WDM Transceivers Supported: 1. DEM-330T (TX-1550/RX-1310nm), up to 10km, Single-Mode 2. DEM-330R (TX-1310/RX-1550nm), up to 10km, Single-Mode 3. DEM-331T (TX-1550/RX-1310nm), up

	to 40km, Single-Mode 4. DEM-331R (TX-1310/RX-1550nm), up to 40km, Single-Mode -Compliant to the following standards: 1. IEEE 802.3z compliance
Chassis	
Dimensions	19-inch, 1U Rack-mount size 440mm x 310mm x 44mm
Reset button on the front panel	A factory reset button x 1
Physical & Environment	
AC input	100~240 VAC, 50/60Hz Internal universal power supply
Operation Temperature	0~40°C
Storage Temperature	-10~70°C
Humidity	Operation: 10%~90% RH Storage: 5%~90% RH
Power consumption	99.7(watts)
Heat Dissipation	339.98(btu/hr)
MTBF	156505 (hours)

Emission (EMI) and Safety Certifications
EMI-EMC Compliance: FCC Class A/ICES-003 Class A(FCC Part 15B), CE Class A(EN55022/24), C-Tick ClassA(AS/NZS CISPR 22) , VCCI Class A(VCCI-2005) Safety Compliance: cUL(UL 60950-1), LVD(EN 60950-1)

UNPACKING AND INSTALLATION

This chapter provides unpacking and installation information for the Smart Switch.

Unpacking

Carefully unpack the contents of the Smart Switch from the box and locate the following items:

One DGS-1248T Gigabit Smart Switch

One AC power cord, suitable for the local electrical power voltage requirements

Four rubber feet to be used for shock cushioning

Screws and two mounting brackets

CD-Rom with the SmartConsole Utility application, which includes the full User's Manual

Quick Installation Guide

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

Installation

The site chosen for installation greatly affects the Web-Smart Switch's performance. When installing, consider the following points:

Install the Switch in a fairly cool and dry place. See Technical Specifications for the acceptable temperature and humidity operating ranges.

Install the DGS-1248T in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
Leave at least 10cm (about 4 inches) of space at the front and rear of the switch for ventilation.
Install the DGS-1248T on a sturdy, level surface that can support its weight, or in an EIA standard-size equipment rack. For information on rack installation, see the next section, Rack Mounting.

When installing the Switch on a level surface, attach the rubber pads (feet) to the bottom. The rubber feet cushion the switch and helps protect the case from scratches.

.

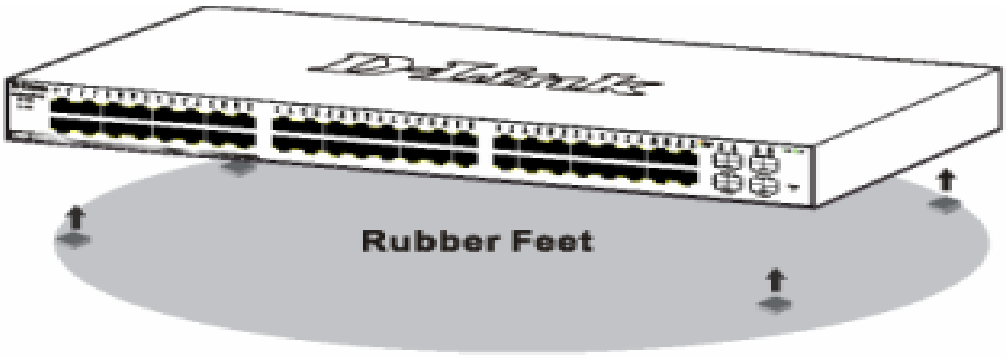


Figure 1 – Attach the adhesive rubber pads to the bottom

Rack Mounting

The Switch can be mounted in an EIA standard-size, 19-inch rack or chassis, which can be placed in a wiring closet with other equipment. Attach the mounting brackets to both sides of the Switch (one on each side), and secure them with the provided screws.

Figure 2 – Attach the mounting brackets to the Switch

Use the screws provided with the equipment rack or chassis to mount the Switch in the rack.

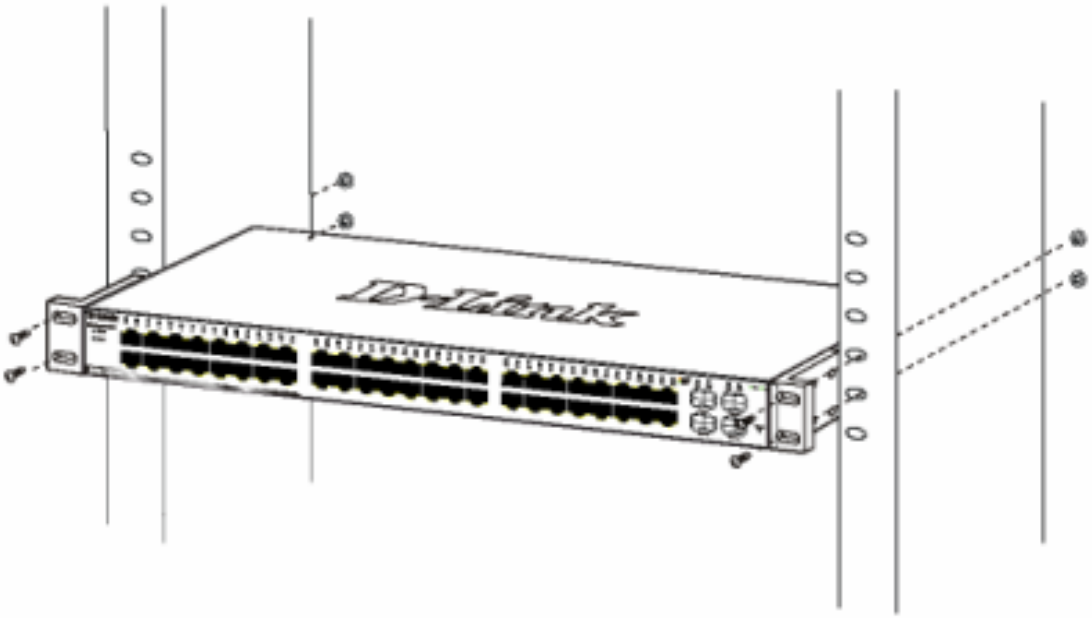


Figure 3 – Mount the Switch in the rack or chassis

Connecting Network Cable

The DGS-1248T has 48-Ports 10/100/1000Mbps that support 1000Mbps Gigabit Ethernet that can operate in Auto-negotiate

mode, and 10Mbps Ethernet or 100Mbps Fast Ethernet modes that run both in half and full duplex modes; it also has 4 Mini GBIC Combo Ports. Each port on the DGS-1248T supports Auto-MDI/MDI-X. Auto-MDI/MDI-X is a feature that eliminates the need for worrying about using either a standard or crossover cable—you can use either one—and allows any port to be an uplink port.

AC Power

The DGS-1248T can be used with an AC power supply of 100~240V AC, 50~60Hz. The power switch is located at the rear of the unit adjacent to the AC power connector and the system fan.

The switch's power supply will adjust to the local power source automatically and may be turned on without having any or all LAN segment cables connected.

IDENTIFYING EXTERNAL COMPONENTS

This chapter describes the front panel, rear panel, and LED indicators of the Switch.

Front Panel

The figure below shows the front panel of the Switch.

Figure 4 – Front panel of the 48-port Web-Smart Switch

Reset button:

The Reset button resets all configuration settings back to the factory default.

Note: Be sure to save or record any custom settings configured on the Switch before pressing the reset button. Resetting the Switch back to factory default settings will erase all custom configurations.

LED Indicator:

Comprehensive LED indicators display the status of the switch and the network (see the ***Understanding LED Indicators*** section).

1000 BASE-T Twisted Pair Ports (Port 1~48)

The DGS-1248T is equipped with 48 gigabit twisted pair ports that are auto negotiable 10/100/1000Mbps and also support auto

MDI/MDIX crossover detection. All these 48 ports can operate in half- and full- duplex modes for 10/100Mbps, and will be automatically activated when a compatible terminal is identified.

10/100/1000 BASE-T / Mini GBIC Combo Ports (Option Port 45~48)

The Switch is also equipped with four combo 10/100/1000 Base-T / Mini GBIC ports, supporting optional 1000BASE-SX/LX Mini GBIC modules for fiber uplinks.

Note: When a port is set to "Forced Mode", the Auto MDI/MDIX will be disabled.

Rear Panel

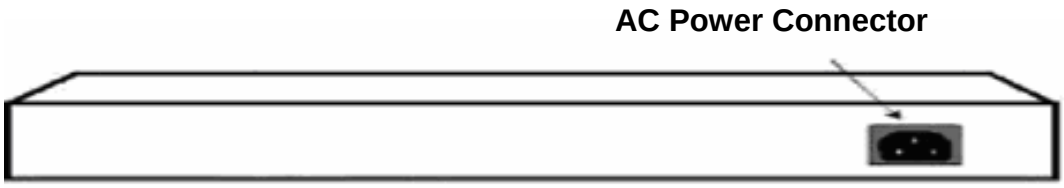


Figure 5 – Rear panel of the Switch

AC Power Connector:

Plug in the female connector of the provided power cord into this connector, and the male into a power outlet. Supported input voltages range from 100-240V AC, and 50-60Hz.

Understanding LED Indicators

The front panel LEDs provides instant status feedback and simplifies monitoring and troubleshooting tasks.

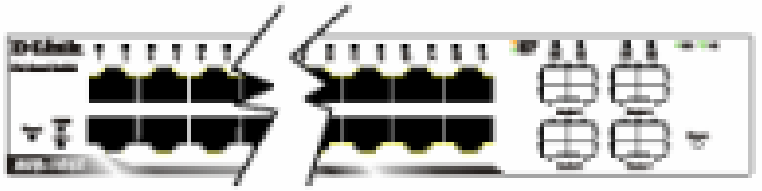


Figure 6 – LED indicators of the Switch

Power and System LEDs

Power LEDs

On	When the Power LED light is on, the Switch is receiving power.
Off	When the Power LED light is off, the power cord is improperly connected.

CPU LEDs (Management Indicator)

Blinking	When the CPU is working, the CPU LED is blinking.
Off	The CPU is idle.

Ports 1 ~ 48 Status LEDs

Link/Act

On	When the Link/Act LED light is on, the respective port is successfully connected to an Ethernet network.
Blinking	When the Link/Act LED is blinking, the port is transmitting or receiving data on the Ethernet network.
Off	No link.

1000Mbps (Shown in Green)

On	When the LED light is a solid green, the respective port is connected to a 1000Mbps Gigabit Ethernet network.
Off	No link.

10/100Mbps (Shown in Amber)

On	When the LED light is solid amber, the respective port is connected to a 1000Mbps Gigabit Ethernet network.
Off	No link.

Option Ports 45~48 Mini GBIC Status LEDs

Link/Act

On	When the Mini GBIC module is installed and connected to a network, the Link/Act LED light is on.
Blinking	When the Link/Act LED is blinking, the Mini GBIC module is receiving data on a network.
Off	No link.

CONFIGURATION

Through a web browser, the features and functions of the DGS-1248T Switch can be configured for optimum use.

Supported web browsers

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

- Microsoft Internet Explorer ver. 6.0, 5.5
- Mozilla ver. 1.7.12, 1.6
- Firefox ver. 1.5, 1.0.7
- Netscape ver. 8.0.4, 7.2
- Opera ver. 8.5, 7.6
- Safari ver. 2.0.2

Installing the SmartConsole Utility

The SmartConsole Utility allows a user to monitor and configure multiple D-Link Web Smart Switches from a workstation connected to the network. Follow these steps to install the SmartConsole Utility:

1. Insert the Utility CD in your CD-Rom Drive.
2. From the **Start** menu on the Windows desktop, choose **Run**.
3. In the **Run** dialog box, type D:\SmartConsole Utility\setup.exe (where D:\ represents the driver letter of your CD-ROM) and click **OK**.
4. Follow the on-screen instructions to install the utility program.
5. Upon completion, go to **Program Files > SmartConsole Utility** and execute the SmartConsole Utility.

SmartConsole Utility Features

The SmartConsole Utility is divided into four parts, a ***Menu Toolbar*** of functions at the top, ***Discovery List***, ***Monitor List***, and ***Device Setting***.

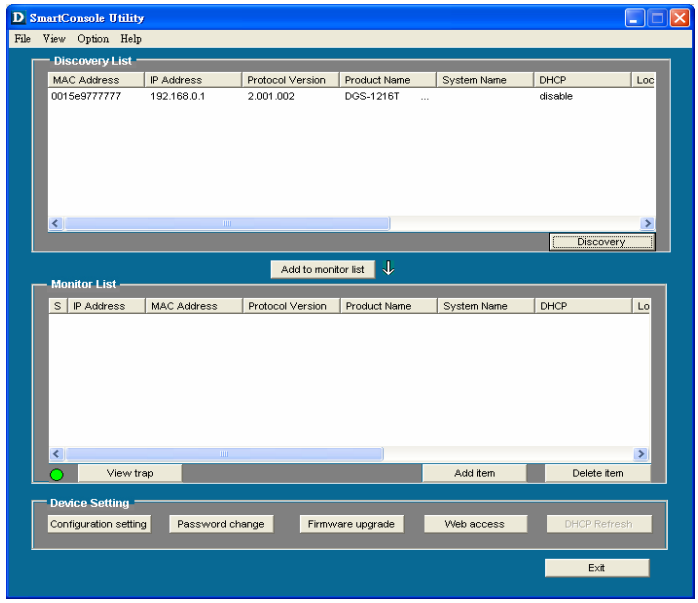


Figure 7 – SmartConsole Utility

Menu Toolbar

The Menu Toolbar in the SmartConsole Utility has four main tabs, File, View, Option, and Help.

File includes: *Monitor save*, *Monitor save as*, *Monitor load* and *Exit*.

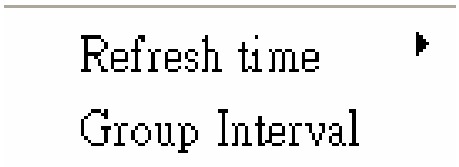
- **Monitor Save:** To record the setting of the Monitor List as default for the next time the SmartConsole Utility is used.
- **Monitor Save As:** To record the setting of the Monitor List in an appointed filename and file path.

- **Monitor Load:** To manually load a Monitor List setting file.
- **Exit:** To exit the SmartConsole Utility.

View includes: *View log* and *Clear Log* functions, which provide trap setting list operations.

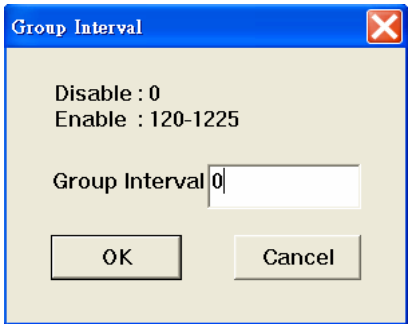
- **View Log:** To show the event of the SmartConsole Utility and the device.
- **Clear Log:** To clear all log entries.

Option includes: *Refresh Time* and *Group Interval* functions.



- **Refresh time** refreshes the monitoring time of the device. Choices include ***15 secs, 30 secs, 1 min, 2 min and 5 min*** for selecting the monitoring time intervals.
- **Group Interval** establishes the intervals (in seconds) that the Web-Smart Switch will be discovered in the SmartConsole Utility Discovery List.

NOTE: If the Group Interval is set to 0, IGMP snooping must be disabled or else the Web-Smart Switch will not be discovered.



Help includes: information *About* the SmartConsole Utility, such as the software version.

Discovery List

This is the list where all Web-Smart devices on the network are discovered.

By pressing the **Discovery** button, all the Web-Smart devices are listed in the discovery list.

Double click or press the **Add to monitor list** button to select a device from the Discovery List and add it to the Monitor List.

Definitions of the Discovery List features:

MAC Address: Shows the device MAC Address.

IP Address: Shows the current IP addresses of devices.

Protocol version: Shows the version of the Utility protocol.

Product Name: Shows the device product name.

System Name: Shows the appointed device system name.

DHCP: uses a client/server model to obtain lease of an IP address from a DHCP server as part of the network boot process.

Location: Shows the appointed description for the device location.

Trap IP: Shows the IP where the Trap information will be sent.

Subnet Mask: Shows the Subnet Mask set of the device.

Gateway: Shows the Gateway set of the device.

Group Interval: Shows the Group Interval of the device.

Monitor List

All Web-Smart devices in the Monitor List can be monitored, with Trap information available to be received for monitoring status information of the device.

Definitions of the Monitor List functions and terms:

S: Shows the system symbol of the Web-Smart device, represents the device system is inactive.

IP Address: Shows the current IP address of the device.

MAC Address: Shows the device MAC Address.

Protocol version: Shows the version of the Utility protocol.

Product Name: Shows the device product name.

System Name: Shows the appointed device system name.

DHCP: uses a client/server model to obtain lease of an IP address from a DHCP server as part of the network boot process.

Location: Shows the appointed description for the device location.

Trap IP: Shows the IP where the Trap to be sent.

Subnet Mask: Shows the Subnet Mask set of the device.

Gateway: Shows the Gateway set of the device.

Group Interval: Shows the Group Interval of the device.

View Trap: The view trap function receives trap events from the Web-Smart Switch.

There is a light indicator to the left of the ***"View Trap"*** button. A green light indicates that the monitor has not received any new traps, while a red light indicates that there are new traps received by the monitor available to view. (Figure 10)

Figure 8 – View trap

When the ***"View Trap"*** button is clicked, a Trap Information window will pop up, showing the trap information, such as Symbol, Time, Device IP and the Event occurred. (Figure 11)

The symbol " " represents a new trap signal, and will disappear after the event record is reviewed (clicked).

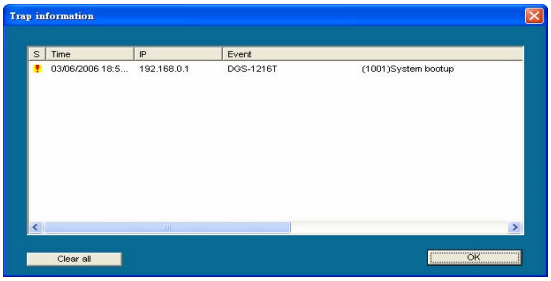


Figure 9 – Trap information

Note: To receive Trap information, the switch must be configured with Trap IP and Trap Events, available from the Trap Setting menu.

Add Item: Adds a device to the Monitor List manually, by entering the IP Address of the device to monitor.

Delete Item: Deletes the device from the Monitor List.

Device Setting

Function buttons of the Device Setting section provide several options.

Configuration Setting: In the Configuration Setting, the following settings are available: Product Name, MAC Address, IP Address, Subnet Mask, Gateway, Set Trap to (Trapping IP Address), System name, Location, Password and DHCP ON/OFF (OFF is default).

After selecting the device from the Discovery List or Monitor List and pressing Configuration Setting, modify the information necessary and press "Set".

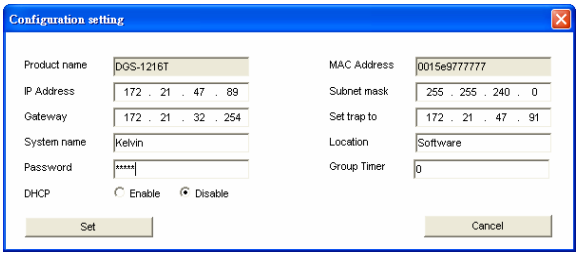


Figure 10 – Configuration Setting

Password Change: To change the password, fill in the new and original password, and press ***"Set"***.

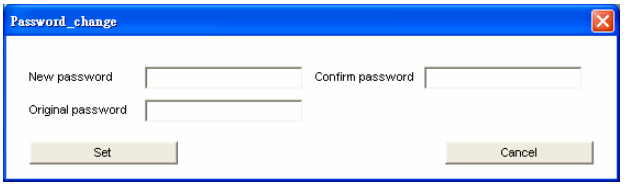


Figure 11 – Password Change

This space has been intentionally reserved for notes:

Firmware Upgrade: To update the device firmware, enter the firmware path and password (if necessary), and click “Start”.)

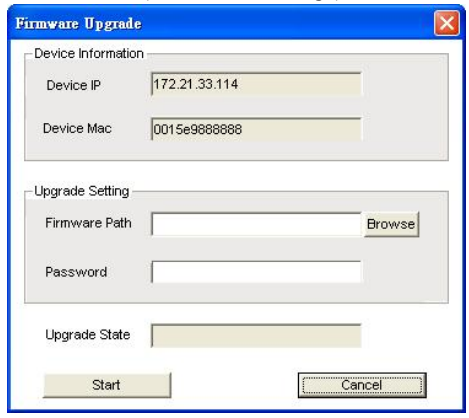


Figure 12 – Firmware Upgrade

Web Access: Double click the device in the Monitor List or select a device in the Monitor List and press the ***“Web Access”*** button to open the Web-based Utility. To see the list of web browsers the Web-based Utility supports, see ***Supported web browsers*** on page 18.

DHCP Refresh: select a device in the Monitor List and press the “**DHCP Refresh**”, and enter the password (if applicable) to trigger the Web-Smart Switch to request an IP address from a DHCP Server.

Figure 13 – DHCP Refresh

Web-based Management

The DGS-1248T Web-Smart Switch has a web browser GUI interface for configuring the Switch through a web browser. To see the list of web browsers the Web-based Utility supports, see ***Supported web browsers*** on page 18. A network administrator can manage, control and monitor the switch from the local LAN. This section indicates how to configure the Switch to enable its smart functions.

Login

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same range as the switch. For example, if the switch has an IP address of 192.168.0.1, the PC should have an IP address of 192.168.0.x (where x is a number between 2 and 254), and a subnet mask of 255.255.255.0. Open your web browser and enter http://192.168.0.1 (the factory-default IP address) in the address box. Then press <Enter> (Figure 16)

Figure 14 – Logging into the Switch's (DHCP assigned) IP address

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

When the following logon box appears, enter "**admin**" for the password. Press **Ok** to enter the main configuration window. (Figure 15)

Figure 15 – Log in screen

Once you have successfully logged in, the device status page will appear. In the top right corner the *user name* (default 'admin') is displayed with the *IP address* of the Switch. Below this is a ***Logout*** option for use when the session is complete.

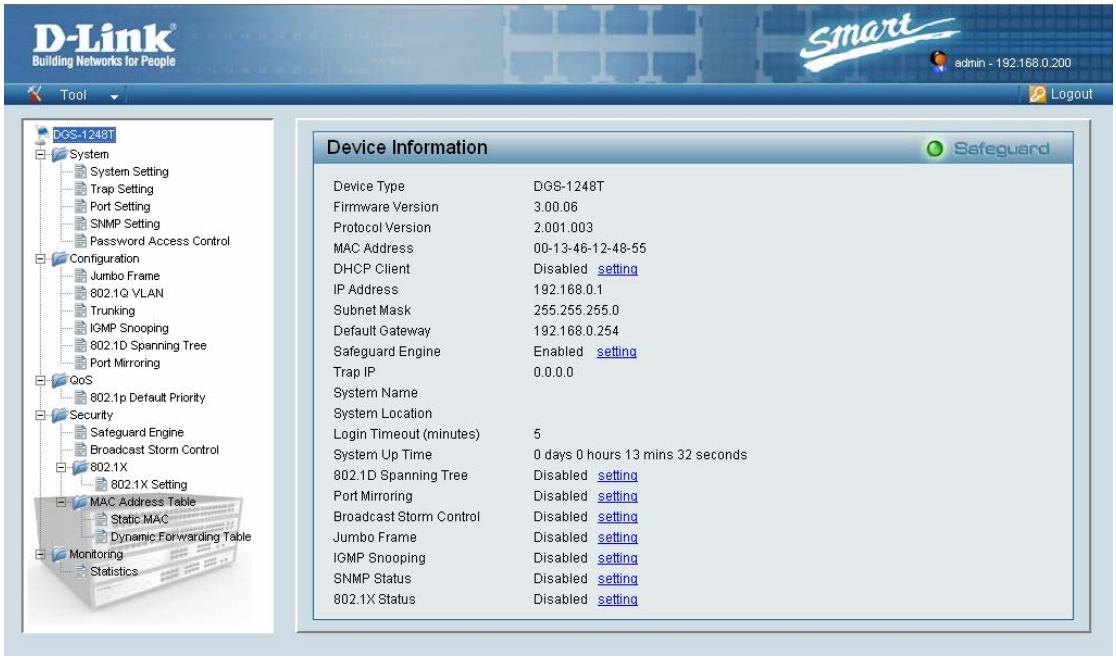


Figure 16 – Device Status

Tool Menu

The Tool Menu offers global function controls such as Reset, Configuring Backup and Restoration, Firmware Backup and Upload, and System Reboot.

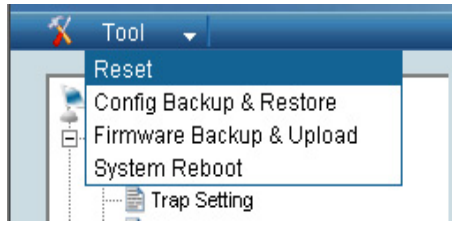


Figure 17 – Tool Menu

Reset: Provides a safe reset option for the Switch. All configurations will be reset to default.

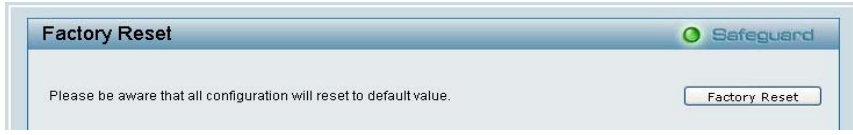


Figure 18 – Tool Menu > Reset

Configure Backup and Restore: Allows the current configuration settings to be saved to a file (not including the password), and if necessary, to be restored from a backup.

Figure 19 – Tool Menu > Configure Backup and Restore

Firmware Backup and Upload: Allows for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch.

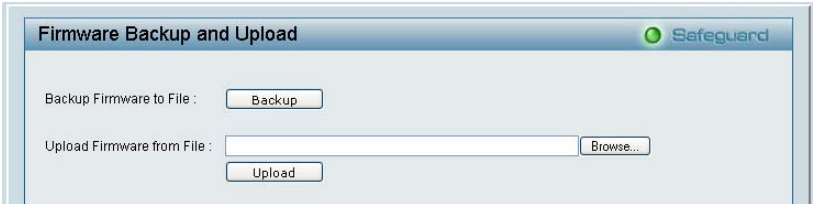


Figure 20 – Tool Menu > Firmware Backup and Upload

System Reboot: Provides a safe way to reboot the system. Ensure the configuration has been saved, or all the changes you just made may be lost after system reboot.

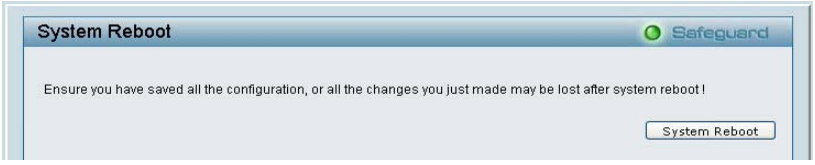


Figure 21 – Tool Menu > System Reboot

Setup Menu

All configuration options on the switch are accessed through the Setup menu on the left side of the screen (Figure 24). Click on the setup item that you want to configure. The following sections describe in more detail each of the features and functions.

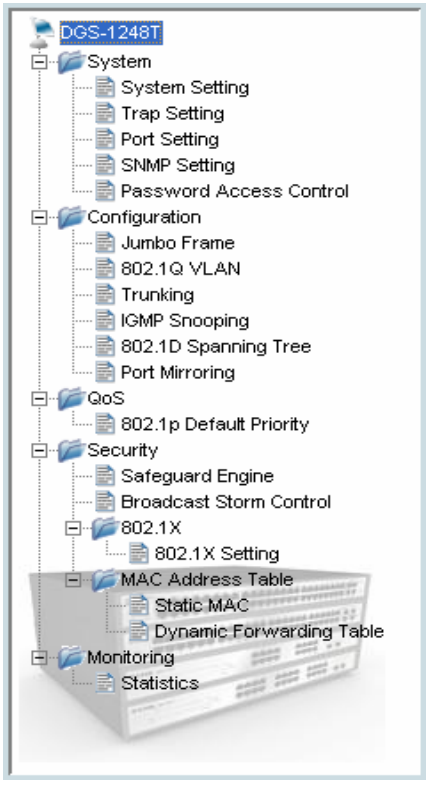


Figure 22 –Setup Menu

System > System Setting

The System Setting includes IP Information and System information. There are two ways for the switch to attain IP: Static and DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol).

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

By entering a **System Name** and **System Location**, the device can more easily be recognized through the SmartConsole Utility and in other Web-Smart devices on the LAN. The **Login Timeout** controls the idle time-out for security purposes, when there is no action in the Web-based Utility. When the Login Timeout expires, the Web-based Utility requires a re-login before using the Utility again. The **Group Interval** send IGMP v1 report packet by switch, it is for SmartConsole Utility to discovery our switch when we in IGMP protocol, zero means disable Group Interval, and 120~1225 means send IGMP v1 report according the value which unit is seconds.

Figure 23 – System > System Setting

System > Trap Setting

By configuring the Trap Setting, it allows SmartConsole Utility to monitor specified events on this Web-Smart Switch. By default, Trap Setting is ***Disabled***. When the Trap Setting is ***Enabled***, enter the **Destination IP** address of the managing PC that will receive trap information.

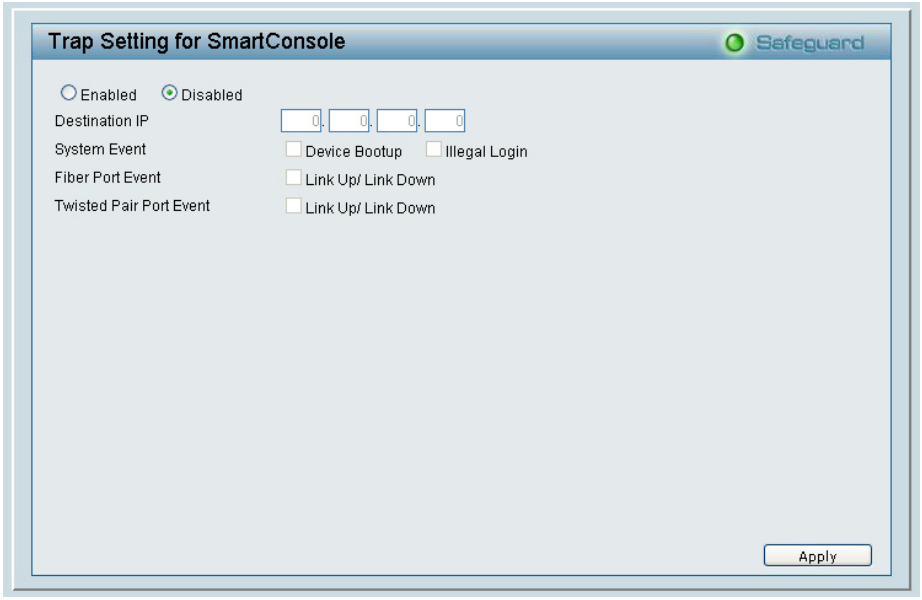


Figure 24 – System > Trap Setting

System Event: Monitors the system's trapping information.

Device Bootup: Traps system boot-up information.

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

Fiber Port Events: Monitors the fiber port status.

Link Up/Link Down: Traps fiber connection information.

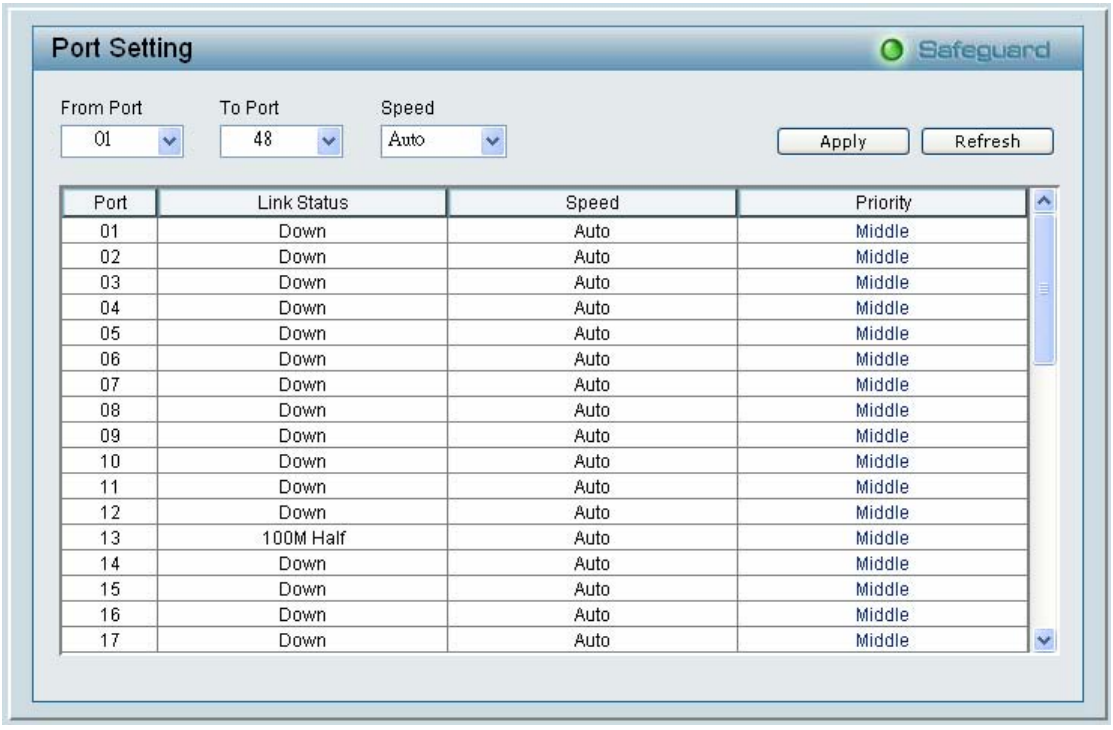
Twisted pair Port Events: Monitors the copper cable port status.

Link Up/Link Down: Traps copper connection information.

System > Port Setting

In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports ("**From Port"** and "**To Port"**), the **Speed** can be set for all such ports,

by clicking **Apply**. To refresh the information table to view the latest Link Status and Priority, press the **Refresh** button.



Port	Link Status	Speed	Priority
01	Down	Auto	Middle
02	Down	Auto	Middle
03	Down	Auto	Middle
04	Down	Auto	Middle
05	Down	Auto	Middle
06	Down	Auto	Middle
07	Down	Auto	Middle
08	Down	Auto	Middle
09	Down	Auto	Middle
10	Down	Auto	Middle
11	Down	Auto	Middle
12	Down	Auto	Middle
13	100M Half	Auto	Middle
14	Down	Auto	Middle
15	Down	Auto	Middle
16	Down	Auto	Middle
17	Down	Auto	Middle

Figure 25 – System > Port Setting

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

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

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

Priority: Displays each port's 802.1p QoS priority level for received data packet handling. Default setting for all ports is *Middle*. You can change the priority settings in *Qos > 802.1p Default Priority*

NOTE: The priority of Gigabit Fiber ports are by default higher than Copper ports.

System > SNMP Setting

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) 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.

Community Setting: In support of SNMP version 1, the Web-Smart Switch accomplishes user authentication by using Community Settings that function as passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from a station that are not authenticated are ignored (dropped).

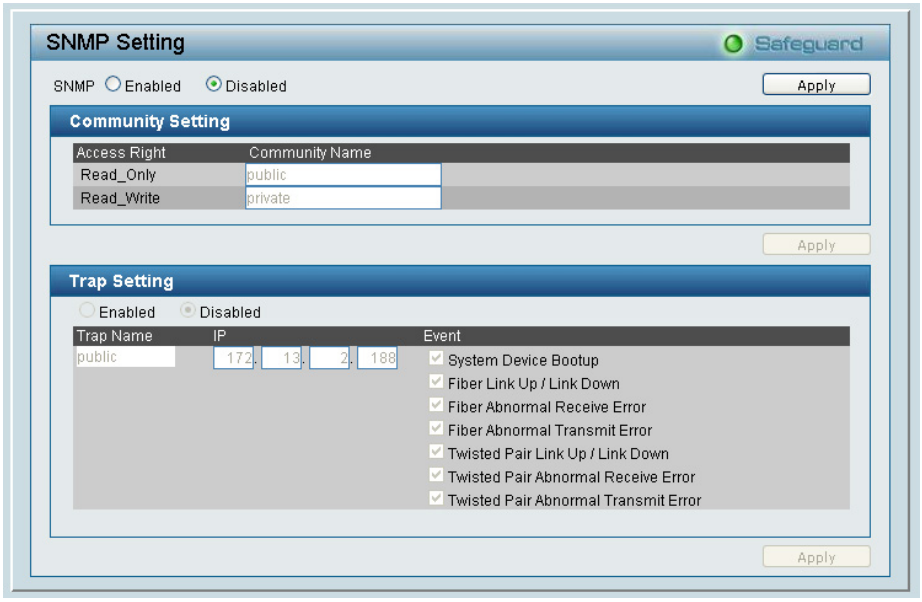


Figure 26 – System > SNMP Setting

Enabled / Disabled: Default setting is *Disabled*. Click *Enable*, then *Apply*, to set Community Settings.

The default community strings for the Switch used for SNMP v.1 management access are:

> **Public:** The community with read-only privilege allows authorized management stations to retrieve MIB objects.
>
> **Private:** The community with read/write privilege allows authorized management stations to retrieve and modify MIB objects.

Trap Setting: Traps are messages that alert network personnel of events that occur on the Switch. Such events can be as serious as a reboot (someone accidentally turned the Switch OFF), or less serious events such as a port status change. The Switch can generate traps and send them to the trap recipient (i.e. network administrator).

Setting up a Trap: Select *Enable*, enter a Trap Name (i.e. Trap Name must be selected from a Community Name), add the IP of the device to be monitored, and choose the event(s) to trap. The available trap Events to choose from include: System Device Bootup, Fiber Link Up / Link Down, Fiber Abnormal Receive Error, Fiber Abnormal Transmit Error, Twisted Pair Link Up / Link Down, Twisted Pair Abnormal Receive Error, Twisted Pair Abnormal Transmit Error.

System > Password Access Control

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

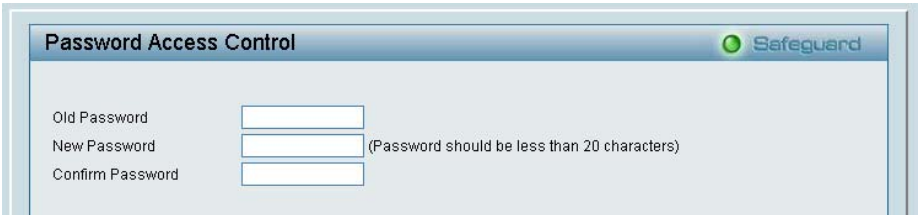


Figure 27 – System > Password Access Control

Configuration > 802.1Q VLAN

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

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

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 01, named “default”, and all 48 ports as “Untagged” (see Figure 29).

Rename: Click to rename the VLAN group.

Delete VID: Click to delete the VLAN group.

Add New VID: Click to create a new VID group, assigning ports from 01 to 48 as *Untag*, *Tag*, or *Not Member*. A port can be “Untagged” in only one VID. To save the VID group, press ***Apply***.

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

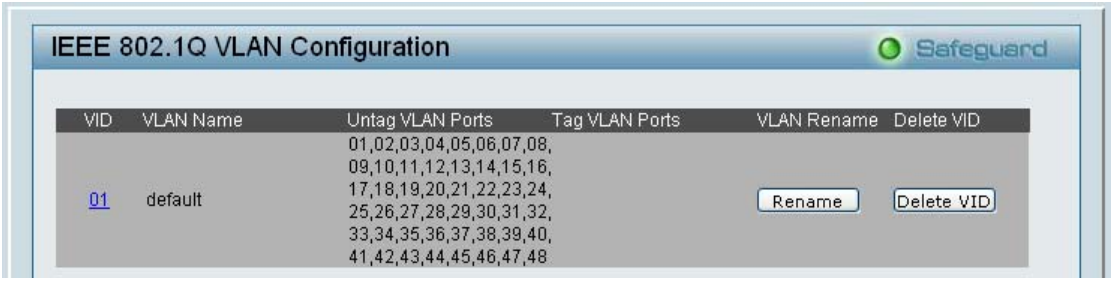


Figure 28 – Configuration > 802.1Q VLAN > Default Setting

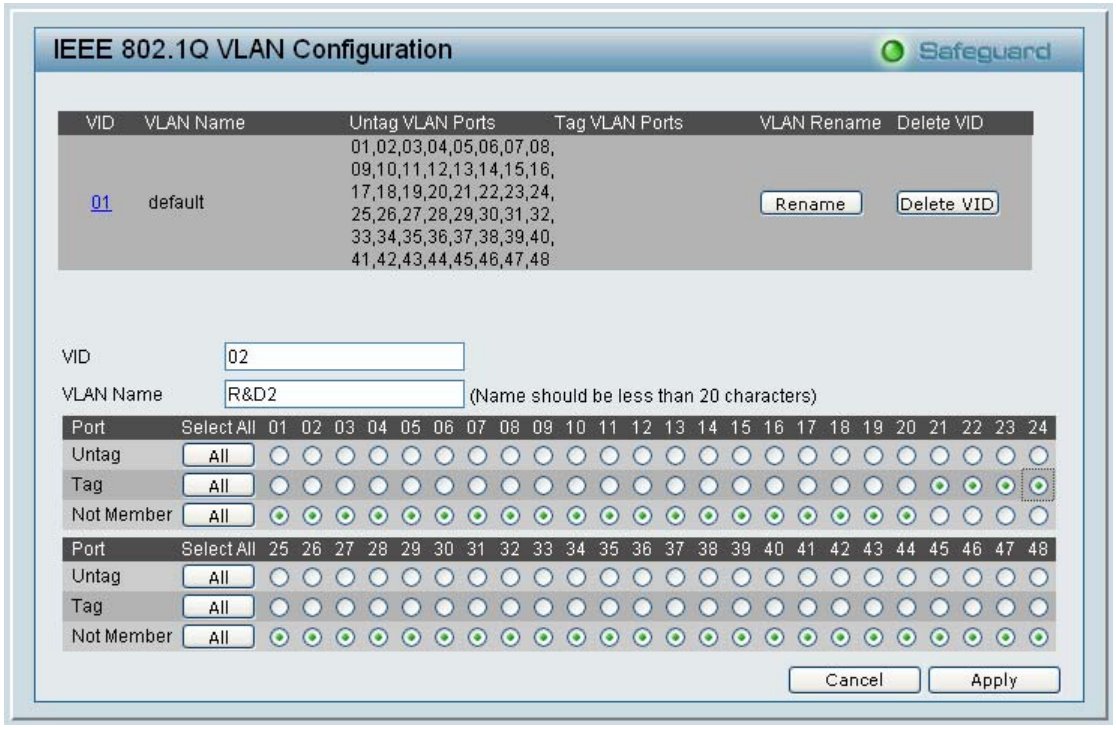


Figure 29 – Configuration > 802.1Q VLAN > Add VID

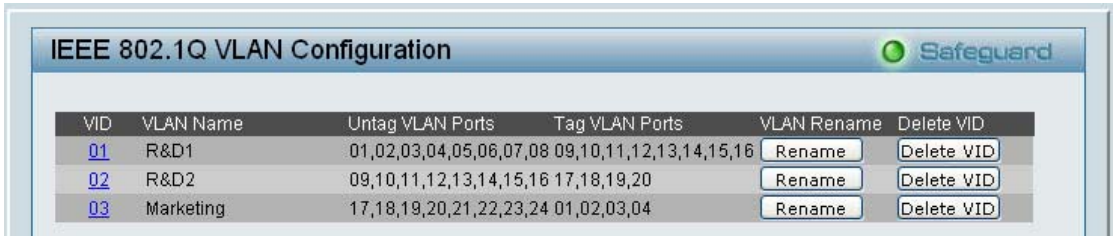


Figure 30 – Configuration > 802.1Q VLAN > Example VIDs

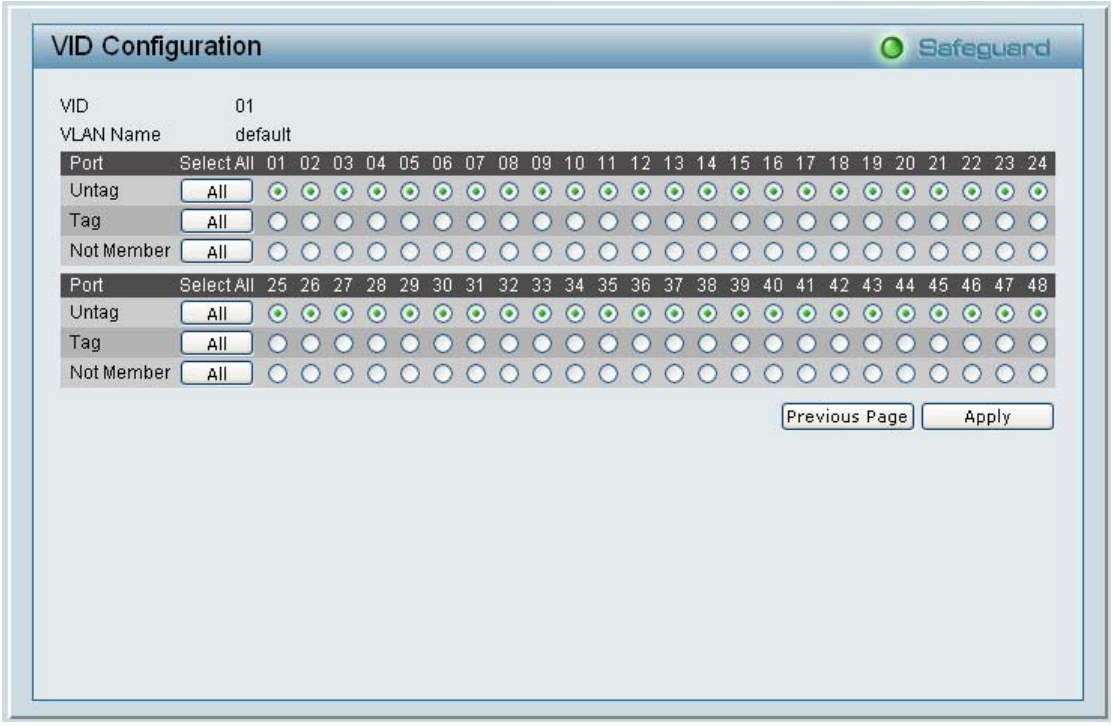


Figure 31 – Configuration > 802.1Q VLAN > VID Assignments

Configuration > Trunking

The Trunking function enables the cascading of two or more ports for a combined larger bandwidth. Up to six Trunk groups may be created, each supporting up to 8 ports. Add a **Trunking Name** and select the ports to be trunked together, and click **Apply** to activate the selected Trunking groups.

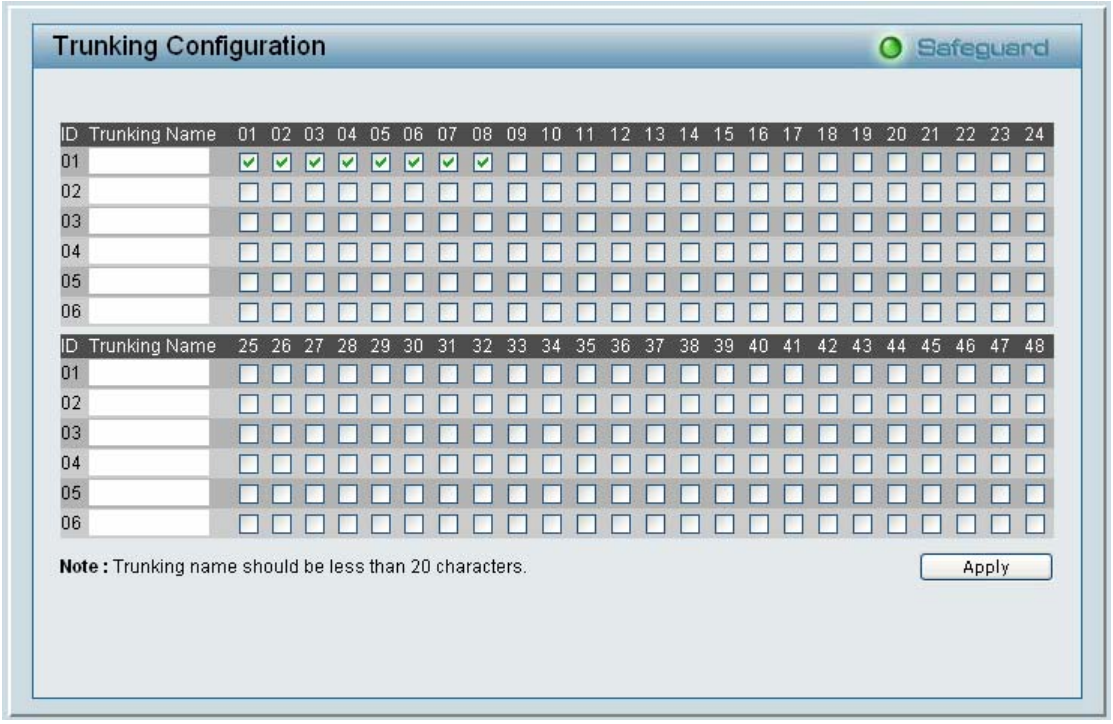


Figure 32 – Configuration > Trunking

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

Configuration > 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.

Please note that IGMP will not alter or route IP multicast packets. To send IP multicast packets across subnetworks a multicast routing protocol will be necessary.

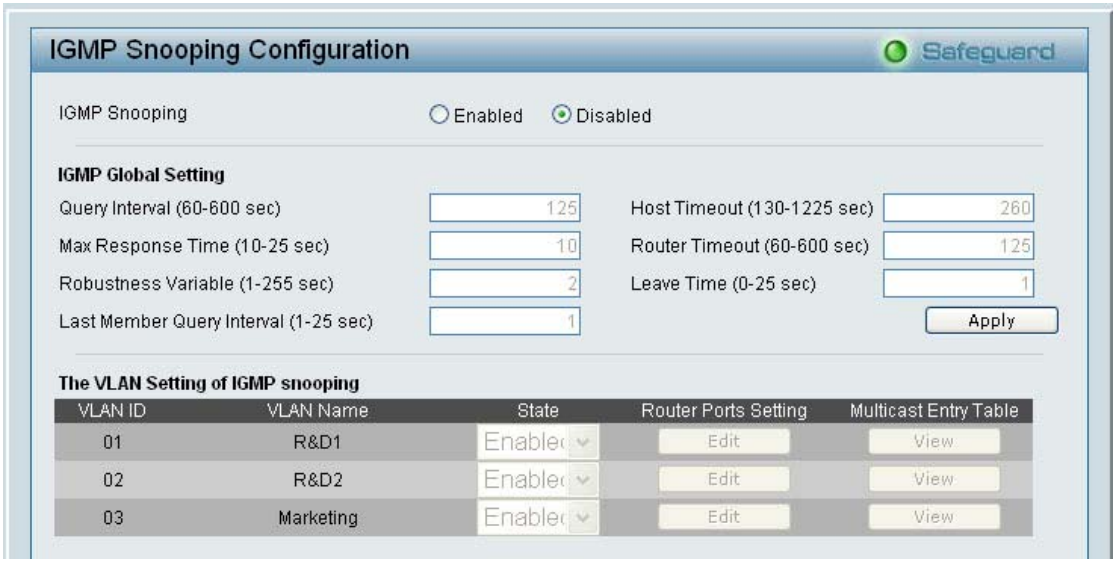


Figure 33 – Configuration > IGMP Snooping Configuration

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

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

Max Response Time (10-25 sec): The Max Response Time specifies the maximum allowed time before sending a responding report. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the routing protocol 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.

Robustness Variable (1-255 sec): The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. The Robustness Variable can not be set zero, and SHOULD NOT be one. Default is 2 seconds.

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

Host Timeout (130-1225 sec): This is the interval after which a learnt host port entry will be purged. For each host port learnt, a 'PortPurgeTimer' runs for 'HostPortPurgeInterval'. This timer will be restarted whenever a report message from host is received over that port. If no report messages are received for 'HostPortPurgeInterval' time, the learnt host entry will be purged from the multicast group. Default is 260 seconds.

Router Timeout (60-600 sec): This is the interval after which a learnt router port entry will be purged. For each router port learnt, a 'RouterPortPurgeTimer' runs for 'RouterPortPurgeInterval'. This timer will be restarted whenever a router control message is received over that port. If no router control messages are received for 'RouterPortPurgeInterval' time, the learnt router port entry will be purged. Default is 125 seconds.

Leave Timer (0-25 sec): This is the interval after which a Leave message is forwarded on a port. When a leave message from a host for a group is received, a group-specific query is sent to the port on which the leave message is received. A timer is started with a time interval equal to IgsLeaveProcessInterval. If a report message is received

before above timer expires, the Leave message is dropped. Otherwise the Leave message is either forwarded to the port. Default is 1 second.

To enable IGMP snooping for a given VLAN, select *Enable* and click on the *Apply* button. Then press the *Edit* button under **Router Port Setting**, and select the ports to be assigned for IGMP snooping for the VLAN, and press **Apply** for changes to take effect.

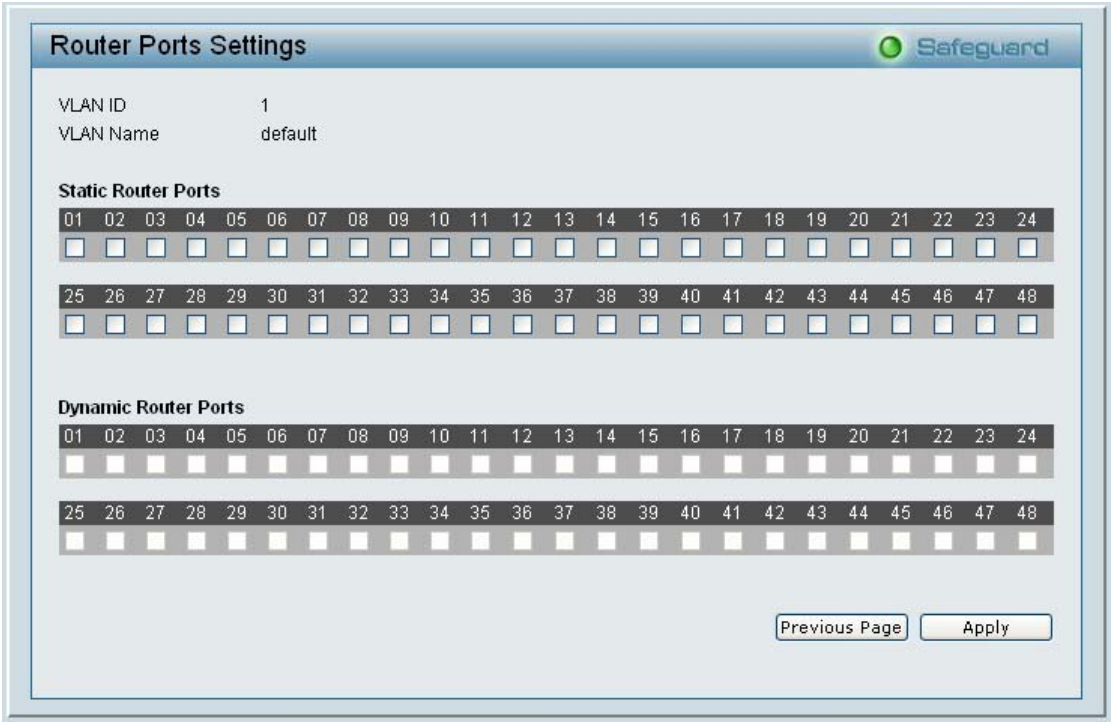


Figure 34 – Configuration > IGMP Router port Settings

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

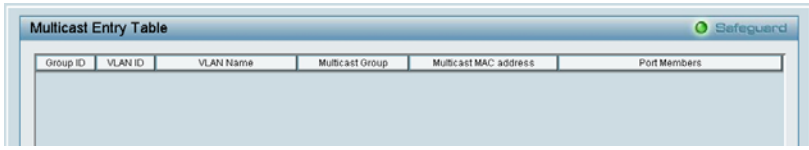


Figure 35 – Configuration > IGMP Multicast Entry Table

Configuration > 802.1D Spanning Tree

802.1D Spanning Tree Protocol (STP) implementation is a backup link(s) between switches, bridges or routers designed to prevent network loops that could cause a broadcast storm. When physical links forming a loop provide redundancy, only a single path will be forwarding frames. If the link fails, STP activates a redundant link automatically.

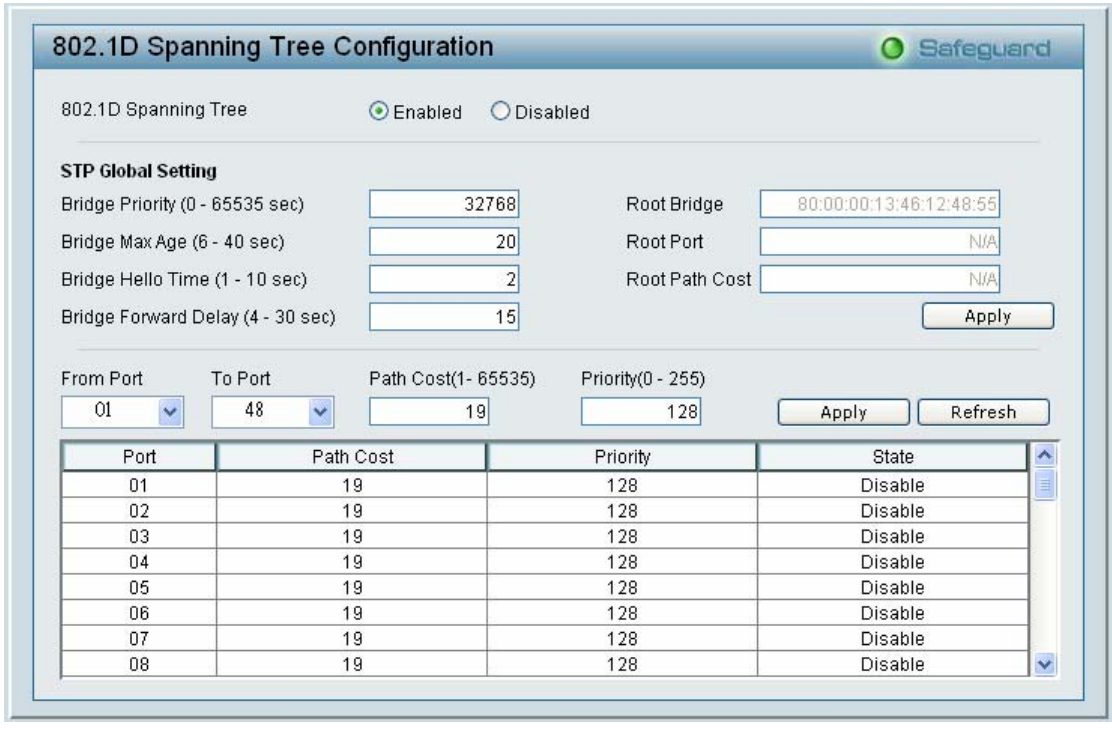


Figure 36 – Configuration > Spanning Tree

By default, Spanning Tree is *Disabled*. If *Enabled,* the Switch will listen for BPDU packets and its accompanying Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A draw-back of 802.1D is this absence of immediate feedback from adjacent bridges.

After *Enabling* STP, setting the STP Global Setting includes the following options:

Bridge Priority: This value between 0 and 65535 specifies the priority for forwarding packets: the lower the value, the higher the priority. The default is 32768.

Bridge Max Age: 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.

Bridge Hello Time: 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. (Max Age has to have a value bigger than Hello Time)

Bridge Forward Delay: 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 port: Displays the root port.

Root Path Cost: Shows the root path cost.

Path Cost: This defines a metric that indicates the relative cost of forwarding packets to specified port list. The lower the number, the greater the probability the port will be chosen to forward packets. The default value is 19.

Path Priority: Select a value between 0 and 255 to specify the priority for a specified port for forwarding packets: the lower the value, the higher the priority. The default is 128.

Configuration > Port Mirroring

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

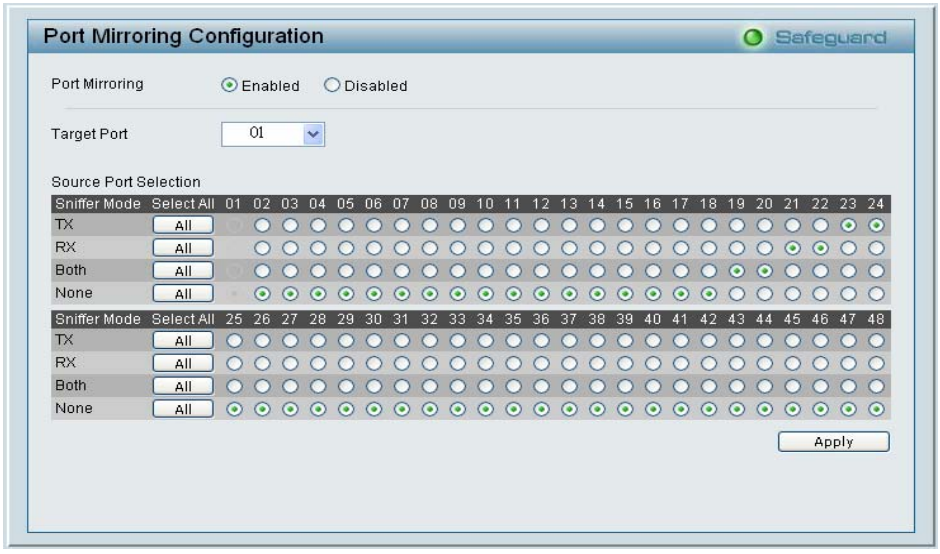


Figure 37 – Configuration > Port Mirroring

Selection options for the Source Ports are as follows:

TX (transmit) mode: Duplicates the data transmitted from the source port and forwards it to the Target Port.

RX (receive) mode: Duplicates the data that gets sent to the source and forwards it to the Target Port.

Both (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.

None: Turns off the mirroring of the port.

QoS > 802.1p Default Priority

This feature displays the status Quality of Service priority levels of each port, and for packets that are untagged, the switch will assign the priority in the tag depending on your configuration.

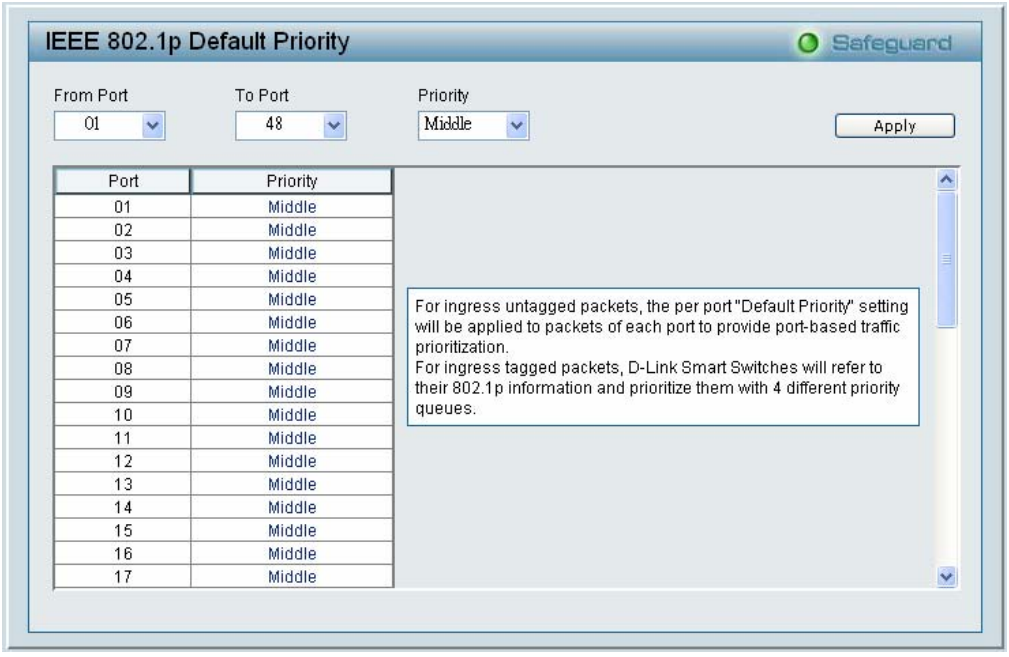


Figure 38 – QoS > 802.1p Default Priority

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. By default this is *Enabled*.

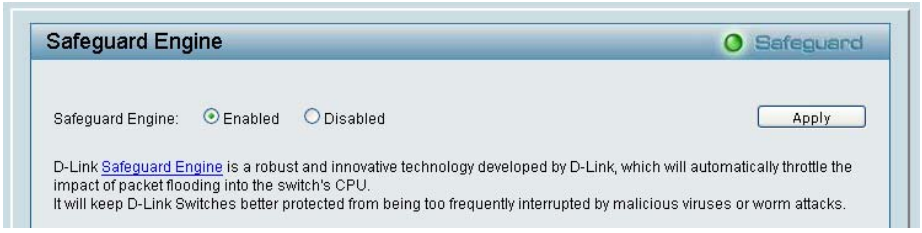


Figure 39 – Security > Safeguard Engine

Security > Broadcast Storm Control

The Broadcast Storm Control feature provides the ability to control the receive rate of broadcasted packets. If *Enabled* (default is *Disabled*), threshold settings of *8,000 ~ 4,096,000* bytes per second can be assigned. Press **Apply** for the settings to take effect.

Figure 40 – Security > Broadcast Storm Control

Security > 802.1X Setting

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.

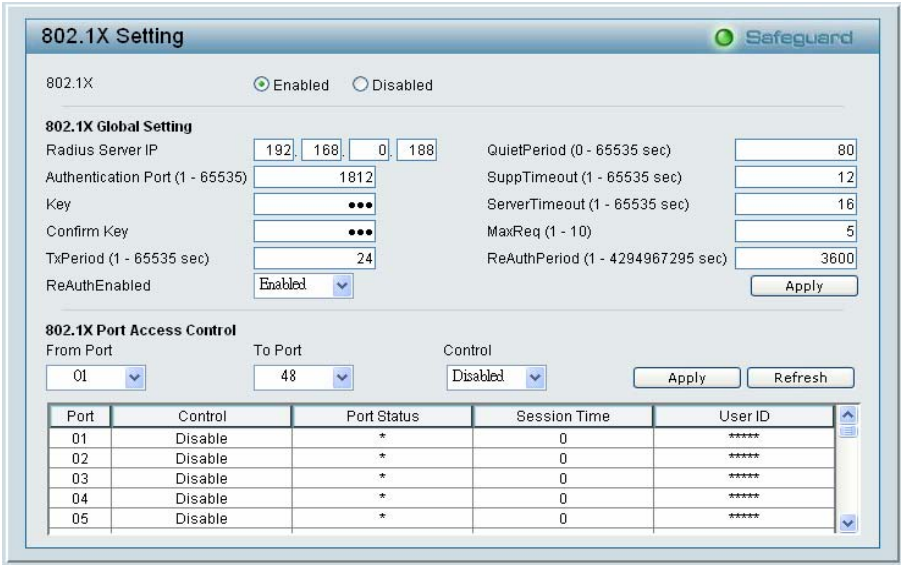


Figure 41 – Security > 802.1X Setting

By default, 802.1X is *Disabled*. To use EAP for security, select *Enabled* and set the 802.1X **Global Settings** for the Radius Server and applicable authentication information.

Authentication Port: sets primary port for security monitoring. Default is 1812.

Key: Masked password matching the Radius Server Key.

Confirm Key: Enter the Key a second time for confirmation.

TxPeriod: Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. Default is 24 seconds.

ReAuthEnabled: This *Enables* or *Disables* the periodic ReAuthentication control. When the 802.1X function is *Enabled*, the ReAuthEnabled function is by default also *Enabled*.

QuietPeriod: Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is 80 seconds

SuppTimeout: Sets the switch-to-client retransmission time for the EAP-request frame. Default is 12 seconds.

ServerTimeout: Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is 16 seconds.

MaxReq: This parameter specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. Default is 5 times.

ReAuthPeriod: This command affects the behavior of the switch only if periodic re-authentication is enabled. Default is 3600.

To establish 802.1X port-specific assignments, select the **From** and **To Ports** and select *Enable*.

Security > Mac Address Table > Static Mac

This page provides two distinct features. The top table provides the ability to turn off auto learning Mac address if a port isn't connected to an uplink Switch (i.e. DHCP Server). By default, this feature is *OFF* (disabled). The Macs listed on this table may only connect from corresponding ports and VIDs, in order to protect the network from illegal Macs.

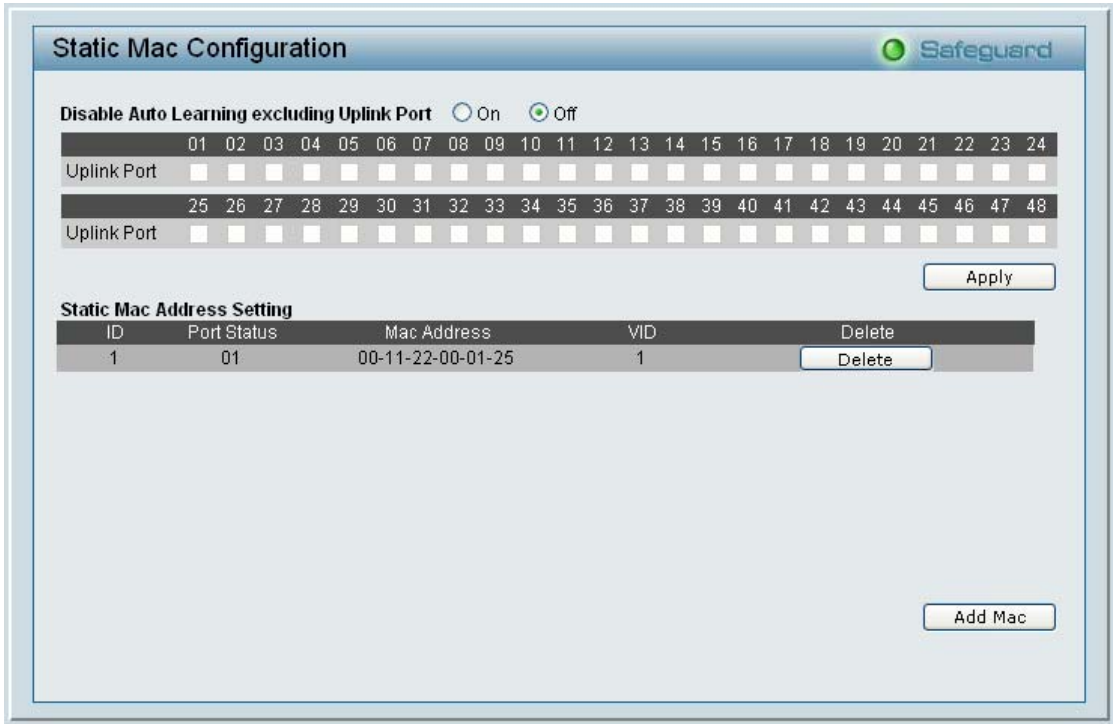


Figure 42 – Security > Static Mac Address

To initiate the removal of auto-learning for any of the uplink ports, press *On* to enable this feature, and select the port(s) for auto learning to be disabled.

The **Static Mac Address Setting** table displays the static Mac addresses connected, as well as the VID. Press **Delete** to remove a device. To add a new Mac address assignment, press **Add Mac**, then select the assigned Port number, enter both the Mac Address and VID and press **Apply**.

Security > Mac Address Table > Dynamic Forwarding Table

For each port, this table displays the Mac address of each packet passing through the Switch. To add a Mac address to the Static Mac Address List, click the **Add** checkbox associated with the identified packet.

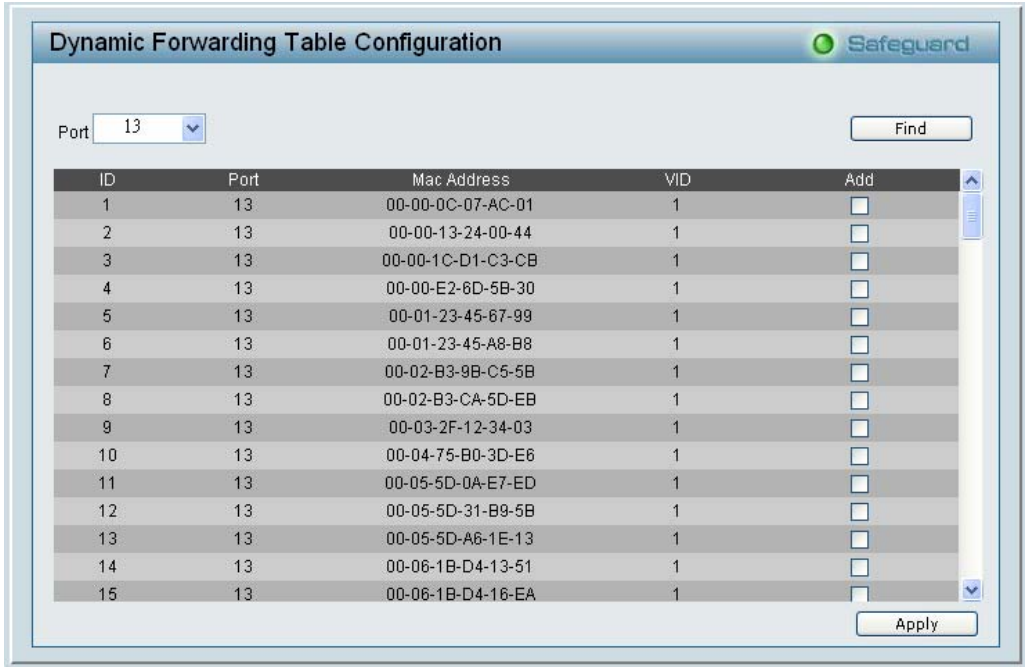


Figure 43 – Security > Dynamic Forwarding Table

Monitoring > Statistics

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

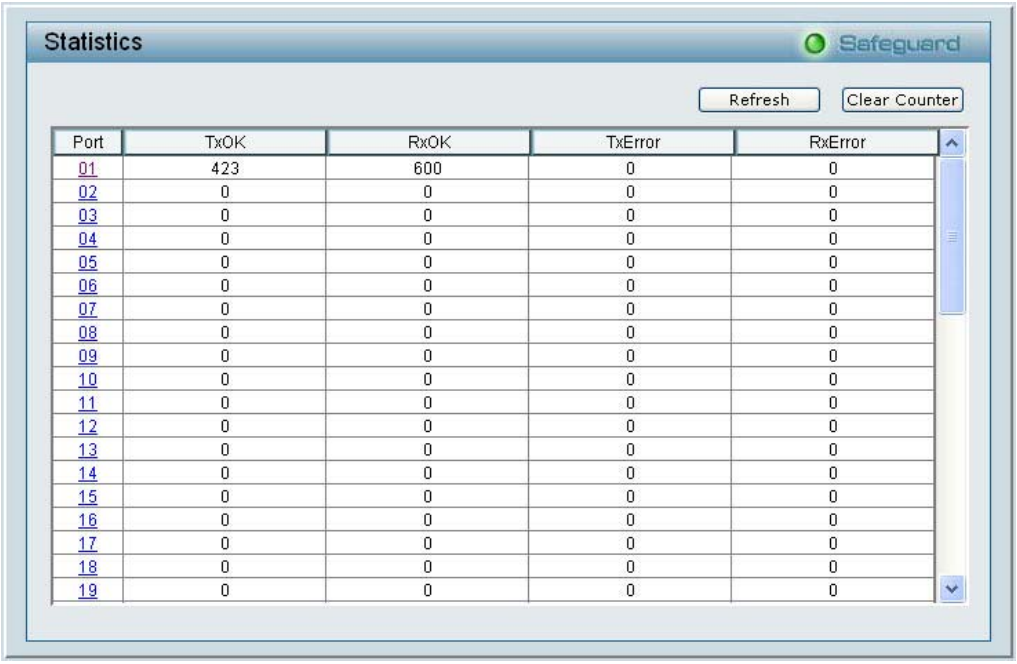


Figure 44 – Monitoring > Statistics

Refresh: To renew the details collected and displayed.

Clear Counter: To reset the details displayed.

TxOK: Number of packets transmitted successfully.

RxOK: Number of packets received successfully.

TxError: Number of transmitted packets resulting in error.

RxError: Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked Port numbers for details.

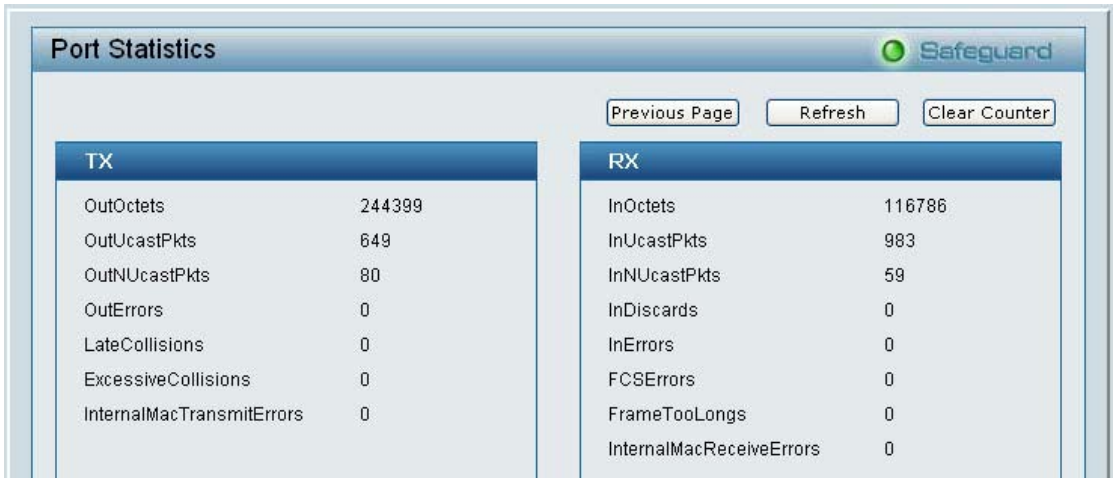


Figure 45 – Monitoring > Port Statistics