DES-2108

8-port 10/100

Fast Ethernet Switch

User's Guide

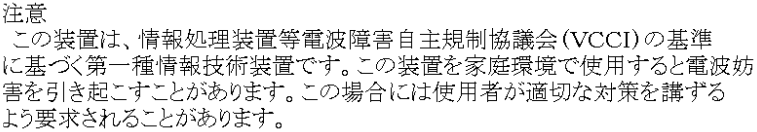
FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

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

VCCI Warning



注意

　この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準
に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨
害を引き起こすことがあります。この場合には使用者が適切な対策を講ずる
よう要求されることがあります。

TABLE OF CONTENTS

ABOUT THIS GUIDE

This user's guide tells you how to install your DES-2108, 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	Tell to how to configuration 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 "two-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.
- Provides parallel LED display for port status such as link/act, speed, etc.

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 cord**
- ✓ **Mounting kit (two brackets and screws)**
- ✓ **CD-ROM (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:

- ◆ Install the Switch on a sturdy, level surface that can support at least 6.6 lb. (3 kg) of weight. Do not place heavy objects on the Switch.
- ◆ The power outlet should be within 1.82 meters (6 feet) of the device.
- ◆ Visually inspect the power cord and see that it is fully secured to the AC power port.
- ◆ Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation

- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.

When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches and prevent it from scratching other surfaces.

Installing the Switch on a Desktop

When installing the Switch on a desktop or shelf, the rubber feet included with the Switch should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow enough ventilation space between the Switch and any other objects in the vicinity.

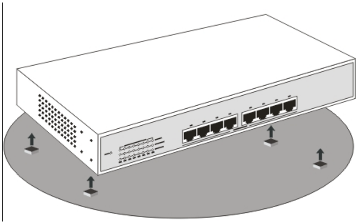


Figure 1. Installed on a Desktop

Installing the Switch on a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.

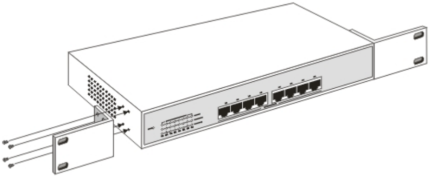


Figure 2. Fasten mounting brackets to Switch

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figure 2-2 on the following page.

Mounting the Switch in a Standard 19" Rack:

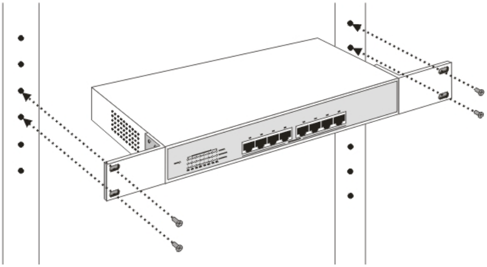


Figure 3.   Installing Switch in a rack

Power on

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

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet.

After the Switch is powered on, the LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system

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 eight (8) 10/100Mbps Fast Ethernet ports, LED indicators and Reset button.

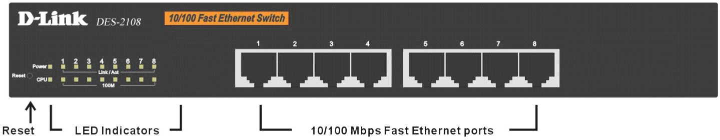


Figure 4. Front panel view

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

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*).

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.

Rear Panel

The rear panel of the Switch contains an AC power connector.

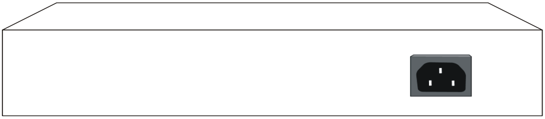


Figure 5. Rear panel view

The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

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.

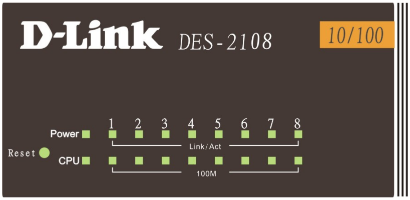


Figure 6. LED indicators

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 cord 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.

Web Management Utility

With the Web Management Utility, you can easily discover all the Web Management Switch, assign the IP Address, changing the password and upgrading the 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.

Web Management Utility

With the attached Web Management Utility, you can easily discover all the Web Management Switch, assign the IP Address, changing the password and upgrading the new firmware.

Installing the Web Management Utility

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

1. Insert the Utility CD in the CD-Rom Drive.
2. From the **Start** menu on the Windows desktop, choose **Run**.
3. In the **Run** dialog box, type D:\Web Management Utility\setup.exe (D:\ depends where your CD-Rom drive is located) and click **OK**.
4. Follow the on-screen instructions to install the utility.
5. Upon completion, go to **Program Files -> web_management_utility** and execute the Web Management utility. (Figure 6.)

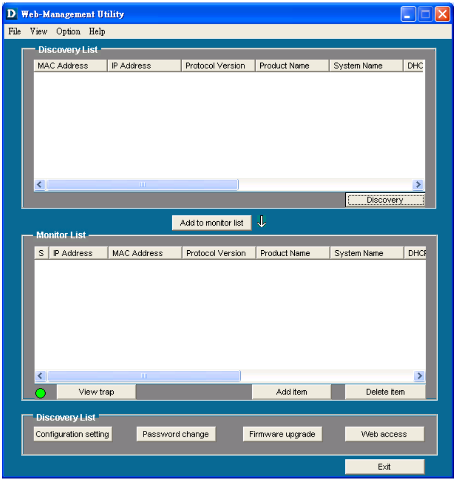


Figure 7. Web Management Utility

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

Discovery List

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

By pressing the ***"Discovery"*** 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.
- ***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.

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, ☒ represent for device system is not alive.
- ***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.
- ***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.

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 8.)

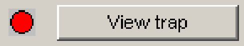
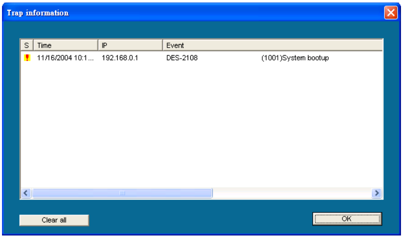


Figure 8.

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 9. Trap information)

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


Trap information

S	Time	IP	Event
!	11/16/2004 10:1...	192.168.0.1	DES-2108 (1001)System bootup

Figure 9. Trap information

Note: In order to receive Trap information, switch has to be configured with Trap IP and Trap Events in Web browser, which are available in the Trap Setting Menu (see Page 47 for detail).

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

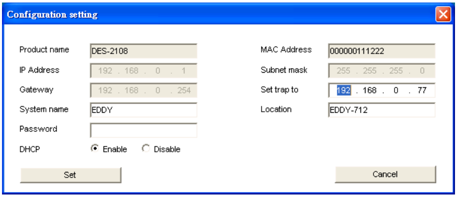
You can set the device by using the function key in the Device Setting Dialog box.

Configuration Setting:

In this Configuration Setting, you can set the IP Address, Subnet Mask, Gateway, Set Trap to (Trap IP Address), System name, Location and DHCP setting.

In factory default, the IP address of the DES-2108 will atomically assign 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 ***"Configuration setting"*** button, then the Configuration Setting window will pop out as Figure 10, after filling up the data that you want to change, you must fill up the password and press the "Set" to process the data changed immediately.



Configuration setting

Product name	DES-2108	MAC Address	000000111222
IP Address	192 . 168 . 0 . 1	Subnet mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 0 . 254	Set trap to	192 . 168 . 0 . 77
System name	EDDY	Location	EDDY-712
Password			
DHCP	● Enable ○ Disable		

Figure 10. Configuration Setting

Password Change:

You can use this Password Change when you need to change the password, fill in the password needed in the dialog box and press ***"Set"*** button to precede the password change immediately.

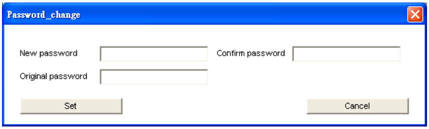
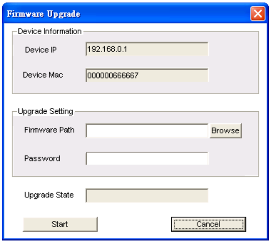


Figure 11. Password Change

Firmware Upgrade:

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


Device IP: 192.168.0.1

Device Mac: 000000666667

Figure 12. Firmware Upgrade

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, Options and Help.

File TAB:

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

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

Monitor Save As: To record the setting of the Monitor List in 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, this function will help you to show trap setting:

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 Refresh Time function, this function helps you to refresh the time of monitoring the device. Choose ***15 secs, 30 secs, 1 min, 2 min and 5 min*** to select the time of monitoring.

Help TAB

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

Configuring the Switch using Web Browser

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.

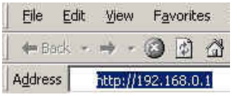
The section indicates how to manage, control and monitor the Switch via Web Browser. The Switch to enable its managed functions including:

- Port Setting
- Virtual LAN Group setting, Port-based or 802.1Q-based
- Port Mirroring
- Spanning Tree
- SNMP
- Static MAC
- IGMP Snooping
- Storm Control
- System Setting
- Device Status and Statistic
- Trap setting
- Password setting
- Backup Setting
- Reset Setting
- System Reboot

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 IP address ***http://192.168.0.1*** (the factory-default IP address setting) to the address location.

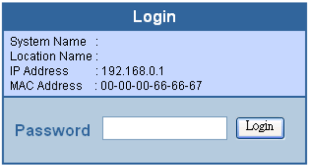


Address: http://192.168.0.1

Figure 13.

Or through the Web Management Utility, you do not need to remember the IP Address, select the device shown in the Monitor List of the Web Management Utility to settle the device on the Web Browser.

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

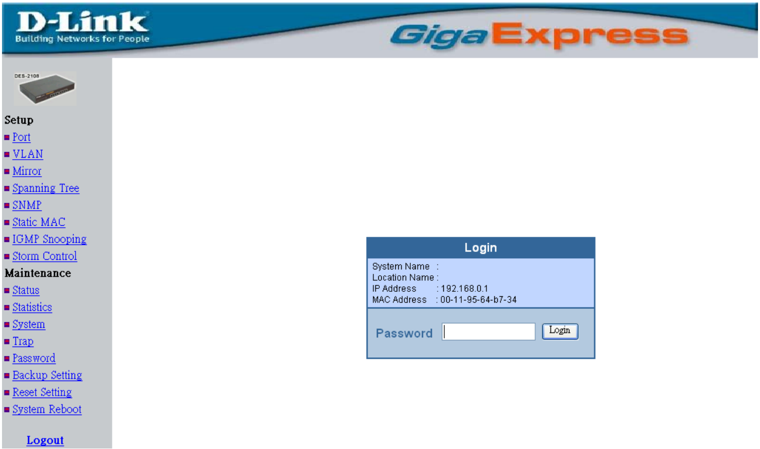


System Name :
Location Name :
IP Address : 192.168.0.1
MAC Address : 00-00-00-66-66-67

Password [ ] Login

Figure 14.

After entering the password, the main page comes up, the screen will display the device status.



System Name :
Location Name :
IP Address : 192.168.0.1
MAC Address : 00-11-95-64-b7-34

Figure 15. Device Status

Setup Menu

When the main page appears, find the ***Setup menu*** in the left side of the screen (Figure 16). Click on the setup item that you want to configure. There are fifteen options: *Port Settings, VLAN Settings, Mirror Setting, Spanning Tree Settings, SNMP Settings, Static MAC Settings, IGMP Snooping Settings, Strom Control Settings, Device Status, Statistic, System Settings, Trap Setting, Password Setting, Backup Setting, Reset Setting and System Reboot Setting* as shown in the Main Menu screen.

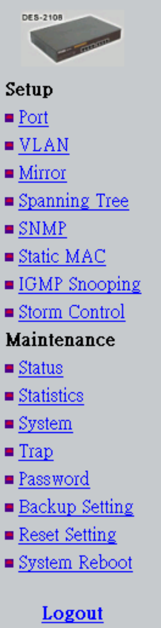


Figure 16. Setup menu

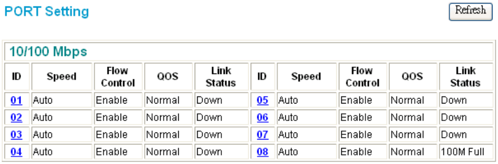
Configuring Setup Setting

Find that there are four items, including Port Settings, VLAN Settings, Mirror Settings, Spanning Tree, SNMP, Static MAC and IGMP Snooping in Setup menu.

Port Settings

In Port Settings menu (Figure 17), this page will show each port's status, press the ID parameter to set each port's *Speed, Flow Control, QoS priority and Link Status*. When you need to renew the posted information, press the "Refresh" button.

The *Link Status* in the screen will show the connection speed and duplex mode; else this dialog box will show ***down*** when the port is disconnected.



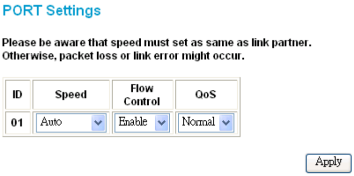
PORT Setting

10/100 Mbps

ID	Speed	Flow Control	QOS	Link Status	ID	Speed	Flow Control	QOS	Link Status
01	Auto	Enable	Normal	Down	05	Auto	Enable	Normal	Down
02	Auto	Enable	Normal	Down	06	Auto	Enable	Normal	Down
03	Auto	Enable	Normal	Down	07	Auto	Enable	Normal	Down
04	Auto	Enable	Normal	Down	08	Auto	Enable	Normal	100M Full

Figure 17. Port Configuration

To change the port setting, click on the ID parameter to enter to the selected port to configure its Speed/Disable, Flow control and QoS setting.



PORT Settings

Please be aware that speed must set as same as link partner.
Otherwise, packet loss or link error might occur.

ID	Speed	Flow Control	QoS
01	Auto	Enable	Normal

Figure 18.

Speed:

This setting has six modes -- ***100M Full***, ***100M Half***, ***10M Full***, ***10M Half, Auto and Disable*** for speed or port disable selections.

Flow Control:

This setting determines whether or not the Switch will be handling flow control. Set **Flow Control** to ***Enable*** for avoiding data transfer overflow. Or it sets to ***Disable***; there is either no flow control or other hardware/software management.

When the port is set to ***forced mode***, then the flow control will automatically set to ***Disable.***

QoS:

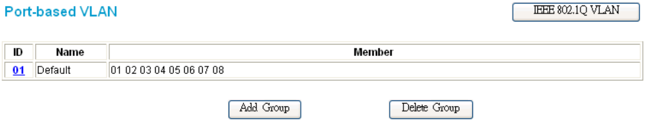
In some ports that need to have a high priority to manage the data transfer, QoS should be change. Set the port's QoS to ***high*** to determine the port will always transfer their data first.

VLAN Settings (Virtual Local Area Network)

The DES-2108 supports two of VLAN type: Port-Based VLAM or IEEE 802.1Q-Based VLAN. The VLAN setting only working on one of the two VLAN types, the default VLAN setting is Port-Based VLAN type, if you change to the other VLAN mode, the current VLAN setting will be erased.

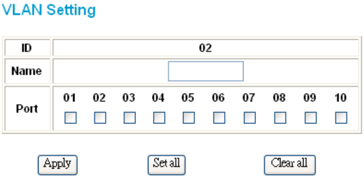
Port-based VLAN:

To add a VLAN group, press ***"Add Group"*** button, the new VLAN configuration window will pop out, you can fill in the description in order to describe this VLAN Group, check on the port to be a member to this VLAN Group, and press ***"Apply"*** button to execute the setting.


Port-based VLAN

ID	Name	Member
01	Default	01 02 03 04 05 06 07 08

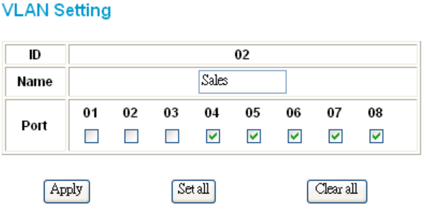
Figure 19. VLAN Group Settings


VLAN Setting

ID	02
Name	
Port	01 □ 02 □ 03 □ 04 □ 05 □ 06 □ 07 □ 08 □ 09 □ 10 □

Figure 20. Add Port-based VLAN Group

Once you want to modify the VLAN Group, check on the ID parameter, the ID VLAN configuration window will pop out.


VLAN Setting

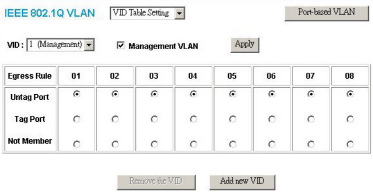
ID	02
Name	Sales
Port	01 □ 02 □ 03 □ 04 ☑ 05 ☑ 06 ☑ 07 ☑ 08 ☑

Figure 21. Port_based VLAN Settings

IEEE 802.1Q VLAN:

VID Table Setting: select the VID group that you set.

When you select VID Table Setting, press "Add new VID" to create new VID group, from port 01 ~ port 48, select Untag Port, Tag Port or Not Member for each port. To save the VID group, press "Apply" button. To remove the selected VID group, select the VID group and press "Remove the VID" button. To modify the VID group setting, select the VID group and change the setting, and press "Apply" button to save the settings.



VID : 1 (Management)

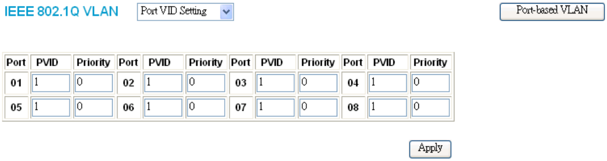
☑ Management VLAN

Egress Rule	01	02	03	04	05	06	07	08
Untag Port	●	●	●	●	●	●	●	●
Tag Port	○	○	○	○	○	○	○	○
Not Member	○	○	○	○	○	○	○	○

Figure 22. 802.1Q VID Table Setting

Port VID Setting:

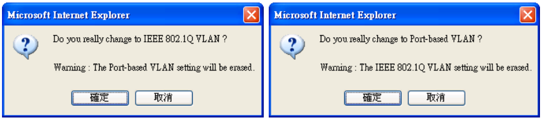
When you select Port VLAN setting, fill in each port's PVID value between 1 and 4094.



Port	PVID	Priority	Port	PVID	Priority	Port	PVID	Priority	Port	PVID	Priority
01	1	0	02	1	0	03	1	0	04	1	0
05	1	0	06	1	0	07	1	0	08	1	0

Figure 23. 802.1Q Port VID Setting

Note: If you change the VLAN mode to the other VLAN mode, the current VLAN setting will be erased.



Do you really change to IEEE 802.1Q VLAN ?

Warning : The Port-based VLAN setting will be erased.

Do you really change to Port-based VLAN ?

Warning : The IEEE 802.1Q VLAN setting will be erased.

Figure 24.

Mirror Setting

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

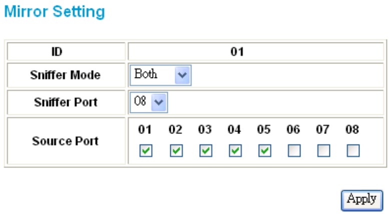
Configuring the port mirroring by assigning a source port from which to copy all packets and a sniffer port where those packets will be sent.

The selection of the sniffer mode is as follow:

TX (transmit) mode: this mode will duplicate the data transmit from the source port and forward to the sniffer port.

RX (receive) mode: this mode will duplicate the data that send to the source and forward to the sniffer port.

Both (transmit and receive) mode: this mode will duplicate both the data transmit from and data that send to the source port, then it will forward to the sniffer port.



Mirror Setting

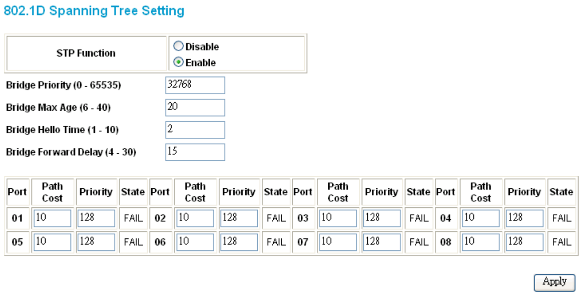
ID	01
Sniffer Mode	Both
Sniffer Port	08
Source Port	01 ☑ 02 ☑ 03 ☑ 04 ☑ 05 ☑ 06 □ 07 □ 08 □

Figure 25. Mirror Setting

Spanning Tree Setting

This Switch supports the 802.1d Spanning Tree Protocol.

Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every 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.



802.1D Spanning Tree Setting

STP Function	○ Disable ● Enable
Bridge Priority (0 - 65535)	32768
Bridge Max Age (6 - 40)	20
Bridge Hello Time (1 - 10)	2
Bridge Forward Delay (4 - 30)	15

Port	Path Cost	Priority	State	Port	Path Cost	Priority	State	Port	Path Cost	Priority	State	Port	Path Cost	Priority	State
01	10	128	FAIL	02	10	128	FAIL	03	10	128	FAIL	04	10	128	FAIL
05	10	128	FAIL	06	10	128	FAIL	07	10	128	FAIL	08	10	128	FAIL

Figure 26. Spanning Tree Setting

STP Function: To selecting enable or disable STP function on the Switch.

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

Bridge Max Age: This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that 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.

Bridge Hello Time: 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.

Bridge Forward Delay: 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.

Port Path Cost: 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.

Port 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.

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, switch group or network.

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

The DES-2108 supports the SNMP versions 1. In SNMP v.1, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

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

public - Allows authorized management stations to retrieve MIB objects.

private - Allows authorized management stations to retrieve and modify MIB objects.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Device boot up, Authentication Failure, Port status change and Abnormal transmit/receive data packet error.

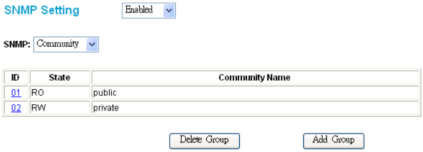
MIBs

Management and counter information are stored by the Switch in the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

Enabled / Disabled: To selecting enable or disable SNMP function on the Switch.

SNMP Community / Trap: To configure the SNMP Community or SNMP Trap configuration.

Configure SNMP Community:



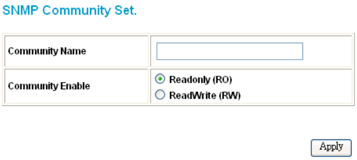
SNMP Setting: Enabled

SNMP: Community

ID	State	Community Name
01	RO	public
02	RW	private

Figure 27. SNMP Community Setting

Add Group: To add a SNMP Community group, press ***"Add Group"*** button, the Add SNMP Community configuration window will pop out; fill in the community name and assign the community enable read_only or read_write. Press "Apply" button to execute the setting.

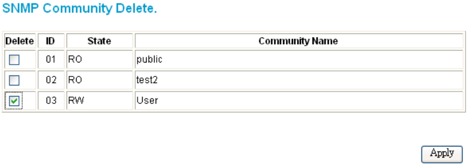


SNMP Community Set.

Community Name	
Community Enable	● Readonly (RO) ○ ReadWrite (RW)

Figure 28. Add SNMP Community group

Delete Group: To delete previously defined SNMP Community group, press ***"Delete Group"*** button, the Delete SNMP Community configuration window will pop out; checked the delete dialog box. Press ***"Apply"*** to delete the selected SNMP Community Group.

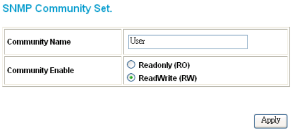


SNMP Community Delete.

Delete	ID	State	Community Name
□	01	RO	public
□	02	RO	test2
☑	03	RW	User

Figure 29. Delete SNMP Community group

Modify Group: To modify previously defined SNMP Community group, click on the ***ID*** parameter to enter to the selected SNMP Community Group to configure its community name and community enable. Press ***"Apply"*** to save change of the SNMP Community Group.

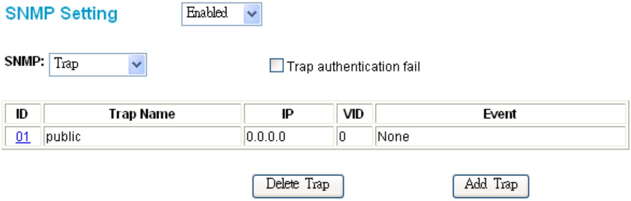


SNMP Community Set.

Community Name	User
Community Enable	○ Readonly (RO) ● ReadWrite (RW)

Figure 30. Modify SNMP Community group

Configure SNMP Trap:



SNMP Setting: Enabled

SNMP: Trap

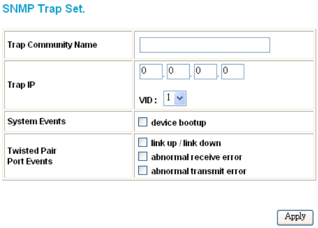
□ Trap authentication fail

ID	Trap Name	IP	VID	Event
01	public	0.0.0.0	0	None

Figure 31. Configure SNMP Trap Setting

Trap authentication fail: When checked the dialog box of the ***Trap authentication fail***, when fail to authentication, the Switch will trap the authentication fail even to the SNMP host.

Add Trap: To create a recipient of SNMP traps generated by the Switch's SNMP agent, press ***"Add Trap"*** button, and the SNMP Trap Set window will pop out; you can fill in the community name and trap IP address of the remote management station that will serve as the SNMP host for the Switch and checked the events selection to enabled selected event traps.

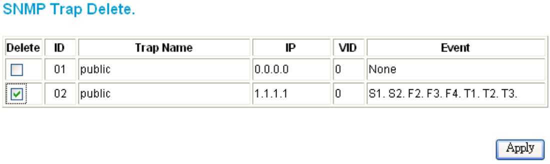


SNMP Trap Set.

Trap Community Name	
Trap IP	0 . 0 . 0 . 0 VID : 1
System Events	□ device bootup
Twisted Pair Port Events	□ link up / link down □ abnormal receive error □ abnormal transmit error

Figure 32. Add SNMP Trap

Delete Trap: To delete previously defined SNMP Trap, press ***"Delete Trap"*** button, the Delete SNMP Trap Delete configuration window will pop out; checked the delete dialog box. Press ***"Apply"*** to delete the selected SNMP Trap setting.

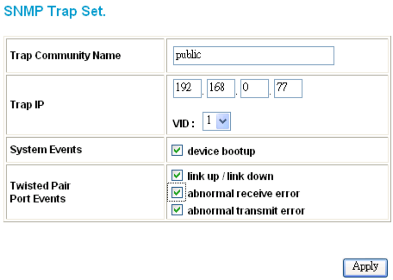


SNMP Trap Delete.

Delete	ID	Trap Name	IP	VID	Event
□	01	public	0.0.0.0	0	None
☑	02	public	1.1.1.1	0	S1. S2. F2. F3. F4. T1. T2. T3.

Figure 33. Delete SNMP Trap

Modify Trap: To modify previously defined SNMP Trap, click on the ***ID*** parameter to enter to the selected SNMP Trap to configure its community name, IP address and events. Press ***"Apply"*** to save change of the SNMP Trap.



SNMP Trap Set.

Trap Community Name	public
Trap IP	192 . 168 . 0 . 77 VID : 1
System Events	☑ device bootup
Twisted Pair Port Events	☑ link up / link down ☑ abnormal receive error ☑ abnormal transmit error

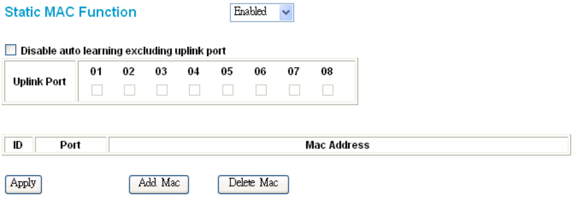
Figure 34. Modify SNMP Trap

Static MAC

The Static MAC function allows you to enable the Switch to forward the data packets to specific MAC address and specific port. Only Static MAC function enabled ports will follow the Static MAC rule from the Static MAC list.

Enabled / Disabled: Selecting the enable or disable Static MAC function on the Switch. Select "***Enabled***" to enabling the Static MAC function on the Switch, the Switch's auto learning function will be disable except the specific port (set in the "Disable auto learning excluding uplink port" setting), and the Switch will forward data following the Static MAC Address Table to the specific port. Select "***Disabled***", the Switch will learn and build MAC address table automatically and the Switch will forward data following the auto learning MAC Address Table to the specific port.

Disable auto learning excluding uplink port: When enable the Static MAC function, the Switch's auto learning function will be disable, check the dialog box of the "*Disable auto learning excluding uplink port*" and then check the dialog box of port numbers to enable the auto learning function of the port, and the Switch will forward data following the Static MAC Address Table and the Switch's auto learn MAC address table to the specific port.



Static MAC Function: Enabled

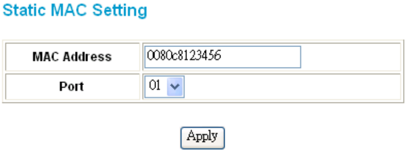
□ Disable auto learning excluding uplink port

Uplink Port	01	02	03	04	05	06	07	08
	□	□	□	□	□	□	□	□

ID	Port	Mac Address

Figure 35. Configure Static MAC Setting

Add Static MAC rule: Press ***"Add Mac"*** button, and the Static MAC Setting window will pop out; fill in the specific MAC address and select the specific port. Press "Apply" to add rule to the list.

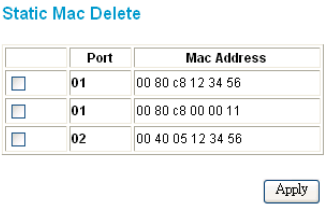


Static MAC Setting

MAC Address	0080c8123456
Port	01

Figure 36. Add Static MAC

Remove Static MAC rule: Press ***"Delete Mac"*** button, and the Static MAC Delete window will pop out; checked the dialog box. Press ***"Apply"*** to delete the selected Static MAC rule from the list.



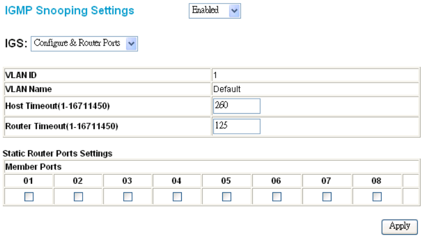
Static Mac Delete

	Port	Mac Address
□	01	00 80 c8 12 34 56
□	01	00 80 c8 00 00 11
□	02	00 40 05 12 34 56

Figure 37. Delete Static MAC

IGMP Snooping Setting

IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The number of IGMP reports that were snooped is displayed in the Reports field.



IGMP Snooping Settings: Enabled

IGS: Configure & Router Ports

VLAN ID	1
VLAN Name	Default
Host Timeout(1-16711450)	260
Router Timeout(1-16711450)	125

Static Router Ports Settings

Member Ports

01	02	03	04	05	06	07	08
□	□	□	□	□	□	□	□

Figure 38. IGMP Snooping Setting

Enabled / Disabled: To selecting enable or disable IGMP Snooping function on the Switch.

IGS Configure & Router Ports / Mcast table: To selecting of configure the IGMP Snooping or view the Multicast Entry Table.

Host Timeout (1-16711450): 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.

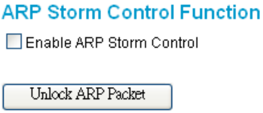
Router Timeout (1-16711450): Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. The default is 125 seconds.

Member Ports: Checked specifies 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.

Storm Control

Storm Control function allows the Switch to avoid continues broadcasting packets causes the performance drop down.

When enabled the ARP Strom Control, the Switch will detect all incoming data packets, if the Switch received more then 500 broadcast packet within a second, the Switch will stop forward the broadcasting packets till 5 minutes. If you would not wait for 5 minutes to recover back to the normal process, press the “Unlock ARP Packet” button to allow the Switch to forward the broadcast packets.



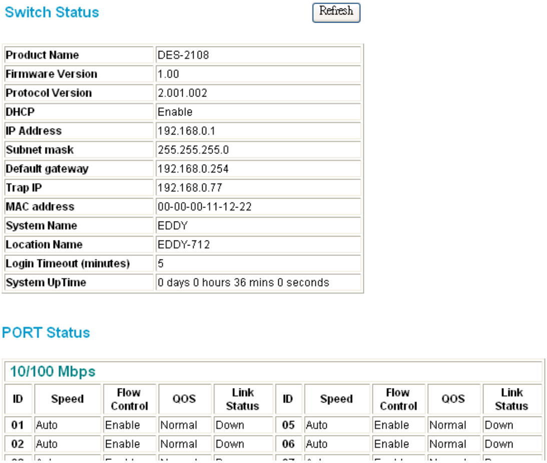
ARP Storm Control Function

□ Enable ARP Storm Control

Figure 39. ***Storm Control***

Device Status

Click on the ***"Status"*** to present the device status on this screen, it will show the System Status, Port Status, VLAN Setting, Mirror Setting, Spanning Tree status, SNMP Setting and IGMP Setting.



Product Name	DES-2108
Firmware Version	1.00
Protocol Version	2.001.002
DHCP	Enable
IP Address	192.168.0.1
Subnet mask	255.255.255.0
Default gateway	192.168.0.254
Trap IP	192.168.0.77
MAC address	00-00-00-11-12-22
System Name	EDDY
Location Name	EDDY-712
Login Timeout (minutes)	5
System UpTime	0 days 0 hours 36 mins 0 seconds

10/100 Mbps

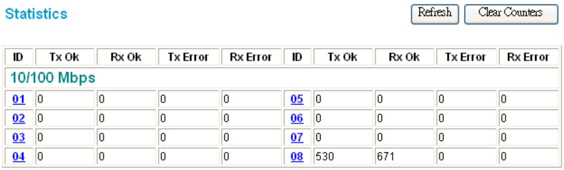
ID	Speed	Flow Control	QOS	Link Status	ID	Speed	Flow Control	QOS	Link Status
01	Auto	Enable	Normal	Down	05	Auto	Enable	Normal	Down
02	Auto	Enable	Normal	Down	06	Auto	Enable	Normal	Down

Figure 40. Device Status.

Press ***"Refresh"*** when you need to renew the posted information.

Statistic

The Statistic Menu screen will show the status of each port packet count.

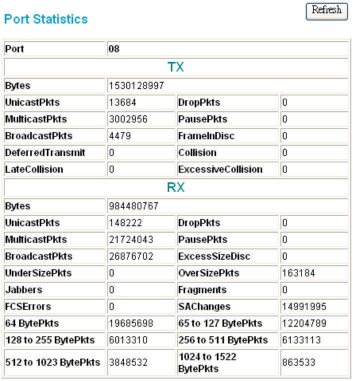


Statistics

ID	Tx Ok	Rx Ok	Tx Error	Rx Error	ID	Tx Ok	Rx Ok	Tx Error	Rx Error
10/100 Mbps									
01	0	0	0	0	05	0	0	0	0
02	0	0	0	0	06	0	0	0	0
03	0	0	0	0	07	0	0	0	0
04	0	0	0	0	08	530	671	0	0

Figure 41. Device Statistics

For Detail packet information, click on the ID parameter as Figure 42.



Port Statistics

Port	08		
TX			
Bytes	1530128997		
UnicastPkts	13684	DropPkts	0
MulticastPkts	3002956	PausePkts	0
BroadcastPkts	4479	FrameInDisc	0
DeferredTransmit	0	Collision	0
LateCollision	0	ExcessiveCollision	0
RX			
Bytes	984480767		
UnicastPkts	148222	DropPkts	0
MulticastPkts	21724043	PausePkts	0
BroadcastPkts	26876702	ExcessSizeDisc	0
UnderSizePkts	0	OverSizePkts	163184
Jabbers	0	Fragments	0
FCSErrors	0	SAChanges	14991995
64 BytePkts	19685698	65 to 127 BytePkts	12204789
128 to 255 BytePkts	6013310	256 to 511 BytePkts	6133113
512 to 1023 BytePkts	3848532	1024 to 1522 BytePkts	863533

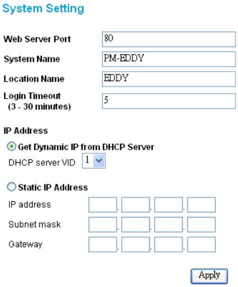
Figure 42. Port Statistics

System Setting

The System Setting includes the System name, Location name, Login Timeout, IP Address, Subnet Mask and Gateway. Through the Web Management Utility, you can easily recognize the device by using the System Name and the Location Name.

The Login Timeout is to set the idle time-out for security issue, when there is no action when running the Web Smart Utility and the time is up, you must re-login to Web Smart Utility before you set the Utility.

Fill up the IP address, Subnet mask and Gateway for the device or enable DHCP get IP address from DHCP server.



System Setting

Web Server Port	80
System Name	PM-EDDY
Location Name	EDDY
Login Timeout (3 - 30 minutes)	5

IP Address

● Get Dynamic IP from DHCP Server

DHCP server VID: 1

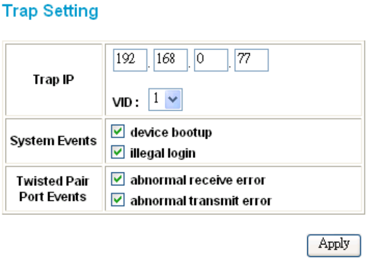
○ Static IP Address

IP address	. . .
Subnet mask	. . .
Gateway	. . .

Figure 43. System Setting

Trap Setting

The Trap Setting enables the device to monitor the Trap through the Web Management Utility, set the Trap IP Address of the manager where the trap to be sent.



Trap Setting

Trap IP	192 . 168 . 0 . 77 VID : 1
System Events	☑ device bootup ☑ illegal login
Twisted Pair Port Events	☑ abnormal receive error ☑ abnormal transmit error

Figure 44. Trap Setting

System Events: Monitoring the system’s trap.

Device Bootup: a trap when booting up the system.

Illegal Login: a trap when there is using a wrong password login, and it will record from where the IP to be login.

Copper Port Events: Monitoring the copper port status.

Abnormal* Receive Error: a trap when there are receive data error in copper port.

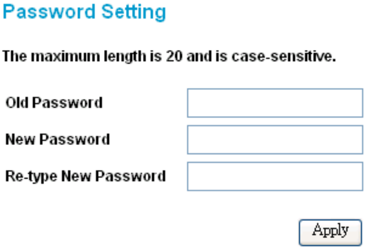
Abnormal* Transmit Error: a trap when there are transmit data error in copper port.

Abnormal*: 50 error packet count within 10 seconds.

Set Password

Password is the invaluable tool for the manager to secure Web Management Switch, use this function to change the password.

If you forget the password, press the “Reset” button in the rear panel of the Switch, the current setting includes VLAN, Port Setting… etc. will be lost and the Switch will restore to the default setting.



Password Setting

The maximum length is 20 and is case-sensitive.

Old Password

New Password

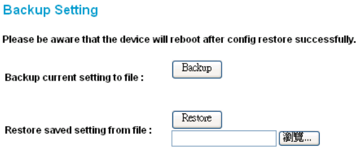
Re-type New Password

Figure 45. Set Password

Backup Setting

The backup tools help you to backup the current setting of the Switch. Once you need to backup the setting, press the ***“Backup”*** button to save the setting.

To restore a current setting file to the device, you must specify the backup file and press ***“Restore”*** button to proceed the setting of the recorded file.



Backup Setting

Please be aware that the device will reboot after config restore successfully.

Backup current setting to file :

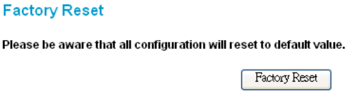
Restore saved setting from file :

Figure 46. Backup Setting

Note: when restoring a recorded file, the current password will not be erased.

Reset Setting

The Factory Reset button helps you to reset the device back to the default setting from the factory. Be aware that the entire configuration will be reset, the IP address of the device will be get from DHCP server (factory default is DHCP enabled) or got the default IP address of 192.168.0.1 when fail to get the IP address from DHCP server.



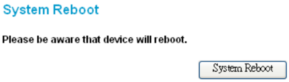
Factory Reset

Please be aware that all configuration will reset to default value.

Figure 47. Reset Setting

System Reboot

Press “System Reboot” button to warm start the Switch



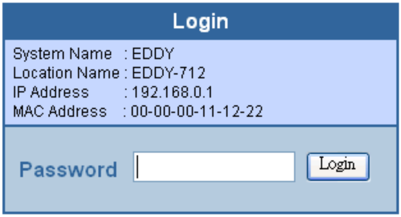
System Reboot

Please be aware that device will reboot.

Figure 48. System Reboot

Logout

When press this function, the web configuration will go back to first Login page.



System Name : EDDY
Location Name : EDDY-712
IP Address : 192.168.0.1
MAC Address : 00-00-00-11-12-22

Figure 49. Logout

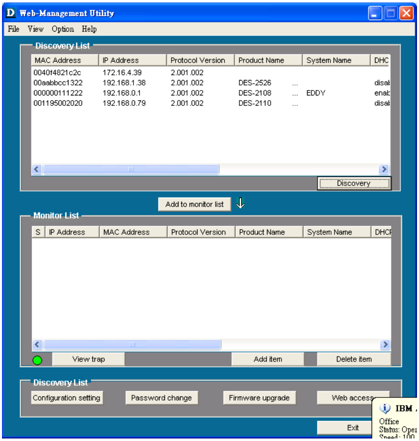
Configuring the Switch using the CLI

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 ***Web Management Utility*** to get or setting the IP address of the Switch.



MAC Address	IP Address	Protocol Version	Product Name	System Name	DHC
0040f4821c2c	172.16.4.39	2.001.002			
00aabbcc1322	192.168.1.38	2.001.002	DES-2526 ...		disal
000000111222	192.168.0.1	2.001.002	DES-2108 ...	EDDY	enak
001195002020	192.168.0.79	2.001.002	DES-2110 ...		disal

Figure 50. Web Management Utility

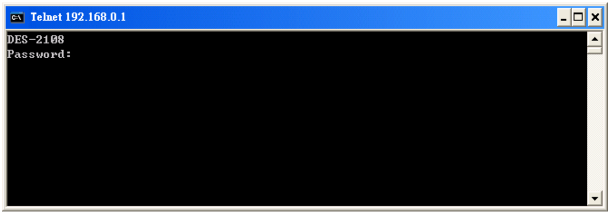
Using the CLI via Telnet interface

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:

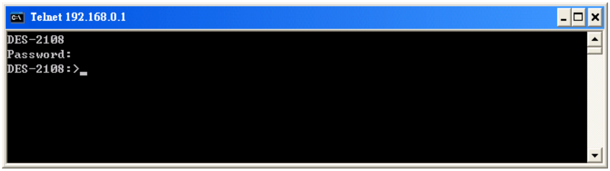


```
DES-2108
Password:
```

Figure 51. The DES-2108 console login

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

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



```
DES-2108
Password:
DES-2108:>_
```

Figure 52. 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**

<table>
<tr><th colspan="2">| vertical bar</th></tr>
<tr><td><b>Purpose</b></td><td>Separates two or more mutually exclusive items in a list, one of which must be entered.</td></tr>
<tr><td><b>Syntax</b></td><td><b>show snmp [community | host]</b></td></tr>
<tr><td><b>Description</b></td><td>In the above syntax sample, you must specify either a community or host configuration to be show.</td></tr>
<tr><td><b>Example Command</b></td><td><b>show snmp host</b></td></tr>
</table>

{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.

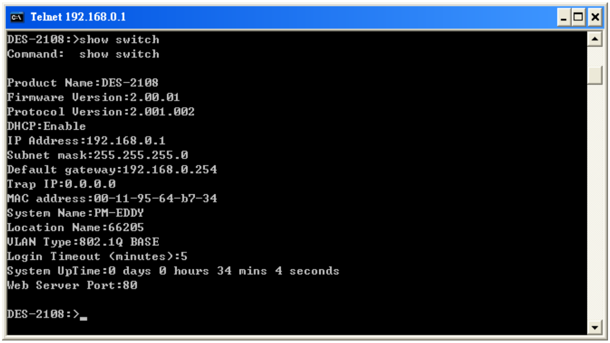
Command	Parameters
show switch	
config snmp system_contact	<system_contact 20>
config snmp system_name	<system_name 20>
config snmp system_location	<location_name 20>
config snmp aging_time	<value 1 -1048575>
reset	<config>
logout	
save	

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:



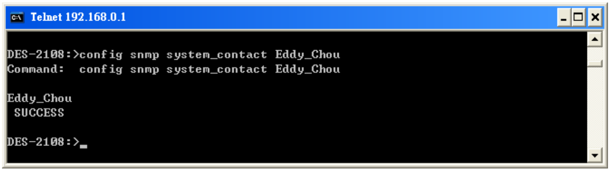
```
DES-2108:>show switch
Command:  show switch

Product Name:DES-2108
Firmware Version:2.00.01
Protocol Version:2.001.002
DHCP:Enable
IP Address:192.168.0.1
Subnet mask:255.255.255.0
Default gateway:192.168.0.254
Trap IP:0.0.0.0
MAC address:00-11-95-64-b7-34
System Name:PM-EDDY
Location Name:66205
VLAN Type:802.1Q BASE
Login Timeout (minutes):5
System UpTime:0 days 0 hours 34 mins 4 seconds
Web Server Port:80

DES-2108:>_
```

Figure 53. ***show switch*** **command**

config snmp system_contact	
Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	**config snmp system_contact <system_contact>**
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> -** A maximum of 20 character can be used, space character is not allowed.

Example usage:

To configure the Switch contact to "Eddy_Chou":



```
DES-2108:>config snmp system_contact Eddy_Chou
Command:  config snmp system_contact Eddy_Chou

Eddy_Chou
 SUCCESS

DES-2108:>_
```

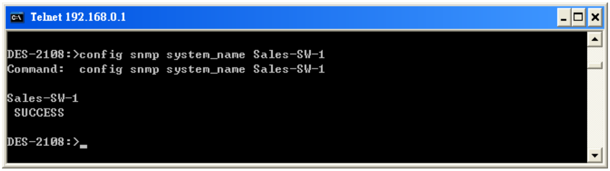
Figure 54. ***config snmp system_contact*** **command**

config snmp system_name

Purpose	Used to configure the name for the Switch.
Syntax	**config snmp system_name <system_name>**
Description	The config snmp system_name command configures the name of the Switch.
Parameters	**<system_name> -** A maximum of 20 character can be used, space character is not allowed.

Example usage:

To configure the Switch name for "Sales-SW-1":



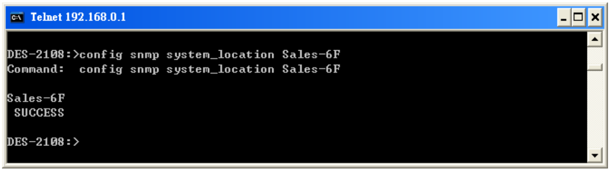
```
DES-2108:>config snmp system_name Sales-SW-1
Command:  config snmp system_name Sales-SW-1

Sales-SW-1
 SUCCESS

DES-2108:>_
```

Figure 55. ***config snmp system_name*** **command**

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

Example usage:

To configure the Switch location for "Sales-6F":



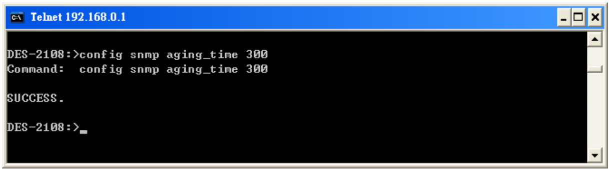
```
DES-2108:>config snmp system_location Sales-6F
Command:  config snmp system_location Sales-6F

Sales-6F
 SUCCESS

DES-2108:>
```

Figure 56. ***config snmp system_location*** **command**

config snmp aging_time	
Purpose	Used to set the aging time of the forwarding database.
Syntax	**config snmp system aging_time <value 1 - 1048575 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 10 to 1048575 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 1 -1048575 sec> -** The aging time for the MAC address forwarding database value. The value in seconds may be between 1 and 1048575 seconds.

Example usage:

To set the aging time:



```
DES-2108:>config snmp aging_time 300
Command:  config snmp aging_time 300

SUCCESS.

DES-2108:>_
```

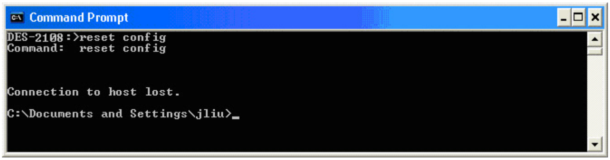
Figure 57. ***config snmp aging_time*** **command**

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:



```
DES-2108:>reset config
Command:  reset config


Connection to host lost.

C:\Documents and Settings\jliu>_
```

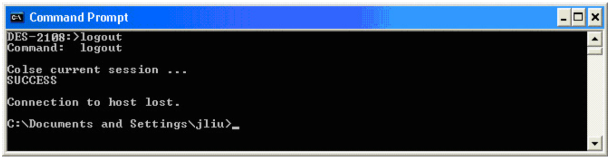
Figure 58. ***reset*** **command**

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:



```
DES-2108:>logout
Command:  logout

Colse current session ...
SUCCESS

Connection to host lost.

C:\Documents and Settings\jliu>_
```

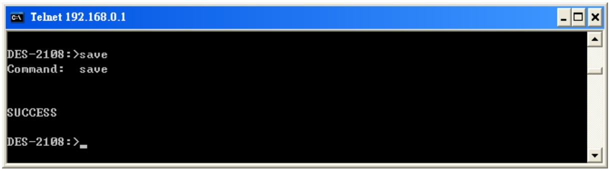
Figure 59. *logout* command

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:



```
DES-2108:>save
Command:  save


SUCCESS

DES-2108:>_
```

Figure 60. *save* 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.

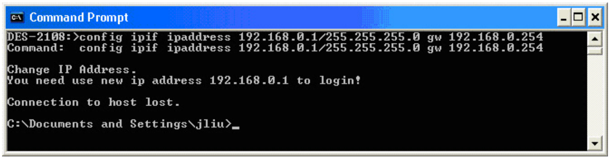
Command	Parameters
config ipif	[ipaddress <network address> {gw <ipaddress>} | dhcp {vid <vlan_id>}]
show ipif	

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 <vlan_id>}]**
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 (for example,
Parameters	192.168.100.100/255.255.255.0 of in CIDR format, 192.168.100.100/24. **dhcp -** Allows the selection of the DHCP protocol for the assignment of an IP address to Switch's system IP address. **<vlan_id> -** Specific the 802.1Q VLAN ID to the Switch. The range between 1 to 4094.

Example usage:

To configure the IP interface System:



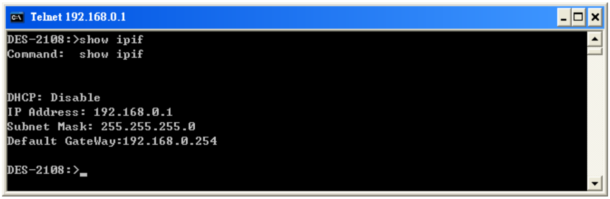
```
DES-2108:>config ipif ipaddress 192.168.0.1/255.255.255.0 gw 192.168.0.254
Command:  config ipif ipaddress 192.168.0.1/255.255.255.0 gw 192.168.0.254

Change IP Address.
You need use new ip address 192.168.0.1 to login!

Connection to host lost.

C:\Documents and Settings\jliu>_
```

Figure 61. ***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:



```
DES-2108:>show ipif
Command:  show ipif


DHCP: Disable
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Default GateWay:192.168.0.254

DES-2108:>_
```

Figure 62. *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.

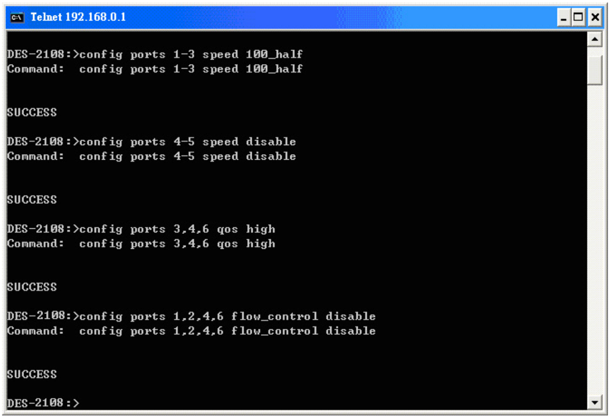
Command	Parameters
config ports	[<portlist | all> {speed [disable |auto |10_half | 10_full | 100_half | 100_full | 1000_full} | {flow_control [enable | disable] | qos {normal | high]}
show ports	{portlist}

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 | 1000_full} | {flow_control [enable | disable] | qos {normal | high]}**
Description	This command allows for the configuration of the Switch's Ethernet ports.
Parameters	**all -** Configure all ports on the Switch. **<portlist> -** Specifies a port or range to be configured. **speed -** Allows the user to adjust the speed for a port or range of ports. The user has a choice of the following: **auto -** Enables auto-negotiation for the specified range of ports. **[10 | 100 | 1000] -** 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 [normal | high] -** 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:



```
DES-2108:>config ports 1-3 speed 100_half
Command:  config ports 1-3 speed 100_half


SUCCESS

DES-2108:>config ports 4-5 speed disable
Command:  config ports 4-5 speed disable


SUCCESS

DES-2108:>config ports 3,4,6 qos high
Command:  config ports 3,4,6 qos high


SUCCESS

DES-2108:>config ports 1,2,4,6 flow_control disable
Command:  config ports 1,2,4,6 flow_control disable


SUCCESS

DES-2108:>
```

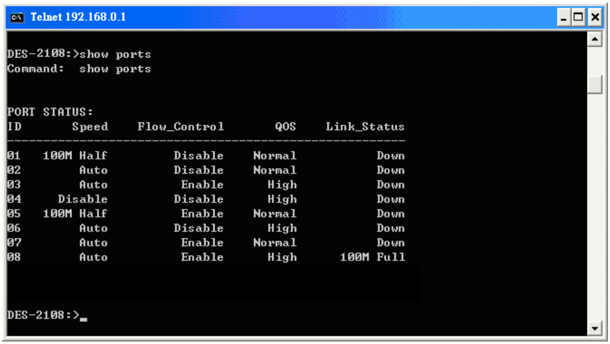
Figure 63. *config ports* command

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:



```
DES-2108:>show ports
Command:  show ports


PORT STATUS:
ID        Speed     Flow_Control        QOS     Link_Status
-----------------------------------------------------------
01    100M Half          Disable     Normal            Down
02         Auto          Disable     Normal            Down
03         Auto           Enable       High            Down
04      Disable          Disable       High            Down
05    100M Half           Enable     Normal            Down
06         Auto          Disable       High            Down
07         Auto           Enable     Normal            Down
08         Auto           Enable       High       100M Full


DES-2108:>_
```

Figure 64. *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	[<vlan_name 8> | tag <vlanid 1~4094>]
delete vlan	<vlan_name 8> {tag <vlanid 1~4094>}
config vlan	[<vlan_name 8> { tag <vlanid 1~4094>} [add {[tagged | untagged]}| delete] <portlist>
show vlan	{[<vlan_name 8> | tag <vlanid 1~4094>]}
config management _vlan	[vlanid 1~4094]
enable port_based vlan	

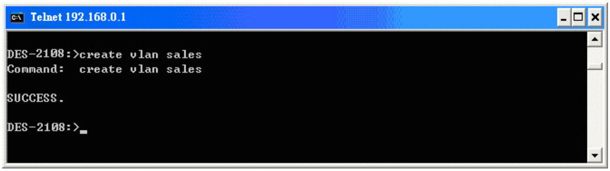
Command	Parameters
disable 802.1q_based vlan	
config pvid	<portlist> <vlanid 1~4094> priority <0-7>
disable port_based vlan	
enable 802.1q_based vlan	

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

create vlan	
Purpose	Used to create a VLAN on the Switch.
Syntax	**create vlan [<vlan_name 8> | tag <vlanid 1~4094>]**
Description	This command allows you to create a VLAN on the Switch.
Parameters	**<vlan_name 8> -** The name of Port_based VLAN to be created. A maximum of 8 characters can be used. **<vlanid 1~4094> -** The VLAN ID of the 802.1Q_based VLAN to be created. Allowed values = 1~4094

Example usage:

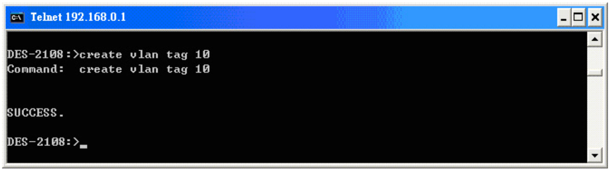
To create a Port_based VLAN, "sales" VLAN group:



```
DES-2108:>create vlan sales
Command:  create vlan sales

SUCCESS.

DES-2108:>_
```

Figure 65. ***create vlan*** **command (port_based VLAN)**

To create an 802.1Q_based VLAN, tag 2:



```
DES-2108:>create vlan tag 10
Command:  create vlan tag 10


SUCCESS.

DES-2108:>_
```

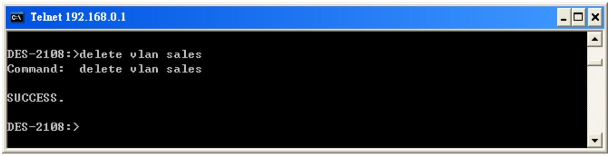
Figure 66. ***create vlan*** **command (802.1q_based VLAN)**

delete vlan

Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	**delete vlan [<vlan_name 8> | tag <vlanid 1~4094>]**
Description	This command will delete a previously configured VLAN on the Switch
Parameters	**<vlan_name 8> -** The VLAN name of the Port_based VLAN you want to delete. **<vlanid 1-4094> -** The VLAN ID of the 802.1Q_Based VLAN you want to delete.

Example usage:

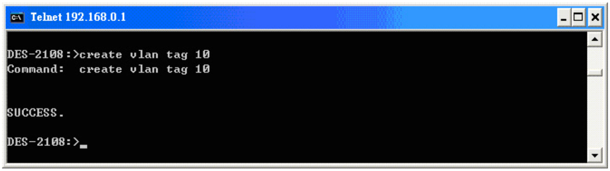
To delete a Port_based VLAN, “sales” VLAN group:



```
DES-2108:>delete vlan sales
Command:  delete vlan sales

SUCCESS.

DES-2108:>
```

Figure 67. ***create vlan*** **command (port_based VLAN)**

To delete an 802.1Q_based VLAN, tag 10:



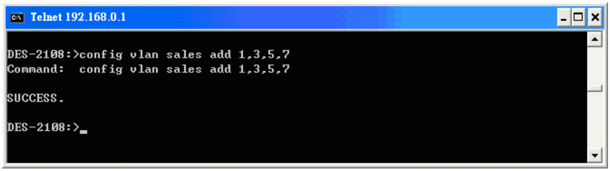
```
DES-2108:>create vlan tag 10
Command:  create vlan tag 10


SUCCESS.

DES-2108:>_
```

Figure 68. ***delete vlan*** **command (802.1q_based VLAN)**

config vlan	
Purpose	Used to additional ports to a previously configured VLAN.
Syntax	**config vlan [<vlan_name 8> | tag <vlanid 1~4094> add {tagged | untagged} | delete <portlist>]**
Description	This command allows you to add ports to the port list of previously configured VLAN.
Parameters	**<vlan_name 8> -** The name of the Port_based VLAN you want to add/delete ports to/from. **<vlanid 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:

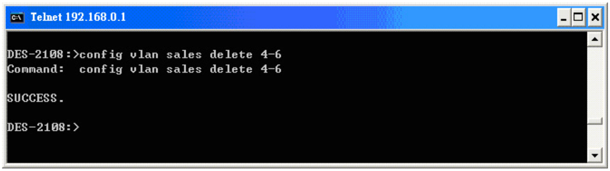
To add port 1, 3, 5, 6 to the “sales” VLAN group:



```
DES-2108:>config vlan sales add 1,3,5,7
Command:  config vlan sales add 1,3,5,7

SUCCESS.

DES-2108:>_
```

Figure 69. ***config vlan*** **command, add VLAN group members (port_based VLAN)**

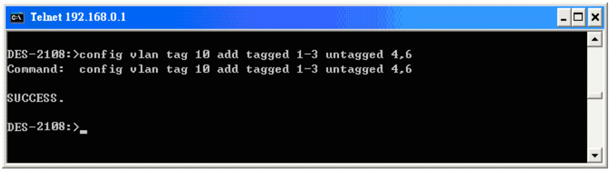
To delete 4 through 6 ports from the “sales” VLAN group:



```
DES-2108:>config vlan sales delete 4-6
Command:  config vlan sales delete 4-6

SUCCESS.

DES-2108:>
```

Figure 70. ***config vlan*** **command, delete VLAN group members (port_based VLAN)**

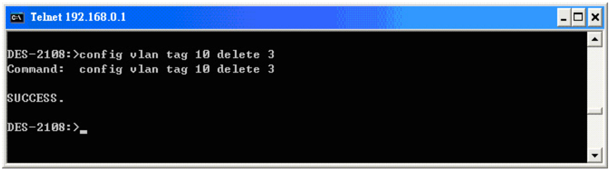
To add 1 through 3 as tagged ports to the VLAN tag 10:



```
DES-2108:>config vlan tag 10 add tagged 1-3 untagged 4,6
Command:  config vlan tag 10 add tagged 1-3 untagged 4,6

SUCCESS.

DES-2108:>_
```

Figure 71. ***config vlan*** **command, add VLAN group members (802.1q_based VLAN)**

To delete port 3 from the VLAN tag 10:



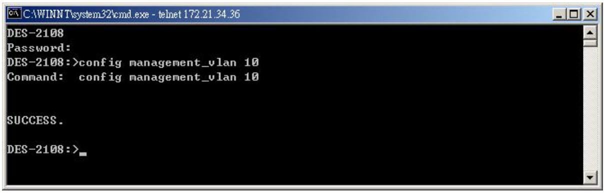
```
DES-2108:>config vlan tag 10 delete 3
Command:  config vlan tag 10 delete 3

SUCCESS.

DES-2108:>_
```

Figure 72. *config vlan* command, delete VLAN group members (802.1q_based VLAN)

config management _vlan	
Purpose	Used to change the management VLAN in 802.1Q_based VLAN type on the Switch.
Syntax	**config management _vlan**
Description	This command allows you to change management VLAN in 802.1Q_based VLAN type on the Switch.
Parameters	[vlanid 1~4094]

Example usage:

To change the management VLAN id to 10:



```
DES-2108
Password:
DES-2108:>config management_vlan 10
Command:  config management_vlan 10


SUCCESS.

DES-2108:>_
```

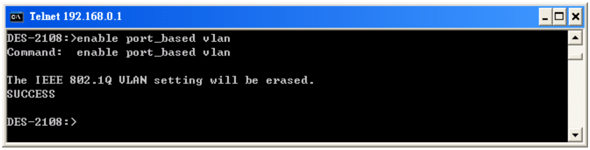
Figure 73. config management _vlan command

enable port_based vlan

Purpose	Used to change the VLAN type to Port_based VLAN type on the Switch.
Syntax	**enable port_based vlan**
Description	This command allows you to change the VLAN type to Port_based VLAN on the Switch.
Parameters	None.

Example usage:

To switched the VLAN type to Port_based VLAN



```
DES-2108:>enable port_based vlan
Command:  enable port_based vlan

The IEEE 802.1Q VLAN setting will be erased.
SUCCESS

DES-2108:>
```

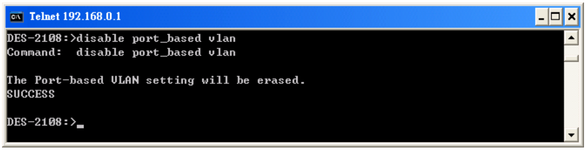
Figure 74. ***enable port_based vlan*** **command**

disable port_based vlan

Purpose	Used to change the VLAN type to 802.1Q_based VLAN on the Switch.
Syntax	**disable port_based vlan**
Description	This command allows you to change the VLAN type to 802.1Q_based VLAN on the Switch.
Parameters	None.

Example usage:

To switched the VLAN type to 802.1Q_based VLAN



```
DES-2108:>disable port_based vlan
Command:  disable port_based vlan

The Port-based VLAN setting will be erased.
SUCCESS

DES-2108:>_
```

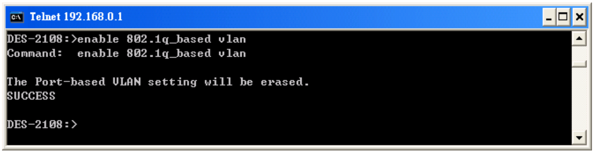
Figure 75. ***disable port_based vlan*** **command**

enable 802.1q_based vlan

Purpose	Used to change the VLAN type to 802.1Q_based VLAN on the Switch.
Syntax	**enable 802.1q_based vlan**
Description	This command allows you to change the VLAN type to 802.1Q_based VLAN on the Switch.
Parameters	None.

Example usage:

To switched the VLAN type to 802.1Q_based VLAN



```
DES-2108:>enable 802.1q_based vlan
Command:  enable 802.1q_based vlan

The Port-based VLAN setting will be erased.
SUCCESS

DES-2108:>
```

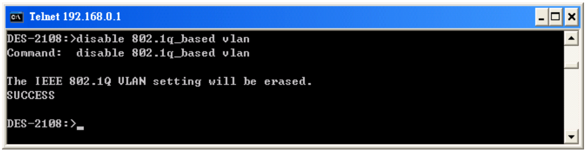
Figure 76. *enable 802.1q_based vlan* command

disable 802.1q_based vlan

Purpose	Used to change the VLAN type to port_based VLAN on the Switch.
Syntax	**disable 802.1q_based vlan**
Description	This command allows you to change the VLAN type to port_based VLAN on the Switch.
Parameters	None.

Example usage:

To switched the VLAN type to Port_based VLAN



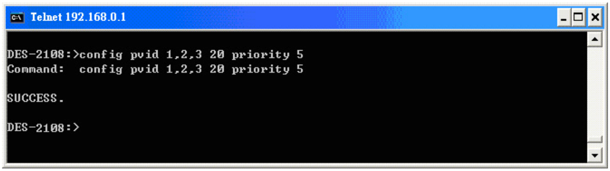
```
DES-2108:>disable 802.1q_based vlan
Command:  disable 802.1q_based vlan

The IEEE 802.1Q VLAN setting will be erased.
SUCCESS

DES-2108:>_
```

Figure 77. *disable 802.1q_based vlan* command

config pvid	
Purpose	Used to configure the 802.1Q Port VLAN ID and priority.
Syntax	**config pvid <portlist> <vlanid 1~4094> priority <0~7>**
Description	This command allows you to configure the 802.1Q Port VLAN ID and priority.
Parameters	**<portlist> -** A port or range of ports to configure to the specified PVID. **<vlanid 1~4094> -** To configure the 802.1Q VLAN ID to the specified ports. **priority <0~7> -** To configure the priority to the specified PVID.

Example usage:

To configure the 802.1Q Port VLAN_ID:



```
DES-2108:>config pvid 1,2,3 20 priority 5
Command:  config pvid 1,2,3 20 priority 5

SUCCESS.

DES-2108:>
```

Figure 78. ***config pvid*** **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 | disable] {<port> source ports <portlist> [rx | tx |both]}

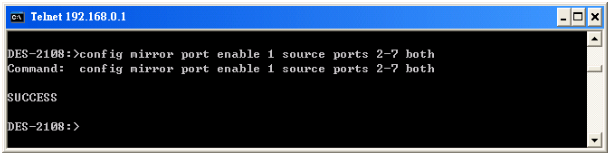
show mirror	

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 | disable] {<port> source ports <portlist> [rx | tx |both]}**
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:

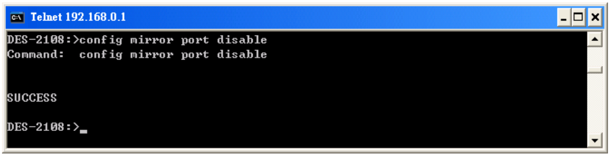
To enable and configure the Port Mirror function of the Switch:



```
DES-2108:>config mirror port enable 1 source ports 2-7 both
Command:  config mirror port enable 1 source ports 2-7 both

SUCCESS

DES-2108:>
```

Figure 79. *config mirror port* command

To disable Port Mirror function of the Switch:



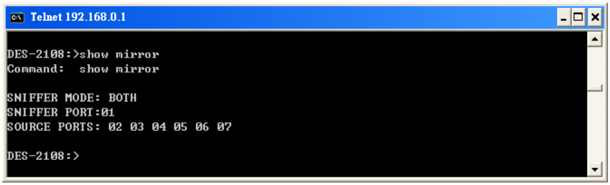
```
DES-2108:>config mirror port disable
Command:  config mirror port disable


SUCCESS

DES-2108:>_
```

Figure 80. *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:



```
DES-2108:>show mirror
Command:  show mirror

SNIFFER MODE: BOTH
SNIFFER PORT:01
SOURCE PORTS: 02 03 04 05 06 07

DES-2108:>
```

Figure 81. ***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.

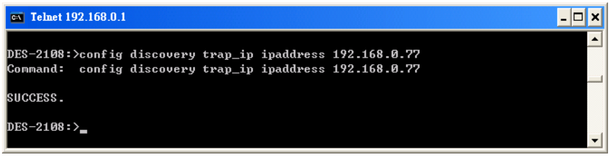
Command	Parameters
config discovery trap_ip	ipaddress <ip_address> {vid <vlan_id>}
config discovery trap_event	{[bootup | illegal_login | t_rx_err | t_tx_err| f_rx_err | f_tx_err| f_link_change]}
delete discovery trap_event	{[bootup | illegal_login | t_rx_err | t_tx_err| f_rx_err | f_tx_err| f_link_change]}
show discovery trap	

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

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> {vid <vlan_id>}**
Description	The command is configure an IP address of the trap recipient of *Web Management Utility* to the Switch.
Parameters	**<ip_address> -** IP address of the Web Management Utility. **<vlan_id> -** Specific the 802.1Q VLAN ID of Web Management Utility. The range is between 1 to 4094.

Example usage:

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



```
DES-2108:>config discovery trap_ip ipaddress 192.168.0.77
Command:  config discovery trap_ip ipaddress 192.168.0.77

SUCCESS.

DES-2108:>_
```

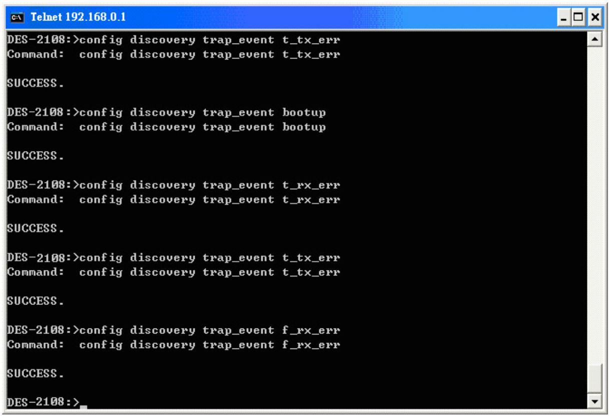
Figure 82. ***config discovery trap_ip*** **command**

config discovery trap_event

Purpose	Used to configure the events of the trap on the Switch.
Syntax	**config discovery trap_event {[bootup | illegal_login | t_rx_err | t_tx_err | f_rx_err | f_tx_err | f_link_change]}**
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_rx_err -** Enabled the Switch's twisted-pair ports (port 1 – 9) error receive data packets event. **t_tx_err -** Enabled the Switch's twisted-pair ports (port 1 – 9) error transmitting data packets event. **f_rx_err -** Enabled the Switch's fiber port (port 10) error receive data packets event. **f_tx_err -** Enabled the Switch's fiber port (port 10) error transmitting data packets event. **f_link_change -** Enabled the Switch's fiber port (port 10) linking status change event.

Example usage:

To configure the events type of the Switch:



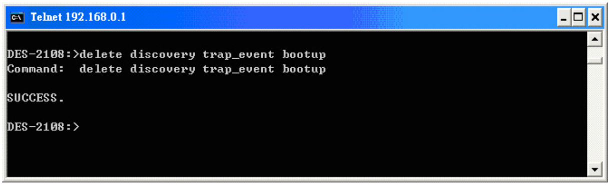
```
DES-2108:>config discovery trap_event t_tx_err
Command:  config discovery trap_event t_tx_err

SUCCESS.

DES-2108:>config discovery trap_event bootup
Command:  config discovery trap_event bootup

SUCCESS.

DES-2108:>config discovery trap_event t_rx_err
Command:  config discovery trap_event t_rx_err

SUCCESS.

DES-2108:>config discovery trap_event t_tx_err
Command:  config discovery trap_event t_tx_err

SUCCESS.

DES-2108:>config discovery trap_event f_rx_err
Command:  config discovery trap_event f_rx_err

SUCCESS.

DES-2108:>_
```

Figure 83. *config discovery trap_event* command

delete discovery trap_event	
Purpose	Used to delete previously configured events of trap on the Switch.
Syntax	**delete discovery trap_event {[bootup | illegal_login | t_rx_err | t_tx_err | f_rx_rtt | f_tx_err | f_link_change]}**
Description	The command is delete previously configured events of trap on the Switch.
Parameters	**bootup -** Disable the Switch's boot up event. **illegal_login -** Disable the Switch's illegal login event. **t_rx_err -** Disabled the Switch's twisted-pair ports (port 1 – 9) error receive data packets event. **t_tx_err -** Disabled the Switch's twisted-pair ports (port 1 – 9) error transmitting data packets event. **f_rx_err -** Disabled the Switch's fiber port (port 10) error receive data packets event. **f_tx_err -** Disabled the Switch's fiber port (port 10) error transmitting data packets event. **f_link_change -** Disabled the Switch's fiber port (port 10) linking status change event.

Example usage:

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



```
DES-2108:>delete discovery trap_event bootup
Command:  delete discovery trap_event bootup

SUCCESS.

DES-2108:>
```

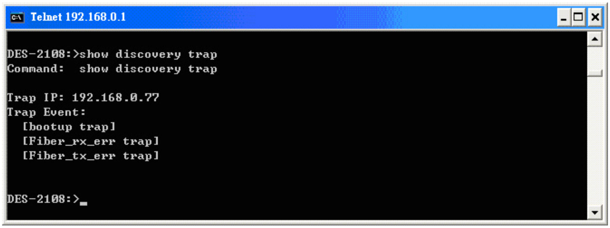
Figure 84. ***delete discovery trap_ip*** **command**

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:



```
DES-2108:>show discovery trap
Command:  show discovery trap

Trap IP: 192.168.0.77
Trap Event:
  [bootup trap]
  [Fiber_rx_err trap]
  [Fiber_tx_err trap]


DES-2108:>_
```

Figure 85. 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.

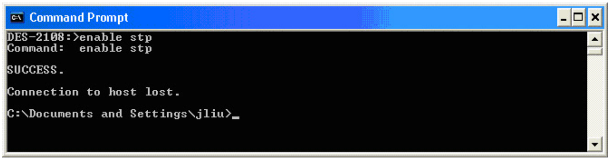
Command	Parameters
enable stp	
disable stp	
config stp	{maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <4-30> | priority <value 1-65535> | fbpdu [enable | disable]}
config stp ports	[all | <portlist>] {cost <value 1-65535> | priority <value 0-254>}
show stp	
show stp ports	<portlist>

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:



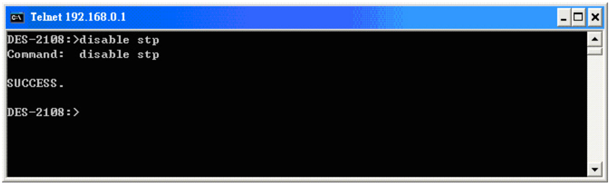
```
DES-2108:>enable stp
Command:  enable stp

SUCCESS.

Connection to host lost.

C:\Documents and Settings\jliu>_
```

Figure 86. 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:



```
DES-2108:>disable stp
Command:  disable stp

SUCCESS.

DES-2108:>
```

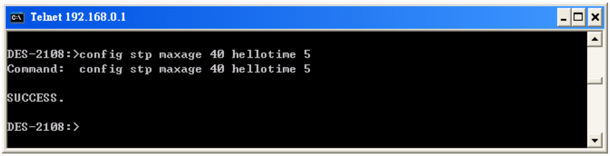
Figure 87. disable stp command

config stp	
Purpose	Used to setup STP on the Switch.
Syntax	**config stp {maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <4-30> | priority <value 1-65535> | fbpdu [enable | disable]}**
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 for forwarding packets. The lower the value, the

	higher the priority. The default is 32768. **fbpdu [enable | disable] -** Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*.

Example usage:

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



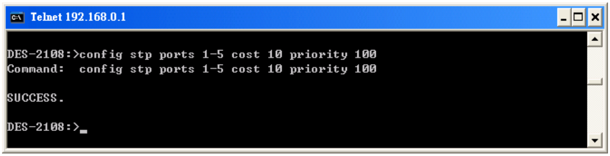
```
DES-2108:>config stp maxage 40 hellotime 5
Command:  config stp maxage 40 hellotime 5

SUCCESS.

DES-2108:>
```

Figure 88. 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 0-254>}**
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 0-254> -** 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:



```
DES-2108:>config stp ports 1-5 cost 10 priority 100
Command:  config stp ports 1-5 cost 10 priority 100

SUCCESS.

DES-2108:>_
```

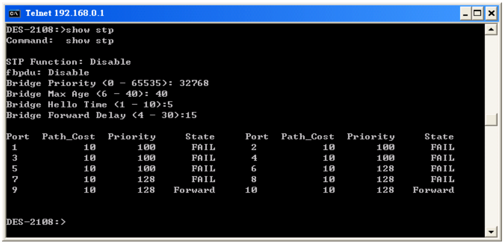
Figure 89. config stp ports command

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:



```
DES-2108:>show stp
Command:  show stp

STP Function: Disable
fbpdu: Disable
Bridge Priority (0 - 65535): 32768
Bridge Max Age (6 - 40): 40
Bridge Hello Time (1 - 10):5
Bridge Forward Delay (4 - 30):15

Port  Path_Cost  Priority     State     Port  Path_Cost  Priority     State
 1           10       100      FAIL      2           10       100      FAIL
 3           10       100      FAIL      4           10       100      FAIL
 5           10       100      FAIL      6           10       128      FAIL
 7           10       128      FAIL      8           10       128      FAIL
 9           10       128   Forward     10           10       128   Forward


DES-2108:>
```

Figure 90. show stp command

show stp ports

Purpose Used to display the Switch’s current STP group of ports configuration on the Switch.

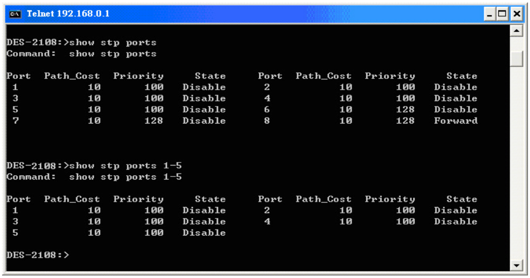
Syntax **show stp ports {portlist}**

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:



```
DES-2108:>show stp ports
Command:  show stp ports

Port  Path_Cost  Priority     State     Port  Path_Cost  Priority     State
 1           10       100   Disable      2           10       100   Disable
 3           10       100   Disable      4           10       100   Disable
 5           10       100   Disable      6           10       128   Disable
 7           10       128   Disable      8           10       128   Forward


DES-2108:>show stp ports 1-5
Command:  show stp ports 1-5

Port  Path_Cost  Priority     State     Port  Path_Cost  Priority     State
 1           10       100   Disable      2           10       100   Disable
 3           10       100   Disable      4           10       100   Disable
 5           10       100   Disable

DES-2108:>
```

Figure 91. 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
create snmp community	<community_string 20> [read_only | read_write]
delete snmp community	<community_string 20> [read_only | read_write]
show snmp	
create snmp host	<ipaddress> {vid <vlan id>} trap_community <community_string>
delete snmp host	[<ipaddress> | trap_community <community_string>]
show snmp host	
enable snmp traps	
disable snmp traps	

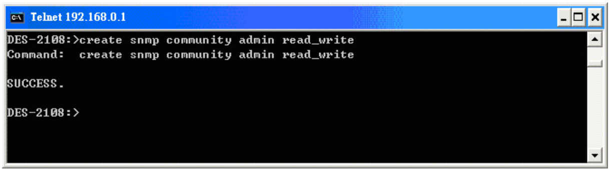
Each command is listed, in detail, in the following sections.

create snmp community	
Purpose	Used to create an 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	**create snmp community <community_string 20> [read_only | read_write]**

create snmp community	
Description	This command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	**<community_string 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. **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.

Example usage:

To create the SNMP community string “admin”:



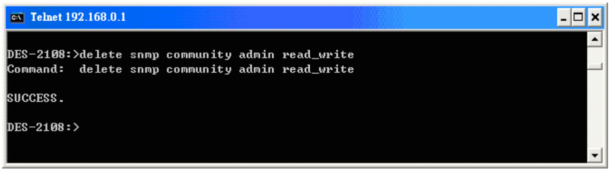
```
DES-2108:>create snmp community admin read_write
Command:  create snmp community admin read_write

SUCCESS.

DES-2108:>
```

Figure 92. create snmp community command

delete snmp community	
Purpose	Used to remove a specific SNMP community string from the Switch.
Syntax	**delete snmp community <community_string 20> [read_only | read_write]**
Description	This command is used to remove a previously defined SNMP community string from the Switch.
Parameters	**<community_string 20> -** Specifies which previously created SNMP community to be delete. **read_only -** Specifies which previously created SNMP community of read_only to be delete. **read_write -** Specifies which previously created SNMP community of read_write to be delete.

Example usage:

To delete the SNMP community string "admin":



```
DES-2108:>delete snmp community admin read_write
Command:  delete snmp community admin read_write

SUCCESS.

DES-2108:>
```

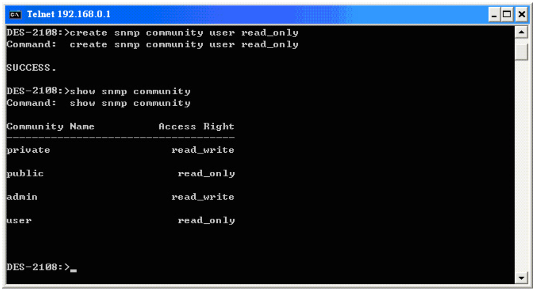
Figure 93. delete snmp community command

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:



```
DES-2108:>create snmp community user read_only
Command:  create snmp community user read_only

SUCCESS.

DES-2108:>show snmp community
Command:  show snmp community

Community Name            Access Right
--------------------------------------
private                     read_write

public                       read_only

admin                       read_write

user                         read_only


DES-2108:>_
```

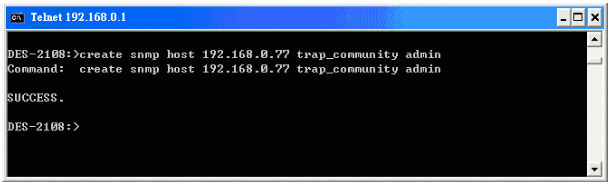
Figure 94. show snmp community command

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch’s SNMP agent.
Syntax	**create snmp host <ipaddress> {vid <vlan_id>} trap_community <community_string>**
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. **<vlan_id> -** Specific the 802.1Q VLAN ID of the SNMP recipient host. The range is between 1 to 4094. **trap_community <community_string> -** An alphanumeric string of up to 20 characters used to authorize a remote SNMP manager to access the Switch’s SNMP agent.

Example usage:

To create an SNMP host to receive SNMP messages:



```
DES-2108:>create snmp host 192.168.0.77 trap_community admin
Command:  create snmp host 192.168.0.77 trap_community admin

SUCCESS.

DES-2108:>
```

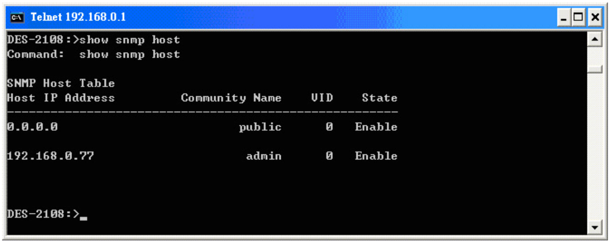
Figure 95. create snmp host command

show snmp host

Purpose	Used to display the recipient of SNMP traps generated by the Switch’s SNMP agent.
Syntax	**show snmp host**
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 hosts on the Switch:



```
DES-2108:>show snmp host
Command:  show snmp host

SNMP Host Table
Host IP Address         Community Name    UID    State
------------------------------------------------------
0.0.0.0                         public      0   Enable

192.168.0.77                     admin      0   Enable


DES-2108:>_
```

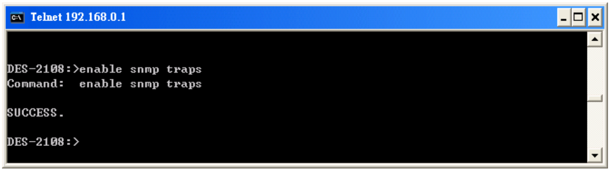
Figure 96. show snmp host command

enable snmp traps

Purpose	Used to enable SNMP trap support on the Switch.
Syntax	**enable snmp traps**
Description	This command is used to enable SNMP trap support on the Switch.
Parameters	None.

Example usage:

To enable SNMP trap support on the Switch:



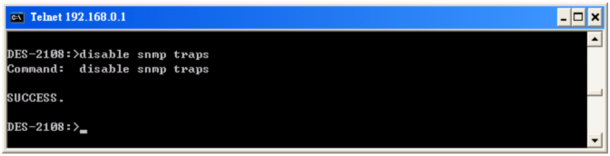
```
DES-2108:>enable snmp traps
Command:  enable snmp traps

SUCCESS.

DES-2108:>
```

Figure 97. enable snmp traps command

disable snmp traps	
Purpose	Used to disable SNMP trap support on the Switch.
Syntax	**disable snmp traps**
Description	This command is used to disable SNMP trap support on the Switch.
Parameters	None.

Example usage:

To disable SNMP trap support on the Switch:



```
DES-2108:>disable snmp traps
Command:  disable snmp traps

SUCCESS.

DES-2108:>_
```

Figure 98. disable snmp traps 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.

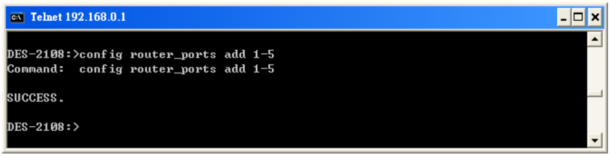
Command	Parameters
config router_ports	[add | delete] <portlist>
enable igmp snooping	{forward_mcrouter_only}
disable igmp snooping	
show router ports	
show igmp_snooping group	
config igmp_snooping	[host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450>]

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] <portlist>**
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:

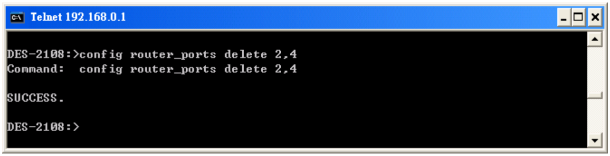
To set up static router ports:



```
DES-2108:>config router_ports add 1-5
Command:  config router_ports add 1-5

SUCCESS.

DES-2108:>
```

Figure 99. ***config router_ports*** **command (add static router ports)**

To delete static router ports:



```
DES-2108:>config router_ports delete 2,4
Command:  config router_ports delete 2,4

SUCCESS.

DES-2108:>
```

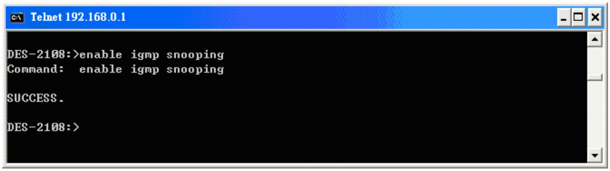
Figure 100. ***config router_ports*** **command (delete static router ports)**

enable igmp snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp snooping {forward_mcrouter_only}**
Description	This command allows you to enable IGMP snooping on the Switch. If forward_mcrouter_only is specified, the Switch will only forward all multicast traffic to the multicast router, only. Otherwise, the Switch forwards all multicast traffic to any IP router.
Parameters	None.

Example usage:

To enable IGMP snooping on the Switch:



```
DES-2108:>enable igmp snooping
Command:  enable igmp snooping

SUCCESS.

DES-2108:>
```

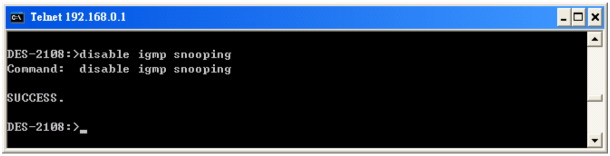
Figure 101. ***enable igmp snooping* command**

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:



```
DES-2108:>disable igmp snooping
Command:  disable igmp snooping

SUCCESS.

DES-2108:>_
```

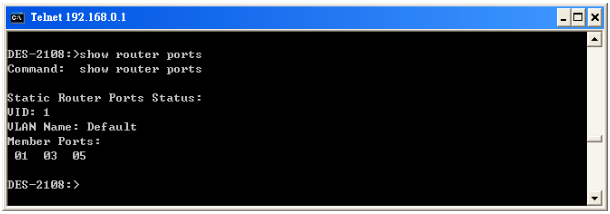
Figure 102. disable *igmp snooping* command

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:



```
DES-2108:>show router ports
Command:  show router ports

Static Router Ports Status:
VID: 1
VLAN Name: Default
Member Ports:
 01  03  05

DES-2108:>
```

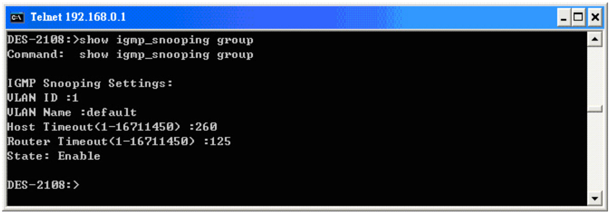
Figure 103. ***show router_ports*** **command**

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:



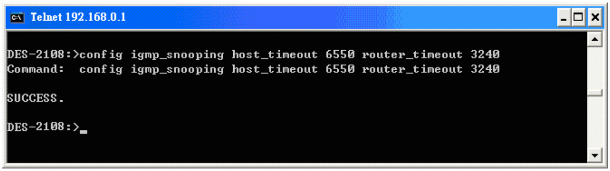
```
DES-2108:>show igmp_snooping group
Command:  show igmp_snooping group

IGMP Snooping Settings:
VLAN ID :1
VLAN Name :default
Host Timeout(1-16711450) :260
Router Timeout(1-16711450) :125
State: Enable

DES-2108:>
```

Figure 104. ***show igmp_snooping*** **command**

config igmp_snooping	
Purpose	Used to configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping [host_timeout <sec 1-16711450> | router_timeout <sec 1-16711450>]**
Description	This command allows you to configure IGMP snooping on the Switch.
Parameters	**host_timeout <sec 1-16711450> –** 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 1-16711450> –** 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.

Example usage:

To configure IGMP snooping:



```
DES-2108:>config igmp_snooping host_timeout 6550 router_timeout 3240
Command:  config igmp_snooping host_timeout 6550 router_timeout 3240

SUCCESS.

DES-2108:>_
```

Figure 105. ***config igmp_snooping*** **command**

Static MAC Commands

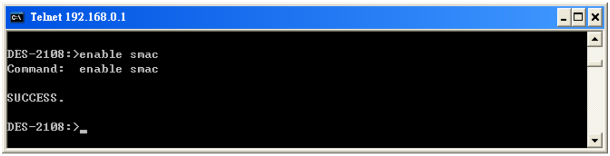
The layer 2 forwarding database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable smac	
disable smac	
config auto_learning	[enable | disable exclude <portlist>]
show smac	
show fdb	port <port no.>
create smac(port-based VLAN)	[mac <macaddress> port <port no.> | idx <mac address index list on fdb>]
create smac(802.1Q VLAN)	[mac <macaddress> port <port no.> 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.

enable smac	
Purpose	Used to enable Static MAC function on the Switch.
Syntax	**enable smac**
Description	This command allows you to enable Static MAC function on the Switch.
Parameters	None.

Example usage:

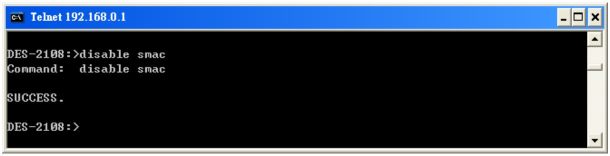


```
DES-2108:>enable smac
Command:  enable smac

SUCCESS.

DES-2108:>_
```

Figure 106. ***enable Static MAC function***

disable smac	
Purpose	Used to disable Static MAC function on the Switch.
Syntax	**disable smac**
Description	This command allows you to disable Static MAC function on the Switch.
Parameters	None.

Example usage:

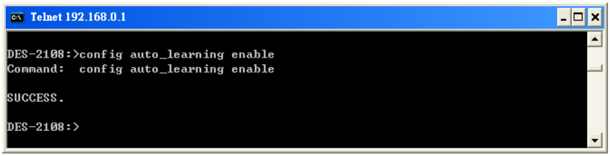


```
DES-2108:>disable smac
Command:  disable smac

SUCCESS.

DES-2108:>
```

Figure 107. ***disable Static MAC function***

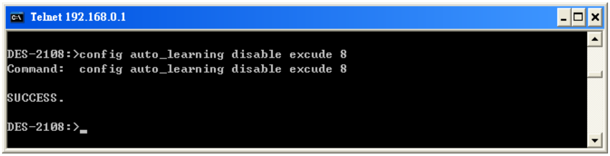
config auto_learning	
Purpose	Used to enables or disables the MAC address learning on the specified range of ports.
Syntax	**config auto_learning [enable | disable exclude <portlist>]**
Description	This command allows you to enables or disables the MAC address learning on the specified range of ports.
Parameters	**[enable | disable] -** Enables or disables the MAC address learning on the specified range of ports. **exclude <portlist> -** Specifies a port or range of ports exclude to config auto_learning function.

Example usage:



```
DES-2108:>config auto_learning enable
Command:  config auto_learning enable

SUCCESS.

DES-2108:>
```

Figure 108. ***enable auto_learning function***

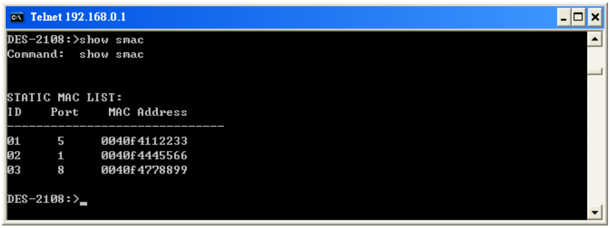


```
DES-2108:>config auto_learning disable excude 8
Command:  config auto_learning disable excude 8

SUCCESS.

DES-2108:>_
```

Figure 109. ***disable 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:

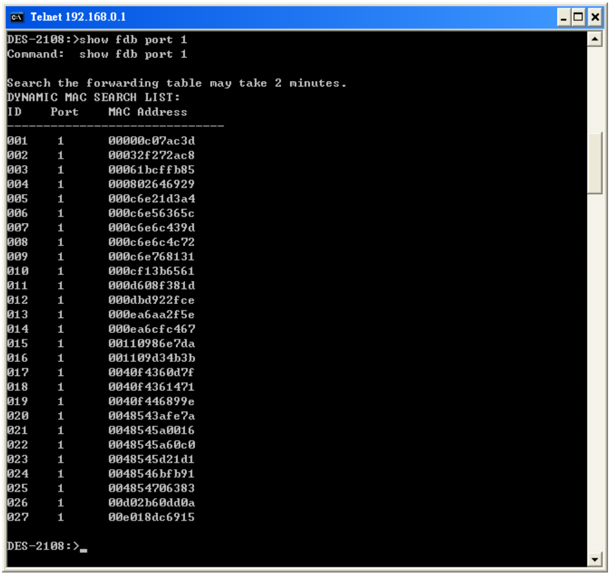


```
DES-2108:>show smac
Command:  show smac


STATIC MAC LIST:
ID     Port     MAC Address
------------------------------
01      5      0040f4112233
02      1      0040f4445566
03      8      0040f4778899

DES-2108:>_
```

Figure 110. show Static MAC address forwarding database

show fdb	
Purpose	Used to display the dynamic MAC address forwarding database.
Syntax	**show fdb port <port no.>**
Description	This command allows you to display the dynamic MAC address forwarding database.
Parameters	**port <port no.> -** To display the dynamic MAC address forwarding database on the specified port number.

Example usage:



```
DES-2108:>show fdb port 1
Command:  show fdb port 1

Search the forwarding table may take 2 minutes.
DYNAMIC MAC SEARCH LIST:
ID     Port     MAC Address
------------------------------
001     1       00000c07ac3d
002     1       00032f272ac8
003     1       00061bcffb85
004     1       000802646929
005     1       000c6e21d3a4
006     1       000c6e56365c
007     1       000c6e6c439d
008     1       000c6e6c4c72
009     1       000c6e768131
010     1       000cf13b6561
011     1       000d608f381d
012     1       000dbd922fce
013     1       000ea6aa2f5e
014     1       000ea6cfc467
015     1       00110986e7da
016     1       001109d34b3b
017     1       0040f4360d7f
018     1       0040f4361471
019     1       0040f446899e
020     1       0048543afe7a
021     1       0048545a0016
022     1       0048545a60c0
023     1       0048545d21d1
024     1       0048546bfb91
025     1       004854706383
026     1       00d02b60dd0a
027     1       00e018dc6915

DES-2108:>
```

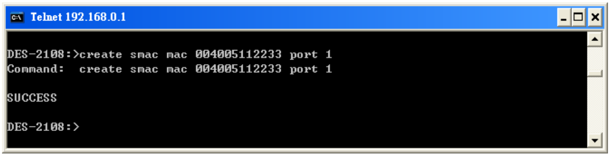
Figure 111. show Dynamic MAC address forwarding database

create smac (port-based VLAN)

Purpose	Used to create a static entry to the unicast MAC address forwarding table (database).
Syntax	**create smac [mac <macaddress> port <port no.> | idx <mac address index list on fdb>]**
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	**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. **idx <mac address index list on fdb> -** Added to the forwarding table for fdb list.

Example usage:

To create a unicast MAC FDB entry:

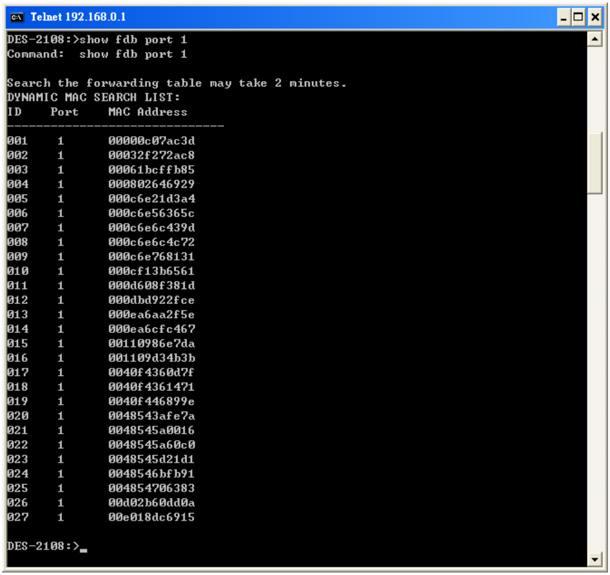


```
DES-2108:>create smac mac 004005112233 port 1
Command:  create smac mac 004005112233 port 1

SUCCESS

DES-2108:>
```

Figure 112. create static MAC address to FDB (port-based VLAN)

To create a unicast MAC FDB entry from DYNAMIC MAC SEARCH LIST:

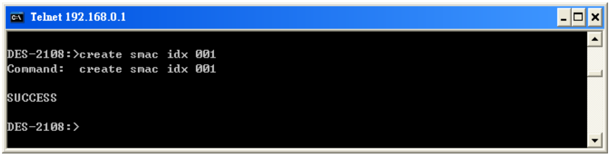
Step1: show the DYNAMIC MAC SEARCH LIST



```
DES-2108:>show fdb port 1
Command:  show fdb port 1

Search the forwarding table may take 2 minutes.
DYNAMIC MAC SEARCH LIST:
ID     Port     MAC Address
------------------------------
001     1       00000c07ac3d
002     1       00032f272ac8
003     1       00061bcffb85
004     1       000802646929
005     1       000c6e21d3a4
006     1       000c6e56365c
007     1       000c6e6c439d
008     1       000c6e6c4c72
009     1       000c6e768131
010     1       000cf13b6561
011     1       000d608f381d
012     1       000dbd922fce
013     1       000ea6aa2f5e
014     1       000ea6cfc467
015     1       00110986e7da
016     1       001109d34b3b
017     1       0040f4360d7f
018     1       0040f4361471
019     1       0040f446899e
020     1       0048543afe7a
021     1       0048545a0016
022     1       0048545a60c0
023     1       0048545d21d1
024     1       0048546bfb91
025     1       004854706383
026     1       00d02b60dd0a
027     1       00e018dc6915

DES-2108:>_
```

Figure 113. ***show the DYNAMIC MAC SEARCH LIST***

Step2: create Static MAC from DYNAMIC MAC SEARCH LIST:



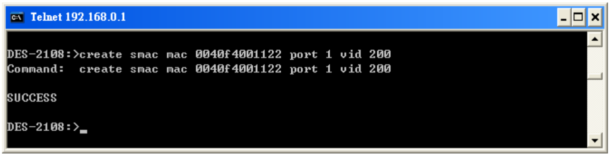
```
DES-2108:>create smac idx 001
Command:  create smac idx 001

SUCCESS

DES-2108:>
```

Figure 114. create Static MAC from DYNAMIC MAC SEARCH LIST ID 001

create smac (802.1Q VLAN)	
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 fdb>]**
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	**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 fdb> -** Added to the forwarding table for fdb list.

Example usage:

To create a unicast MAC FDB entry:



```
DES-2108:>create smac mac 0040f4001122 port 1 vid 200
Command:  create smac mac 0040f4001122 port 1 vid 200

SUCCESS

DES-2108:>_
```

Figure 115. create static MAC addres to FDB (port-based VLAN)

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	
AC inputs:	100-240 VAC, 50-60 Hz
Power Consumption:	9 watts maximum
Operating Temperature:	0 ~ 40 degrees Celsius
Storage Temperature:	-10 ~ 70 degree Celsius
Humidity:	10% ~ 90% RH, non-condensing
Dimensions:	280 mm x 180 mm x 44 mm
EMI:	FCC Class A, CE Mark Class A, VCCI Class A
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

WARRANTY AND REGISTRATION INFORMATION

(All countries and regions excluding USA)

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.

13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.

14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.

15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:

    a. Netzkabel oder Netzstecker sint beschädigt.

    b. Flüssigkeit ist in das Gerät eingedrungen.

    c. Das Gerät war Feuchtigkeit ausgesetzt.

    d. Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.

    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.

    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.

16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.

17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.

18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht grőßer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.