DES-2108

8-port 10/100

Fast Ethernet Switch

User's Guide

D-Link®

RECYCLABLE

2007/6/13

CE Mark Warning

This is a Class B 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 B. 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 B. 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 B. 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 B. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

TABLE OF CONTENTS

ABOUT THIS GUIDE

This user's guide will show you how to install your DES-2108, and how to connect it to your network.

Terms

For simplicity, this documentation uses the terms "Switch" (first letter upper case) to refer to the DES-2108, and "switch" (first letter lower case) to refer to all Ethernet switches, including the DES-2108.

Overview of this User's Guide

Introduction	Describes the Switch and its features.
Unpacking and Setup	Helps you get started with the basic installation of the Switch.
Identifying External Components	Describes the front panel, rear panel, and LED indicators of the Switch.
Configuration the Switch	Show how to configure the management functions of the Switch.
Technical Specification	Lists the technical specifications of the Switch.

INTRODUCTION

This section describes the features of the DES-2108, as well as giving some background information about Fast Ethernet and Switching technology.

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 are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from 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 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Switching Technology

Another key development pushing the limits of Ethernet technology is in the field 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 making it possible for a local area network to be divided into different segments, which are not competing with each other for network transmission capacity, and therefore decreasing the load on each segment. The Switch acts as a high-speed selective bridge between the individual segments. Traffic

that needs to go from one segment to another (from one port to another) is automatically forwarded by the Switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards. For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "four-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205-meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks. Switching LAN technology is a marked improvement over the previous generation of network bridges, which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. Today's switches are an ideal solution to most kinds of local area network congestion problems.

Switch Description

The DES-2108 is equipped with unshielded twisted-pair (UTP) cable ports providing dedicated 10 or 100 Mbps bandwidth. The Switch has 8 UTP ports and Auto MDI-X/MDI-II convertible ports that can be used for up-linking to another switch. These ports can be used for connecting PCs, printers, servers, hubs, routers, switches and other networking devices. The dual speed ports use standard twisted-pair cabling and are ideal for segmenting networks into small, connected sub-networks for superior performance. Each 10/100 port can support up to 200 Mbps of throughput in full-duplex mode. This stand-alone Switch enables the network to use some of the most demanding multimedia and imaging applications concurrently with other user

applications without creating bottlenecks. The built-in Light-Management engine can be configure the Switch's settings for priority queuing, VLANs, and port monitoring, and port speed.

Features

The DES-2108 was designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously.

The Switch features include:

- IEEE 802.3 10BASE-T compliant.
- IEEE 802.3u 100BASE-TX compliant.
- IEEE 802.3x flow control in full duplex mode.
- IEEE 802.1Q VLAN & Port_based VLAN.
- IEEE 802.1D Spanning Tree.
- Port_based QoS.
- System Log Support.
- High performance switching engine performs forwarding and filtering at full wire speed.
- Full- & Half- duplex operation for both of 10Mbps and 100Mbps and connections. Full duplex allows the switch port to simultaneously transmit and receive data. It only works with connections to full-duplex-capable end stations and switches.
- Non-blocking store and forward switching scheme capability to support rate adaptation and protocol conversion.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.
- Support port-based enable and disable.
- Address table: Supports up to 4K MAC addresses per device.

- Supports a packet buffer of up to 256 Kbytes.
- IGMP Snooping support.
- SNMP support.
- Port Mirror support.
- MIB support for:
- RFC1213 MIB II.
- Private MIB.

Ports

Eight (8) 10/100Mbps 100BASE-TX (Auto MDI-X/MDI-II) ports for connecting to end stations, servers, hubs and other networking devices. All UTP ports can auto-negotiate between 10Mbps and 100Mbps, half-duplex and full duplex, and flow control.

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Switch.

Unpacking

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

One DES-2108 Fast Ethernet Switch

Four rubber feet with adhesive backing

One AC power adapter

Mounting kit

CD-ROM (Including this User's Guide and Utility)

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

Setup

The setup of the Switch can be performed using the following steps:

- The power outlet should be within 1.82 meters (6 feet) of the device.
- Visually inspect the DC power jack and make sure that it is fully secured to the power adapter.
- Do not cover the ventilation holes on the sides of the Switch, and make sure there is adequate ventilation around it.
- Do not place heavy objects on the switch.

Mounting the Switch on a Wall

The DES-2108 can also be mounted on a wall. Two mounting slots are provided on the bottom of the switch for this purpose. Please make sure that the front panel is exposed in order to view the LEDs. Please refer to the illustration below.

A.) Mounting on a cement wall

1. Mount the Nylon screw anchors into a cement wall.

2. Drive the T3 x 15L screws into the Nylon screw anchors.

3. Hook the mounting holes of the switch back on the screws; you have completed the wall-mount.

B.) Mounting on a wood wall

1. Drive the T3 x 15 L screws into the wood wall.

2. Hook the mounting holes of the switch back on the screws; you have completed the wall-mount.

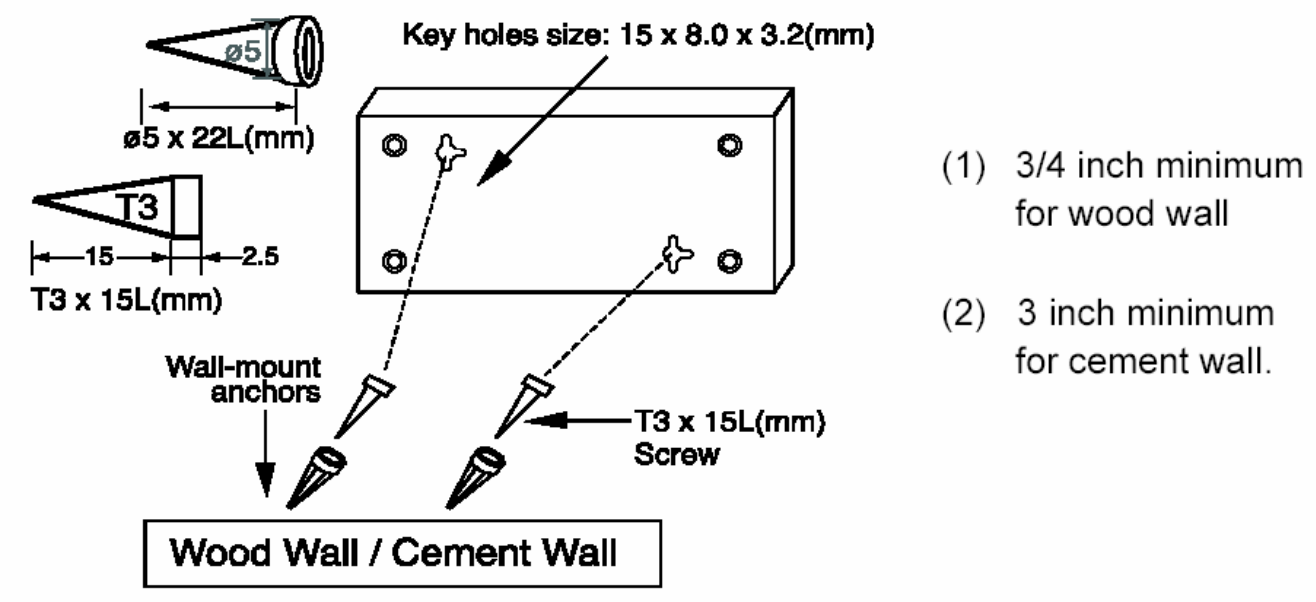

Figure 1. Mounting on a Wall

Power on

The DES-2108 can be used with AC power sources 100 - 240 VAC, 50 - 60 Hz. The Switch's power adapter will adjust to the local power source automatically.

Plug one end of the DC output into the power jack of the Switch and the other end into the local power source outlet.

IDENTIFYING EXTERNAL COMPONENTS

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

Front Panel Components

The front panel of the Switch consists of Power, CPU and port LED indicators.

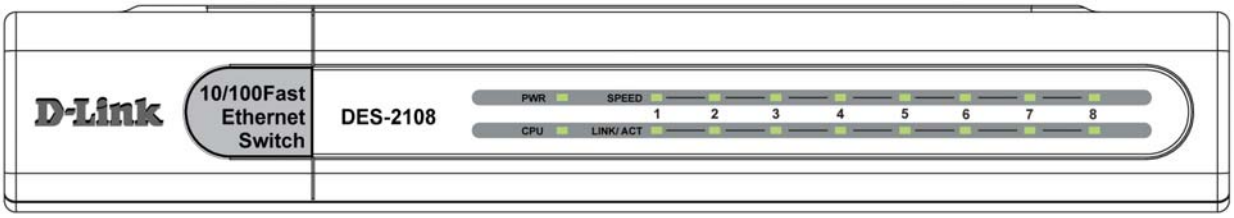

Figure 2. Front panel view

LED Indicators: Comprehensive LED indicators that display the conditions of the Switch and status of the network. A description of these LED indicators follows (see *LED Indicators*).

Rear Panel

The rear panel of the Switch contains an DC power phone jack, eight (8) 10/100Mbps Fast Ethernet ports and Reset button.

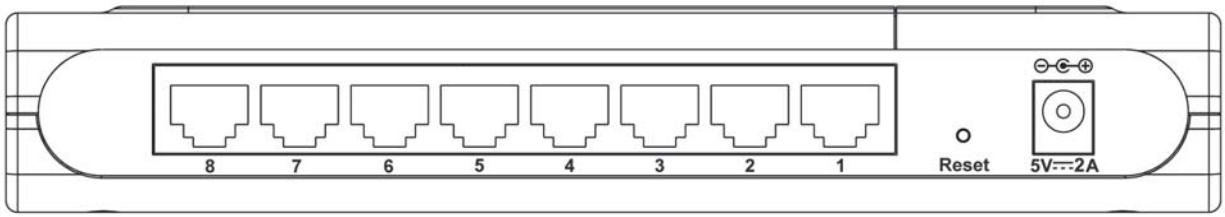

Figure 3. Rear panel view

RJ-45: Eight 10/100Mbps Fast Ethernet ports.

Reset: The Reset button is to reset all the setting back to the factory default.

Note: Be sure that you recorded the setting of your device, else all the setting will be erased when pressing the "Reset" button.

DC Power Jack: Power is supplied through an external DC power adapter. Check the technical specification section for information about the DC power input voltage.

DES-2108 does not include a power button, plugging its power adapter into a power outlet will immediately power it on.

LED Indicators

The LED indicators of the Switch include Power, CPU and Port Status LEDs. The following shows the LED indicators for the Switch along with an explanation of each indicator.

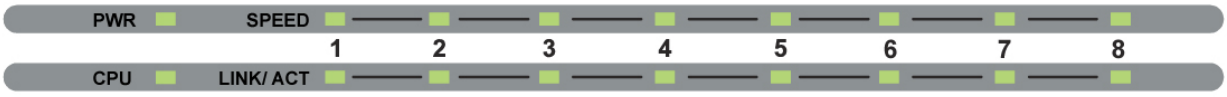

Figure 4. LED indicators

Power and CPU LEDs

Power

On	**:**	This LED will light green after the Switch is powered on to indicate the ready state of the device.
Off	**:**	When the switch powered off or the power adapter has improper connection.

CPU

Blinking	**:**	When the CPU is working, the CPU LED is blinking.
On/Off	**:**	The CPU is not working.

10/100M Fast Ethernet Ports Status LEDs

Link/Act

On	**:**	When the Link/Act LED lights 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.

100M

On	**:**	When the 100Mbps LED lights on, the respective port is connected to a 100Mbps Fast Ethernet network.
Off	**:**	When the respective port is connected to a 10Mbps Ethernet network

INTRODUCTION TO SWITCH MANAGEMENT

Management Options

Web Management Utility

Web-based Management Interface

Command Line Interface (CLI)

SNMP-Based Management Managing

Management Options

This system may be managed in-band using TCP/IP Telnet protocol and web-based management, accessible through a web browser.

SmartConsole Utility

With the SmartConsole Utility, you can easily discover all the Web Management Switch, assign the IP Address, change the password and upgrade to new firmware.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, display statistics using a web browser, such as Netscape Navigator (version 6.2 and higher) or Microsoft® Internet Explorer (version 5.0).

Command Line Interface (CLI)

The Switch supports a Command Line Interface (CLI) that allows the user to connect to the Switch’s management agent using the TCP/IP Telnet protocol.

SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

CONFIGURATION THE SWITCH

Through the Web Browser, Telnet and SNMP you can configure the Switch such as Port setting, VLAN, QoS, SNMP, Spanning Tree… etc.

SmartConsole Utility

With the included Web Management Utility, you can easily discover all the Web Management Switch, assign the IP Address, change the password and upgrade to new firmware.

Installing SmartConsole Utility

The following gives instructions guiding you through the installations of the SmartConsole utility.

Insert the Utility CD in the CD-Rom Drive.

From the **Start** menu on the Windows desktop, choose **Run**.

In the **Run** dialog box, type D:\SmartConsole Utility\setup.exe (D:\ depends where your CD-Rom drive is located) and click **OK**.

Follow the on-screen instructions to install the utility.

Upon completion, go to **Program Files -> SmartConsole_Utility** and execute the SmartConsole utility. (Figure 5.)

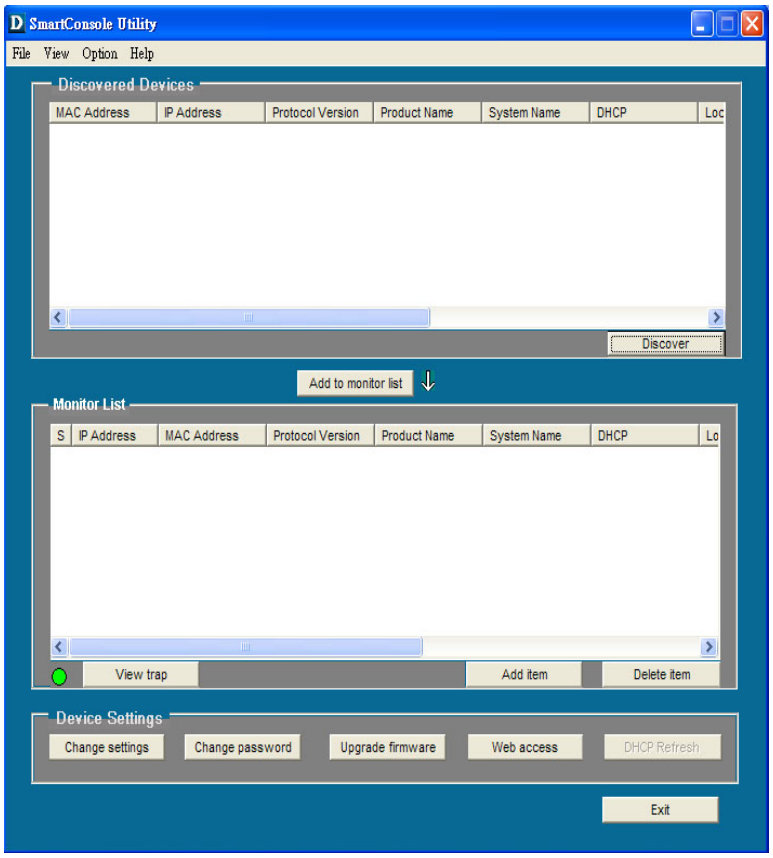

Figure 5. SmartConsole Utility

The SmartConsole Utility was divided into four parts, ***Discovery List, Monitor List, Device Setting*** and ***Toolbar function***, for details instruction, follow the below section.

Discovered Devices

This is the list where you can discover all the Web management devices in the entire network.

By pressing the ***"Discover"*** button, you can list all the Web Management devices in the discovery list.

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

System word definitions in the Discovery List:

- ***MAC Address:*** Shows the device MAC Address.

- ***IP Address:*** Shows the current IP address of the device.
- ***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:*** Shows whether the switch's DHCP is Enabled or Disabled.
- ***Location:*** Shows where the device is located.
- ***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 time that the switch will be discovered in the SmartConsole Utility List.

Monitor List

All the Web Smart Device in the Monitor List can be monitored; you can also receive the trap and show the status of the device.

System word definitions in the Monitor List:

- ***S:*** Shows the system symbol of the Web-Smart device,  represents the device system is down.
- ***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:*** Shows whether the switch's DHCP is Enabled or Disabled.
- ***Location:*** Shows where the device is located.
- ***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 time that the switch will be discovered in the SmartConsole Utility List.
-

View Trap: The Trap function can receive the events that happen from the Web Management Switch in the Monitor List.

There is a light indicator behind the ***"View Trap"*** button, when the light indicates in green, it means that there is no trap transmitted, and else when it indicates in red, it means that there is new trap transmitted, this is to remind us to view the trap. (Figure 6.)

Figure 6.

When the ***"View Trap"*** button is clicked, a Trap Information window will pop out, it will show the trap information including the Symbol, Time, Device IP and the Event occurred. (Figure 7. Trap information)

The symbol "" represents the trap signal arise, this symbol will disappear after you review and click on the event record.

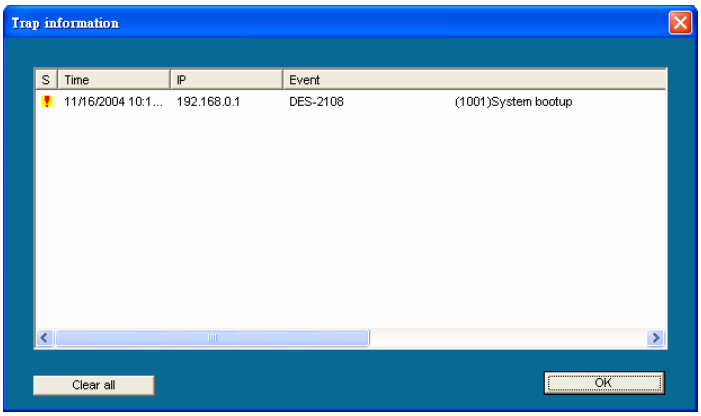

Figure 7. Trap information

Note: In order to receive Trap information, the switch has to be configured with Trap IP and Trap Events in Web browsers, which are available in the Trap Setting Menu (See the appropriate sections of this Guide for details).

Add Item: To add a device to the Monitor List manually, enter the IP Address of the device that you want to monitor.

Delete Item: To delete the device in the Monitor List.

Device Setting

You can set the device by using the function key in the Device Setting Dialog box.

Change Settings:

In Change Settings, you can set the IP Address, Subnet Mask, Gateway, Set Trap to (Trap IP Address), System name, Location, Password, Group Interval and DHCP setting.

In factory default, the IP address of the DES-2108 will be automatically assigned from DHCP server *(DHCP enabled)*. If your network has no DHCP server, the DES-2108 will fail to get IP address, and the IP address of DES-2108 will be assigned to default IP address of 192.168.0.1 and netmask is 255.255.255.0.

Select the device in the Discovery List or Monitor List and press the ***"Change settings"*** button, then the Configuration Setting window will pop up as shown in Figure 8. After filling in the data that you want to be changed, you must input the password and press the "Set" to process the data change.

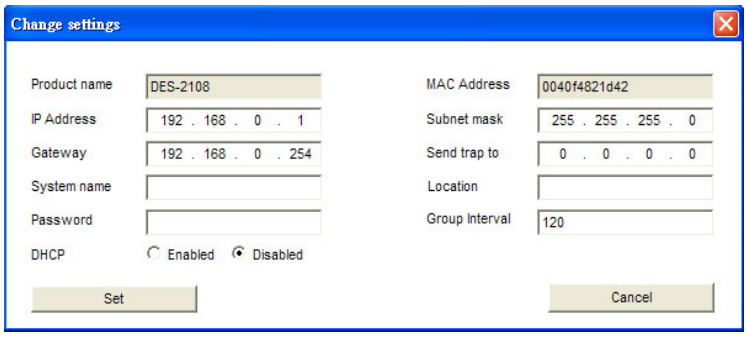

Figure 8. Change settings

Change password:

Used to change the password when deemed necessary. Fill in the desired password and press the ***"Set"*** button to change the password.

Figure 9. Change password

Upgrade firmware:

When the device has a new function, there will be a new firmware. Use this function to update.

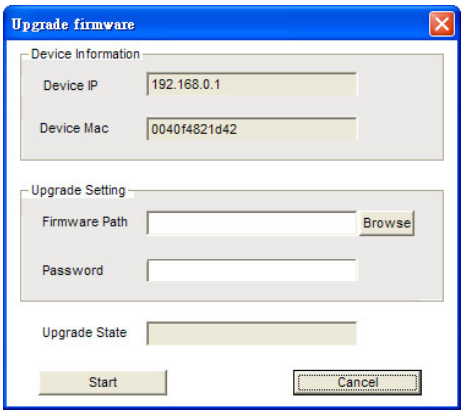

Figure 10. Upgrade firmware

Web Access:

Double click the device in the Monitor List or select a device in the Monitor List and press this ***"Web Access"*** button to access the device in Web browser.

Toolbar

The toolbar in the Web Management Utility have four main tabs: File, View, Option and Help.

File TAB:

In the ***"File TAB"***, there are the options Monitor Save, Monitor Save As, Monitor Load and Exit:

Monitor Save: To record the setting of the Monitor List to the default folder, when you open the Web Management Utility next time, it will automatically load the default recorded setting.

Monitor Save As: To record the setting of the Monitor List in the appointed filename and file path.

Monitor Load: To manually load the setting file of the Monitor List.

Exit: To exit the Web Management Utility.

View TAB

In the ***"View TAB"***, there are view log and clear log function, these functions will show you the trap settings:

View Log: To show the event of the Web Management Utility and the device.

Clear Log: To clear the log.

Option TAB:

In the ***"Option TAB"***, there are the Refresh Time function and the Group Interval function. The Refresh Time function helps to refresh the time for monitoring the device. Choose from ***15 secs, 30 secs, 1 min, 2 min and 5 min*** to select the time for monitoring.

Group Interval establishes the intervals (in seconds) that the Switch will be discovered in the SmartConsole Discovered List.

Help TAB

In the ***"Help TAB"***, there is the About function, it will show the current version of the Web Management Utility.

Configuring the Switch using Web Browsers

All software functions of the DES-2108 can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Netscape Navigator or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol. The Web-based management module and the Console program (Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

This section indicates how to manage, control and monitor the Switch via Web Browsers. The functions available for configuration are listed below:

- System Settings
- Trap Settings
- Port Settings
- SNMP Settings
- Password Access Control
- Syslog
- SNTP Settings
- 802.1Q VLAN

- Trunk
- IGMP Snooping
- 802.1D Spanning Tree
- Port Mirroring
- 802.1d Default Priority
- Trusted Host
- Storm Control
- Bandwidth Control
- 802.1x Settings
- Static MAC
- Dynamic Forwarding Table
- Statistics
-

Login to Web Manager

Before you configure this device, note that when the Web Smart Switch is configured through an Ethernet connection, make sure the manager PC must be set on same the **IP network**. For example, when the default IP address of the Web Smart Switch is ***192.168.0.1***, then the manager PC should be set at 192.168.0.x (where x is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Open the web browser program and enter the IP address ***http://192.168.0.1*** (the factory-default IP address setting) in the address location.

Figure 11.

Or you may access the above address through the Web Management Utility, this way you do not need to remember the IP Address. Select the device shown in the Monitor List of the Web Management Utility to configure the device on the Web Browser.

When the following dialog page appears, enter the default password ***"admin"*** and press OK to enter the main configuration window.

Figure 12.

After entering the password, you will see the main page as shown below.

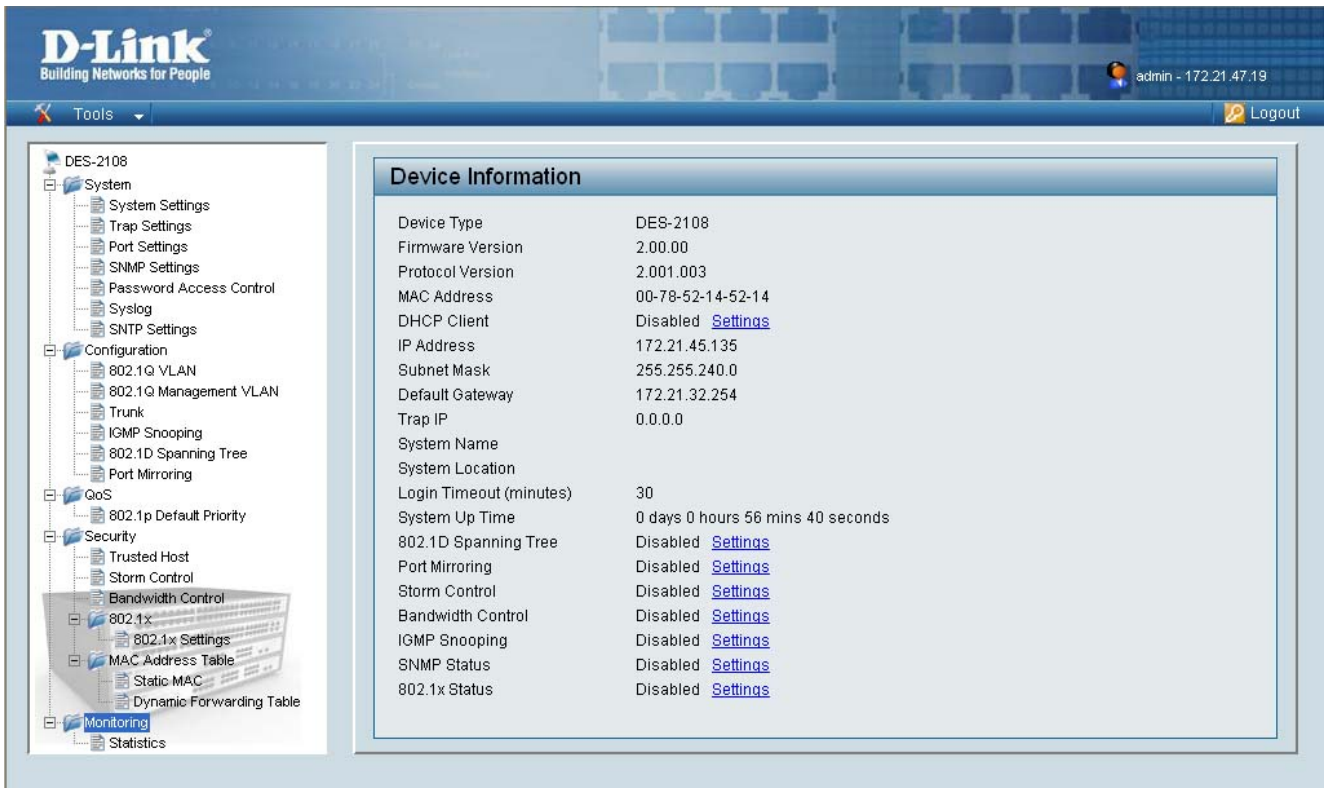

Figure 13. Device Status

Setup Menu

When the main page appears, find the ***Setup menu*** in the left side of the screen (Figure 4). Click on the setup item that you want to configure. There are twenty options: *System Settings*, *Trap Settings*, *Port Settings*, *SNMP Settings*, *Password Access Control*, *Syslog*, *SNTP Settings*, *802.1Q VLAN*, *802.1Q Management VLAN*, *Trunk*, *IGMP Snooping*, *802.1D Spanning Tree*, *Port Mirroring*, *802.1p Default Priority*, *Trusted Host*, *Storm Control*, *Bandwidth Control*, *802.1x Settings*, *Static MAC*, *Dynamic Forwarding Table* and *Statistics.*

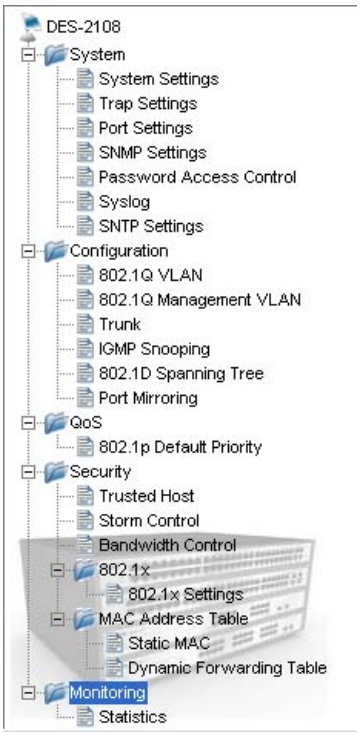

Figure 14. Setup menu

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 **(Dynamic Host Configuration Protocol).**

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 be more easily 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** shows the time period (in seconds) that SmartConsole will check for the switch's presence. Entering 0 disables this function.

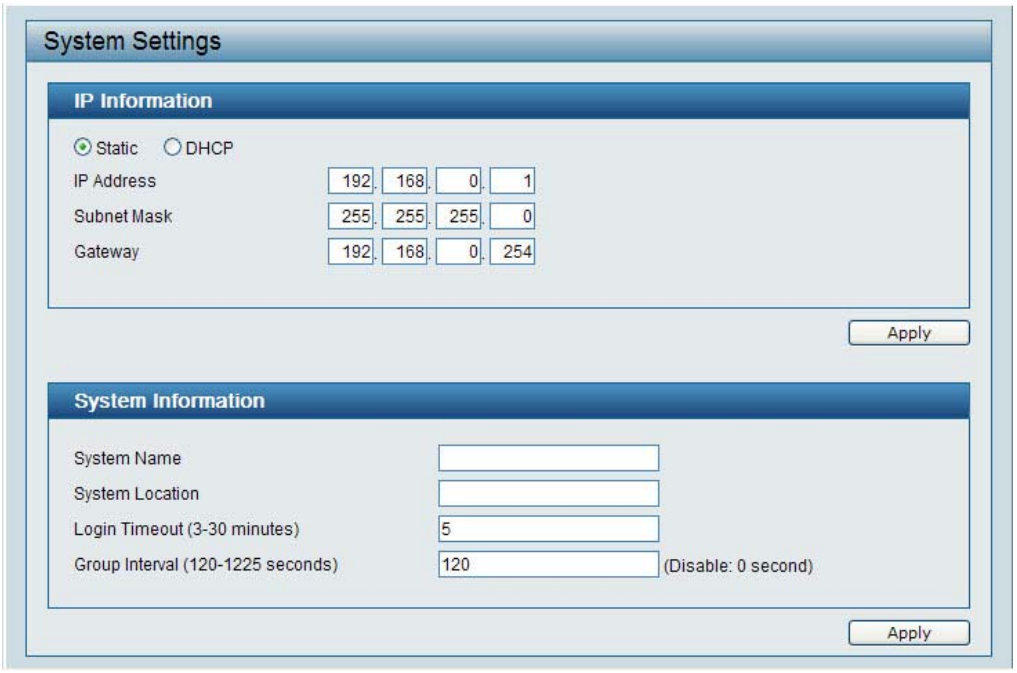

Figure 15. System > System Setting

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.

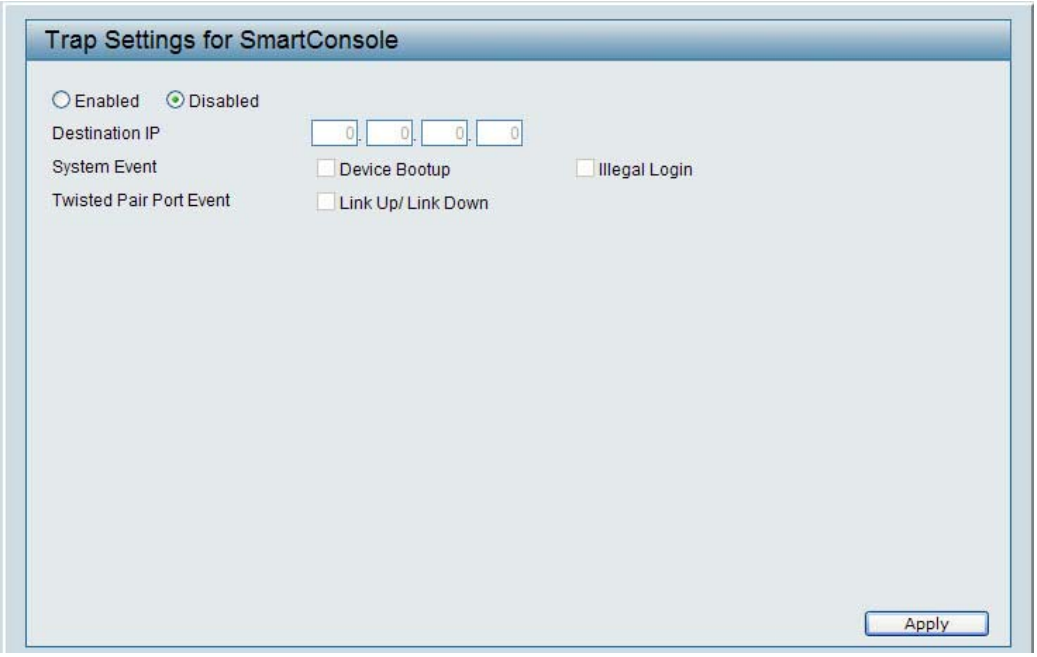

Figure 16. System > Trap Setting

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.

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** and **Flow Control** 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.

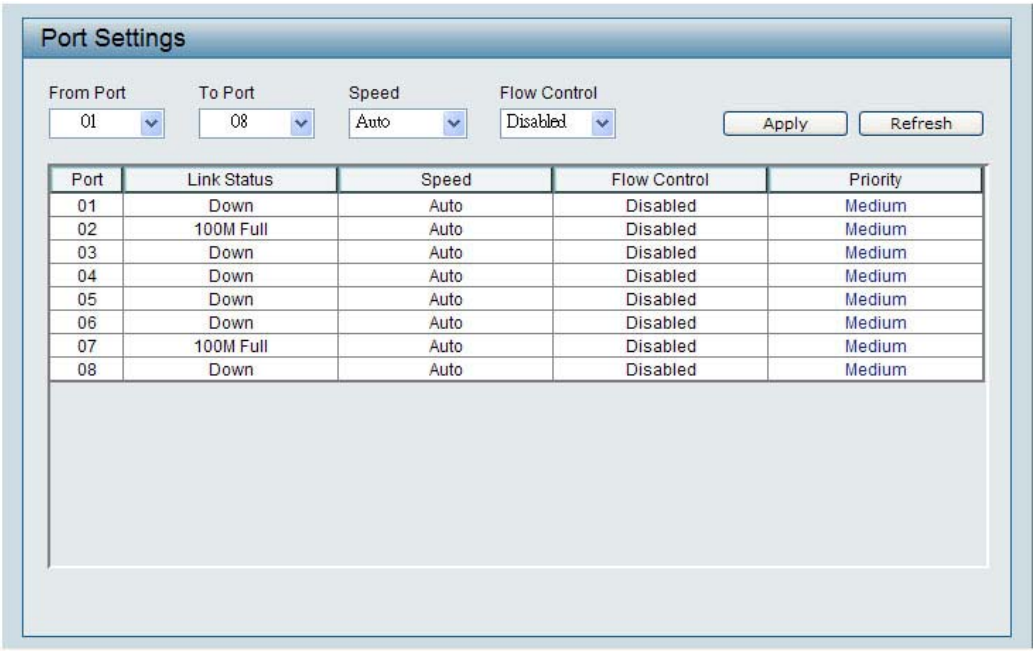

Figure 17. System > Port Setting

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

Speed: 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.

Flow Control: Enables or Disables Flow Control. The default setting is *Disabled*.

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*

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 Settings: 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).

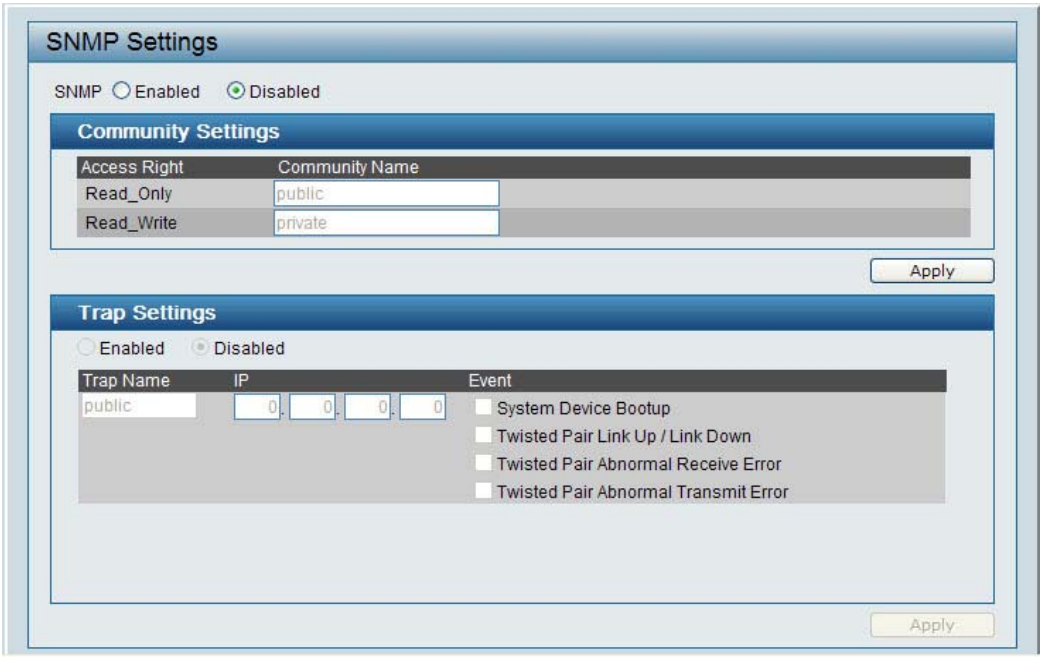

Figure 18. System > SNMP Setting

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, 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.

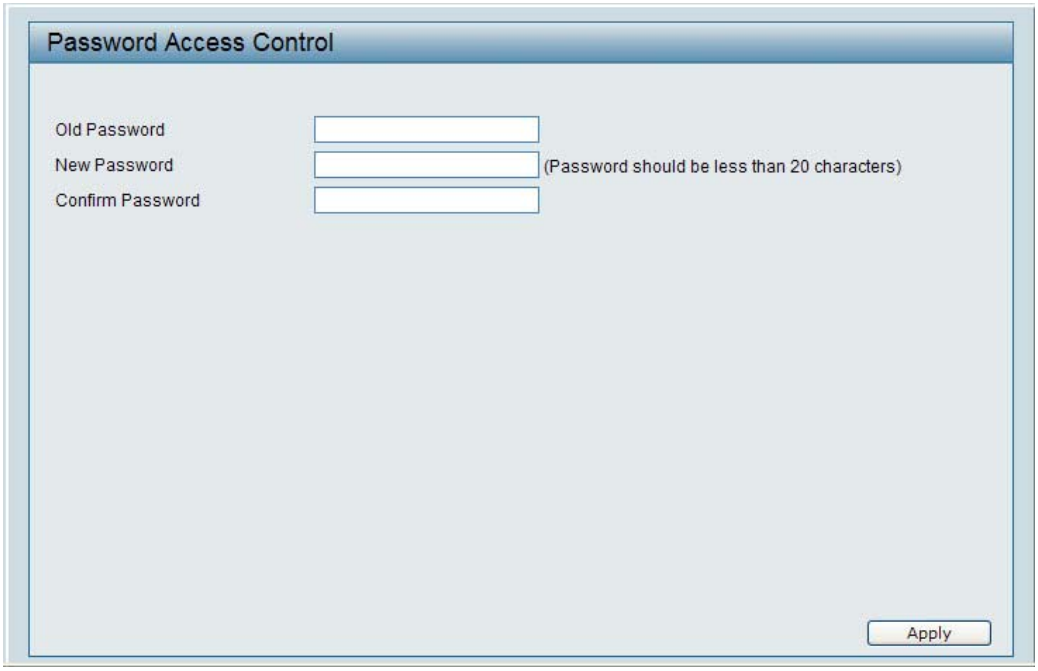

Figure 19. System > Password Access Control

System > Syslog

The Switch can send Syslog messages to designated servers using the System Log Server.

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

To add a new Syslog Server, press Add Syslog Server and type in the desired IP Address. The default Port is *514*.

Some operating processes have been assigned Facility values. Processes that have not been explicitly assigned a value may use any of the “local” facilities.

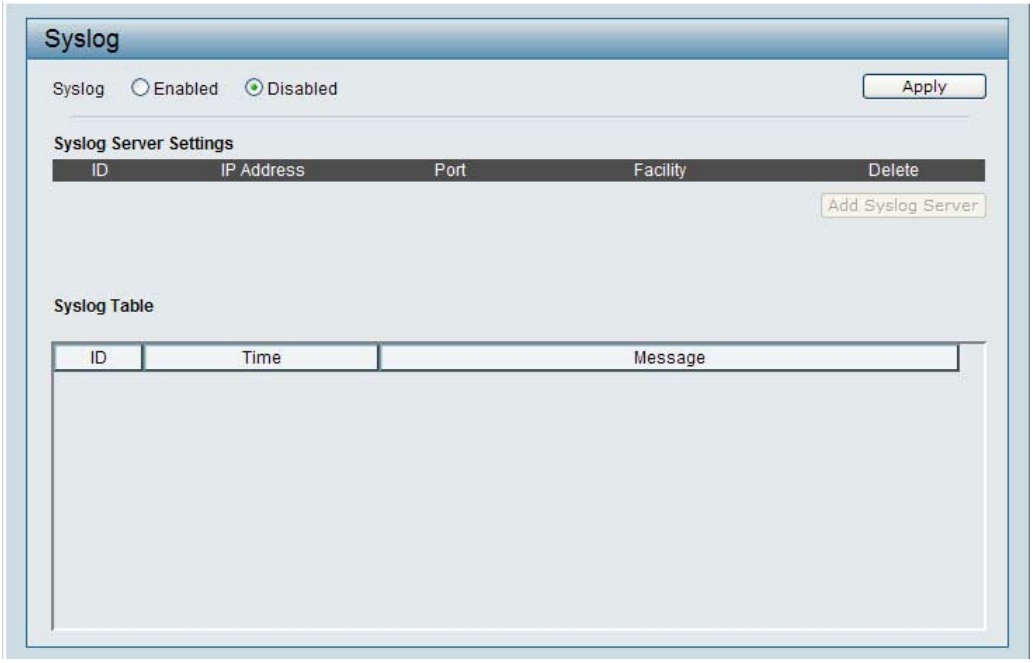

Figure 20. System > Syslog

System > SNTP Settings

Enabled / Disabled: Default setting is *Disabled*. Click *Enable*, then *Apply*, to configure the SNTP Settings.

Daylight Saving Time State: Default setting is *Disabled*. Click *Enable* to configure the below time parameters.

To add a new SNTP Server, press Add SNTP Server and enter the desired IP address, then press Apply.

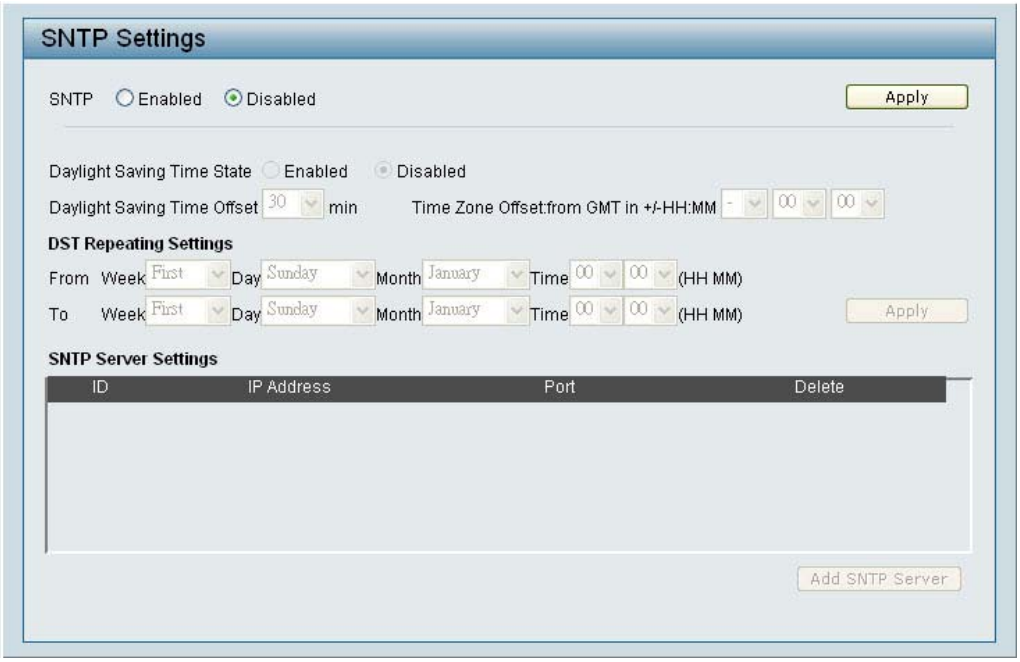

Figure 21. System > SNTP Settings

Configuration > 802.1Q VLAN

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

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

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 01, named “default”, and all 8 ports as “Untagged” (see Figure 24).

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 08 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.

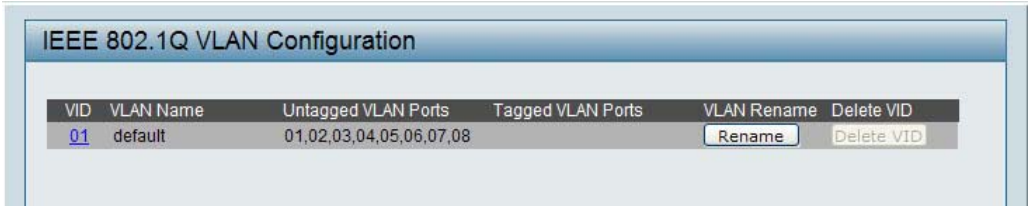

Figure 22. Configuration > 802.1Q VLAN > Default Setting

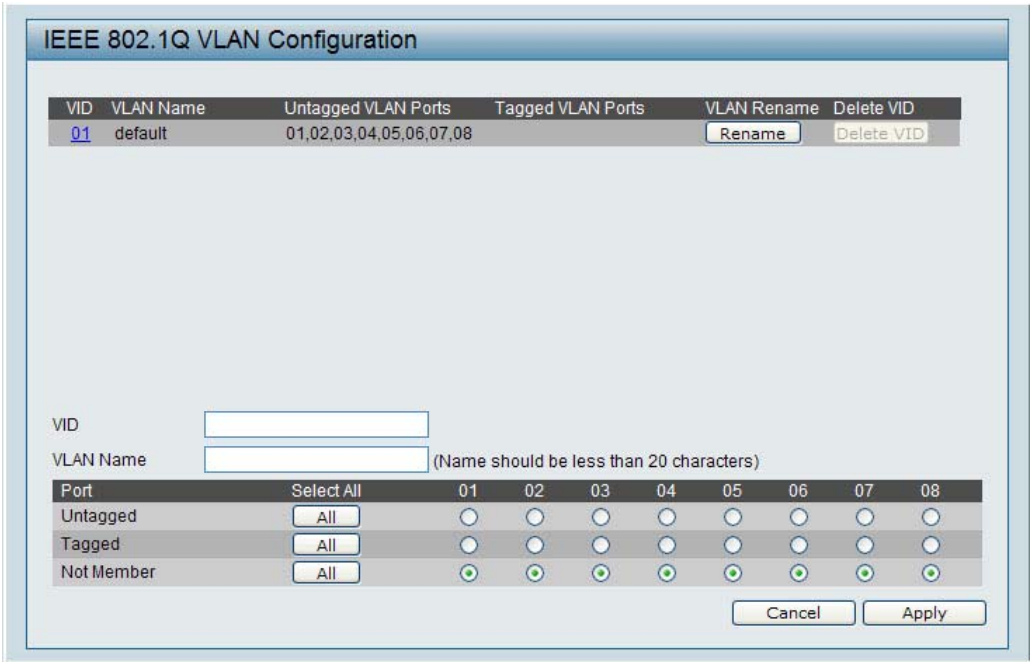

Figure 23. Configuration > 802.1Q VLAN > Add VID

To make changes to an existing VID, click on the number under VID. By pressing the **All** button you can mark all the ports as Untag, Tag, or Not Member.

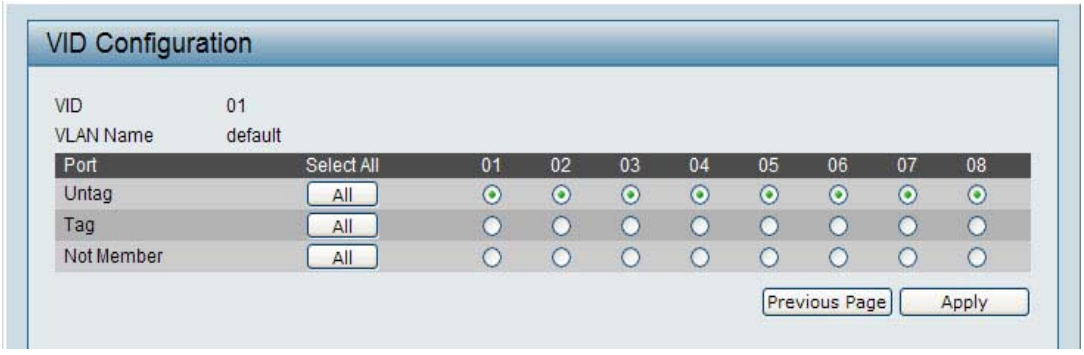

Figure 24. Configuration > 802.1Q VLAN > VID Configuration

Configuration > 802.1Q VLAN Management VLAN

This allows to select a VLAN from which a management station will be allowed to manage the Switch using Web or Telnet. Management stations that are on VLANs other than the selected one will not be able to manage the Switch. By default, the management VLAN is disabled, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified.

Figure 25. Configuration > 802.1Q VLAN Management VLAN

Configuration > Trunk

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 **Trunk Name** and select the ports to be trunked together, and click **Apply** to activate the selected Trunking groups.

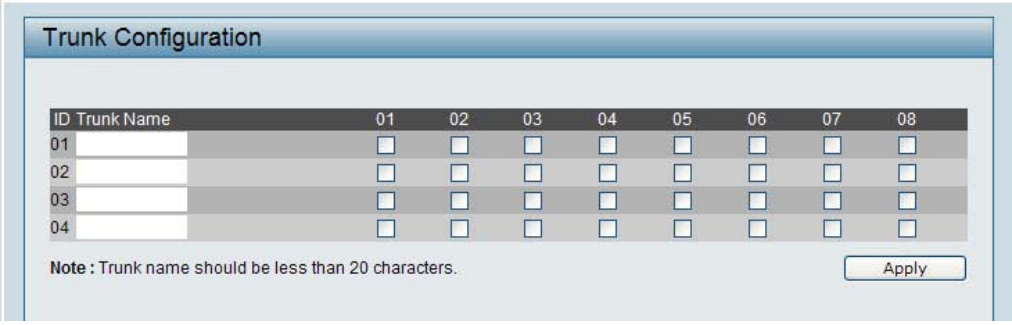

Figure 26. Configuration > Trunk

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 3 IP header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the Web-Smart Switch will forward IP 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.

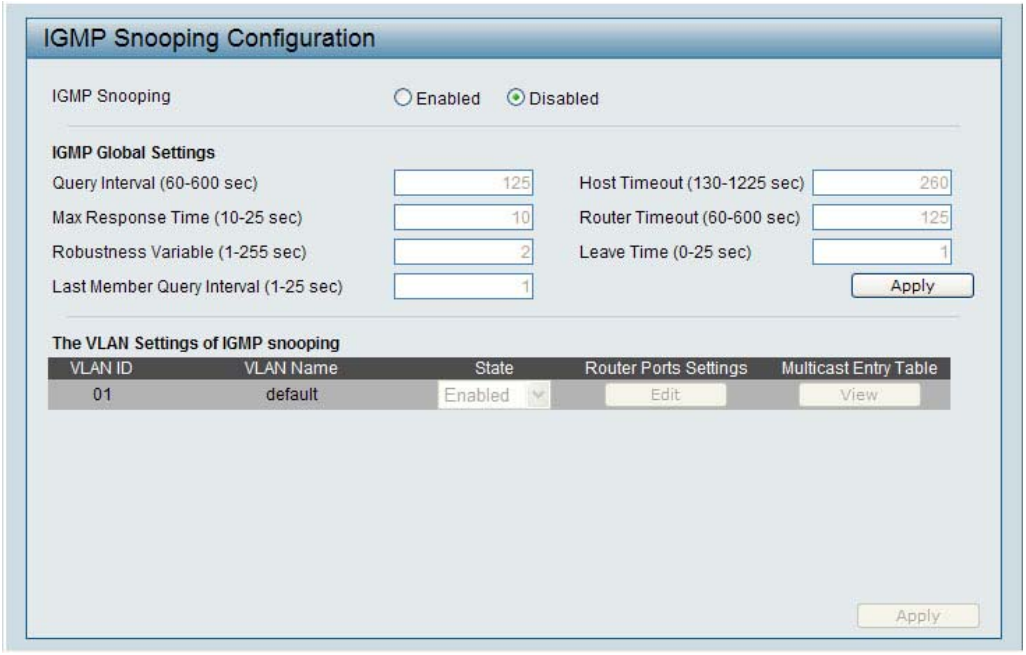

Figure 27. Configuration > IGMP Snooping Configuration

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 lost, the Robustness Variable may be increased. The Robustness Variable can not be set to zero, and SHOULD NOT be one in a normal case. 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 Time (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 the timer expires, the Leave message is dropped. Otherwise the Leave message is 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.

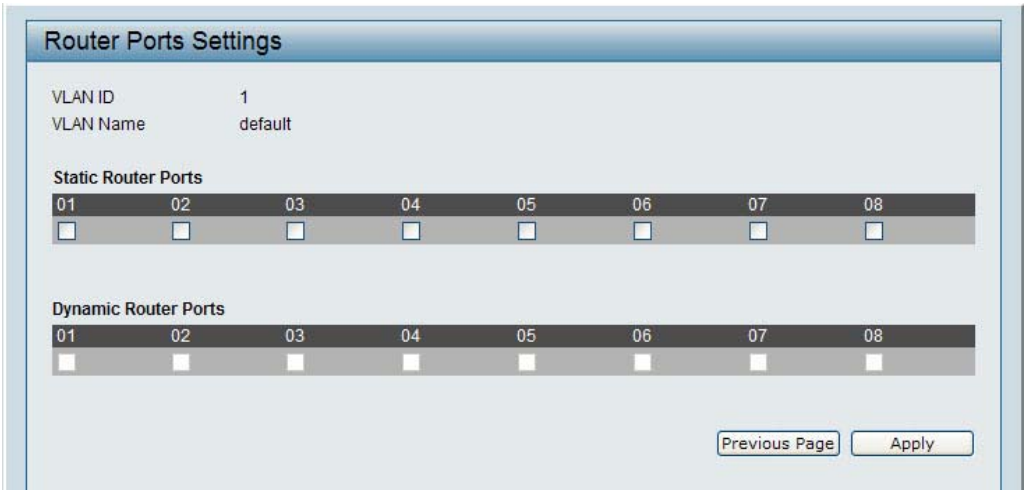

Figure 28. Configuration > IGMP Router Port Settings

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

Figure 29. 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.

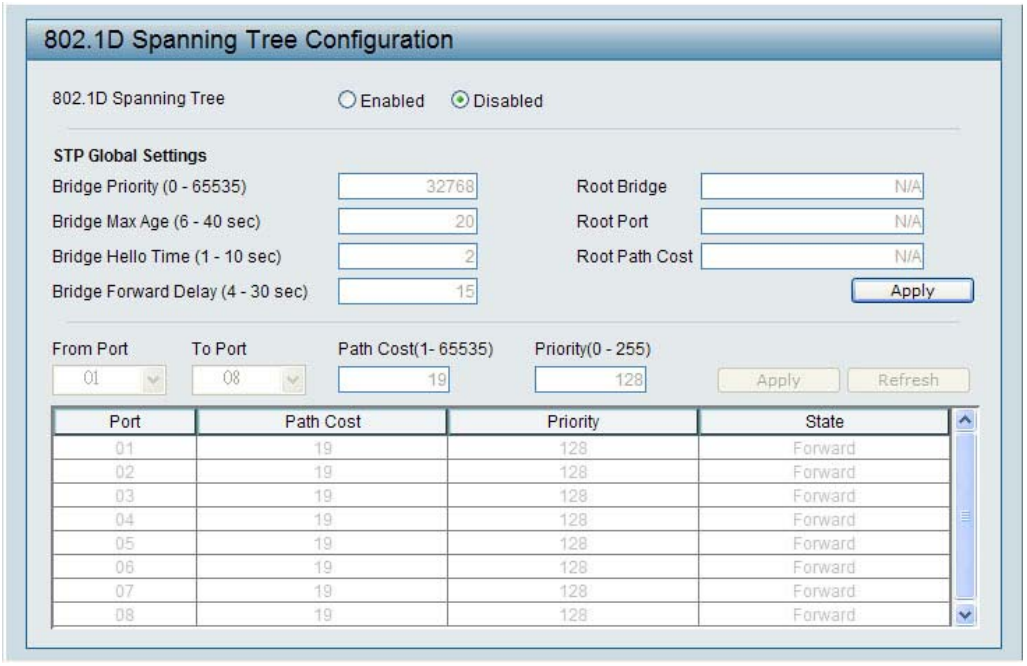

Figure 30. Configuration > 802.1D Spanning Tree

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 root switch: 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.

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.

To refresh the information table and view the latest status, press the **Refresh** button.

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.

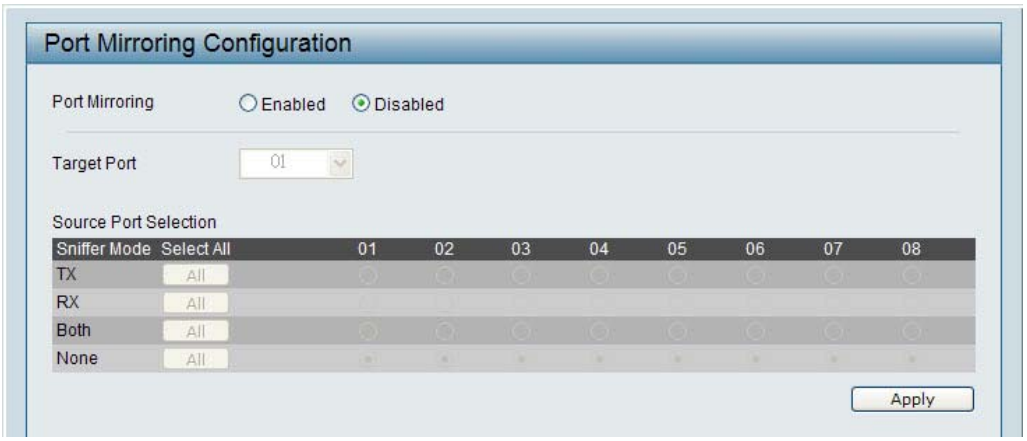

Figure 31. Configuration > Port Mirroring

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.

Press the **All** button to assign all ports to the respective mode.

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.

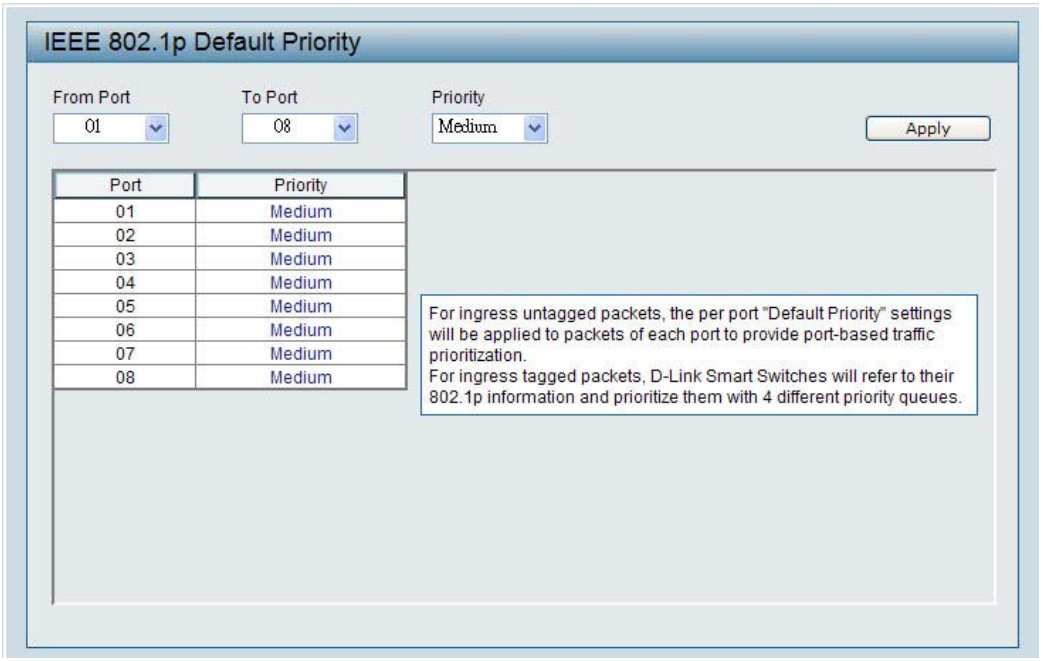

Figure 32. QoS > 802.1p Default Priority

Security > Trusted Host

Use **Trusted Host** to permit remote stations to manage the Switch. If choosing to define one or more designated management stations, only the chosen stations, as defined by the IP address, will be allowed management privilege through the web manager or telnet session.

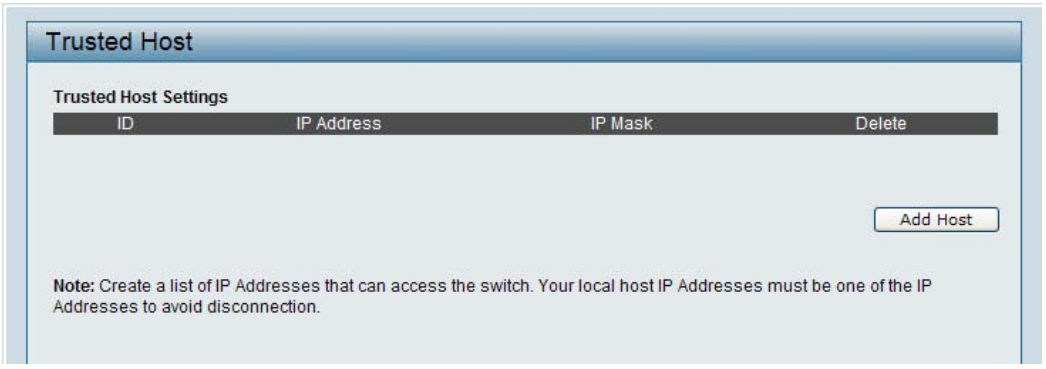

Figure 33. Security > Trusted Host

To define a management station IP setting, click the **Add Host** button and type in the IP address and subnet mask then click the **Apply** button.

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

Security > Storm Control

The 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.

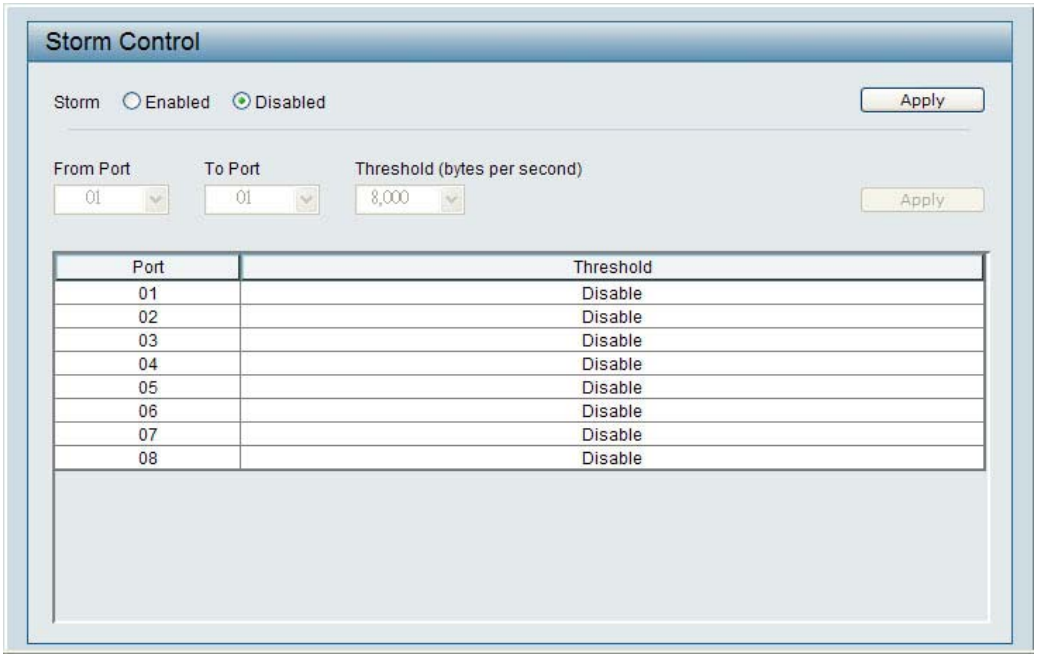

Figure 34. Security > Storm Control

Security > Bandwidth Control

Bandwidth Control limits the amount of Multicast and Broadcast frames accepted and forwarded by this device.

Enabled / Disabled: Default setting is *Disabled*. Click *Enable*, then *Apply*, to configure Bandwidth Control.

The default value for RX Rate is *8000* bytes per second.

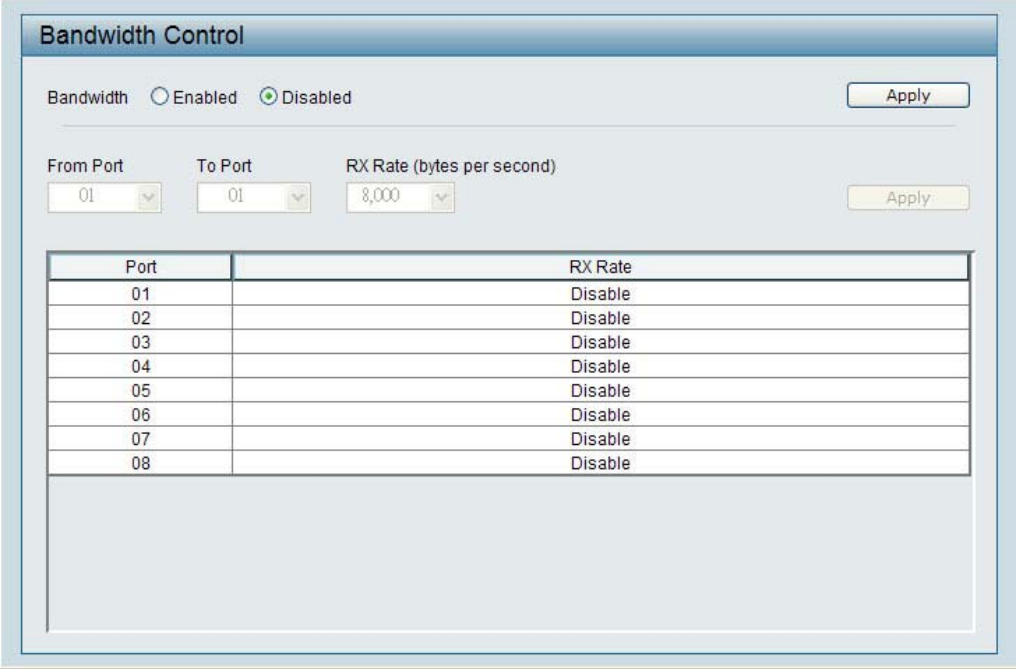

Figure 35. Security > Bandwidth Control

Security > 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.

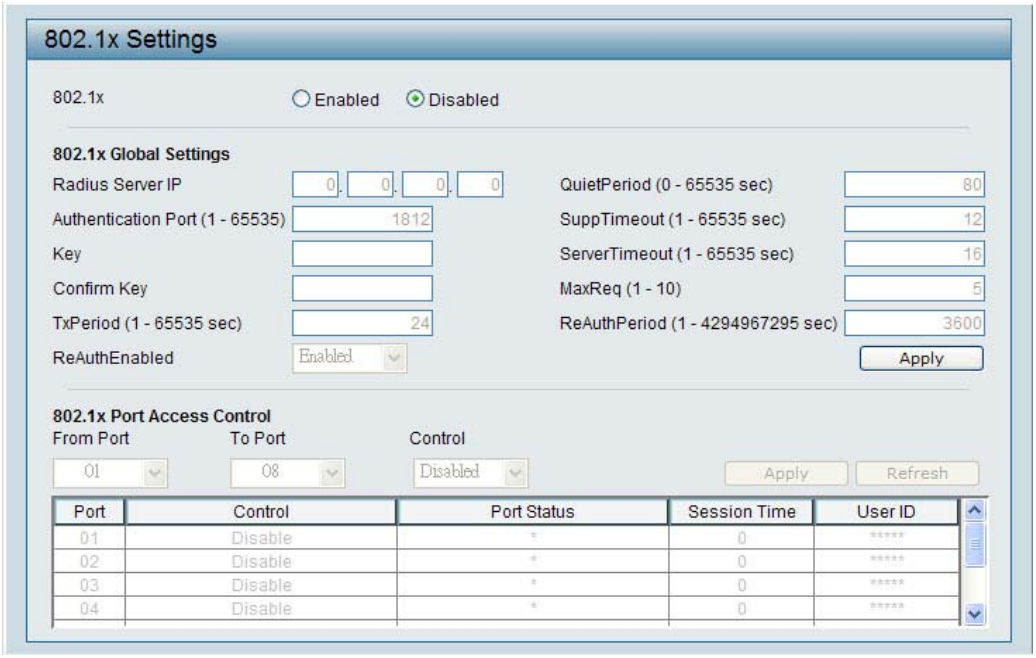

Figure 36. Security > 802.1x Settings

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 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.

Please make the changes in Port Access Control only after changing the Global Settings first.

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.

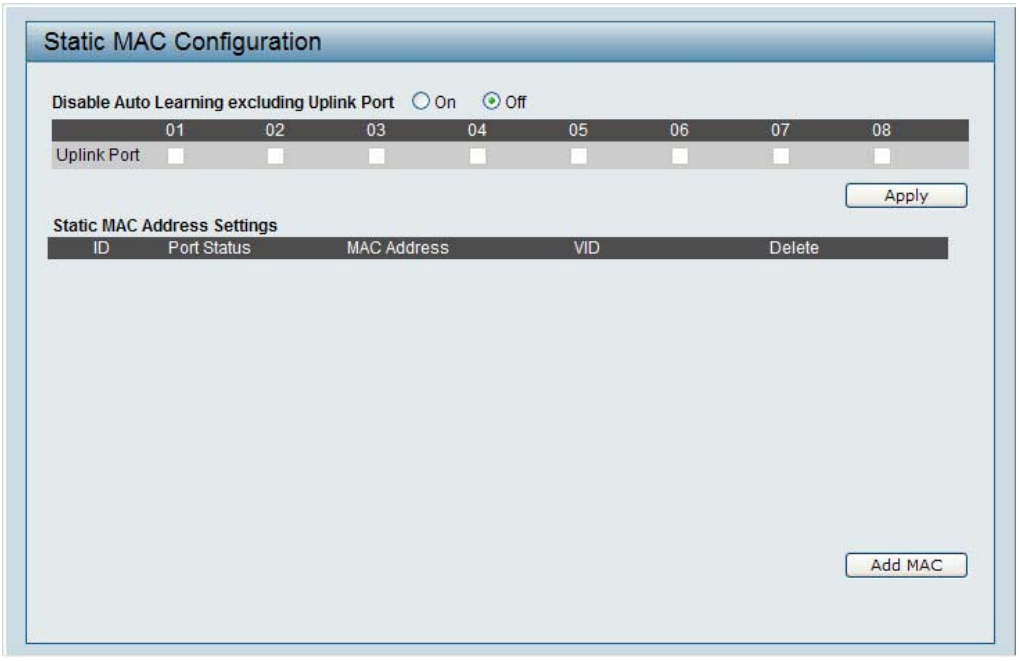

Figure 37. Security > MAC Address Table > Static MAC Configuration

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.

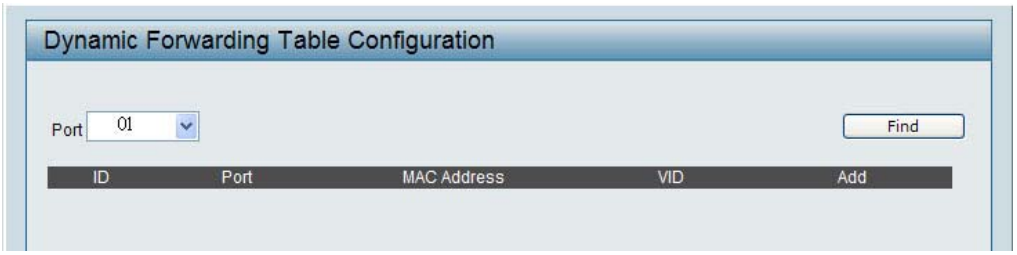

Figure 38. Security > MAC Address Table > Dynamic Forwarding Table

Monitoring > Statistics

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

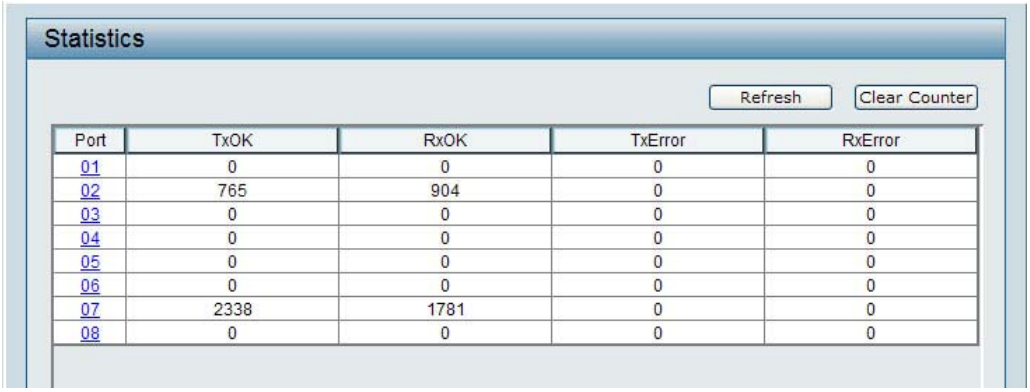

Figure 39. Monitoring > Statistics

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.

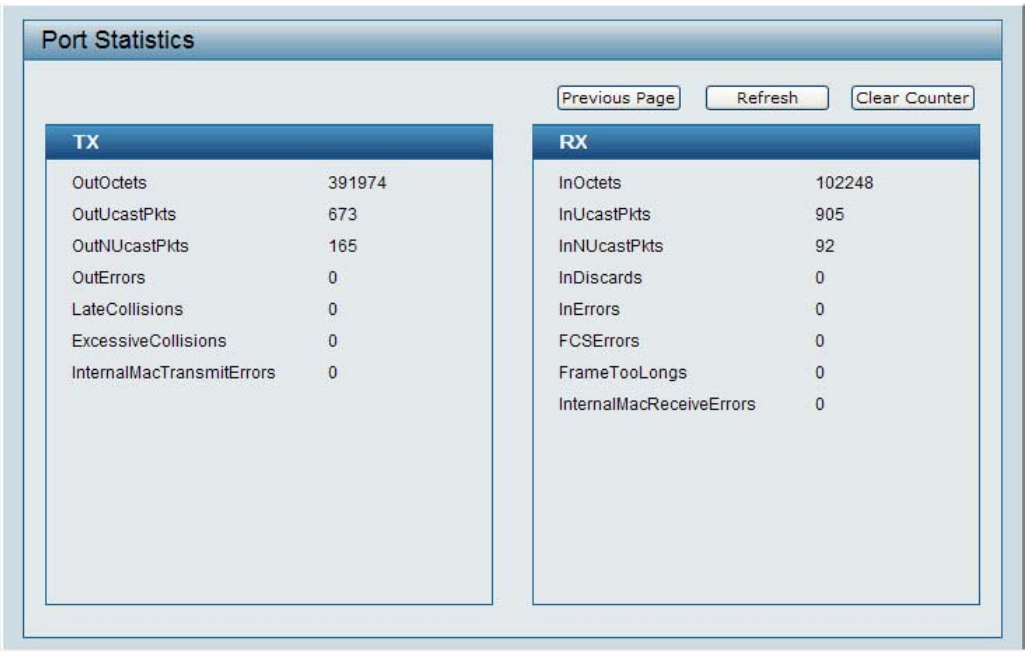

Figure 40. Monitoring > Port Statistics

Configuring the Switch using the CLI

The Switch can be managed through the TCP/IP Telnet protocol. The Command Line Interface (CLI) can be used to configure and manage the Switch via TCP/IP Telnet protocol.

This section provides a reference for all of the commands contained in the CLI.

IP Address of the Switch

The Switch IP address can be automatically set using DHCP protocols, in which case the actual address assigned to the Switch must be known. You can use the ***SmartConsole Utility*** to get or setting the IP address of the Switch.

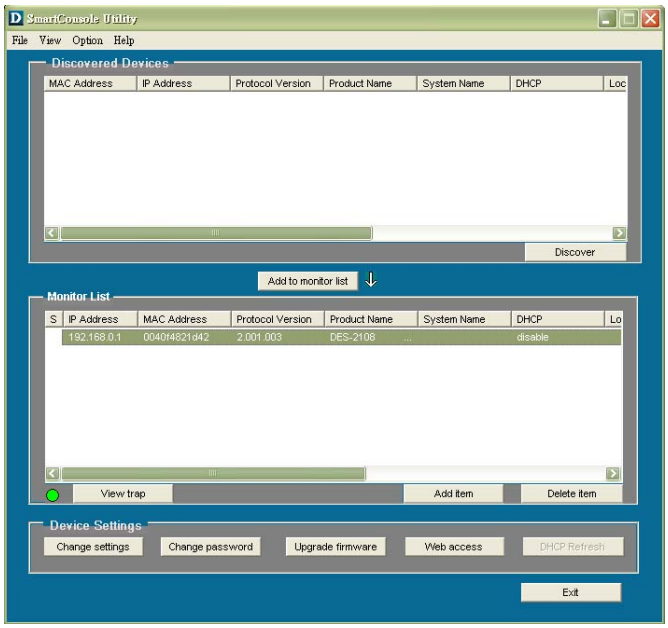

Figure 41. SmartConsole Utility

Using the CLI via Telnet interface

To configure the Switch through the TCP/IP Telnet protocol, using an ordinary telnet client program. On many systems to invoke a telnet client is:

telnet ip-address

Where *ip-address* is the IP address you have assigned to the Switch.

When you telnet to the Switch, it displays its login-in message:

Figure 42. The DES-2108 console login

At this point you can enter the password you have assigned to your Switch. *The factory default password is "**admin**".*

The Switch will then display the telnet interface CLI command prompt:

Figure 43. DES-2108 CLI command prompt

Command Syntax

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through console interface uses the same syntax.

Note: All commands are case sensitive. Be sure to disable Caps Lock or any other unwanted function that changes text case.

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	show stp ports <portlist>
Description	This command displays the STP group of configuration on the Switch.
Example Command	show stp ports 1-5

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.

Syntax	**show snmp [community | host]**
Description	In the above syntax sample, you must specify either a community or host configuration to be show.
Example Command	**show snmp community**

| vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	**show snmp [community | host]**
Description	In the above syntax sample, you must specify either a community or host configuration to be show.
Example Command	**show snmp host**

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**reset {config}**
Description	The command is used to restore the Switch's configuration to the default setting assigned from the factory.
Example Command	**reset config**

Basic Switch Commands

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

Command	Parameters
show switch	
reset	<config>
logout	
save	
config switch system_contact	<system_contact 96>
config switch system_name	<system_name 20>
config switch system_location	<system_location 20>
config switch system_agingtime	< value 0~1000000 sec>
config switch system_timeout	<value 3~30 min>

Each command is listed, in detail, in the following sections.

show switch	
Purpose	Used to display general information about the Switch.
Syntax	**show switch**
Description	This command displays information about the Switch.
Parameters	None.

Example usage:

To display the Switch's information:

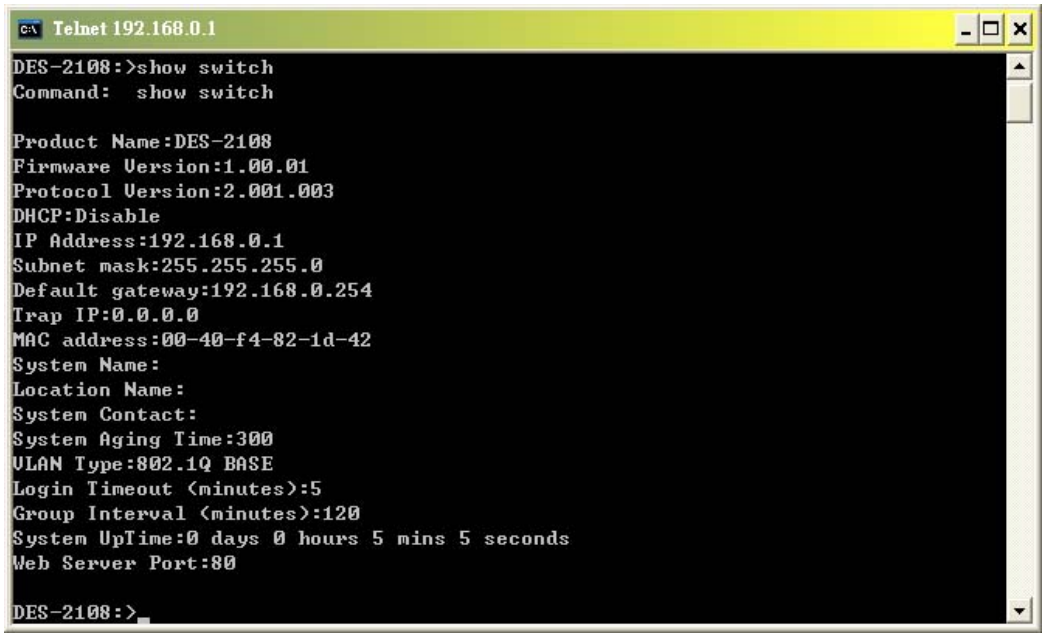

Figure 44. show switch command

reset	
Purpose	Used to reset the Switch to the factory default setting
Syntax	**reset <config>**
Description	The command is used to restore the Switch's configuration to the default setting assigned from the factory.
Parameters	**config -** All of the factory default settings are restored on the Switch including the IP address.

Example usage:

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

Figure 45. reset command

logout	
Purpose	Used to log out a user from the Switch's console.
Syntax	**logout**
Description	This command terminates the current session on the Switch's console.
Parameters	None.

Example usage:

To terminate the current telnet console session:

Figure 46. logout command

save	
Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	**save**
Description	This command is used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	None.

Example usage:

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

Figure 47. save command

config switch system_contact	
Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	**config switch system_contact <system_contact 96>**
Description	The config snmp system_contact command is used to enter the name and/or other information to identify a contact person who is responsible for the Switch.
Parameters	**<system_contact 96> -** A maximum of 96 character can be used, space character is not allowed.

Example usage:

To configure the Switch contact to “arthur”:

Figure 48. config switch system_contact command

config switch system_name	
Purpose	Used to configure the name for the Switch.
Syntax	**config switch system_name <system_name 20>**

Description	The config switch system_name command configures the name of the Switch.
Parameters	**<system_name 20> -** A maximum of 20 character can be used, space character is not allowed.

Example usage:

To configure the Switch name for “Sales-SW-1”:

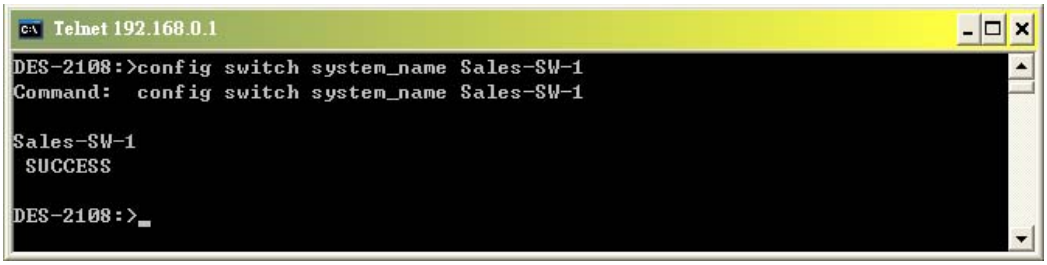

Figure 49. config switch system_name command

config switch system_location

Purpose	Used to enter a description of location of the Switch.
Syntax	**config switch system_location <system_location 20>**
Description	The command is used to enter a description of the location of the Switch.
Parameters	**<system_location 20> -** A maximum of 20 character can be used, space character is not allowed.

Example usage:

To configure the Switch location for “Sales-6F”:

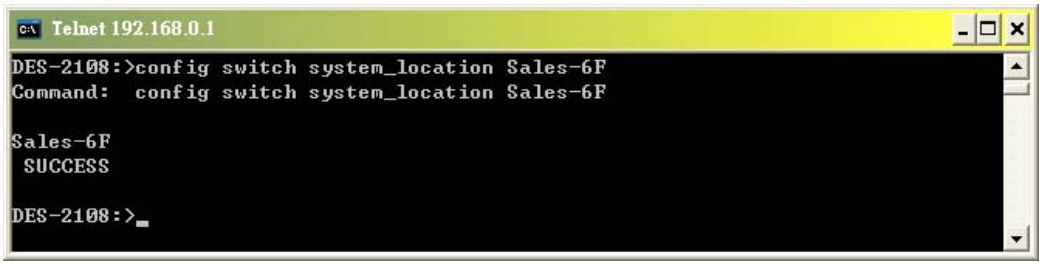

Figure 50. config switch system_location command

config switch system_agingtime	
Purpose	Used to set the aging time of the forwarding database.
Syntax	**config switch system_agingtime <value 0~1000000 sec>**
Description	The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 0 to 1000000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a switch.
Parameters	**<value 0~1000000 sec> -** The aging time for the MAC address forwarding database value. The value in seconds may be between 0 and 1000000 seconds. 0 means never age out the forwarding entries

Example usage:

To set the aging time:

Figure 51. config switch system_agingtime command

config switch system_timeout	
Purpose	Specifies the maximum amount of time a host can access the management interface. The default is 5 minutes
Syntax	**config switch system_timeout <value 3~30 min>**
Description	The command is used to configure the maximum amount of time a host can access the management interface.
Parameters	**<value 3~30 min> -** The timeout time for management access. The value in minutes may be between 3 and 30 seconds.

Example usage:

To set the timeout time:

Figure 52. config switch system_timeout command

Basic IP Commands

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

Command	Parameters
config ipif	[ipaddress <network address> {gw <ipaddress>} | dhcp {vid <vid 1~4094>}]
show ipif	

Each command is listed, in detail, in the following sections.

config ipif	
Purpose	Used to configure the System IP interface.
Syntax	**config ipif [ipaddress <network address> | {gw <ipaddress>} | dhcp {vid <vid 1~4094>}]**
Description	This command is used to configure the System IP interface on the Switch.
Parameters	**ipaddress <network address> -** IP address and netmask of the IP interface to created. You can specify the address and mask information using traditional format 192.168.100.100/255.255.255.0 or in CIDR format 192.168.100.100/24. **gw <network address> -** Designates the gateway IP address. **dhcp -** Allows the selection of the DHCP protocol for the assignment of an IP address to Switch's system IP address. **<vid 1~4094> -** Specific the 802.1Q VLAN ID to the Switch. The range between 1 to 4094.

Example usage:

To configure the IP interface System:

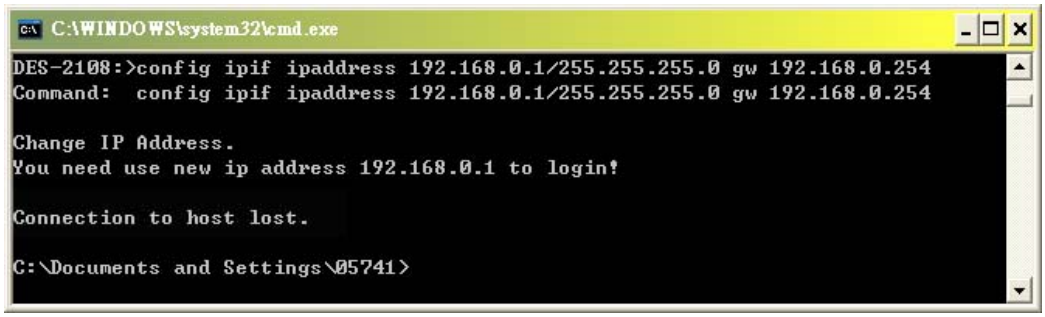

Figure 53. config ipif command

show ipif	
Purpose	Used to display the configuration of an IP interface on the Switch.
Syntax	**show ipif**
Description	This command will display the configuration of an

	IP interface of the Switch.
Parameters	None.

Example usage:

To display IP interface settings:

Figure 54 show ipif command

Switch Port Commands

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

Command	Parameters
config ports	<portlist | all> [speed <disable |auto |10_half | 10_full | 100_half | 100_full> | flow_control <enable | disable> | qos <low | medium | high | highest>]
show ports	{portlist}

Each command is listed, in detail, in the following sections.

config ports	
Purpose	Used to configure the Switch's Ethernet port settings.
Syntax	**<portlist | all> [speed <disable |auto |10_half | 10_full | 100_half | 100_full> | flow_control <enable | disable> | qos <low | medium | high | highest>]**
Description	This command allows for the configuration of the Switch's Ethernet ports.
Parameters	**<portlist> -** Specifies a port or range to be configured. **all -** Configure all ports on the Switch. **speed -** Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following: **disable –** Disable ports **auto -** Enables auto-negotiation for the specified range of ports. **[10 | 100] -** Configures the speed in Mbps for the specified range of ports. **[half | full] -** Configures the specified range of ports as either full-duplex or half-duplex. **flow_control [enable | disable] -** Enable or disable flow control for the specified ports. **qos [low | medium | high | highest] -** Configures the QoS priority level for the specified ports.

Example usage:

To configure the speed of port 1-3 to be 100 Mbps, half duplex, disable of port 4-5, QoS of port 3, 4, 6 to be high priority and disable flow control of port 1, 2, 4, 6:

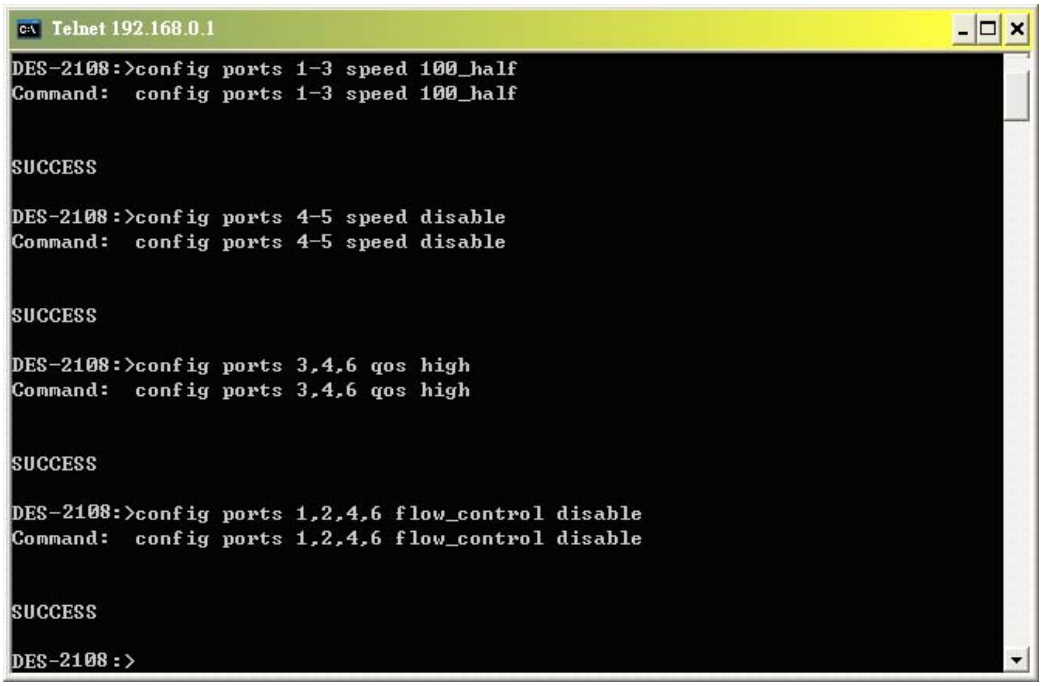

Figure 55. config ports command

show ports	
Purpose	Used to display current configuration of a range of ports.
Syntax	**show ports <portlist>**
Description	This command is used to display current configuration of a range of ports.
Parameters	**<portlist> -** Specifies a port or range of ports to be displayed.

Example usage:

To display the configuration of all ports on the switch:

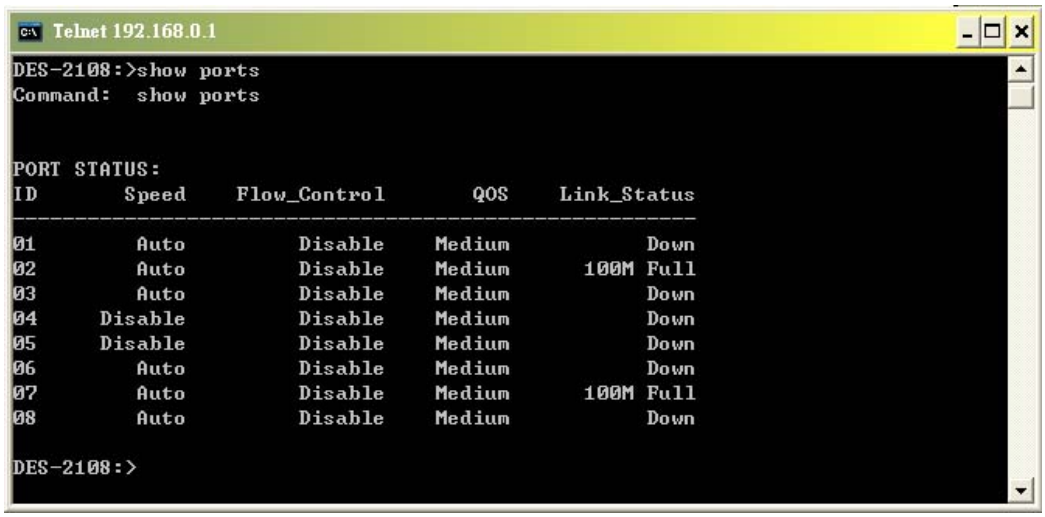

Figure 56. show ports command

VLAN Commands

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

Command	Parameters
create vlan	create vlan tag <vid 1~4094> desc <vlan_name 20>
delete vlan	delete vlan tag <vid 1~4094>
config vlan	config vlan vid <vid 1~4094> {add [tagged | untagged] | delete} <port_list>
show vlan	show vlan {tag <vid 1~4094>}

Each command is listed, in detail, in the following sections.

create vlan	
Purpose	Used to create a VLAN on the Switch.
Syntax	**create vlan tag <vid 1~4094> desc <vlan_name 20>**
Description	This command allows you to create a VLAN on the Switch.

Parameters	**<vid 1~4094> -** The VLAN ID of the 802.1Q_based VLAN to be created. Allowed values = 1~4094 **<vlan_name 20> -** The name of VLAN to be created. A maximum of 20 characters can be used.

Example usage:

To create a VLAN group “sales” with VID 2:

Figure 57. create vlan command

delete vlan	
Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	**delete vlan tag <vid 1~4094>**
Description	This command will delete a previously configured VLAN on the Switch
Parameters	**<vlanid 1-4094> -** The VLAN ID of the 802.1Q_Based VLAN you want to delete.

Example usage:

To delete VLAN group with vid 2:

Figure 58. delete vlan command

config vlan	
Purpose	Used to add ports to a previously configured VLAN.
Syntax	**config vlan vid <vid 1~4094> {add [tagged | untagged] | delete} <port_list>**
Description	This command allows you to add ports to the port list of previously configured VLAN.
Parameters	**<vid 1~4094> -** The VLAN ID of the 802.1Q_based VLAN you want to add/delete ports to/from. **tagged -** Specifies the additional ports as tagged. **untagged -** Specifies the additional ports as untagged. **add -** Entering the add parameter will add ports to the VLAN **delete -** Delete ports from the specified VLAN. **<portlist> -** A port or range of ports to add to, or delete from the specified VLAN.

Example usage:

To add port 1, 3, 5, 6 to the VLAN group with vid 2:

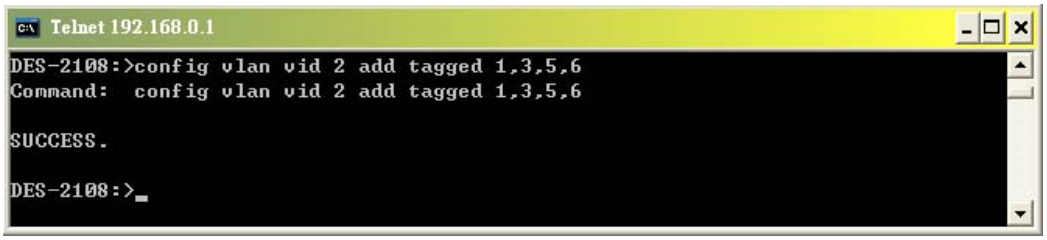

Figure 59. config vlan command, add VLAN group members

To delete port 3 from the VLAN tag 2:

Figure 60. config vlan command, delete VLAN group members

show vlan	
Purpose	Used to show VLAN status.
Syntax	**show vlan {tag <vid 1~4094>}**
Description	This command allows you to show VLAN status on the Switch.
Parameters	**<vid 1~4094> -** The VLAN ID of the 802.1Q_based VLAN to be created. Allowed values = 1~4094

Example usage:

To show VLAN status:

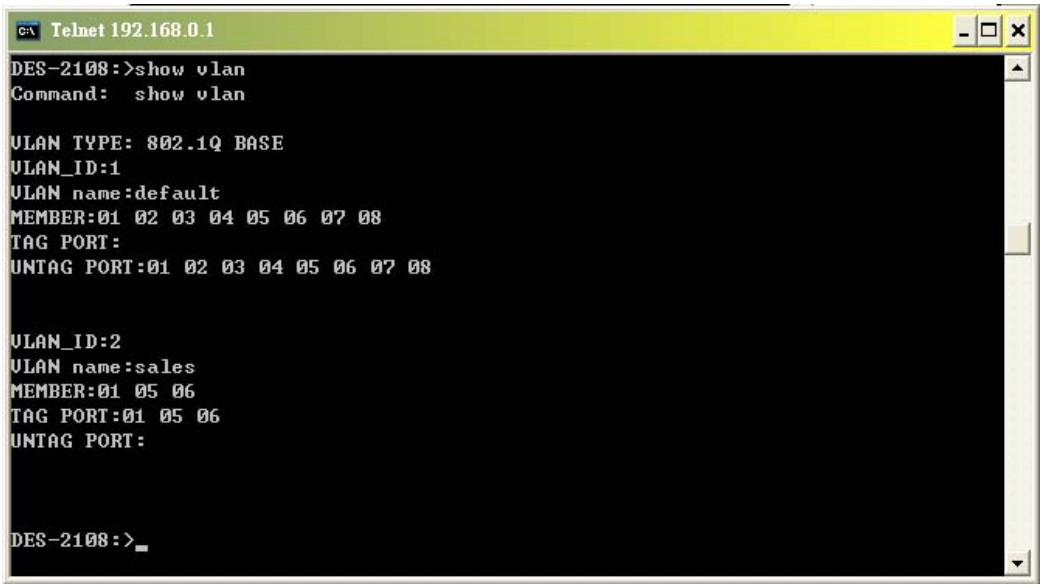

Figure 61. show vlan command

Port Mirroring Commands

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

Command	Parameters
config mirror port	{enable [<port> source ports <portlist> [rx | tx |both]] | disable}
show mirror	

Each command is listed, in detail, in the following sections.

config mirror port	
Purpose	Used to configure a mirror port – source port pair on the Switch. Traffic for any source port to a target port can be mirrored for real-time analysis.
Syntax	**{enable [<port> source ports <portlist> [rx | tx |both]] | disable}**
Description	This command allows you configure a mirror port - source port pair on the Switch.
Description	**<port> -** This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operating at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that the target port. **source ports -** The port or ports being mirrored. This can not include the Target port.
Description	**<portlist> -** This specifics a port or range of ports that will be mirrored. That is the range of ports which all traffic will be copied and sent to the Target port. **rx -** Allows the mirroring of only packets received by (flowing into) the port or ports in the port list. **tx -** Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. **both -** Mirrors all the packets received or sent by the port in the port list.

Example usage:

To enable and configure the Port Mirror function of the Switch:

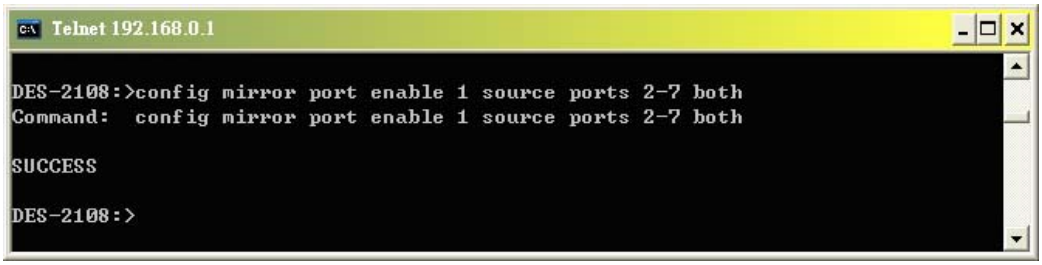

Figure 62. config mirror port command

To disable Port Mirror function of the Switch:

Figure 63. config mirror port command, disable port mirror function

show mirror	
Purpose	Used to show the current mirroring configuration on the Switch.
Syntax	**show mirror**
Description	This command displays the current mirroring configuration on the Switch
Parameters	None

Example usage:

To display port mirroring configuration:

Figure 64. show mirror command

Trap Commands

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

Command	Parameters
enable discovery	
disable discovery	
config discovery trap_ip	ipaddress <ip_address>
config discovery trap_event	trap_event [bootup | illegal_login | t_link]
delete discovery trap_event	trap_event [bootup | illegal_login | t_link |]
show discovery trap	

Each command is listed, in detail, in the following sections.

enable discovery	
Purpose	Used to the enable the discovery trap function to *SmartConsole Utility*.
Syntax	**enable discovery**
Description	The command is used to the enable the discovery trap function to *SmartConsole Utility*.

Parameters	None.

Example usage:

To enable the discovery trap function:

Figure 65. enable discovery command

disable discovery	
Purpose	Used to the disable the discovery trap function to *SmartConsole Utility*.
Syntax	**disable discovery**
Description	The command is used to the disable the discovery trap function to *SmartConsole Utility*.
Parameters	None.

Example usage:

To disable the discovery trap function:

Figure 66. disable discovery command

config discovery trap_ip	
Purpose	Used to configure an IP address of the trap recipient of *Web Management Utility* to the Switch.

Syntax	**config discovery trap_ip ipaddress <ip_address>**
Description	The command is configure an IP address of the trap recipient of *SmartConsole Utility* to the Switch.
Parameters	**<ip_address> -** IP address of the Web Management Utility.

Example usage:

To assigned IP address of the Web Configuration Utility to receive trap message:

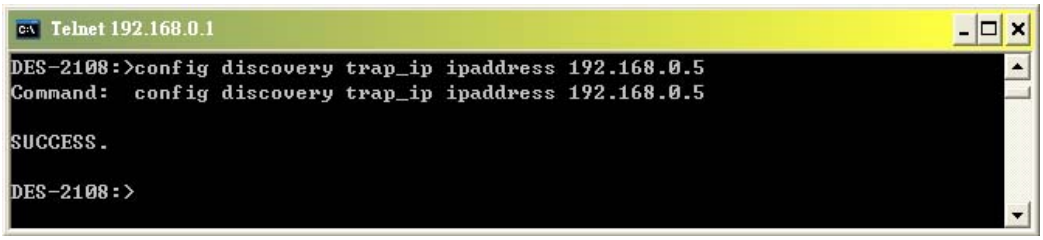

Figure 67. config discovery trap_ip command

config discovery trap_event	
Purpose	Used to configure the events of the trap on the Switch.
Syntax	**trap_event [bootup | illegal_login | t_link]**
Description	The command is configure the events of the trap on the Switch..
Parameters	**bootup -** Enabled the Switch's boot up event. **illegal_login -** Enabled the Switch's illegal login event. **t_link -** Enabled the Switch's twisted-pair ports (port 1 – 8) linking status change event.

Example usage:

To configure the events type of the Switch:

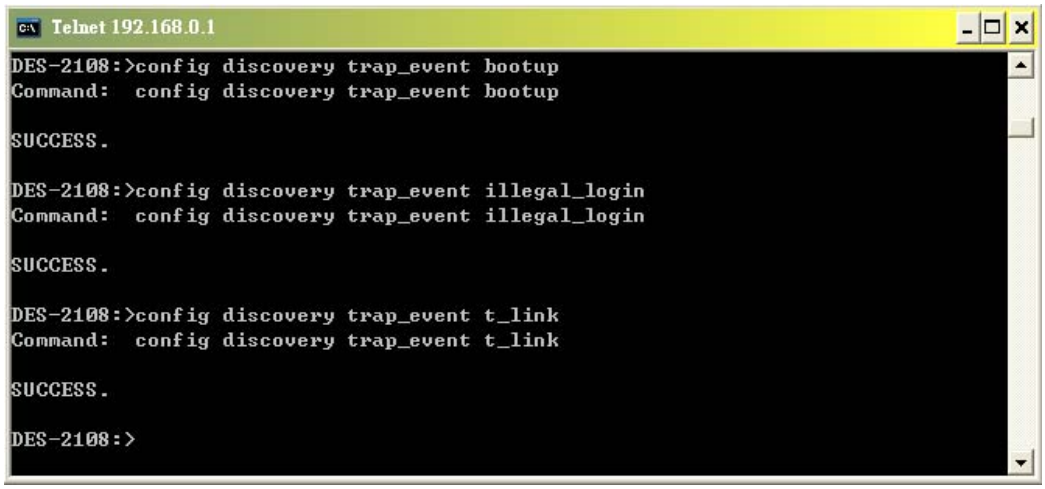

Figure 68. config discovery trap_event command

delete discovery trap_event	
Purpose	Used to delete previously configured events of trap on the Switch.
Syntax	**trap_event [bootup | illegal_login | t_link]**
Description	The command is delete previously configured events of trap on the Switch.
Parameters	**bootup -** Enabled the Switch's boot up event. **illegal_login -** Enabled the Switch's illegal login event. **t_link -** Enabled the Switch's twisted-pair ports (port 1 – 8) linking status change event.

Example usage:

To delete the event type from current event configuration of the Switch:

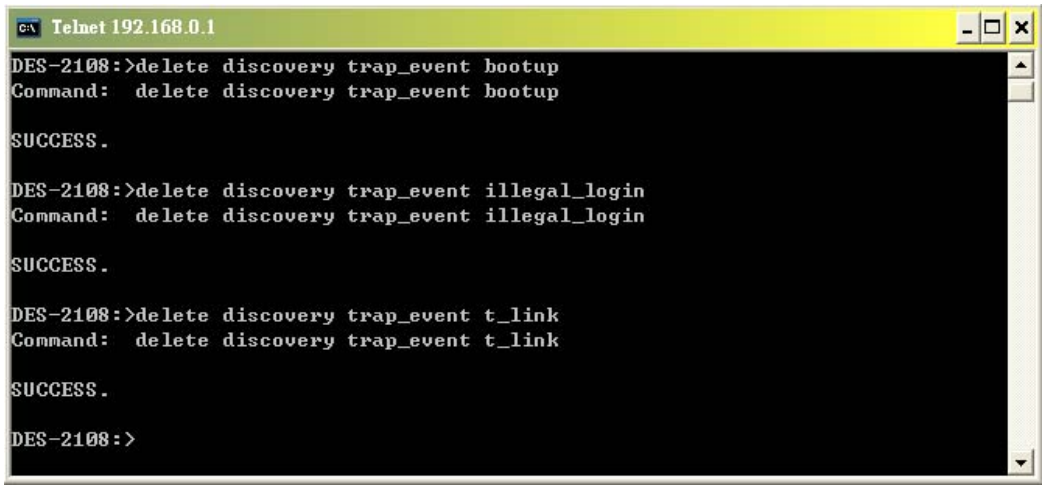

Figure 69. delete discovery trap_event command

show discovery trap	
Purpose	Used to show the configuration of the discovery trap on the Switch.
Syntax	**show discovery trap**
Description	The command is display the configuration of the discovery trap on the Switch..
Parameters	None.

Example usage:

To display discovery trap configuration:

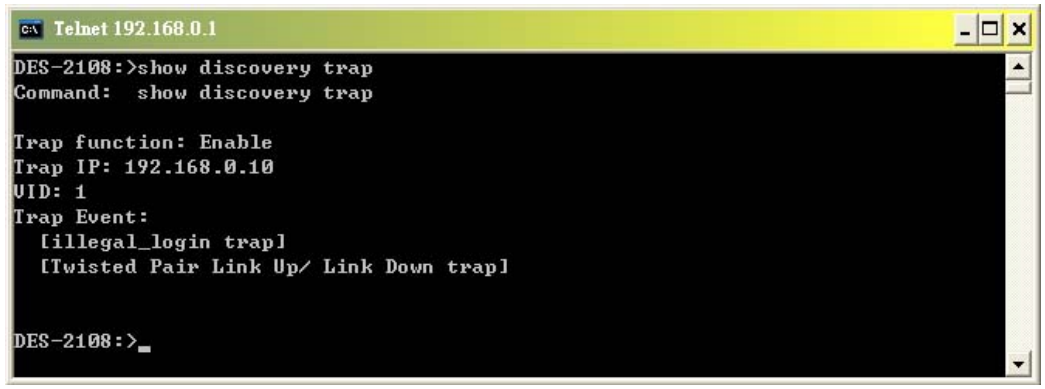

Figure 70. show discovery trap command

Spanning Tree Commands

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

Command	Parameters
enable stp	
disable stp	
config stp	[maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30> | priority <value 1-65535>]
config stp ports	[all | <portlist>] {cost <value 1-65535> | priority <value 0-255>}
show stp	
show stp ports	<portlist>

Each command is listed, in detail, in the following sections.

enable stp	
Purpose	Used to enable STP on the Switch.
Syntax	**enable stp**
Description	This command allows the Spanning Tree Protocol to be enabled on the Switch.
Parameters	None.

Example usage:

To enable STP on the Switch:

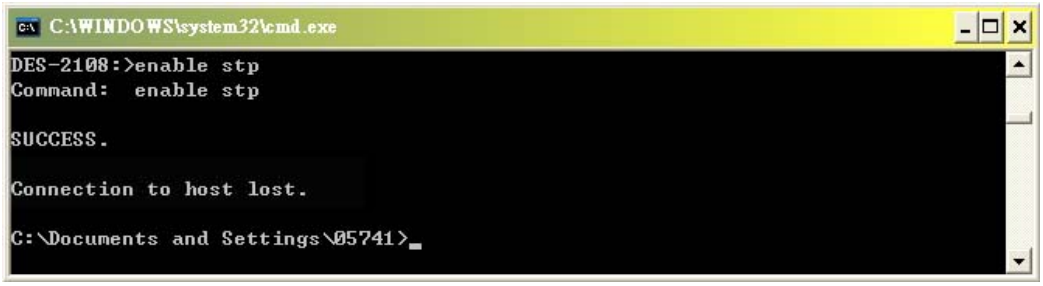

Figure 71. enable stp command

disable stp	
Purpose	Used to disable STP on the Switch.
Syntax	**disable stp**
Description	This command allows the Spanning Tree Protocol to be disabled on the Switch.
Parameters	None.

Example usage:

To disable STP on the Switch:

Figure 72. disable stp command

config stp	
Purpose	Used to setup STP on the Switch.
Syntax	**[maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30> | priority <value 1-65535>]**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire Switch.
Parameters	**maxage <value 6-40> -** The 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
Parameters	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 sending its own BPDU to all other switches for permission become the Root Bridge. If it turns on that your switch has the lowest Bridge identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20.

hellotime <value 1-10> - The user may set the time interval between transmission of configuration messages by the root device, thus stating that the Switch is still functioning. A time between 1 and 10 seconds may be chosen, with a default setting of 2 seconds.

forwarddelay <value 4-30> - The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between 4 and 30 seconds. The default is 15 seconds.

priority <value 1-65535> - Select a value between 1 and 65535 to specify the priority of the Switch. The lower the value, the higher the priority. The default is 32768.

Example usage:

To configure STP with maxage 40 and hellotime of 5 seconds:

Figure 73. config stp command

config stp ports	
Purpose	Used to setup STP on the port level.
Syntax	**config stp ports [all | <portlist>] {cost <value 1-65535> | priority <value 0-255>}**
Description	This command is used to create and configure STP for a group of ports.
Parameters	**[all | <portlist>] -** Specifies all ports or range of ports to be configured. **cost <value 1-65535> -** This defines a metric that indicates the relative cost of forwarding packets to specified port list. The value between 1 and 65535 to determine the cost. The lower the number, the greater the probability the port will be chosen to forward packets. The default value is 10. **priority <value 0-255> -** Select a value between 0 and 254 to specify the priority for a specified port for forwarding packets. The lower the value, the higher the priority. The default is 128.

Example usage:

To configure STP with path cost 10, priority of 100 for ports 1-5:

Figure 74. config stp ports command

show stp	
Purpose	Used to display the Switch's current STP configuration.
Syntax	**show stp**

Description	This command displays the Switch's current STP configuration.
Parameters	None.

Example usage:

To display the status of STP on the Switch:

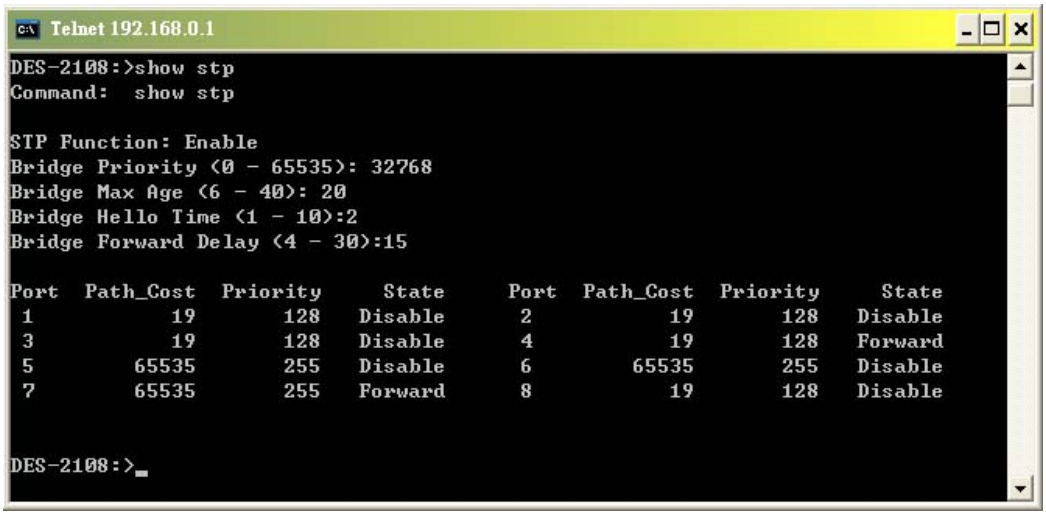

Figure 75. show stp command

show stp ports	
Purpose	Used to display the Switch's current STP group of ports configuration on the Switch.
Syntax	**show stp ports {portlist}**
Description	This command displays the STP group of configuration on the Switch.
Parameters	**<portlist> -** Specifies a port or range of ports to be viewed.

Example usage:

To display the STP status of port on the Switch:

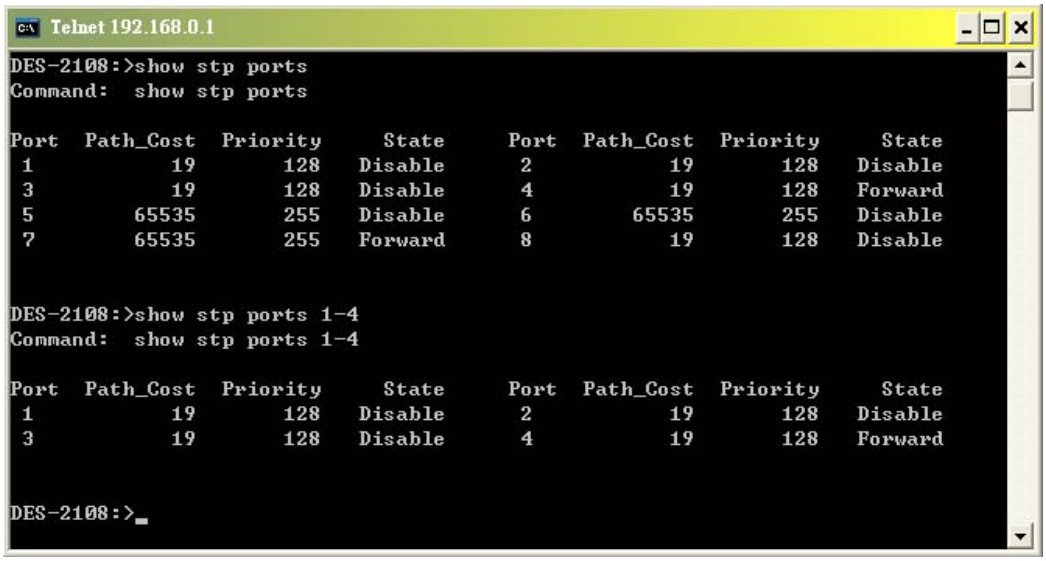

Figure 76. show stp ports command

SNMP Commands

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

Command	Parameters
enable snmp	
disable snmp	
config snmp community	[read_only|read_write] comm_name <name 20>
show snmp community	
enable snmp traps	
disable snmp traps	
config snmp trap	trap_ip < ipaddress > trap_name <name 20> trap_event <bootup | t_link | t_rx_error | t_tx_error>
show snmp trap	

Each command is listed, in detail, in the following sections.

enable snmp	
Purpose	Used to enable SNMP community string from the Switch.
Syntax	**enable snmp**
Description	This command is used to enable SNMP community string from the Switch .
Parameters	None

Example usage:

To enable the SNMP community string:

Figure 77. enable snmp command

disable snmp	
Purpose	Used to disable SNMP community string from the Switch.
Syntax	**disable snmp**
Description	This command is used to disable SNMP community string from the Switch .
Parameters	None

Example usage:

To disable the SNMP community string:

Figure 78. enable snmp command

config snmp community

Purpose	Used to configure a SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string.
Syntax	**[read_only|read_write] comm_name <name>**
Description	This command is used to configure a SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	**read_only -** Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. **read_write -** Specifies that SNMP community members using the community string created with this command can only read from and write to the contents of the MIBs on the Switch. **<name 20> -** An alphanumeric string of up to 20 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. The default community strings for SNMP v.1 management access are: **Public:** Read-only privilege allows authorized management stations to retrieve MIB objects. **Private:** Read/write privilege

Example usage:

To config the SNMP community read only community name "public":

Figure 79. config snmp community command

show snmp community	
Purpose	Used to display SNMP community strings configured on the Switch.
Syntax	**show snmp community**
Description	This command is used to display SNMP community strings that are configured on the Switch.

Example usage:

To display the currently entered SNMP community strings:

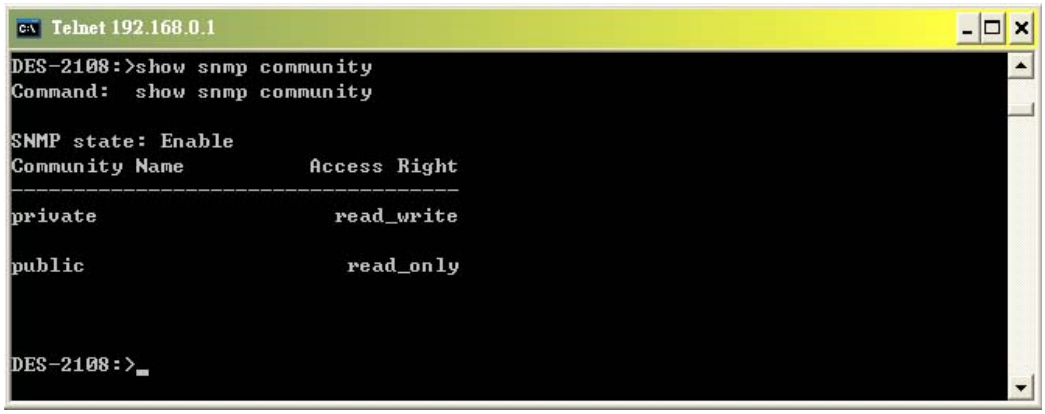

Figure 80. show snmp community command

enable snmp traps	
Purpose	Used to enable the Switch to send traps to the recipient .
Syntax	**enable snmp traps**
Description	This command is used to enable the Switch to send traps to the recipient .
Parameters	None

Example usage:

To enable the SNMP trap generator:

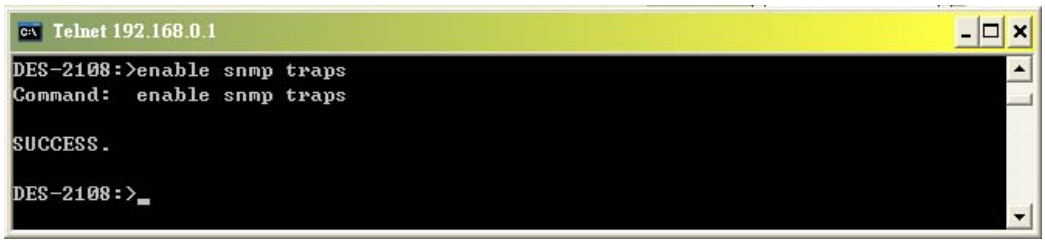

Figure 81. enable snmp traps command

disable snmp traps	
Purpose	Used to disable the Switch to send traps to the recipient .
Syntax	**disable snmp traps**
Description	This command is used to disable the Switch to send traps to the recipient .
Parameters	None

Example usage:

To disable the SNMP trap generator:

Figure 82. disable snmp command

config snmp trap	
Purpose	Used to config a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**config snmp trap trap_ip < ipaddress > trap_name <name 20> trap_event <bootup | t_link | t_rx_error | t_tx_error>**
Description	This command creates a recipient of SNMP traps generated by the Switch's SNMP agent
Parameters	**<ipaddress> -** The IP address of the remote management station that will serve as the SNMP host for the Switch. **<name 20> -** An alphanumeric string of up to 20 characters used to authorize a remote SNMP manager to access the Switch's SNMP agent (Trap Name must be selected from a Community Name). **<bootup> -** System device bootup **<t_link> -** Twisted Pair Link Up / Link Down **<t_rx_error> -** Twisted Pair Abnormal Receive Error **<t_tx_error> -** Twisted Pair Abnormal Transmit Error

Example usage:

To configure an SNMP host to receive SNMP traps type "bootup", "t_link", "t_rxd_error", "t_tx_error" :

Figure 83. config snmp trap command

show snmp trap	
Purpose	Used to display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp trap**
Description	This command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps that are generated by the Switch's SNMP agent.
Parameters	None.

Example usage:

To display the currently configured SNMP trap state on the Switch:

Figure 84. show snmp trap command

IGMP Snooping Commands

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

Command	Parameters
config router_ports	[add | delete] vid <vid> port <port_list>
enable igmp snooping	

disable igmp_snooping	
show router_ports	
show igmp_snooping group	
config igmp_snooping	{[host_timeout <sec 130-1225> | router_timeout <sec 60-600> | query_interval <sec 60-600> | response_time <sec 10-25> | robustness_variable <sec 1-255> | lmquery_interval <sec 1-25> | leave_time <sec 0-25>] | [enable|disable] vid <vid>}

Each command is listed, in detail, in the following sections.

config router_ports	
Purpose	Used to configure ports as router ports.
Syntax	**config router_ports [add | delete] <vid> <port_list>**
Description	This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router − regardless of protocol, etc.
Parameters	**add / delete -** Add or delete the specifies a port or range of ports that will be configure as router ports. **<portlist> -** Specifies a port or range of ports that will be configured as router ports.

Example usage:

To set up static router ports:

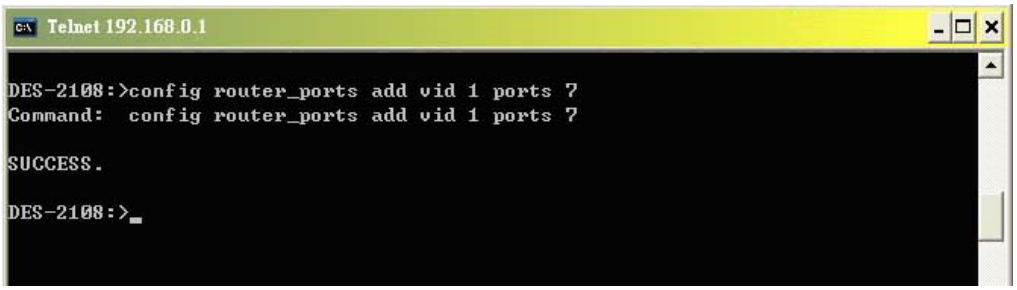

Figure 85. config router_ports command (add static router ports)

To delete static router ports:

Figure 86. config router_ports command (delete static router ports)

enable igmp snooping	
Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping**
Description	This command allows you to enable IGMP snooping on the Switch. If f
Parameters	None.

Example usage:

To enable IGMP snooping on the Switch:

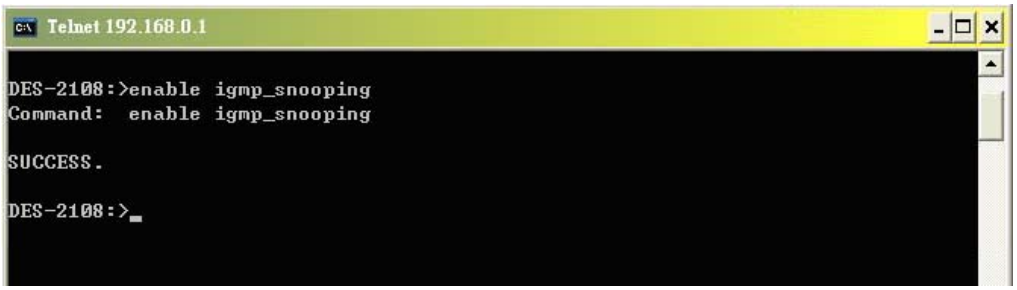

Figure 87. enable igmp snooping command

disable igmp snooping	
Purpose	Used to disable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping**
Description	This command disables IGMP snooping on the Switch.
Parameters	None.

Example usage:

To disable IGMP snooping on the Switch:

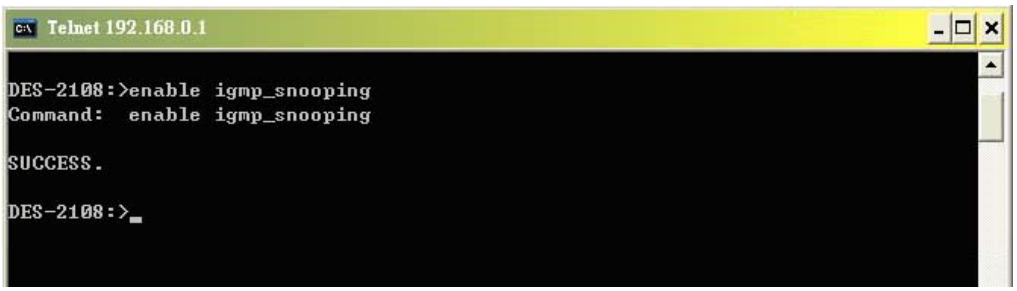

Figure 88. disable igmp snooping command

show router_ports	
Purpose	Used to display the currently configured router ports on the Switch.
Syntax	**show router_ports**
Description	This command is used to display the currently configured router ports on the Switch.
Parameters	None.

Example usage:

To display the router ports:

Figure 89. show router_ports command

show igmp_snooping group	
Purpose	Used to display the current IGMP snooping configuration on the Switch.
Syntax	**show igmp_snooping group**
Description	This command will display the current IGMP setup currently configured on the Switch.
Parameters	None.

Example usage:

To view the current IGMP snooping group:

Figure 90. show igmp_snooping command

config igmp_snooping	
Purpose	Used to configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping {[host_timeout <sec 130-1225> | router_timeout <sec 60-600> | query_interval <sec 60-600> | response_time <sec 10-25> | robustness_variable <sec 1-255> | lmquery_interval <sec 1-25> | leave_time <sec 0-25>] | [enable|disable] vid <vid>}**
Description	This command allows you to configure IGMP snooping on the Switch.

Parameters	**host_timeout <sec 1-1225> −** Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. **router_timeout <sec 1-600> −** Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 125 seconds. **query_interval <sec 60-600> -** Configures 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. **response_time <sec 10-25> -** 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 <sec 1-255> -** This allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lost, the robustness variable may be increased. The robustness variable can not be set to zero, and SHOULD NOT be one in a normal case. Default is 2 seconds.

Parameters	**lmquery_interval <sec 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. **leave_time <sec 0-25> -** 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 the timer expires, the Leave message is dropped. Otherwise the Leave message is forwarded to the port. Default is 1 second. **enable/disable -** To enable or disable IGMP snooping for a given VLAN.

Example usage:

To configure IGMP snooping:

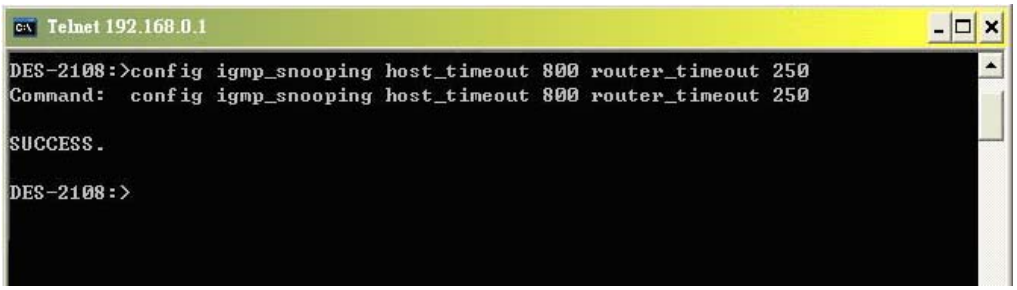

Figure 91. config igmp_snooping command

Static MAC Commands

The layer 2 forwarding database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config auto_learning	[on ports <port_list | null> | off]
show smac	
show fdb	port <port no.>
create smac (802.1Q)	[mac <macaddress> port <port> vid <vid> | idx <mac address index list on fdb>]
delete smac	[mac <macaddress> | idx <mac address index on smac>]

Each command is listed, in detail, in the following sections.

config auto_learning	
Purpose	Used to enables or disables the MAC address learning on the specified range of ports.
Syntax	**config auto_learning [on ports <port_list | null> | off]**
Description	This command allows you to enables or disables the MAC address learning on the specified range of ports.
Parameters	**null<null>** disables auto_learn on all ports.

Example usage:

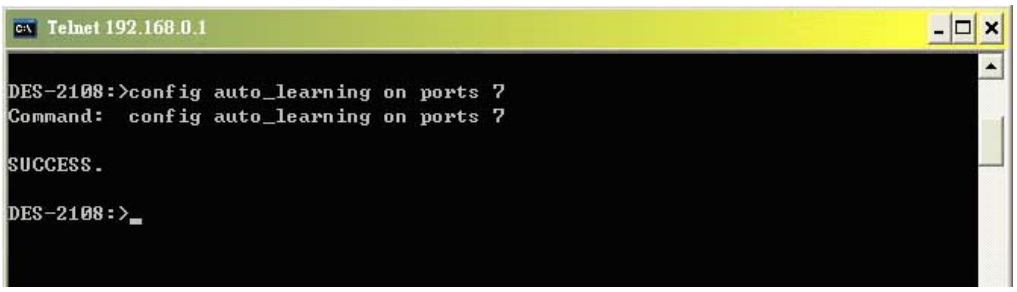

Figure 92. enable auto_learning function

show smac	
Purpose	Used to display the Static MAC address forwarding database.
Syntax	**show smac**
Description	This command allows you to display the Static MAC address forwarding database.
Parameters	None.

Example usage:

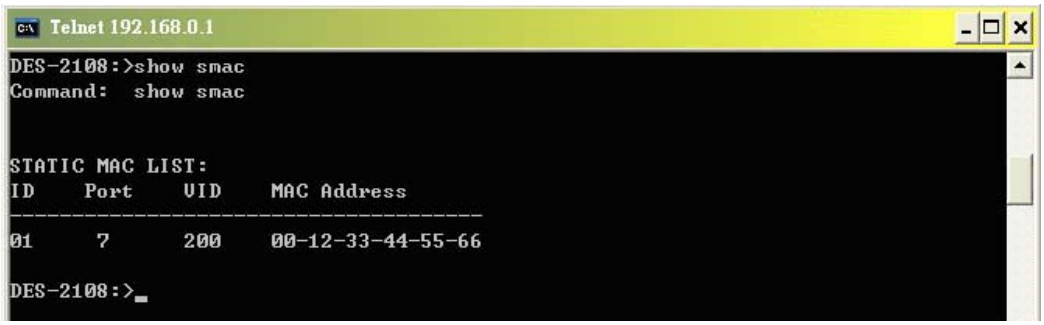

Figure 93. show Static MAC address forwarding database

show fdb	
Purpose	Used to display the dynamic MAC address forwarding database.
Syntax	**show fdb port <port>**
Description	This command allows you to display the dynamic MAC address forwarding database.
Parameters	**port <port> -** To display the dynamic MAC address forwarding database on the specified port number.

Example usage:

Figure 94. show Dynamic MAC address forwarding database

create smac (802.1Q)	
Purpose	Used to create a static entry to the unicast MAC address forwarding table (database).
Syntax	**[mac <macaddress> port <port no.> vid <vid> | idx <mac address index list on smac>]**
Description	This command allows you to create a static MAC entry in the forwarding table for the specified VLAN.
Parameters	**mac <macaddress> -** The MAC address that will be added to the forwarding table. **port <port no.> -** The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. **vid <vid> -** Specific the 802.1Q VLAN ID to the port. **idx <mac address index list on smac> -** Added to the forwarding table for smac list.

Example usage:

To create a unicast MAC FDB entry:

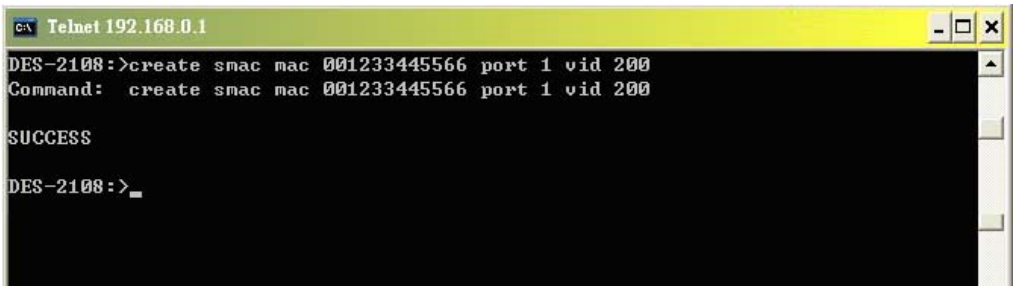

Figure 95. create static MAC address to FDB

Trusted Host Commands

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

Command	Parameters
create host	[ipaddress <ipaddress>/<ipmask>]
delete host	[ipaddress <ipaddress> | idx <trusted host index>]
show host	

Each command is listed, in detail, in the following sections.

create host	
Purpose	Used to create the trusted host.
Syntax	**[ipaddress <ipaddress>/<ipmask>]**
Description	This command is used to permit remote stations to manage the Switch.
Parameters	**ipaddress <ipaddress>/<ipmask> -** IP address and netmask of the IP interface to created. You can specify the address and mask information using traditional format 192.168.100.100/255.255.255.0 or in CIDR format 192.168.100.100/24.

Example usage:

To create trusted host:

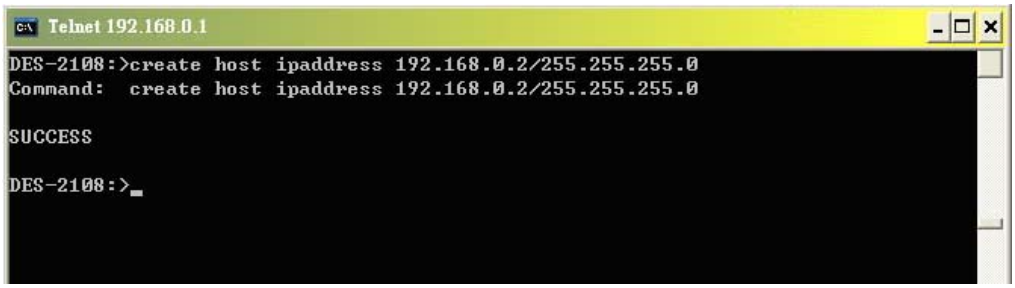

Figure 96. create host command

delete host	
Purpose	Used to remove the trusted host.
Syntax	**[ipaddress <ipaddress> | idx <trusted host index>]**
Description	This command will remove the trusted host that has been created.
Parameters	**ipaddress <ipaddress> -** Delete a existing trusted host according to the host IP address. **idx <trusted host index> -** Delete an existing trusted host according to the host ID that system assigned.

Example usage:

To delete the trusted host IP “192.168.0.2”:

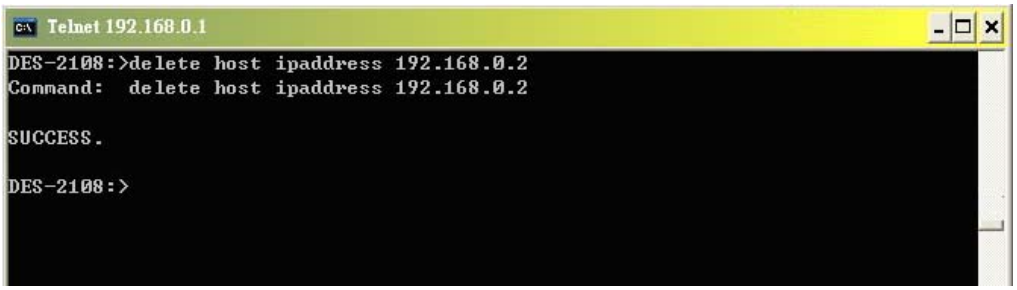

Figure 97. delete host command

To delete the trusted host ID “1”:

Figure 98. delete host command

show host	
Purpose	Used to display the trusted host that has been created.
Syntax	**show host**
Description	This command allows you to display the trusted remote stations to manage the Switch.
Parameters	None.

Example usage:

Figure 99. show host command

Trunk Commands

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

Command	Parameters
config link_aggregation	group_id <group_id 1-4> ports <port_list | null > desc <trunk name 20>
show link_aggregation	<group_id 1-4>

Each command is listed, in detail, in the following sections.

config link_aggregation

Purpose	Used to configure trunk groups.
Syntax	**config link_aggregation group_id <group_id 1-4> ports <port_list | null > desc <trunk name 20>**
Description	This command is used to configure trunk groups.
Parameters	**<group_id 1-4> -** Specify which trunk group to configure **<port_list> -** Configure a port or range of ports to add to the selected trunk group **<null > -** Remove all ports from the selected group **<trunk name 20> -** The name of trunk group to be created. A maximum of 20 characters can be used.

Example usage:

To configure port 1~4 to “trunk1” group:

Figure 100. config link_aggregation command

show link_aggregation	
Purpose	Used to display trunk groups status.
Syntax	**show link_aggregation <group_id 1-4>**
Description	This command is used to display trunk groups status.
Parameters	**<group_id 1-4> -** Specify which trunk group to display

Example usage:

To display the status of all trunk group:

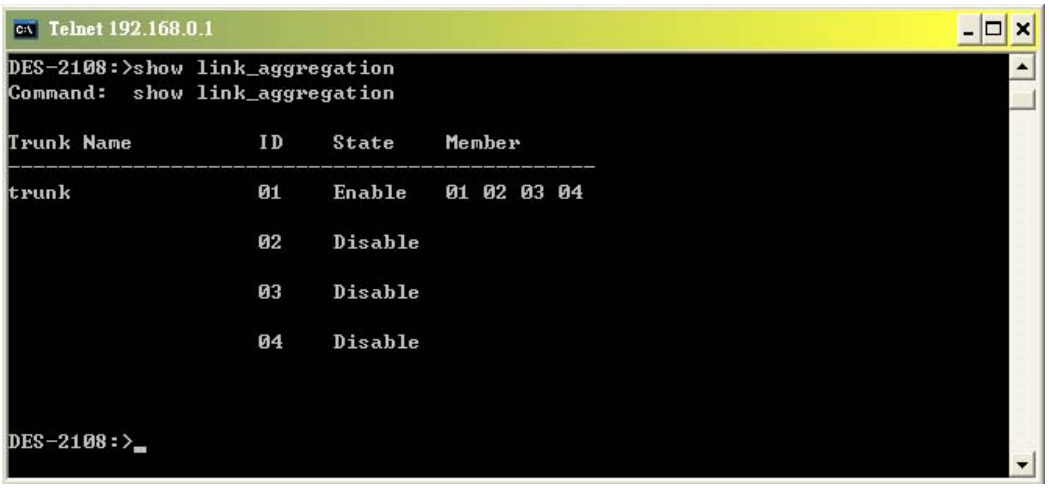

Figure 101. show link_aggregation command

SNTP Commands

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

Command	Parameters
enable sntp	
disable sntp	
show sntp	
create sntp_server	ipaddress <ipaddress> port <port>
delete sntp_server	idx <index 1-10>
show sntp_server	
enable sntp_dst	
disable sntp_dst	
config sntp_dst timezone	offset <30|60|90|120> time <±HHMM>
config sntp_dst from/to	**week <first-last> day <mon-sun> month <month> time <HHMM> config sntp_dst timezone offset**

	<30|60|90|120> time <±HHMM> config sntp_dst from/to day <day> week <week> month <month> time <HHMM>

Each command is listed, in detail, in the following sections.

enable sntp	
Purpose	Used to enable SNTP support.
Syntax	**enable sntp**
Description	This command is used to enable SNTP server support .
Parameters	None.

Example usage:

To enable SNTP server support for the switch:

Figure 102. enable sntp command

disable sntp	
Purpose	Used to disable SNTP support.
Syntax	**disable sntp**
Description	This command is used to disable SNTP server support .
Parameters	None.

Example usage:

To disable SNTP server support for the switch:

Figure 103. disable sntp command

show sntp	
Purpose	Used to display SNTP status.
Syntax	**show sntp**
Description	This command is used to display SNTP status .
Parameters	None.

Example usage:

To display SNTP status of the switch:

Figure 104. show sntp command

create sntp_server	
Purpose	Used to add.SNTP server which the SNTP information will be taken, the maximum SNTP server number is 10.
Syntax	**create sntp_server ipaddress <ipaddress> port <port number 1~65535>**
Description	This command is used to add.SNTP server which the SNTP information will be taken.

Parameters	**<ipaddress> -** The IP address of SNTP server **<port number 1~65535> -** The UDP port number of SNTP server

Example usage:

To add SNTP server 192.168.0.100 into server list:

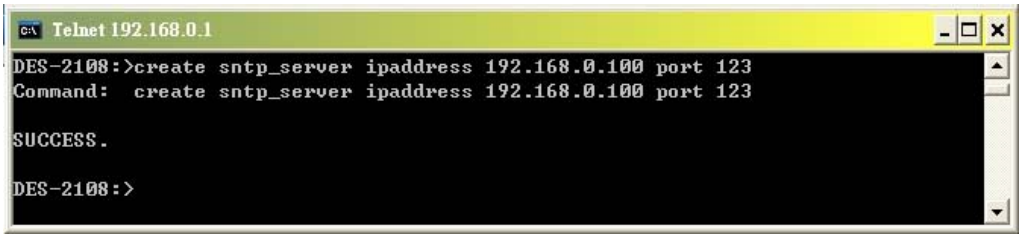

Figure 105. create sntp_server command

delete sntp_server

Purpose	Used to remove SNTP server from server list.
Syntax	**delete sntp_server idx <index 1-10>**
Description	This command is used to remove SNTP server from server list.
Parameters	**<index 1-10> -** The sntp server index in server list

Example usage:

To remove SNTP server 01 from server list:

Figure 106. delete sntp_server command

show sntp_server

Purpose	Used to display the SNTP server list.
Syntax	**show sntp_server**
Description	This command is used to display the SNTP server list.
Parameters	**<index 1-10> -** The sntp server index in server list

Example usage:

To display the SNTP server list:

Figure 107. show sntp_server command

enable sntp_dst	
Purpose	Used to enable time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	**enable sntp_dst**
Description	This command is used to enable time adjustments of DST
Parameters	None

Example usage:

To enable Daylight Savings Time adjustment:

Figure 108. enable sntp_dst command

disable sntp_dst	
Purpose	Used to disable time adjustments to allow for the use of DST.
Syntax	**enable sntp_dst**
Description	This command is used to disable time adjustments of DST
Parameters	None

Example usage:

To disable Daylight Savings Time adjustment:

Figure 109. disable sntp_dst command

config sntp_dst timezone	
Purpose	Used to configure time zone adjustments of DST.
Syntax	**config sntp_dst timezone offset <30|60|90|120> time <±HHMM>**
Description	This command is used to configure time zone adjustments of DST.
Parameters	**offset <30|60|90|120> -** Indicates number of minutes to add or to subtract during the

	summertime. The possible offset times are 30,60,90,120. **time <±HHMM> -** Indicates time adjustment +/- HH:MM from GMT

Example usage:

To configure the SNTP Daylight Savings Time offset minutes and timezone:

Figure 119. config sntp_dst timezone command

config sntp_dst from/to	
Purpose	Used to configure the repeating mode of DST time adjustment.
Syntax	**config sntp_dst from/to week <sun-sat> day <1st|2nd|3rd|4th|last> month <jan-dec> time <HHMM>**
Description	This command is used to configure the repeating mode of DST time adjustment, the end time should be configure before the beginning time and equal or greater than beginning time
Parameters	**day <1st|2nd|3rd|4th|last> -** Specify the begin/end day of repeating mode. **week <sun-sat> -** Specify the begin/end weekday of repeating mode. **month <jan-dec> -** Specify the begin/end month of repeating mode. **time <HHMM> -** Specify the begin/end time of repeating mode

Example usage:

To configure the repeating mode:

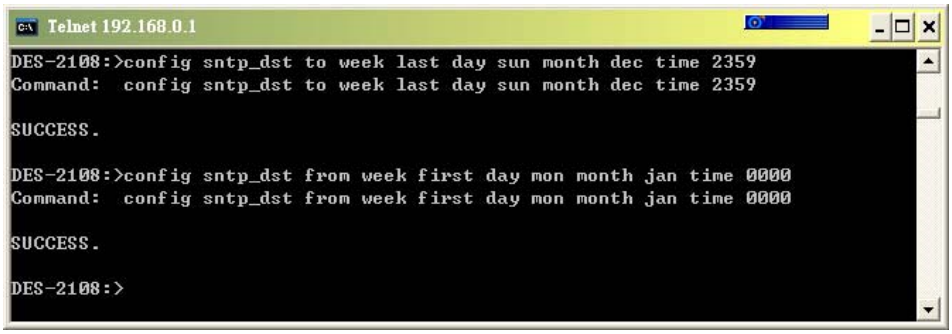

Figure 110. config sntp_dst command from/to

System Log Commands

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

Command	Parameters
enable syslog	
disable syslog	
create syslog_server	Ipaddress <ipaddress> port <port> facility <local0-7>
delete syslog_server	Idx <idx>
show syslog_server	
show syslog	

Each command is listed in detail below.

enable syslog	
Purpose	Used to enable the System Log on the switch.
Syntax	**enable syslog**
Description	This command allows you to enable System Log on the switch.

Parameters	None.

Example Usage:

Figure 111. enable syslog command

disable syslog	
Purpose	Used to disable the System Log on the switch.
Syntax	**disable syslog**
Description	This command allows you to disable System Log on the switch.
Parameters	None.

Example Usage:

Figure 112. disable syslog command

create syslog_server	
Purpose	Used to create a new server for the System Log.
Syntax	**[ipaddress <ipaddress> port <port> facility <local0-7>]**
Description	This command allows you to create a new server for the System Log.

Parameters	**Ipaddress <ipaddress> -** The IP address of syslog server. **port <port> -** The port number corresponding to the system log address. **facility <local0-7> -** Assign a facility value to the system log

Example Usage:

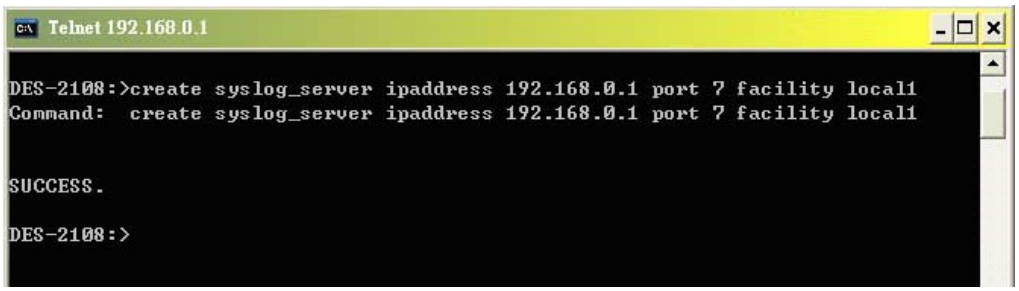

Figure 113. create syslog_server command

delete syslog_server	
Purpose	Used to delete a server for the system log.
Syntax	**idx <idx>**
Description	This command allows you to delete a server for the System Log on the switch.
Parameters	**idx <idx> -**.Deleting an existing system log according to the host ID that system assigned.

Example Usage:

Figure 114. delete syslog_server command

show syslog_server	
Purpose	Used to display the System Log server status.
Syntax	**show syslog_server**
Description	This command allows you to see the System Log server status on the switch.
Parameters	None.

Example Usage:

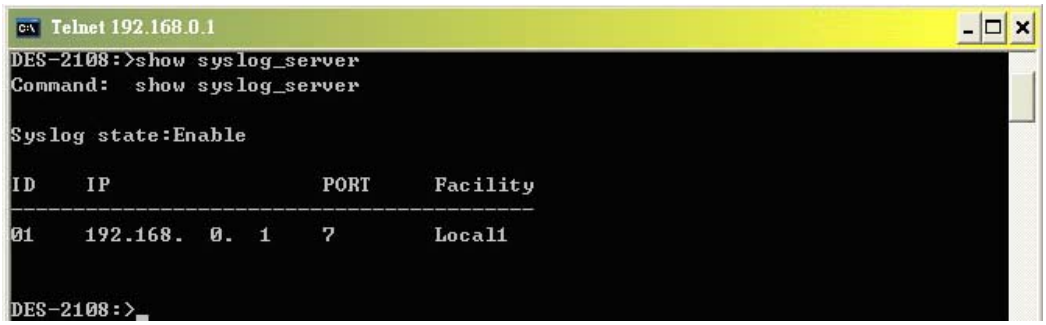

Figure 115. show syslog_server command

show syslog	
Purpose	Used to display the System Log on the switch.
Syntax	**Show syslog**
Description	This command allows you to see the System Log on the switch.
Parameters	None.

Example Usage:

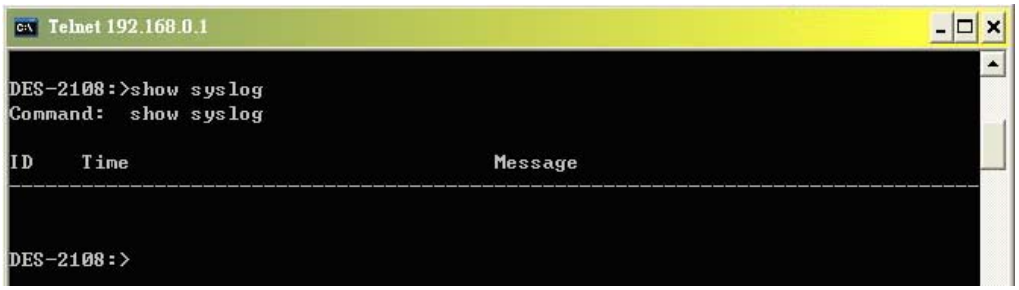

Figure 116. show syslog command

802.1x Commands

The 802.1x commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable 802.1x	
disable 802.1x	
config radius	<IP> port <port> key <key>
config 802.1x	[auth_configuration [enable_reauth <enable | disable> | quiet_period <secs 0-65535> | tx_period <secs 1-65535> | supp_timeout <secs 1-65535> | server_timeout <secs 1-65535> | max_req <secs 1-10> | reauth_period <1>] Port <port_list> <enable | disable>]
show 802.1x	[auth_configuration | auth_state | port <port_list>]

Each command is listed in detail below.

enable 802.1x	
Purpose	Used to enable 802.1x on the switch
Syntax	**enable 802.1x**
Description	This command allows you to enable 802.1x
Parameters	None.

Example Usage:

Figure 117. enable 802.1x command

disable 802.1x	
Purpose	Used to disable 802.1x on the switch
Syntax	**Disable 802.1x**
Description	This command allows you to disable 802.1x
Parameters	None.

Example Usage:

Figure 118. disable 802.1x command

config radius	
Purpose	Used to configure the radius of 802.1x on the switch.
Syntax	**<IP> port <port> key <key>**
Description	This command allows you to configure the radius of 802.1x the switch.
Parameters	**IP <IP> -** assigns a radius server according to the host IP address **port <port> -** the port number corresponding to the radius server **key <key> -** assigns the key to the radius server

Example Usage:

Figure 119. config radius 802.1x command

config 802.1x	
Purpose	Used to configure 802.1x on the switch.
Syntax	[auth_configuration [enable_reauth <enable | disable> | quiet_period <secs 0-65535> | tx_period <secs 1-65535> | supp_timeout <secs 1-65535> | server_timeout <secs 1-65535> | max_req <secs 1-10> | reauth_period <1>] **Port <port_list> <enable | disable>]**
Description	This command allows you configure 802.1x on the switch.
Parameters	**quiet period <quiet_period> -** Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default 80 seconds **tx period <tx_period> -** 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. **supp timeout <supp_timeout> -** Sets the switch-to-client retransmission time for the EAP-request frame. Default is 12 seconds **server timeout <server_timeout> -** 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. **max req <max_req> -** 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.

reauth period - <reauth_period> This command affects the behavior of the switch only if periodic re-authentication is enabled. Default is 3600

port <port_list> - the port number set for direct monitoring

Example Usage:

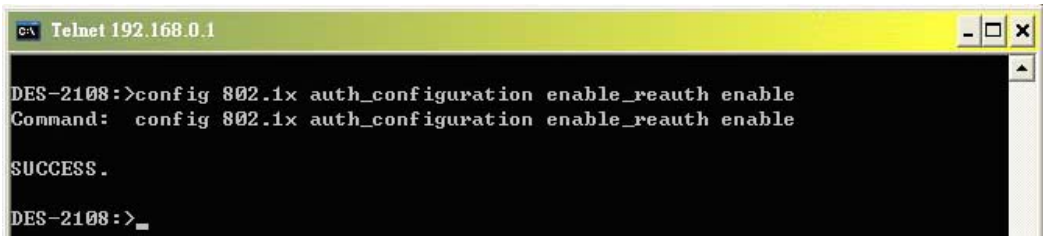

Figure 120. config 802.1x command

show 802.1x	
Purpose	Used to display the current status of 802.1x on the switch.
Syntax	**[auth_configuration | auth_state | port <port_list>]**
Description	This command allows you to see the current status of 802.1x on the switch.
Parameters	**port <port_list>** the list of ports and the port number set for direct monitoring

Example Usage:

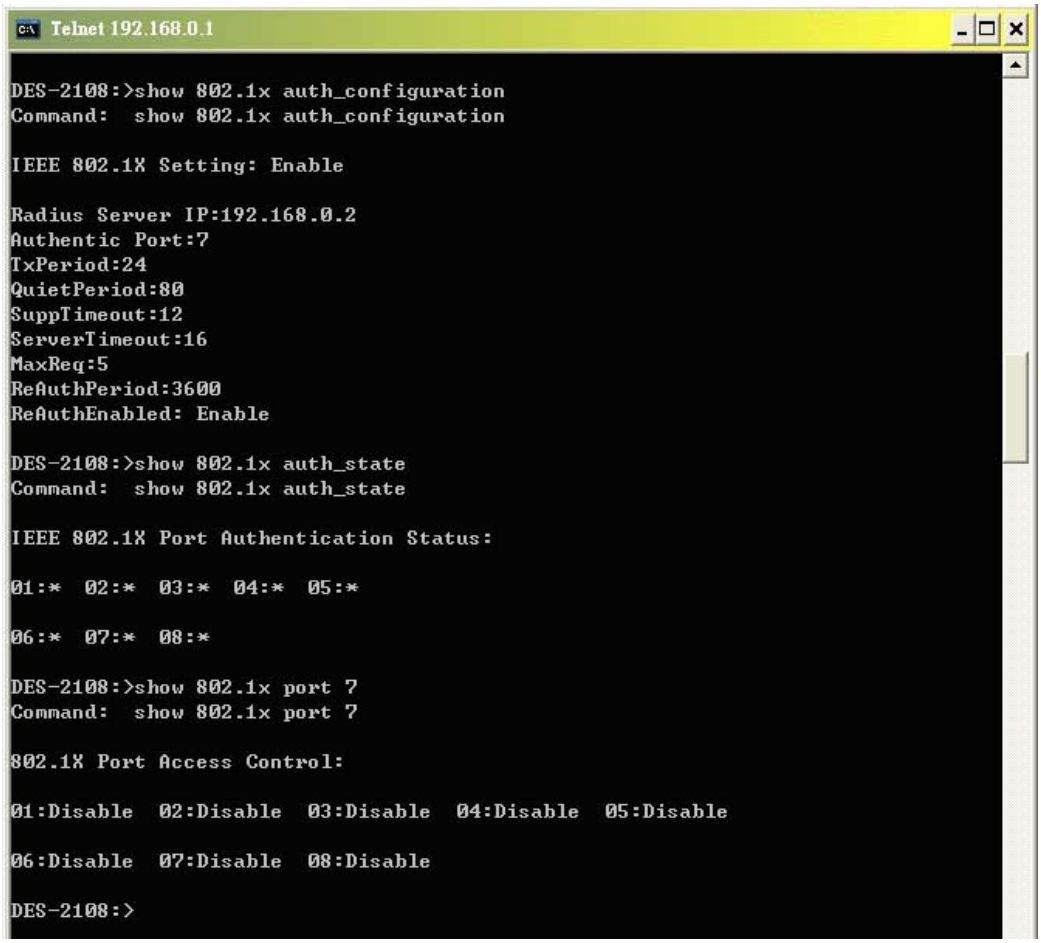

Figure 121. show 802.1x command

Management VLAN Commands

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

Command	Parameters
config mgt_vlan	[enable <vid>|disable]

Each command is listed, in detail, in the following sections.

config mgt_vlan	
Purpose	Used to configure the management VLAN
Syntax	**[enable <vid>|disable]**
Description	This command is used to enable or disable the management VLAN of the switch.
Parameters	**<vid> -** To specify which VLAN to be the management VLAN.

Example usage:

To set the VLAN 2 as the management VLAN:

Figure 122. config mgt_VLAN command

To disable the management VLAN:

Figure 123. config mgt_VLAN disable command

TECHNICAL SPECIFICATIONS

General	
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet ANSI/IEEE 802.3 Auto-negotiation IEEE 802.3x Full duplex Flow Control
Protocol:	CSMA/CD
Data Transfer Rate:	Ethernet: 10Mbps (half-duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half-duplex), 200Mbps (full-duplex)
Topology	Star
Network Cables:	Ethernet: 2-pair UTP Cat. 3/4/5, EIA/TIA- 568 STP Fast Ethernet: 2-pair UTP Cat. 5, EIA/TIA-568 STP
Number of Ports:	8 x 10/100BASE-TX Auto-MDIX UTP ports

Physical and Environmental	
DC inputs:	DC 5V/2A
Power Consumption:	9 watts maximum
Operating Temperature:	0 ~ 40 degrees Celsius
Storage Temperature:	-10 ~ 70 degree Celsius
Humidity:	10% ~ 90% RH, non-condensing
Dimensions:	192.5 x 118.5 x 32 mm (W x H x D)
EMI:	CE Class B
Performance	
Transmission Method:	Store-and-forward
RAM Buffer:	256 Kbytes per device
Filtering Address Table:	4K MAC address per device
Packet Filtering / Forwarding Rate:	Ethernet: 14,880pps Fast Ethernet: 148,800pps
MAC Address Learning:	Self-learning, Auto-aging