DES-7000/DES-7100

Layer 2 Modular Chassis-based Switch

User's Manual

First Edition (February, 2003)

6DES7000..01

Printed In Taiwan

RECYCLABLE

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 größer 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.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.

Trademarks

Copyright Statement

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.

Table of Contents

1

Introduction

This section describes the features of the DES-7000 and DES-7100 Switch.

Features

The DES-7000/DES-7100 Switch is a high performance modular chassis-based switch platform that allows a customized array of Layer 2 functions to be easily installed and managed in a single device. The Switch is ideal for expanding enterprise networks and environments where traffic volume and needs fluctuate. CPU and power redundancy are built-in for extremely reliable performance. Switch features include:

Chassis

The chassis is the main unit into which network modules are installed.

Chassis features include:

DES-7000 Switch Chassis

- Fourteen slots for installing networking modules
- Two slots reserved for the preinstalled DES-7003 Management CPU/Uplink modules
- Duplicate CPU modules support redundant backup function
- Twelve slots to install DES-7000 Series switch modules

DES-7100 Switch Chassis

- Eight slots for installing networking modules
- Two slots reserved for the preinstalled management CPU/Uplink modules
- Duplicate CPU modules support redundant backup function
- Six slots to install DES-7000 Series slave modules

DES-7003 Management/Uplink CPU Module

Each module supports

- 24 Gbps back-plane bandwidth capability
- 32K MAC address
- 2MB packet buffer memory
- LED indicators
- Six GBIC-based Gigabit Ethernet ports for Uplink
- Store & forward packet switching
- Broadcast/Multicast storm control function.
- Port Mirroring
- IGMP Snooping
- Link Aggregation support for all the ports within the same blade
- Ether Channel compatible
- 802.1d Spanning Tree support.
- 802.1Q Tagged VLAN support
- Supports 802.1p priority queuing
- Management through local out-of-band console, or remotely with Telnet or Web-based manager.
- CLI (Command Line Interface) for console or Telnet management

All DES-7003 GBIC Gigabit Ethernet Uplink ports support the following:

- Full complaint with IEEE 802.3z standards
- Support Full Duplex operations
- IEEE 802.3x compliant Flow Control support

Switch Modules

The DES-7000 Series Switch modules offer a diverse selection to custom fit the needs of changing and expanding networks. All modules are hot swappable. Key feature of the modules are described below.

DES-7005 24-Port 10BASE-T/100BASE-TX Ethernet Module

The DES-7005 Ethernet module delivers a high-capacity switching fabric with all the standard features plus the convenience of auto-polarity detection for all ports.

The DES-7005 includes:

- 24 Ethernet/Fast Ethernet ports (RJ-45)
- Fully compliant with IEEE 802.3 10BASE-T and IEEE 802.3u 100BASE-TX standards
- All ports support auto-negotiation 10M/100M speed function
- All ports support auto-negotiation Full/Half Duplex operations
- All ports support auto-polarity detection and correcting
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x compliant Flow Control support for Full-duplex
- Supports 16 MB packet buffer memory per module
- Supports 8K MAC address per Switch blade

  Two LED indicators for each port for Link/Activity and Speed

DES-7006 24-Port 100BASE-FX (SFF-type, SMF/MMF) Ethernet Switch Module

The DES-7006 includes:

- 24 Fast Ethernet ports (SFF-type, LC Duplex)
- Fully compliant with IEEE 802.3u standard
- IEEE 802.3x compliant Flow Control supported for Full-duplex
- Supports 16MB packet buffer memory per module
- Supports 8K MAC address per Switch blade
- One LED indicators for each port for Link/Activity

DES-7010 Ethernet over VDSL Module

The DES-7010 is an Ethernet over VDSL (Very-high-rate Digital Subscriber Line) module supporting 24 client ports. Ethernet over VDSL systems are used for delivery of fast network services to dwellings and businesses with a high concentration of subscribers. Typical applications would include:

- § Multiple Tenant Units (MTU) such as hotels
- § Multiple Dwelling Units (MDU) such as high-rise apartment buildings
- § Campus Networking
- § LAN Extensions

The DES-7010 includes:

- 24 Ethernet over VDSL ports (Two RJ-21 connectors)
- 2 RJ-21 ports on the front panel provide VDSL and PSTN link
- Complies with the approved ETSI VDSL requirements
- Supports full duplex mode operation
- Built-in 24 ports splitter.
- Supports symmetrical data transfer rate depend on distance between Line Terminals:

Redundant Power Supply Modules

The Switch is equipped with a single DES-7011 RPS unit. Up to three power supply units can be installed on the switch chassis. As network modules are added to the chassis, RPS units can be added for better load balancing and increased RPS lifespan. Two RPS units must be used for full loading operation of the Switch. Refer to the power consumption per module data in the table below.

DES-7011 RPS Unit

- One plus two power module design (one pre-installed)
- Each RPS unit supports up to 730 Watts (see power consumption information below)
- Current sharing/ load balancing design
- Full redundant feature design to ensure continuous operation
- Hot-swappable
- Power management functions enabled

Use this table to calculate total power consumption for the Switch chassis. Do not exceed the 730 Watt maximum for each RPS unit. For best load balancing performance and RPS lifespan it is recommended to allow for redundancy. Two RPS units must be used for full loading operation of the Switch, for these installations, an additional third RPS unit is also recommended for redundancy.

Unit/Module	Total Power Consumption
Fan Tray Module	105 Watts (max.) per unit
DES-7003	64 Watts (max.) per unit
DES-7005	37 Watts (max.) per unit
DES-7006	60 Watts (max.) per unit
DES-7010	54 Watts (max.) per unit
Four small system fans (fixed)	57 Watts (max.) for all fans

2

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:

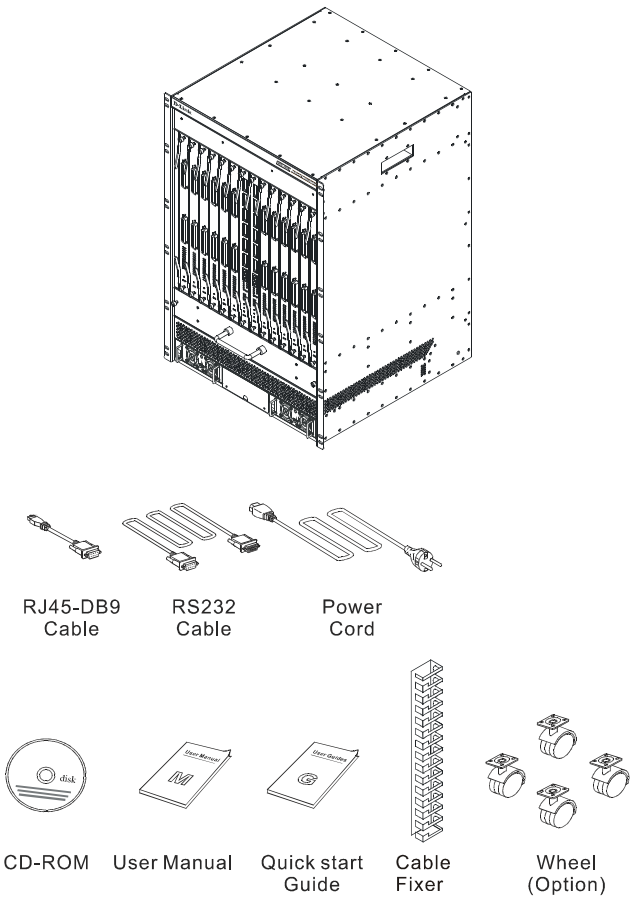


Figure 2 - 1. DES-7000 Switch chassis with shipped components

1. One switch chassis including:
   - § One pre-installed DES-7003 CPU/uplink module
   - § One pre-installed DES-7011 power supply unit
   - § For DES-7000 chassis only - one pre-installed fan tray module with four fans
2. One cable bearer (DES-7000 only)
3. Four wheels (DES-7000 only)
4. One AC power cord
5. One RJ-45 to RS-232 9-pin (male) serial adapter
6. One CD-ROM containing documentation for the device
7. This printed Quick Installation Guide

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

Setup

The DES-7000 is shipped with the DES-7003 management module preinstalled. There are some additional pieces that the user may opt to install. These are described below. The Quick Installation Guide included with the switch contains illustrations and information that may be useful for installing the additional hardware.

Make sure the location used is a suitable environment for the Switch and there is adequate ventilation. Have the necessary cabling required to connect the Switch to the network.

You may install DES-7000 series network modules at any time before or after the switch has been installed and powered on. Modules can be hot swapped to meet the changing demands of the network.

Attaching Wheels

The DES-7000 is shipped with four wheels that may be install but are not required. To install the wheels, gently place the chassis on either of its sides to access the wheel mounts. Make sure the fan module is firmly in place before tilting the chassis. Each wheel is held in place with four screws (included in the package with the wheels).

Rack Installation

The chassis may be placed into a standard 19" equipment rack with or without the wheels attached. The ears at the front of both sides of the chassis should be used to hold it firmly in place with screws.

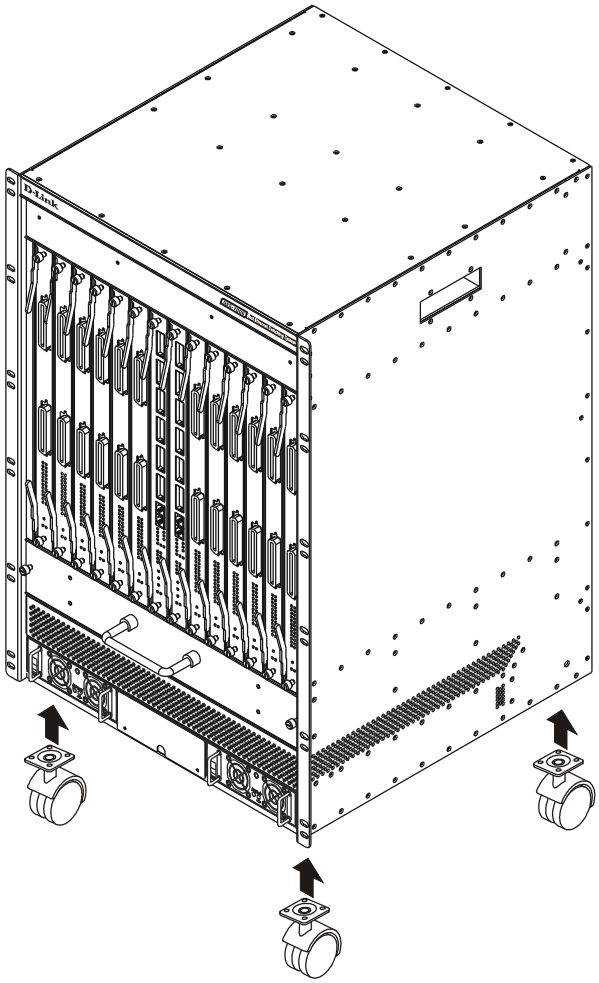


Figure 2 - 2. DES-7000 Switch Chassis with optional wheels

Cable Bearer

The cable bearer is attached to the top of the chassis front panel on the DES-7000 chassis. Use the four screws included in the packaging.

Installing Modules

The DES-7000 and DES-7100 Switch chassis' has one DES-7003 management/uplink module installed when shipped. In order to use other available modules you will need to install them. Follow the instructions below. Modules can be installed into any free slot, except the CPU module.

WARNING

When handling Switch modules be sure to wear an ESD wrist strap or suitable grounding device to prevent damage from electrostatic discharge. Do not attach the strap to any part of the power supply if the Switch is powered on.

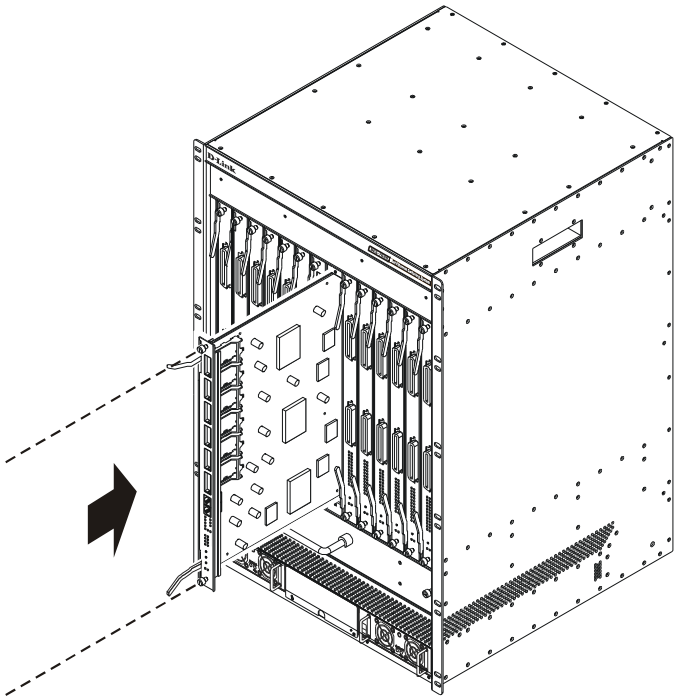


Figure 2 - 3. Inserting a module into the DES-7000

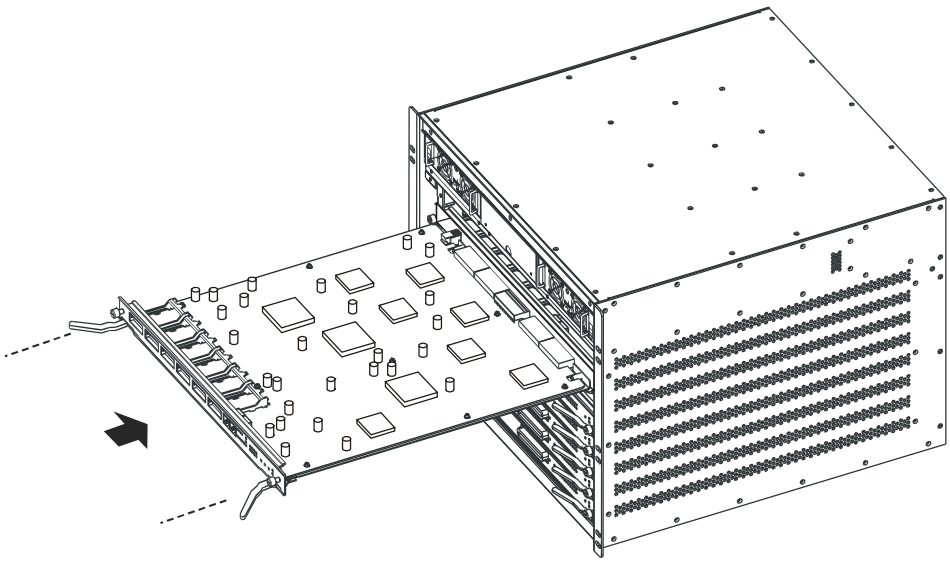


Figure 2 - 4. Inserting a module into the DES-7100

To install a module, follow these steps:

WARNING

When using an ESD wrist strap or other grounding device, do not attach it to any part of the power supply if the switch is powered on.

1. Remove the faceplate from the slot intended for module insertion. Keep the faceplate in case it is needed in the future.
2. Carefully remove the module from its packaging.
3. Line up the module with the grooved slot guides and insert it into the chassis. It should glide easily toward the back of the chassis. Push it in until the module ejector levers are in contact with the chassis. Be careful not to bend the circuit board of the module. Modules for the DES-7000 should be oriented so the model number of the module is at the top and the LED indicators are on the bottom. Modules installed in the DES-7100 should be inserted horizontally in the upright position, that is, so the model number and LED indicator labels are displayed so they can be read from left to right.
4. Push the ejector levers toward the center of the module until they touch the front of the module. This will push the bus connectors into backplane of the chassis.
5. Hand-tighten the installation screws at each end of the module. The module is now firmly seated in the backplane of the chassis.

Removing a Module

To remove a module from the chassis follow these steps:

WARNING

When using an ESD wrist strap or other grounding device, do not attach it to any part of the power supply if the switch is powered on.

1. Loosen the two installation screws on the front of the module.
2. Pull the ejector levers out and away from the center of the module front panel. This will pull the module out of the backplane.
3. Cover the empty slot with a faceplate that was shipped with chassis.

Power on the Switch

The Switch is shipped with two DES-7011 RPS modules installed and is therefore ready to be powered on after you have assembled the hardware. Follow these steps to power on the Switch:

1. Plug the device end of either power cord into either power supply.
2. Plug the outlet end of the power cord into a suitable AC power source.
3. Observe the LED indicators to make sure the Switch is functioning normally.

Upon powering on the LED indicators on the DES-7003 management/uplink module should operate as follows:

- All indicators will flash momentarily indicating a system reset.
- The Power indicator will flash for a few seconds during the POST
- The System Status LED indicator will be dark during CPU arbitration for several seconds

The System Status and Power LED indicators will light steady green indicating normal system and power supply function. An amber light in either of these indicates a problem.

Power Failure

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

Battery Back Up System

The DES-7000 and DES-7100 can be equipped with a battery back up system. Battery back ups may only be installed by qualified technicians. Please contact your vendor for information on purchasing and installing such a system.

Hot Swap Procedure for Switch Modules

All switch modules including the Primary Master and Primary Back Up CPU modules can be changed while the Switch is powered on. Follow the procedures listed here to remove a module or to insert a module while the Switch is powered on. Changing a module while the Switch is operating is commonly called "hot swapping" which is the term we use in this document.

WARNING

When handing Switch modules be sure to wear an ESD wrist strap to prevent damage from static electric discharge. Do not attach the strap to any part of the power supply if the Switch is powered on.

Hot Swap Removal of a Switch Module

Remove a single switch module following the procedure listed below. Only one module should be removed at a time. Wait for the process to be completed before removing (or inserting) another module. Wear an ESD wrist strap to prevent damage to the module from possible static electric discharge.

To perform a hot swap removal of a switch module follow these steps:

1. Gently depress the **Hot Swap button** on the front panel of the module you want to remove. The Hot Swap button is located between the Per Port Link LED indicators and the Power and Hot Swap Status indicators. The button can be pressed using your finger, a ballpoint pen or other suitable instrument.
2. Observe the **Hot Swap & Card Status** LED indicator on the switch module being removed. It should blink amber. During this phase the module is sending a message to the master (CPU) module that a removal has been initiated.
3. The master module detects the removal and updates its database. The master module cuts power to the switch module being removed. The **Power** LED indicator and all other LED indicators on the switch module will go dark.
4. When you see that the switch module has been powered off you may remove it. Unscrew the installation screws and pull both ejector levers toward the center of the front panel of the module to unseat it from the backplane of the Switch.
5. If the module is not being reinserted, completely remove it from the slot. It should slide out easily in the guides. Be sure to properly store the module.
6. If you do not intend to install another module in the vacant slot, cover it with one of the slot faceplates included with the original shipment.

Note

When performing a hot swap of a Master CPU module the procedure is essentially the same as a hot swap of other switch modules. The procedure for removing a Primary Master CPU module is slightly different since the designation of Primary Master must be transferred to the current Back Up Master before the unit is powered off. This takes a few seconds. The Master LED Indicator will light on the new Primary Master CPU module indicating that the unit is the active master. The former Primary Master module is powered off and may then be removed.

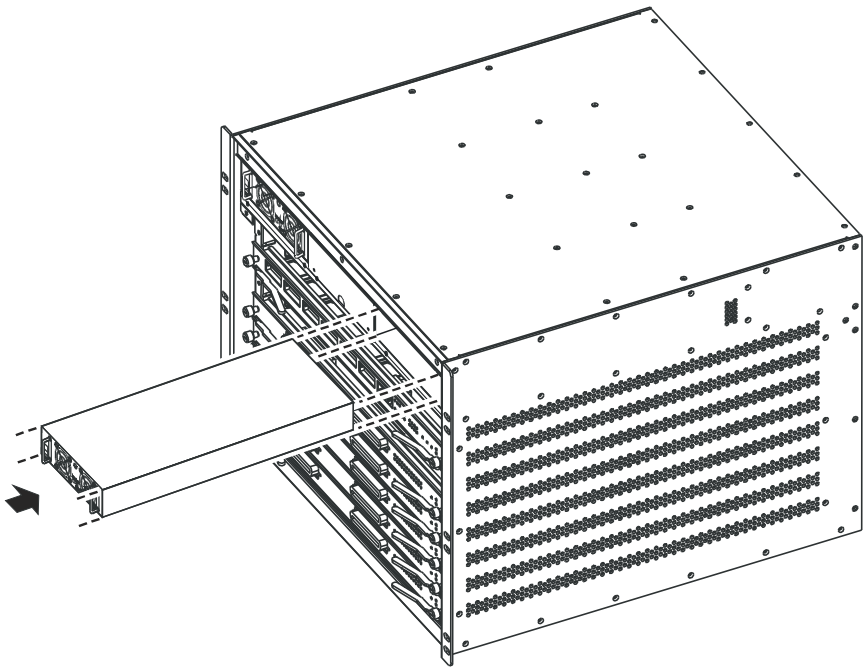
Hot Swap Insertion of a Switch Module

Follow the procedure listed below to insert a new switch module into an available slot while the Switch is powered on. Only one module should be inserted at a time. Wait for the process to be completed before inserting or removing another module. Wear an ESD wrist strap to prevent damage to the module from possible static electric discharge.

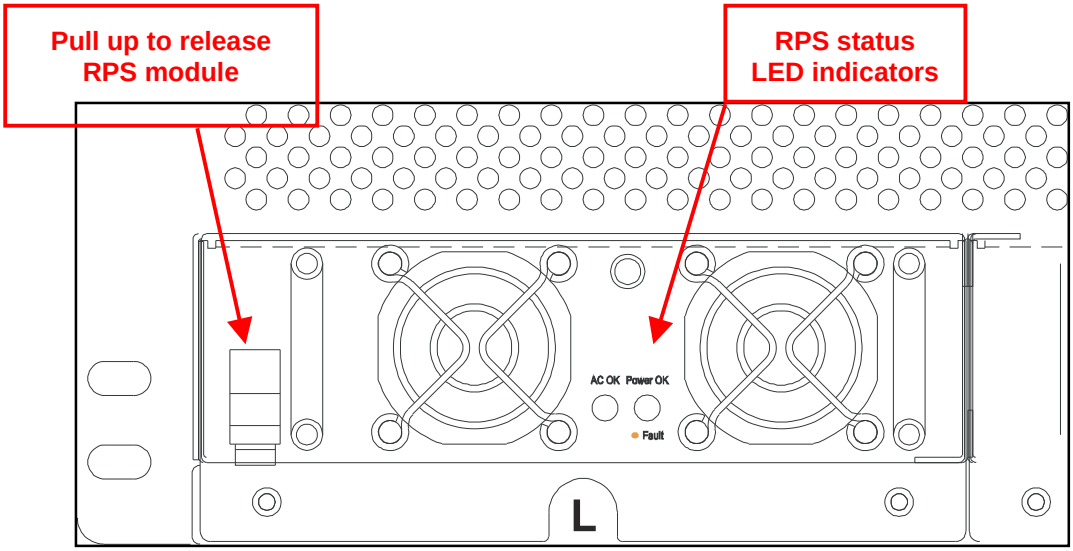
1. If the slot is covered with a faceplate, remove and save it for later use.
2. Carefully remove the module from its packaging.
3. Line up the module with the grooved slot guides and insert it into the chassis. It should glide easily toward the back of the chassis. Push it in until the module ejector levers are in contact with the chassis. Be careful not to bend the circuit board of the module. Modules for the DES-7000 should be oriented so the model number of the module is at the top and the LED indicators are on the bottom.
4. Push the ejector levers toward the center of the module until they touch the front of the module. This will push the bus connectors into backplane of the chassis.
5. Observe the **Hot Swap & Card Status** LED indicator on the switch module. This will blink amber for about 13 seconds after being inserted. During this time the CPU is recognizing the new switch module and the switch module is booting. A steady amber light indicates a system failure.
6. A steady green Hot Swap & Card Status LED indicator on the switch module indicates the module is ready and running normally. The master (CPU) module recognizes the new switch module.
7. Hand-tighten the installation screws at each end of the module. The module is now firmly seated in the chassis and powered on. This completes the hot swap insertion.

Hot Swap Procedure for Power Supply

DES-7011 RPS modules can be easily hot swapped. Follow the instructions below to replace a redundant power supply.

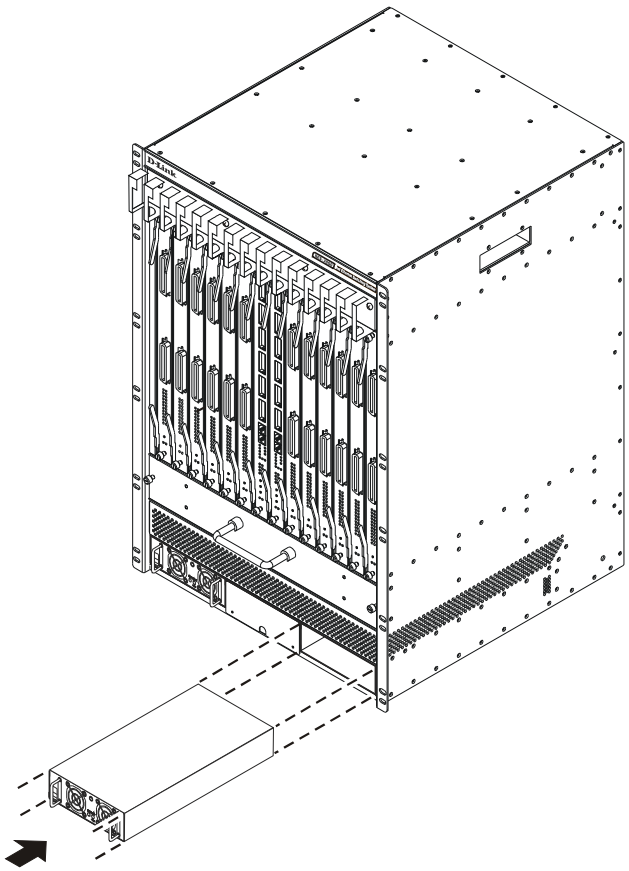


Inserting DES-7011 RPS Module into DES-7100 Chassis



To remove a DES-7011 RPS module:

1. Grasp the unit by the handles on the front using both hands.
2. Release the catch by applying upward pressure on the catch release near the left side of the unit.
3. Pull the RPS unit straight out from the chassis.



Inserting a DES-7011 RPS Module into the DES-7000 chassis

To insert an RPS module push the unit straight in toward the back of the chassis until the catch snaps into place securely holding the RPS in position.

Hot Swap Procedure for Fan Tray Module

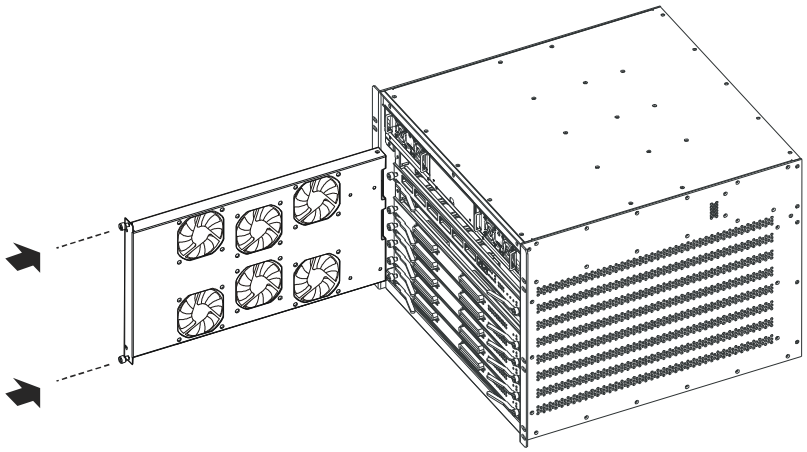
CAUTION

The Fan Tray Module can be replaced with the power on. If you cannot replace the fan tray immediately (within two minutes) the Switch chassis should be powered off to avoid damage from overheating before the fan tray is removed.

Changing the fan tray module for the DES-7000 and DES-7100 is a simple procedure however if you choose to do this while the Switch is powered on, be sure to have the replacement fan tray ready at hand so the procedure can be completed as quickly as possible. It is not necessary to initiate the hot swap procedure, the Master CPU will be aware of fan tray removal and insertion. Removal of the fan tray will trigger the system alert buzzer and the Fan Fail LED indicator. Be sure to use proper ESD grounding procedures to avoid electrostatic discharge. The procedure below describes this procedure and changes to the LED indicators that occur.

WARNING

The fans will continue rotating for several seconds after power to the unit is cut off. Use only the handle on the front of the fan tray when removing the device to avoid risk of injury.



Inserting the fan tray into the DES-7100 chassis

To change the fan tray:

1. Unscrew the installation screws on each side of the module and pull the module from out of the chassis. Be careful not to drop the fan tray when removing it.
2. Replace the fan tray module immediately if the Switch is powered on; insert the new unit using the guides built into the chassis. It should glide easily into position if it is properly lined up.
3. Push the module toward the backplane of the chassis until the front of the module is flush with the front panel of the chassis. You will need to apply firm pressure for about the last half centimeter to establish the contacts and firmly position the unit in the backplane.
4. The fan tray will power on and be recognized by the Master CPU. You should see the Hot Swap & Card Status LED indicator on the Master CPU module blink for about 13 seconds while the unit is recognized.

Tighten the installation screws on the fan tray module. Observe the Fan/Fail LED indicator on the Master CPU module to make sure it is functioning normally: dark for normal function, blinking amber if there is a problem. The unit is now completely installed.

3

Identifying External Components

This chapter provides a description of the external hardware features for the DES-7000 and DES-7100 as well as the features of the DES-7000 Series Modules. Included are descriptions of the LED indicators, ports and power supply.

Front Panel Views

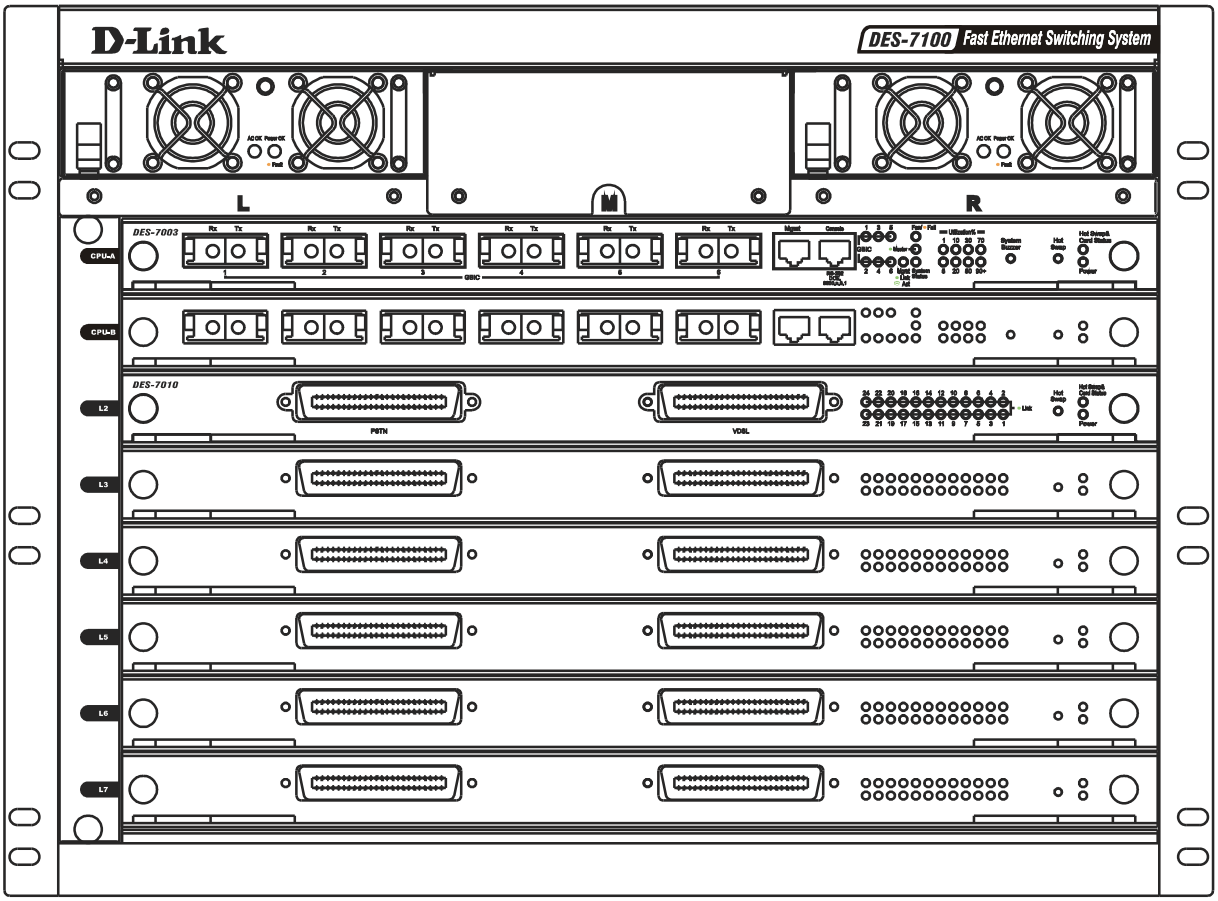


Figure 3-1. Front panel view of DES-7100 with DES-7010 Ethernet over VDSL Modules

The front panel of the DES-7100 features one installed redundant power supply. The remaining two slots are available for additional RPS units. RPS slots are located along the top of the device and are labeled L (left) M (middle) and R (right). Network module slots are labeled with the name of the slot along the left side. The master CPU module is installed in the uppermost slot labeled CPU-A.

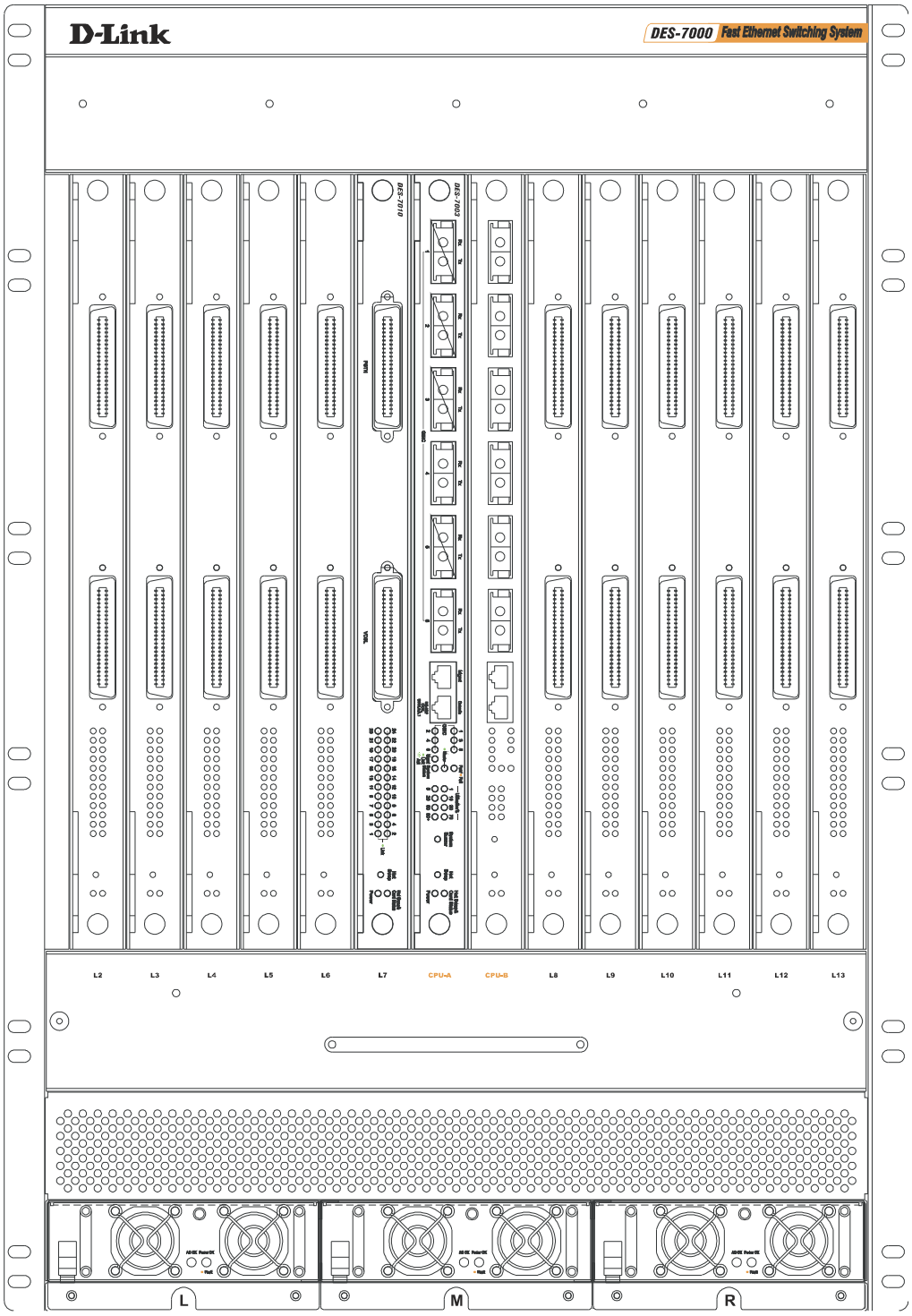


Figure 2 - 5. Front panel view of DES-7000 with DES-7010 Ethernet over VDSL Modules

The front panel of the DES-7000 features one installed redundant power supply. The remaining slots are available for additional RPS units. RPS slots are located along the bottom of the device and are labeled L (left) M (middle) and R (right). Network module slots are labeled with the name of the slot along the top of the fan tray. The master CPU module is installed in the center slot labeled CPU-A.

Side Panels

The DES-7000 and DES-7100 have vents to allow adequate airflow to the system fans. The system fans are used to dissipate heat. Do not block these openings, and leave adequate space at the rear and sides of the Switch for proper ventilation. Without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

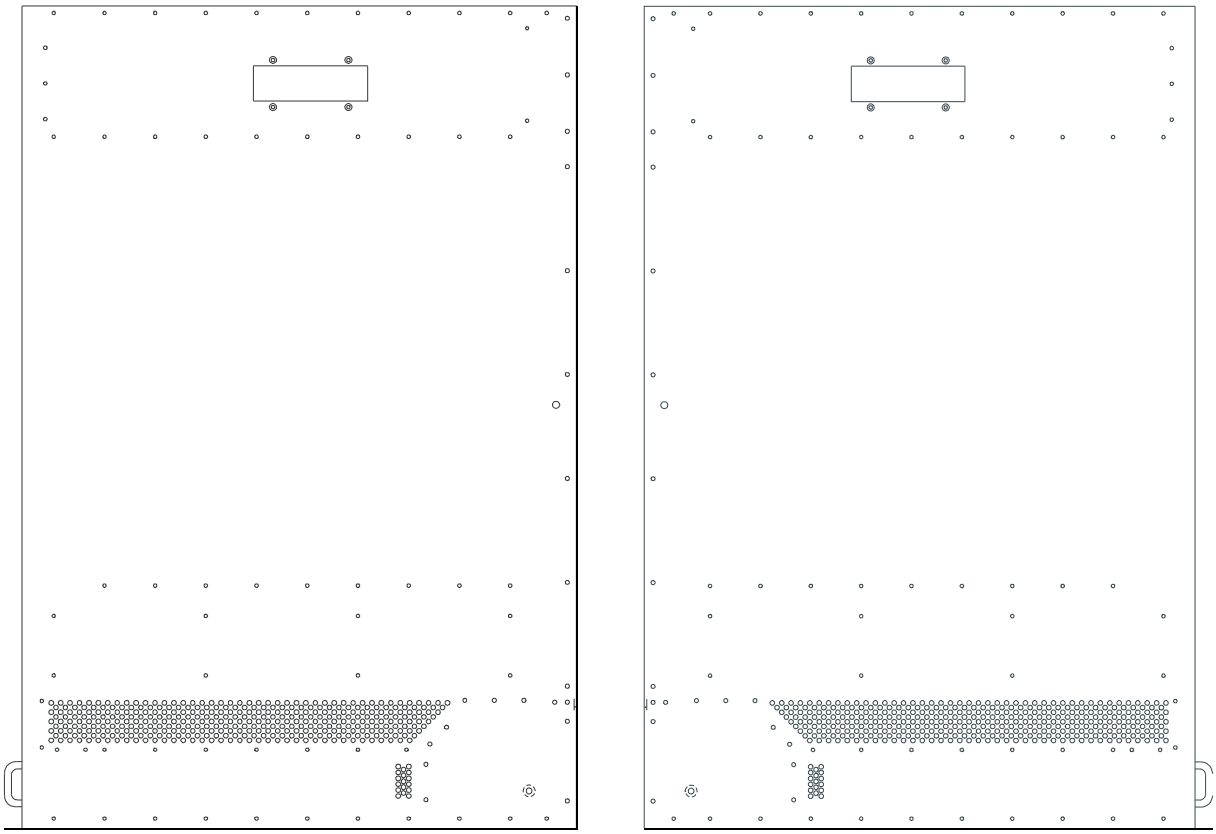


Figure 3- 1. Right and Left Side Panel Views of the DES-7000

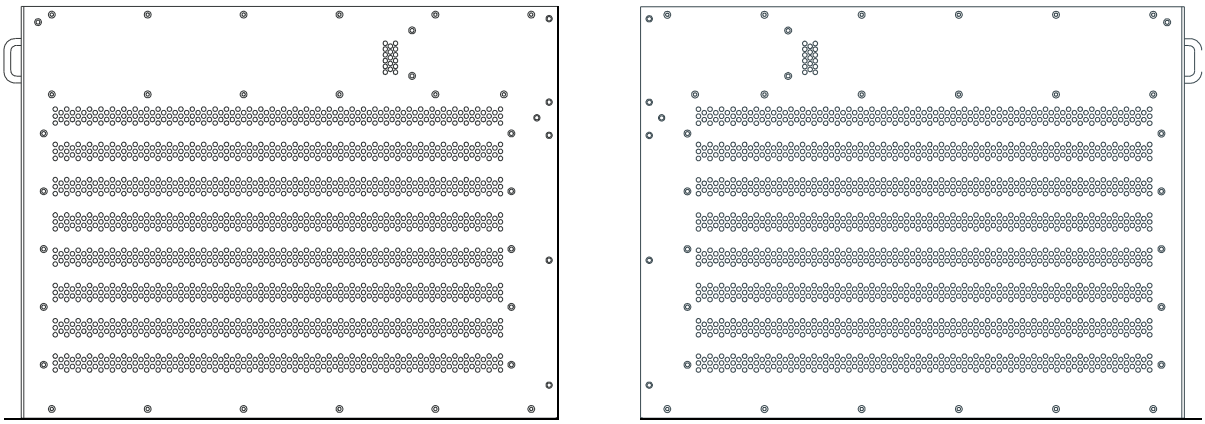


Figure 3- 2. Right and Left Side Panel View of the DES-7100

Rear Panel Views

Be sure to allow ample room at the back of the Switch for proper ventilation. Do not obstruct any vents on the Switch.

Please read and observe the cautionary statement regarding removal of the back panel.

The battery connection terminals are used with battery back up systems. These systems should be installed by a qualified technician. Please contact your vendor for information about battery back up systems.

The RS-232 console port on the lower right side of the rear panel is used with DES-7012 RPS units only. The console port is not used with DES-7011 RPS units.

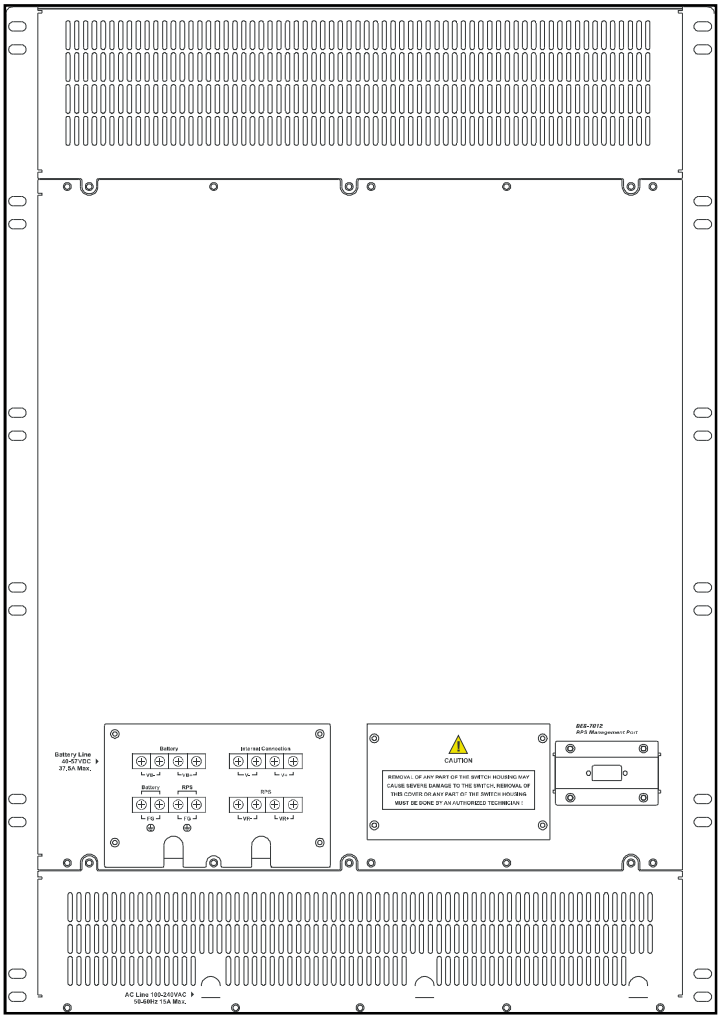


Figure 2 - 6. Rear panel of DES-7000

WARNING	Do not remove the panels covering the power supply or any other panel covering the back of the Switch.

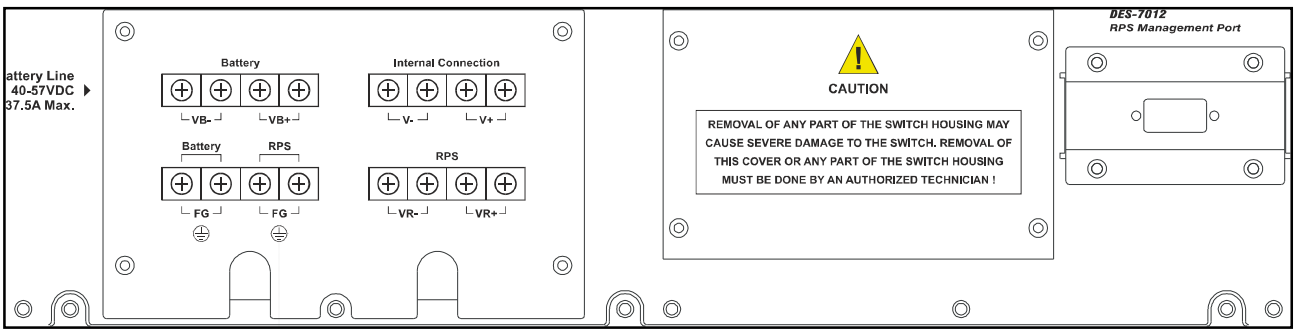
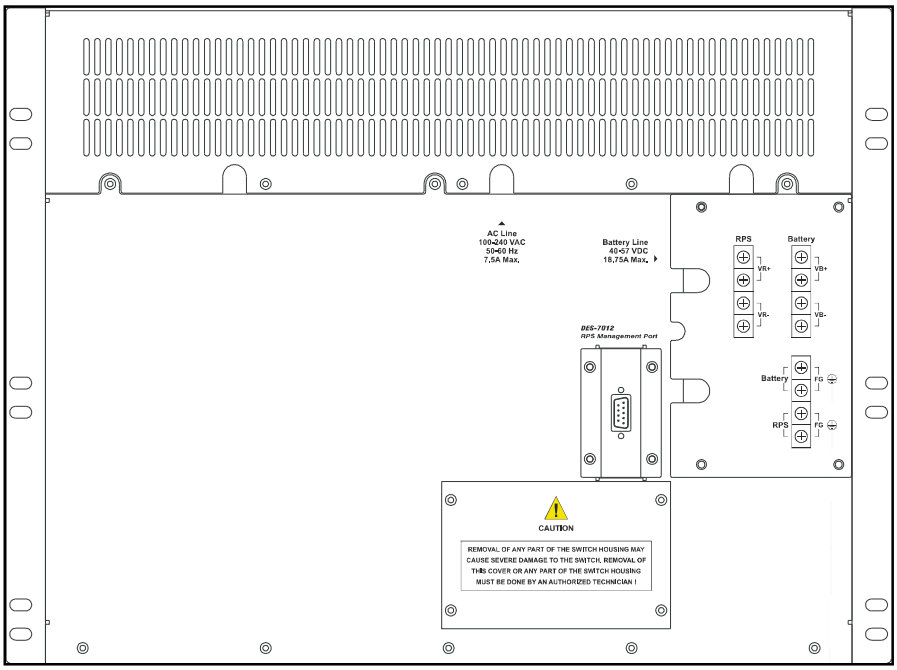


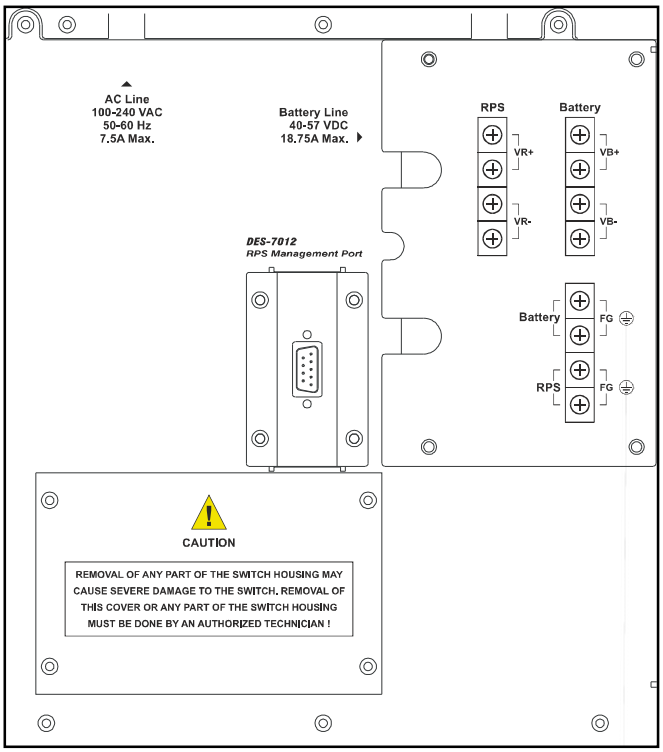
Figure 2 - 7. DES-7000 Battery Terminals and DES-7012 Management Console Port



Do not obstruct the vent on the back panel or on any part of the Switch.

Figure 2 - 8. Rear panel of DES-7100

WARNING	Do not remove the panels covering the power supply or any other panel covering the back of the Switch.



Please read and observe the cautionary statement regarding removal of the back panel.

The battery connection terminals are used with battery back up systems. These systems should be installed by a qualified technician. Please contact your vendor for information about battery back up systems.

The RS-232 console port is used with DES-7012 RPS units only. The console port is not used with DES-7011 RPS units.

Figure 2 - 9. DES-7100 Battery Connection Terminals

Slot Numbering

Slot numbers on the chassis are labeled on the front panel of the fan tray modules for both the DES-7000 and DES-7100. Each slot is given a Slot Name, Physical ID number and Logical ID number. Slot numbering is permanent and absolute regardless of what type of module is installed. Management modules may only be installed in the CPU slots. CPU slots for the DES-7000 are located in the centermost slot positions and are labeled CPU-A and CPU-B. CPU slots for the DES-7100 are located in the uppermost slot positions and are labeled CPU-A and CPU-B. Switch modules may be installed in any of the remaining slots in any order regardless of the type of module. Refer to the tables in Appendix B for Slot Name, Physical Slot ID and Logical Slot ID numbers.

Ports

DES-7003 CPU/Uplink Module

- 1 RJ-45 Management Port (Mgmt) dedicated Switch management through Telnet or Web-based management
- 1 RJ-45 Console Port for out-of-band management and system configuration (requires adapter included with Switch)
- 6 GBIC Gigabit Ethernet Ports for Uplinking Switch to network backbone
- LED Indicators for monitoring status, system alerts and hot swapping

DES-7005 Ethernet/Fast Ethernet Module

- 24 10BASE-T/100BASE-TX RJ-45 Ports
- All ports support auto-polarity detection (MDI-X/MDI-II)
- Connects to 10BASE-T and 100BASE-TX devices at full- or half-duplex
- Supports Category 3, 4, 5 or better UTP or STP connections of up to 100 meters each
- LED Indicators for per port link/activity and speed (above each port) plus hot swapping and module status

DES-7006 100BASE-FX (SFF) Fast Ethernet Module

- 24 100BASE-FX (SFF) Fast Ethernet ports
- Connects to 100BASE-FX devices at full- or half-duplex
- Fully compliant with IEEE 802.3u 100BASE-FX
- IEEE 802.3x compliant Flow Control support for Full duplex
- LED Indicators for link/activity (one above each port) plus hot swapping and module status

DES-7010 Ethernet over VDSL Module

- 2 RJ-21 Ports for connection to 24 clients (ports)
- Compliant with ETSI VDSL requirements
- Supports symmetrical data transfer
- LED Indicators for per port link status (grouped on right side of front panel) plus hot swapping and module status

LED Indicators

The tables below list all the LED indicators for all switch modules and include illustrations of the different LED indicators as they appear on the front panel. All switch modules, including CPU modules, have LED indicators for Power and Hot Swap & Card Status useful when hot swapping the module.

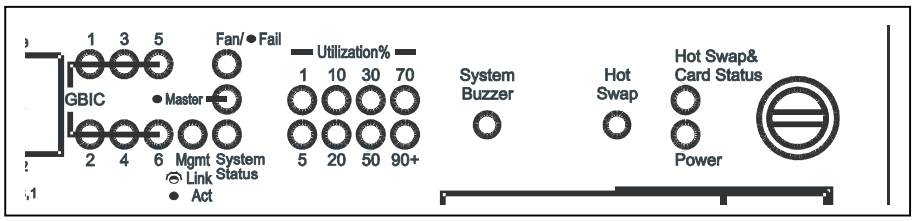


Figure 3-9. DES-7003 Module Front Panel LED Indicators

DES-7003 Management Module LED Indicators	
Per Port GBIC	Lights green to indicate a link for the port. Blinks green when there is activity on the port.
Mgmt	Lights steady green if there is a link on the Mgmt port. Blinks green when there is activity on the port. Remains dark when there is no link.
Fan Fail*	Steady amber light indicates one or more fans not functioning. This does not light when the fans are functioning normally. A fan failure will also trigger the system buzzer (alarm).
Master	Lights steady green when module is performing as active primary master.
System Status	Steady green light indicates normal system function. Amber light indicates abnormal function. Abnormal function can include RPS failure, fan failure or temperature problem. Any of these problems will also trigger an audible alarm, the system buzzer.
Utilization**	Eight scales are used, 1%, 5%, 10%, 20%, 30%, 50%, 70%, 90%+ to indicate traffic rate to the CPU.
Hot Swap & Card Status	This will begin to blink amber when a hot swap of the unit has been initiated. It should begin blinking immediately after the Hot Swap button has been pushed. After a few seconds the module will be powered off and it may be safely removed. Please read the instructions for hot swap removal and insertion of DES-7000 Series modules for a complete description.
Power	Steady green light indicates normal voltage status the module. Amber light indicates a voltage problem in this module.

*Please see the page 26 for more detailed information about the system fans and the shutdown sequence associated with fan failure.

**Utilization rates can be approximated to the number of packets per second using the table to the right. The indicators remain dark if there is no traffic.

1%	1~200 packets per second
5%	201~400 packets per second
10%	401~600 packets per second
20%	601~800 packets per second
30%	801~1000 packets per second
50%	1001~1200 packets per second
80%	1201~1400 packets per second
90+%	>1400 packets per second

Switch Network Module LED Indicators

The different network modules for the Switch present different arrangements for the per port LED indicators.

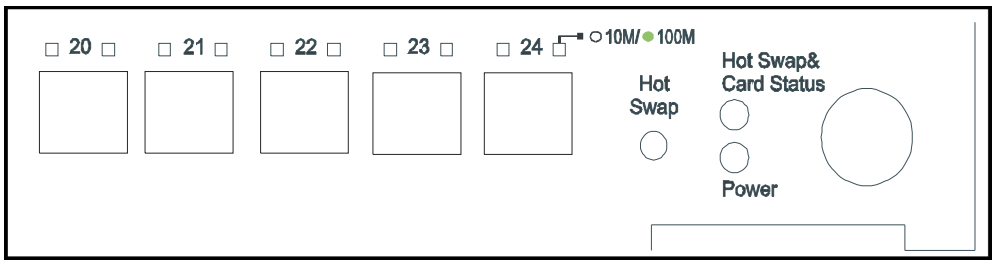


Figure 3- 3. DES-7005 LED Indicators

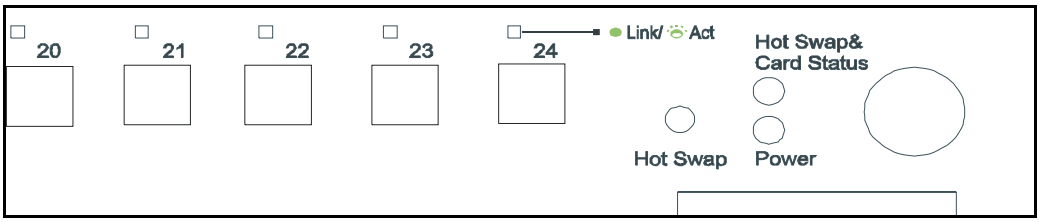


Figure 3- 4. DES-7006 LED Indicators

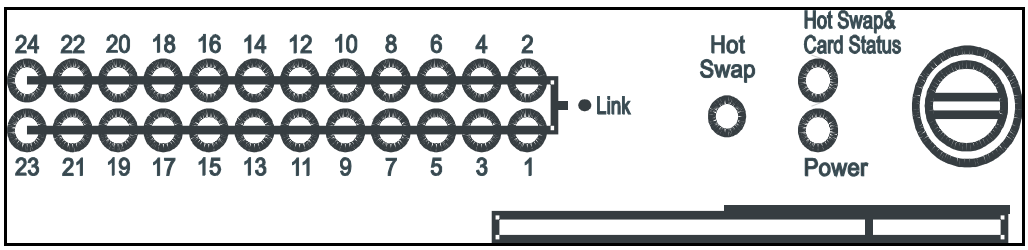


Figure 3- 5. DES-7-10 LED Indicators

Switch Module LED Indicators	
Power	Steady green light indicates normal voltage status in this module. Amber light indicates a voltage problem with this module.
Hot Swap & Card Status	This will begin to blink amber when a hot swap of the unit has been initiated. It should begin blinking immediately after the Hot Swap button has been pushed. After a few seconds the module will be powered off and it may be safely removed.
Per Port Indicators	Switch modules include per port LED indicators that differ for each module. The **DES-7005** has one indicator per port for link/activity and another per port indicator for speed above each port. The **DES-7006** has one per port indicator for link/activity above each port. The **DES-7010** has per port indicators for link status on the right side of the front panel.

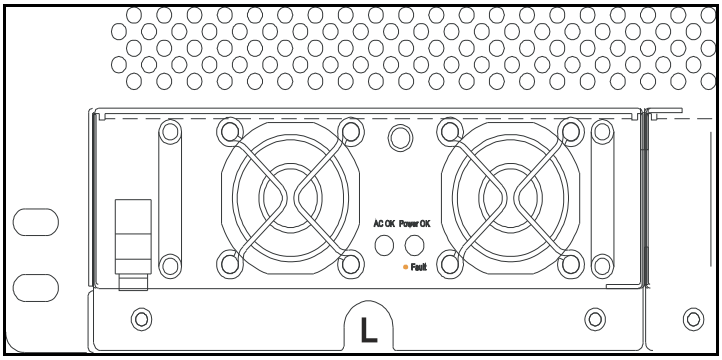


Figure 3- 6. Front Panel of DES-70011 RPS Unit and LED Indicators

LED Indicators for RPS Modules	
AC OK	Steady green light indicates normal function. A dark indicator means the unit is not receiving power or a problem exists.
Power OK	Steady green light indicates normal output level. Amber light indicates abnormal output level. An RPS failure will also trigger the system buzzer (alarm).

AC Power Redundant Power Supplies

The chassis includes two pre-installed power supplies removable from the front with an additional RPS slot available for a third module. The connector for each power supply is embedded on the rear panel. The LED indicators for each power supply are located in the center of the front panel The LED indicators will light green when the unit functioning normally. An amber LED indicator indicates the RPS is not functioning properly.

Push Buttons

Two recessed push buttons are visible on the front panel of the DES-7003 CPU module a System Buzzer and Hot Swap button. Each switch module, including DES-7003 CPU modules, has a Hot Swap push button.

Push buttons are recessed to avoid accidental activation. They can be activated by gently depressing them with a ballpoint pen or other suitable instrument. The functions activated by the buttons are described as follows:

- **System Buzzer** (DES-7003 CPU modules only) A warning sounds when any system fans fail or when the fan tray unit has been removed. Depressing the System Buzzer button will silence the fan fail alarm.

Hot Swap This is used to initiate a hot swap of the module (See the section on hot swapping modules below).

Fans

For the DES-7000 chassis, there are a total of 8 system fans arranged on two plains. At the top of the backside of the Switch chassis are four fans (dimensions = 92 x 92 x 25 mm) arranged in a single horizontal row spanning the width of the Switch. The upper fans run any time power is supplied to the chassis. The remaining 4 fans (dimensions = 172 x 150 x 51 mm) are located in a separate slide-in fan tray module oriented horizontally below the module slots. The fan tray fans are positioned to maintain adequate airflow between installed switch modules. The fan tray fans are power on or off as needed automatically by the CPU using temperature information from built-in sensors.

The DES-7100 has a fan tray module with 6 fans (dimensions = 80 x 80 x 20 mm) oriented vertically on the right side of the switch chassis. The fan tray fans power on or off as needed automatically by the CPU using temperature information from built-in sensors. Fan trays may be replaced from the front of the chassis while the switch is powered on.

System fan failure can result in one or all modules being powered down. The shutdown sequence is as follows:

If two fans fail, all slave modules and the backup Master will be powered off after 30 minutes if not replaced.

If three fans fail, all slave modules and the backup Master will be powered off after 10 minutes.

If four fans fail, all slave modules and the backup Master will be powered off after 5 minutes.

4

Network Cabling and Connections

This chapter describes cabling and connectors used to connect the module to a network and using the LED indicators to evaluate network function.

Connect to the DES-7003 CPU Management/Uplink Module

The DES-7003 module has six Gigabit Ethernet port to uplink the Switch as well as two ports, a Console port and an SNMP port, used for device management.

- GBIC Uplink ports – Install 1000BASE-SX or 1000BASE-FX GBIC plug-in module. These ports are used to link the Switch to the network backbone.
- Console port – Use this for an out-of-band connection to manage the Switch. Connection requires the RJ-45 to RS-232 serial adapter included with the Switch and an Ethernet cable. Connect this directly to the serial port on a computer used for managing the Switch.
- Mgmt port – This port is for out-of-band management of the Switch using either Telnet or web-based management. The Switch can be connected directly to a computer with standard Ethernet cable to the Ethernet port on a computer.

Connect to the DES-7005 10BASE-T/100BASE-TX Module

Network connections to the 24 ports of the Ethernet module are made using Category 5 or better cabling with RJ-45 UTP connectors. Ports may be connected to network devices that support 10BAES-T or 100BASE-TX operation. All ports support auto-negotiation by default for speed, duplex and flow control (in Full duplex mode). All ports are configurable to force different speed, duplex and flow control operation. All ports supports auto-detection of polarity and adjust for MDI/MDI-X connectors to establish a valid link.

The per port LED Link indicators on the DES-7005 will:

- Light green when a link has been established
- Blink green when there is activity in the port
- Remain dark when there is no link

Connect to the DES-7006 100BASE-FX Module

Network connections to the 24 ports of the 100BASE-FX module are made using single multimode fiber (SMF/MMF) optic cabling with SFF (LC Duplex) type connectors.

The per port LED Link indicators on the DES-7006 will:

- Light green when a link has been established
- Blink green when there is activity in the port
- Remain dark when there is no link

Connect to the DES-7010 Ethernet over VDSL Module

The network connections to the DES-7010 Ethernet over VDSL module are provided using Telco 50 cabling to connect to two male RJ-21 ports at the front panel of the module. These ports are labeled PSTN and VDSL. These connections are defined as follows:

- **PSTN** – Use a female RJ-21 connector and Telco 50 cabling to connect the system to a PBX system or other appropriate connection to the Public Switched Telephone Network. This provides the uplink to the VDSL service from the telephone or networks services provider.
- **VDSL –** Use a female RJ-21 connector and Telco 50 cabling to connect up to 24 VDSL subscriber ports (i.e. connect to one remote CPE unit per port) to the module. The switch/module to end users connection can be done through a variety means depending on the circumstances including using a Main Distribution Frame, Cabling Cabinet, patch panels or other suitable wiring systems. This provides the combined data and voice channels to the VDSL accounts.

The per port LED Link indicators on the DES-7010 will:

- Light green when a link has been established
- Remain dark when there is no link

Cable Lengths

Use this table to determine the maximum allowable distance for each cable media type.

Standard	Media Type	MHz/km Rating	Maximum Distance
100BASE-FX	50/125µm Multimode Fiber (half-duplex operation)		400 Meters
	50/125µm Multimode Fiber (full-duplex operation)		2000 Meters
	62.5/125µm Multimode Fiber (half-duplex operation)		400 Meters
	52.5/125µm Multimode Fiber (full-duplex operation)		2000 Meters
100BASE-TX	Category 5 UTP Cable (100Mbps)		100 Meters
10BASE-T	Category 3 UTP Cable (10Mbps)		100 Meters

5

Switch Management

This chapter discusses many of the features used to manage the switch and explains many concepts and important points regarding these features. Configuring the switch to implement these concepts is discussed in the next chapter on using the Web-based management software and the CLI Reference Guide.

- **Local Console Management**
- **Using the CLI Interface**
- **Saving Changes**
- **Remote Management**
- **Packet Forwarding and Filtering**
- **SNMP**
- **Spanning Tree Protocol**
- **VLANs**

Local Console Management

A local console is a terminal or a workstation running a terminal emulation program that is connected directly to the switch via the console port on the front of the switch. A console connection is referred to as an out-of-band connection, meaning that console is connected to the switch using a different circuit than that used for normal network communications. You will need the RJ-45 to DB-9 (RS-232) adapter included with you shipment to complete the console connection.

Local console management uses the terminal connection to operate the console program built-in to the switch. A network administrator can manage, control and monitor the switch from the console program.

The DES-7003 management module contains a CPU, memory for data storage, flash memory for configuration data, operational programs, and SNMP agent firmware. These components allow the switch to be actively managed and monitored from either the console port or the network itself (out-of-band, or in-band).

Use the console connection to setup user accounts and assign IP settings. When these tasks have been completed the Switch can be connected to the network and configured as desired. There are three options available to safely access the management software; direct out-of-band connection through the console port, or in-band using Telnet or web-based management through the network. Both the Telnet and console interface use a Command Line Interface (CLI) structure. The CLI Reference Guide contains a complete listing of all the available commands.

Console Port (RJ-45 UTP)

Use the RJ-45 console port on the front panel of the management module for the initial configuration. To use the console port, you can run terminal emulation software on a computer or use a VT100-compatible terminal. You will need the RJ-45 to DB-9 (RS-232) adapter included with you shipment to complete the console connection.

To establish a console connection to the Switch:

1. Insert the RJ-45 to DB-9 adapter into the RJ-45 console port on the front panel of either management/uplink module. The console port is labeled and is located next to the LED indicators.
2. Attach the female end of the RS-232 cable (included with shipment) to the male RS-232 connector on the adapter.
3. Connect the RS-232 cable to a standard COM port on a computer.

4. The RS-232 connection to the computer should be configured as follows:
   Baud rate = 9600
   Parity = none
   Data bits = 8
   Stop bits = 1
   Flow control = none

Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a computer, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try typing Ctrl + R to refresh the screen.

Boot Screen

Each Switch CPU module is assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found from the initial boot console screen - shown below.

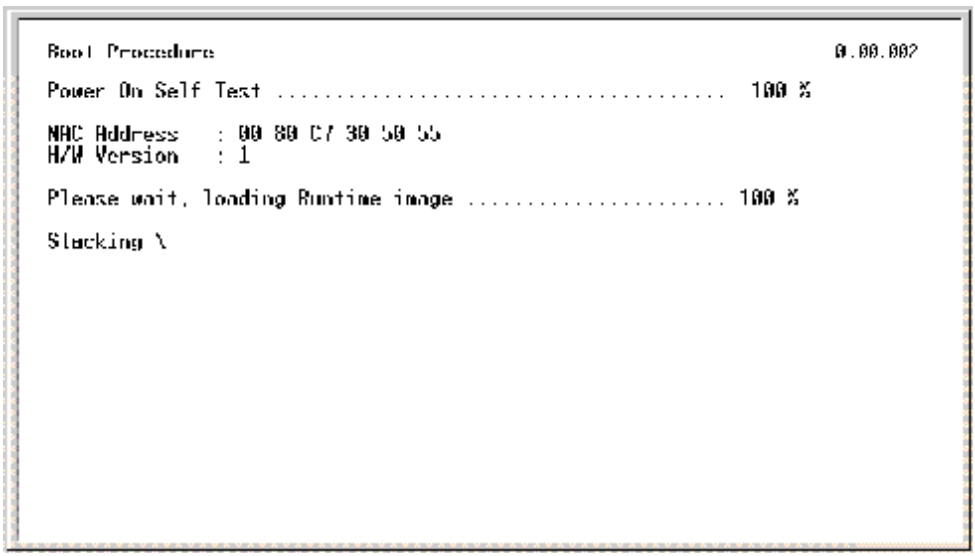


Figure 5- 1. Boot Screen

Using the CLI Interface

After start up process is completed the CLI interface prompts for a user name and password. If you have not yet set up user accounts for the Switch it is recommended that you do this before the Switch is connected to the network. User accounts not configured at the factory and there is no default user account. The first time the Switch is set up or following a **`reset {all}`** command you may simply press the Enter key when prompted for a user name and again for the password prompt. The command prompt, **`DES-7000:4#`** will now appear. You may proceed to enter CLI commands.

If a portion of a command is not recognized or if you enter a command without its required parameters, the CLI will prompt you with a **`Next possible completions:`** message followed by a list of acceptable commands or required parameters. If a command is not recognized the **`Available commands:`** message lists the basic top-level commands. You can use the **`dir`** or **`?`** commands to list may be used to view available commands.

Save Changes

It is necessary to save any changes to Switch configuration including IP settings and user accounts information. Use the **`save`** command in the CLI interface to save changes to non-volatile RAM. Simply type *save* and press the Enter key. It will take a few seconds to save any changes to the Switch. Make sure the Switch remains powered on until the save is completed.

User Accounts

The DES-7000 Series Switch is not assigned administrator-level user account information when shipped. If this is the first time you setting up the switch, assigning an administrator-level user account should be a priority. Once user accounts have been assigned, at least one administrator-level user account should be kept. The exception might be if you use the **reset {all}** command, in this case all user account information is erased.

Use the **create account** command to create a new administrator-level user account. To set up an administrator account, type the command **create account admin** followed by a user name. The command syntax is **create account admin <user name>**. Then you are be prompted for a new password, type the case-sensitive password and press Enter. Type the same password again to confirm it.

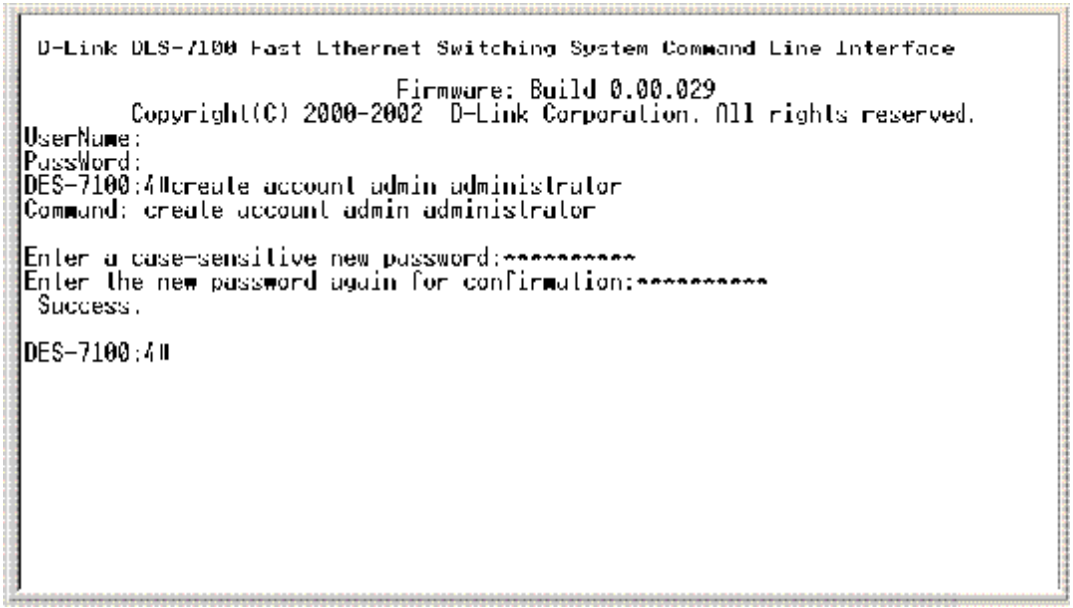


Figure 5- 2. Create Administrators User Account

The **Success** message indicates the new user account has been successfully created. If the new password entry does not match the confirmation you will be prompted to repeat the password entry. Be sure to save the new user accounts information before powering off or rebooting the Switch.

To create additional user accounts, use the following syntax: **create account [admin/user] <user name>.** The **admin** or **user** declares the level of user privilege. At least one administrator-level user account should be maintained in the system.

To delete a user account, use the following syntax: **delete account <user name>.** Remember to keep at least one administrator-level user account in the system.

To view existing user accounts use the **show account** CLI command.

Basic Switch Information

The switch's MAC address can also be found along with other basic information about the Switch using CLI as shown below. Basic switch information may be listed using the command **show switch**.

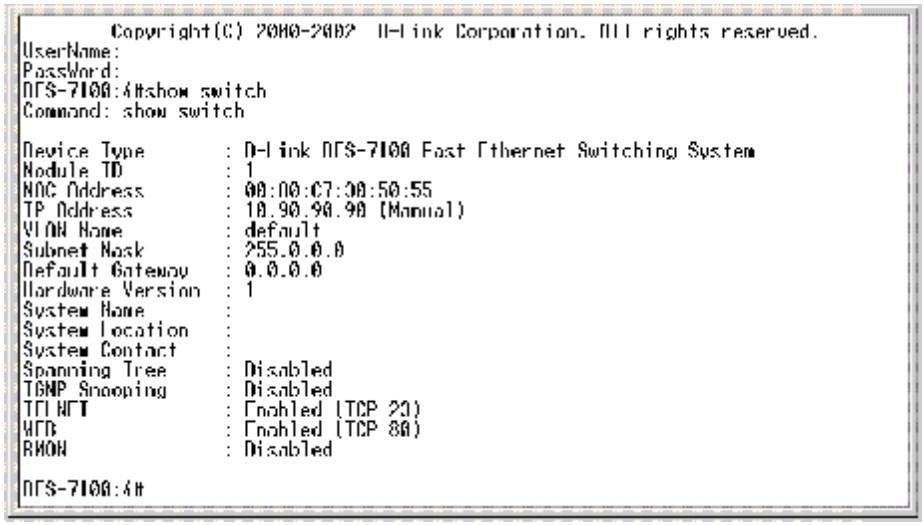


Figure 5- 3. Basic Switch Information Screen

Information about installed modules can be viewed with the **show unit_information** command. Modules are listed by slot number and include information on the unit type, Prom code version, Runtime code version and hardware version.

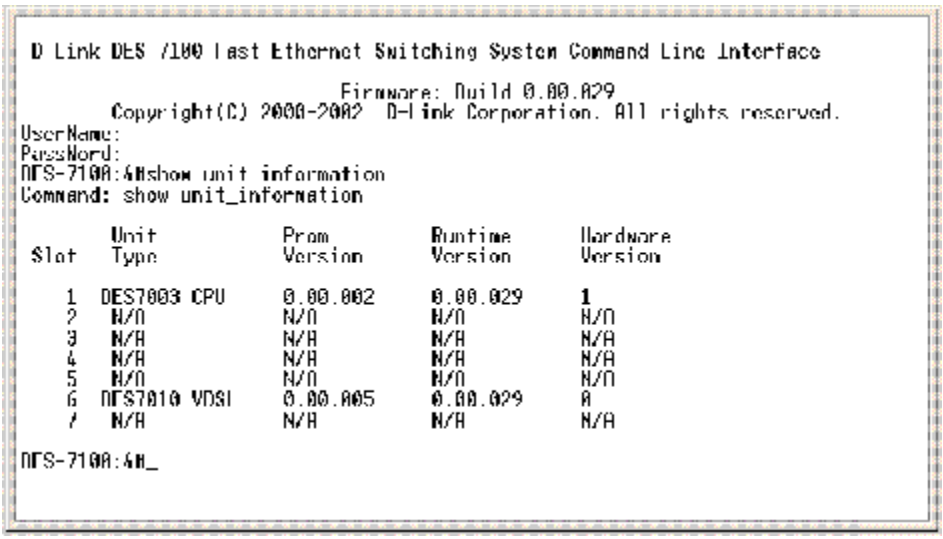


Figure 5- 4. Unit Information

Remote Management

Remote management through the Web-based management software or Telnet is enabled by default. Once you have the IP settings of the Switch configured you can use either of these methods to manage the Switch. In-band management can be done remotely through the network using Telnet the web-based management. You may also use a Telnet or web interface for out-of-band management by connecting directly to the Switch's dedicated Management port (labeled Mgmt) on the Primary Master CPU module. The Mgmt port is an RJ-45 connection with auto-polarity detection so you can use standard Ethernet cable to connect it to the Ethernet port on a desktop PC or notebook computer.

Telnet uses the same CLI commands you would use for the console connection. See the CLI Reference Guide for a complete list of commands. The following chapter describes how to access the Web-based management interface.

SNMP

The Simple Network Management Protocol (SNMP) is an OSI layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package.

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.
- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The Switch has a software program called an 'agent' that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

Packet Forwarding

The Switch learns the network configuration and uses this information to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all segments, are transmitted to the destination only. Example: if Port 1 receives a packet destined for a station on Port 2, the Switch transmits that packet through Port 2 only, and transmits nothing through the other ports.

A listing of CLI commands for Switch forwarding and related settings can be found in the CLI Reference Manual in the chapter titled, Layer 2 FDB Commands. Use the menus contained in the Forwarding and Filtering folder of the web manager to make entries into the Unicast and Multicast forwarding tables (see page 65).

MAC Address Aging Time

The Aging Time affects the learning process of the Switch. Dynamic forwarding table entries are made up of the source and destination MAC addresses and their associated port numbers and are deleted from the table if they are not accessed within the aging time.

The aging time can be adjusted from 10 to 2200 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. To change MAC Address Aging Time use the CLI command **`config fdb aging_time`** or use the Advanced Settings menu of the web manager (page 52).

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.

Static forwarding entries are not affected by the aging time.

Packet Filtering

The switch uses a filtering database to segment the network and control communication between segments. It can also filter packets off the network for intrusion control. Static filtering entries can be made by MAC Address.

Each port on the switch is a unique collision domain and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

For intrusion control, whenever a switch encounters a packet originating from or destined to a MAC address or an IP Address entered into the filter table, the switch will discard the packet.

The switch does some filtering automatically:

Dynamic Filtering: automatic learning and aging of MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.

Filtering done by the Spanning Tree Protocol, which can filter packets based on topology, making sure that signal loops don't occur.

Filtering done for VLAN integrity. Packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3) will be filtered.

Some filtering requires the manual entry of information into a filtering table:

MAC address filtering - the manual entry of specific MAC addresses to be filtered from the network. Packets sent from one manually entered MAC address can be filtered from the network. The entry may be specified as a source, a destination, or both.

A listing of CLI commands for filter MAC addresses and related settings can be found in the CLI Reference Manual in the chapter titled, Layer 2 FDB Commands. Use the menus contained in the Forwarding and Filtering folder of the web manager to make entries into the Unicast and Multicast forwarding tables (see page 65).

Spanning Tree Protocol

The IEEE 802.1D Spanning Tree Protocol (STP) allows for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows the duplicate links to be used in case of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically - without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please carefully read understand this section before making any changes from the default values.

The Switch allows two levels of spanning trees to be configured. The first level constructs a spanning tree among all links between network switches. This first level is referred to as the Switch or Global level. The second level is based on port groups. Groups of ports are configured as being members of a spanning tree and the algorithm and protocol are applied to the group of ports. This is referred to as the Port or VLAN level.

Spanning Tree on the Switch performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees - from any combination of ports contained within a single switch, in user-specified groups (usually VLANs).
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Spanning is disabled system-wide by default and must be enabled in order to function switch-wide and on a per port basis. Use the CLI command **`enable stp`** or use the web manager menu STP Switch Settings (see page 63) to enable STP. To disable any individual port, use the STP Port Settings menu (see page 64).

STP Operation Levels

STP operates on two levels: the switch level and the port or VLAN level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

On the switch level, STP calculates the bridge identifier for each switch and then sets the root bridge and the designated bridges.

On the port level, STP sets the root port and designated ports.

Switch Level STP

The user may configure the switch STP parameters listed here:

Parameter	Description	Default Value
Bridge Identifier (Not user-configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

Port Level STP

The user may configure the VLAN or port STP parameters listed here:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	32768
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path.	10

Bridge Protocol Data Units

The Switch uses the following information for STP to stabilize network topology:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

This STP information is shared among switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

One switch is elected as the root switch

The shortest distance to the root switch is calculated for each switch

A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.

A port for each switch is selected. This is the port providing the best path from the switch to the root switch.

Ports included in the STP are selected.

Creating a Stable STP Topology

If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Transition States

Each port on a switch using STP exists is in one of the following five states:

Figure 5.4 below illustrates the STP port transition states.

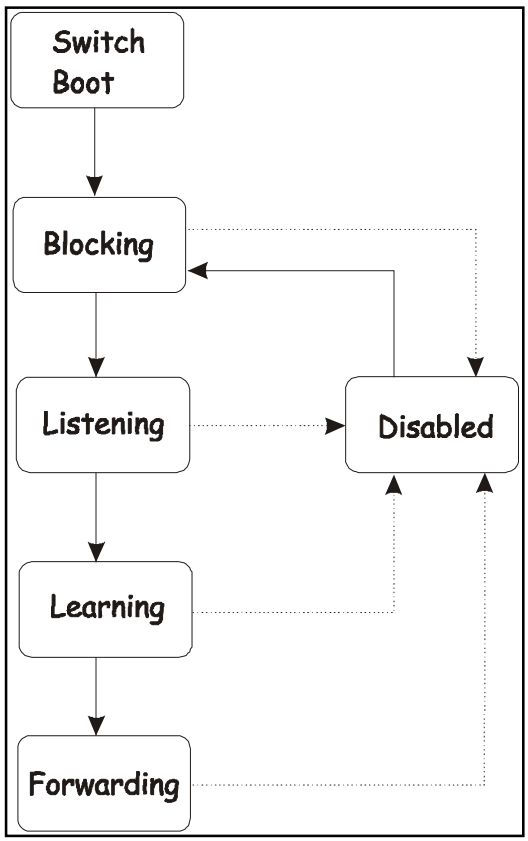


Figure 5-4. STP Transition States

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

Blocking

The port is blocked from forwarding or receiving packets.

Listening

The port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.

Learning*

The port is adding addresses to its forwarding database, but not yet forwarding packets.

Forwarding

The port is forwarding packets.

Disabled

The port only responds to network management messages and must return to the blocking state first.

Port State Transition

When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state.

No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

*Learning may be enabled or disabled for individual ports, please read Port Configuration on page 55 for a description of how the DES-7000/DES-7100 implements learning on the Switch. If it is disabled for the port, this port state is skipped.

User-Changeable STP Parameters

The factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory, unless it is absolutely necessary. The user changeable parameters described below are configured using the menus located in the Spanning Tree folder of the web manager. The CLI Reference Manual contains a listing of Spanning Tree Commands in its own section.

- **Bridge Hello Time**

The Bridge Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge. The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

- **Bridge Max Age**

The Bridge Maximum Age Timer can be from 6 to 40 seconds. At the end of the Max. Age, if 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 the Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **Bridge Forward Delay**

The Bridge Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

- **Bridge Priority**

Bridge Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

- **Forwarding BDPU**

Enabled by default. This may be disabled, in which case BDPU packets (also called Hello messages) are no longer forwarded.

Observe the following formulas when setting the above parameters:

- Max. Age = 2 x (Forward Delay - 1 second)
- Max. Age = 2 x (Hello Time + 1 second)
- Port Priority. A Port Priority can be from 0 to 255. The lower the number, the greater the probability the port will be chosen as the Root Port.*
- Port Cost. A Port Cost can be set from 1 to 65535. The lower the number, the greater the probability the port will be chosen to forward packets.*

* Port Cost and Port Priority can be configured for individual ports using the STP Port settings menu (page 64) or use the CLI command group **`config stp_ports`**.

Illustration of STP

A simple illustration of three Bridges (or three switches) connected in a loop is depicted in Figure 5.5. In this example, you can anticipate some major network problems if the STP assistance is not applied. If Bridge A broadcasts a packet to Bridge B, Bridge B will broadcast it to Bridge C, and Bridge C will broadcast it to back to Bridge A ... and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure.

STP can be applied as shown in Figure 5.6. In this example, STP breaks the loop by blocking the connection between Bridge B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings. Now, if Bridge A broadcasts a packet to Bridge C, then Bridge C will drop the packet at port 2 and the broadcast will end there.

Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

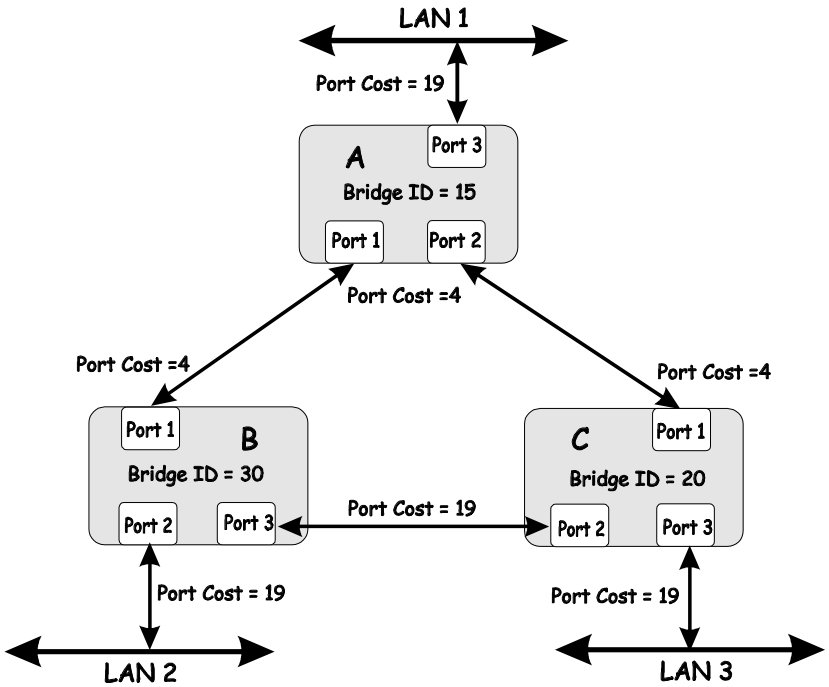


Figure 5-5. Before Applying the STA Rules

In this example, only the default STP values are used.

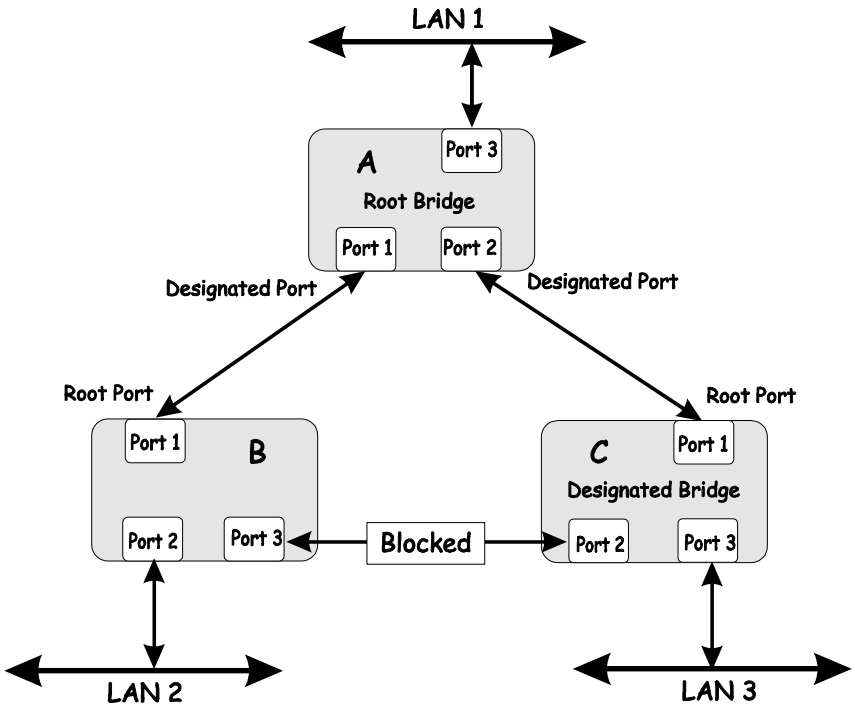


Figure 5-6. After Applying the STA Rules

Sample Network using STP

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C.

Note also that the example network topology is intended to provide redundancy to protect the network against a link or port failure – not a switch failure or removal. For example, a failure of switch A would isolate LAN 1 from connecting to LAN 2 or LAN 3.

VLANs

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so packets that are forwarded only between ports within the VLAN.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains. Although VLANs are a function of Layer 2 networking, it is common on many networks to coordinate the creation of VLANs with an IP addressing scheme, so that each subnet has its own VLAN.

A VLAN is essentially a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Within the Layer 2 switching environment, all end nodes are identified on the network by their unique MAC address. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

For VDSL applications, VLANs can be used for a group of ports used by a single subscriber. For example, one client may have a company network of a size that requires more than one port on the Switch. In this case, the Switch can be used to create one VLAN for the group of port leased the single subscriber. The client can then administer VDSL access on the private network as desired. All the ports within the client's VLAN can freely exchange packets through the VDSL Switch. Once the VLAN has been created, there should not be any more configurations decisions for the VDSL Switch manager, as long as there are no additional ports required by the client. If the client prefers to lease additional bandwidth (i.e. more ports), these can be easily added to the client's VLAN if there are unused ports available on the Switch.

The Switch supports only IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

By default the Switch assigns all ports to a single 802.1Q VLAN named "default". The VLAN "default" has a VID = 1.

IEEE 802.1Q VLANs

To help you understand 802.1Q VLANs as implemented by the Switch, it is necessary to understand the following:

Tagging - The act of putting 802.1Q VLAN information (a tag) into the header of a packet.

Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

Ingress Port - A port on a switch where packets are flowing into the switch and VLAN decisions must be made.

Egress Port - A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allow VLANs to work with legacy switches that don't recognize VLAN tags in packet headers.

The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering
- Assumes the presence of a single global spanning tree
- Uses an explicit tagging scheme with one-level tagging

802.1Q Packet Forwarding Decisions

Packet forwarding decisions are made based upon the following three types of rules:

- **Ingress rules** - rules relevant to the classification of received frames belonging to a VLAN.
- **Forwarding rules** between ports - decides filter or forward the packet
- **Egress rules** - determines if the packet must be sent tagged or untagged.

Packet Forwarding in 802.1Q VLANs

The diagram below illustrates packet-forwarding decisions with 802.1Q VLANs.

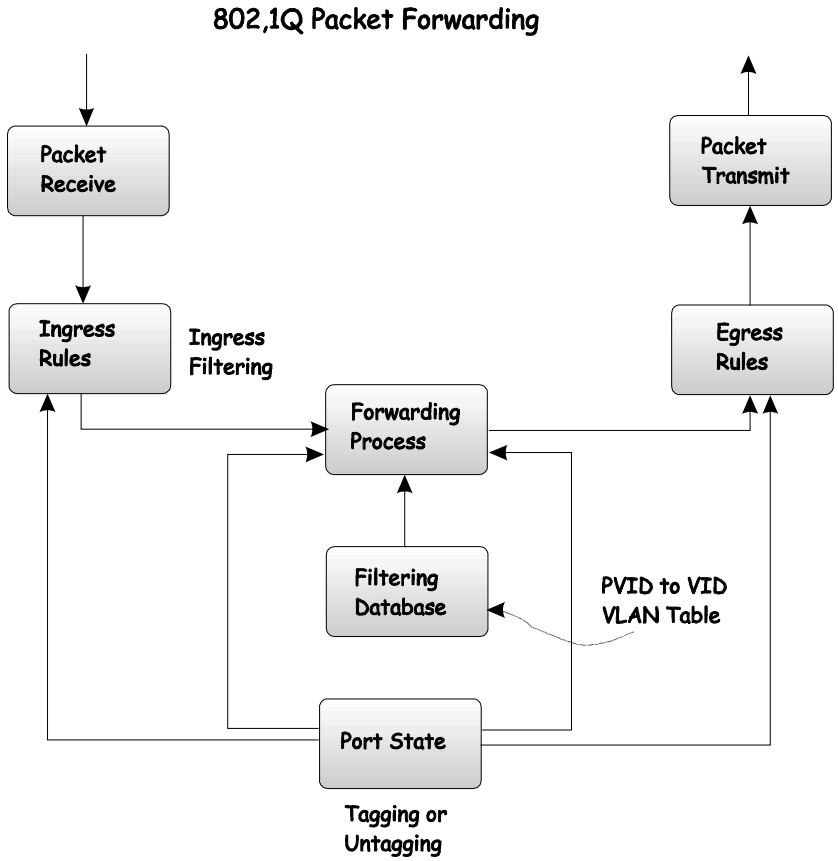


Figure 5-7. Packet Forwarding with VLANs

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones) and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information contained in the packet originally is retained.

The figure below illustrates the elements of the IEEE 802.1Q tag.

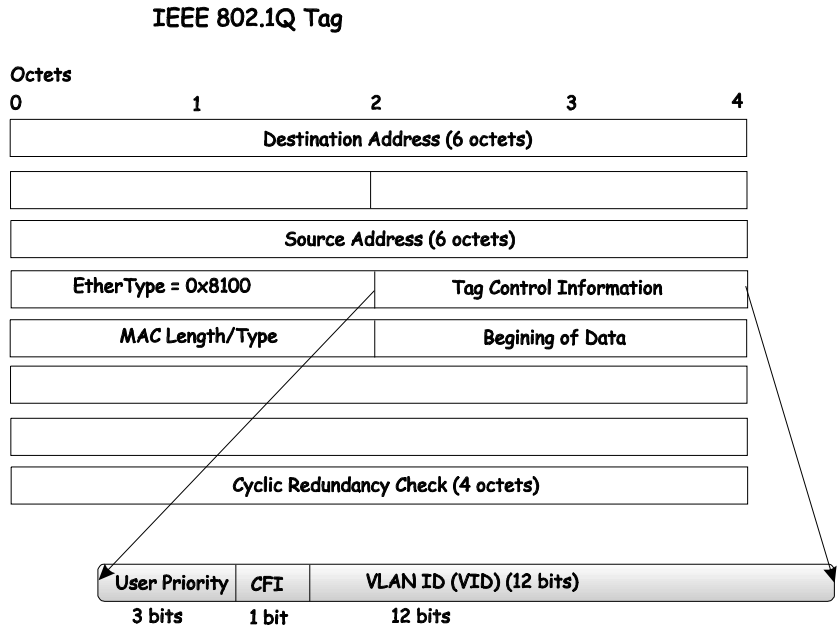


Figure 5-8. IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

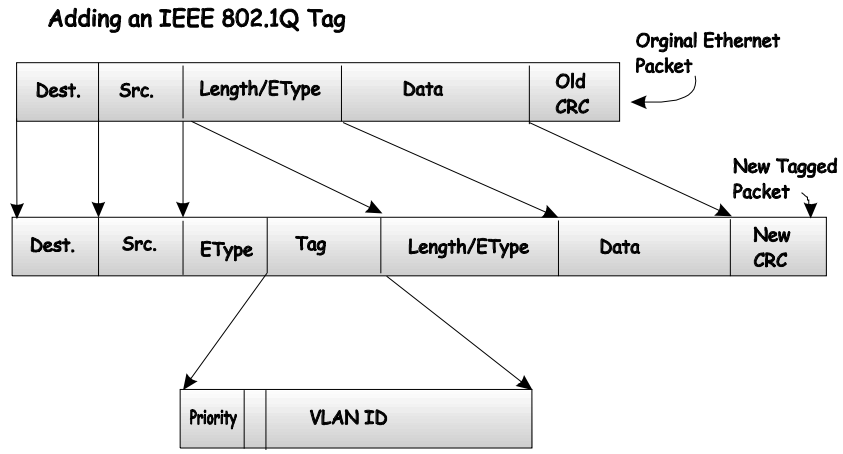


Figure 5-9. Adding 802.1Q Tag to a Packet Header

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network - if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the

packet's destination address (found in the switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet.

Within the switch, different PVIDs mean different VLANs. (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch.

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the switch to VIDs on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted - should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging Packets

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Configuring VLANs

The switch initially configures one VLAN, VID = 1, called the default VLAN. The factory default setting assigns all ports on the switch to the default VLAN. As new VLANs are configured, there respective member ports are removed from the default VLAN.

Packets cannot be transmitted accross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

If no VLANs are configured on the switch all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

Traffic Control

Broadcast and multicast storms consist of broadcast packets that flood and/or are looped on a network causing noticeable performance degradation and in extreme cases, network failure. Broadcast storms can be caused by malfunctioning NICs, bad cable connections and applications or protocols that generate broadcast traffic, among others.

Broadcast and multicast storms have long been a concern for network administrators with routers traditionally being used to prevent their occurrence, and if that failed, limit their scope. However, with the advent of VLANs, switches are now able to limit broadcast domains better and cheaper than routers. Also, many managed and unmanaged switches have broadcast sensors and filters built into each port to further control broadcast storms.

Segmenting Broadcast Domains

VLANs can be used to segment broadcast domains. They do this by forwarding packets only to ports that are members of the same VLAN. Other parts of the network are effectively shielded. Thus, the smaller the broadcast domain, the smaller effect a broadcast storm will have. Because VLANs are implemented at each switch port, they can be quite effective in limiting the scope of broadcast storms.

Eliminating Broadcast Storms

SNMP agents can be programmed to monitor the number of broadcast packets on switch ports and act on the data. When the number of broadcast packets on a given port rises past an assigned threshold, an action can be triggered. When enabled, the rate of broadcast packets coming in through the affected port will be limited. Any traffic above the threshold limit will be discarded. The Switch also supports multicast storm control.

In the Switch, the default trigger threshold is set to 128,000 broadcast packets per second (128 Kbps) for both 100 Mbps Fast Ethernet ports and the 1000 Mbps GBIC ports.

Multicasting

Multicasting enables a single network source to send packets to multiple interested recipients with persistent connections. An interested recipient is defined as a host that has requested beforehand to be associated with a multicast group. This distinguishes it from traditional unicast (one-to-one) and broadcast (one-to-all) methods of delivery. The main advantage to multicasting is that when it is correctly configured it can decrease network load for communications that would otherwise use broadcasting.

Typically multicasting is implemented for specific applications and functions such as video and other multimedia streaming across campus or extended networks, distribution of operating system images to staff workstations using tools like Ghost, and certain VoIP features such as conference calling. When properly implemented, the Switch can support multicasting applications by forwarding multicast traffic only to participating hosts and only for the amount of time required for the application.

For multicasting to function successfully on a network, it is necessary to have the participating systems set up with the proper configuration. At a minimum, the following requirements should be met:

- The application running on the multicasting source device must determine the multicast address (address/port combination) on which to send multicast data packets.
- The application on the receiving hosts must listen for the required multicast address (or multiple addresses).

- The TCP/IP stack of the operating systems at both the sending and receiving end must be capable of sending and receiving multicast traffic. Most modern operating systems for servers and workstations support multicasting.
- Intervening devices (Layer 3 and Layer 2) must be capable of supporting multicast discovery and routing protocols.

Multicast Addressing

Multicast addresses do not identify individual hosts like Class A, B or C IP networks and multicast address cannot appear as a source address. Multicasting uses group membership, employing a address/port combination to define the members of a multicast group. A host may be a member of one or several multicast groups, but each host must request and be granted membership in the group before it will be allowed to receive multicast data.

The Class D IP address range is assigned to network devices that comprise a multicast group. The four most significant four bits of a Class D address are set to "1110". The following 28 bits are referred to as the 'multicast group ID'. Some Class D address groups are registered with the Internet Assigned Numbers Authority (IANA) for special purposes. For example, the block of multicast addresses ranging from 224.0.0.1 to 224.0.0.225 is reserved for use by routing protocols and some other low-level topology discovery and maintenance protocols. A full listing of multicast addresses and other useful information can be found at http://www.iana.org/assignments/multicast-addresses.

Multicast Groups

There are three types of IP v4 addresses: unicast, broadcast, and multicast. Unicast addresses are used to transmit messages from a single network device to another, single network device. Broadcast packets are sent to all devices on the subnet. Multicast defines a group of network devices or hosts that will receive the multicast packets. The members of this group are not necessarily on the same subnet or VLAN. Specially designated multicast addresses are used to send multicast packets to the group members. The Ethernet multicast destination address is a function of a portion of the multicast IP address (within the reserved range) and the MAC address of the recipient.

Multicast groups can be administered manually using the Static Multicast Forwarding table (see page 66).

IGMP

Internet Group Management Protocol (IGMP) is a Layer 3 protocol used by multicast recipient hosts to communicate multicast group membership information to local (or nearest) routers. Receiving hosts use IGMP to indicate to their desire to join a multicast group with a membership report (one per group), the routers in turn periodically send a membership query to establish whether any hosts are still interested in receiving an active group. If a router receives no reply after three consecutive membership queries, the router can stop the transmission of the group to the LAN, and prune itself from a multicast routing tree.

A later version of IGMP (IGMPv2) allows hosts to indicate a desire to leave a multicast group by sending a leave group message. A leave message instructs the multicasting agent and (and the Switch if IGMP Snooping is enabled) to discontinue transmission of multicast data, without having to wait for a timeout. This can save resources, particularly if hosts are involved in frequent group changing (e.g. an application that "changes channels", selecting from various video/audio streams).

IGMP Snooping

Even though IGMP is a Layer 3 function, the Switch is capable of inspecting IGMP packets that pass through it. The ability to examine IGMP information from multicast source and destination systems (i.e. group membership reports, leave group messages and group membership queries) enables much more efficient management of multicast data. Without IGMP snooping it would be necessary to broadcast all multicast traffic to all ports and all VLANs. This would cause sever bandwidth problems on networks that are simultaneously running just a few multicast applications. When IGMP snooping is enabled (IGMP snooping is disabled by default on the DES-7000 and DES-7100), the Switch makes delivery decisions on multicast traffic, matching multicast groups to Switch ports and eliminating the need to broadcast. In order to use IGMP Snooping it must first be enabled for the entire Switch using the Advanced Settings (see page 52) and then enabled for individual VLANs (see IGMP Snooping Settings on page 60).

The diagram to the right illustrates IGMP Snooping. When it is enabled on the Switch, only the branches of the tree containing interested hosts (shaded) receive the multicast stream.

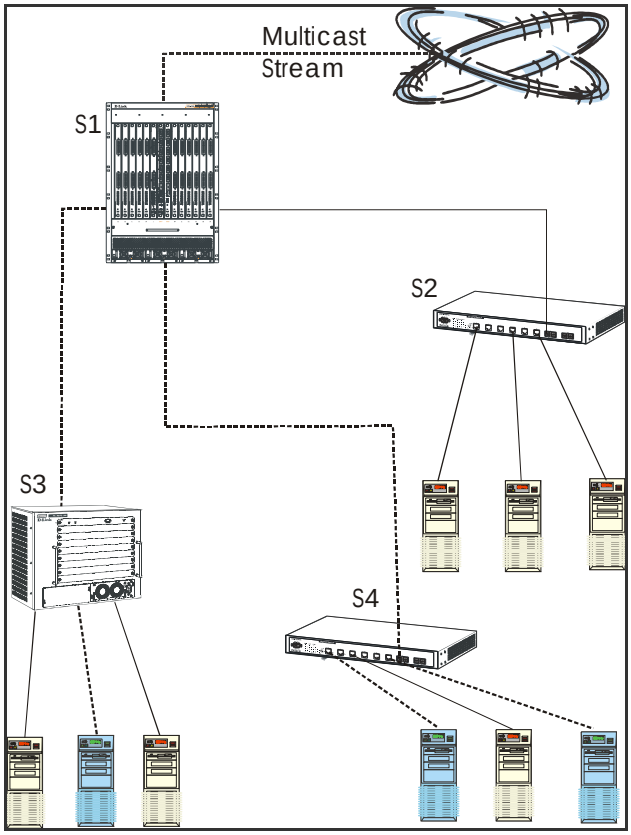


Figure 5- 5. IGMP Snooping

The table below describes the IGMP Snooping variables that can be adjusted for any single VLAN or switch-wide to fine tune multicasting implementation on the network. This table also appears in the next chapter.

Query Interval	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 65,535 seconds are allowed. Default = 125.
Max Response Time	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Variable	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 2 to 255. Default = 2.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1.
Host Timeout	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260.
Route Timeout	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260.
Leave Timer	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted.
Querier State	Choose *Querier* to enable transmitting IGMP Query packets or *Non-Querier* to disable. The default value is *Non-Querier*.
State	Select *Enabled* to implement IGMP Snooping. IGMP Snooping is *Disabled* by default.

6

Using the Web-based Management Software

The DES-7000 Series Modular Switch provides an embedded Web-based (HTML) interface, allowing users to manage the Switch from a remote workstation. The network administrator can communicate directly with any standard HTML-based web browser. The web-based management module and the Console program (and Telnet) access the same internal switching software and configure it.

***Note:** This Web-based Management Module does not accept Chinese language input (or other languages requiring 2 bytes per character).*

Getting Started

If this is the first time you are configuring the Switch you can use the CLI management interface through the console port first to change the IP settings of the Switch. Instructions for changing the IP settings for first-time set up are listed in the Quick Installation Guide included with your shipment (use CLI command **`config ip`**). Once the Switch and the workstation used for configuration have compatible IP settings you may configure the device using the web-based management or CLI (Telnet) interface. To access the Switches web manager through the network, the workstation used should be on the same subnet as the Switch. You may also use Telnet or the web-based software if the Switch is connected directly to a computer via the Mgmt port on the front of the Primary Master CPU module. The Mgmt port is a dedicated Ethernet port used for out-of-band access to the management software. User accounts (user name and password) for the Switch should be set up prior to connecting it to the network (use CLI command **`config account`**). Instructions for establishing user names and passwords are also found in the Quick Installation Guide.

The factory default IP settings for DES-7000 and DES-7100 Switches are:

IP Address = 10.90.90.90

Subnet Mask = 255.0.0.0

Make sure the workstation used to access the web management software has a suitable web browser installed and be sure to disable any proxy settings for the web browser in order to allow for direct connection to the Switch.

Log On to Web Manager

Now that your workstation is ready you can simply start your preferred web browser and direct it to the Switch. Type the IP address in the address bar on the browser so the URL reads **http://** followed by the IP address of the Switch. For example, using the factory default IP address the URL should read:

http://10.90.90.90

The Login page will appear in the browser window similar to the page illustrated below. Click on the animated *Login* icon near the D-Link logo.

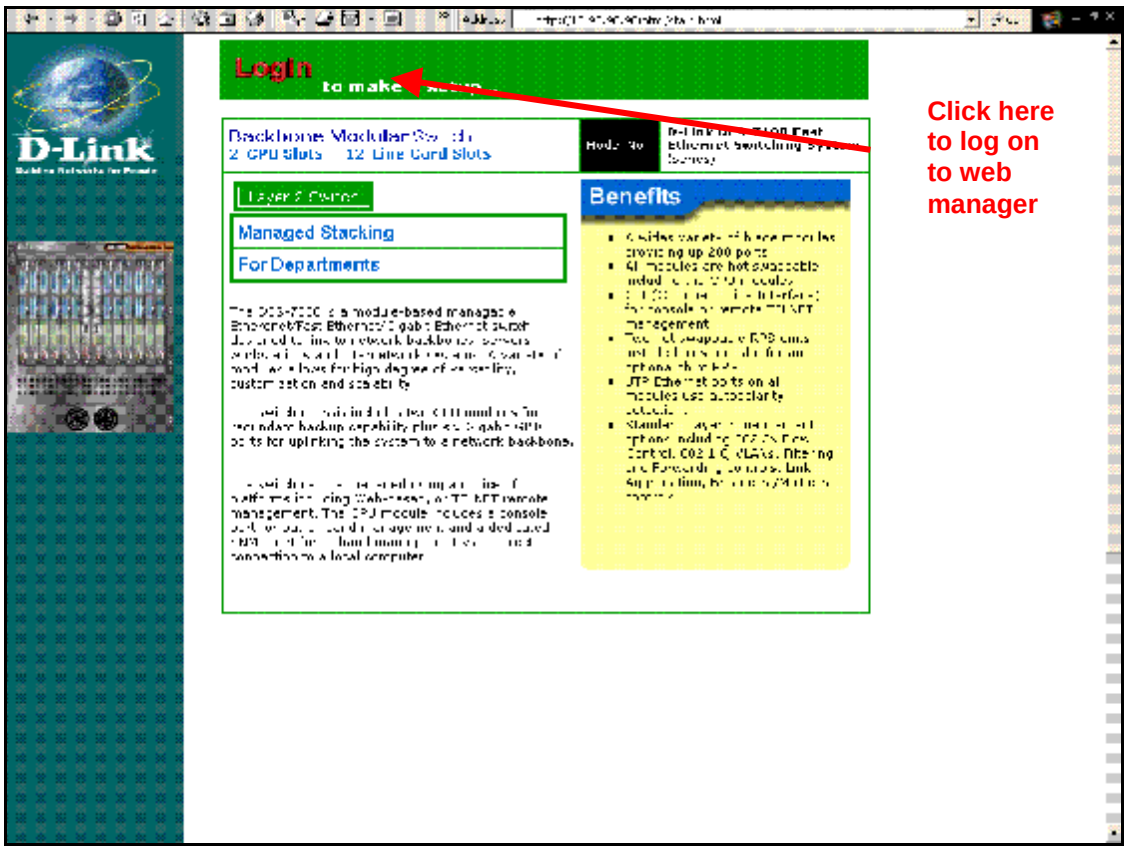


Figure 6- 1. Web Manager Login

Click on *Login* to bring up the authorization screen prompt. You must supply the User Name and Password assigned to the Switch in order to access configuration software.

IMPORTANT	*There is no default user name or password for the Switch. Be sure to set up User Accounts before connecting it to the network.*

Accessing Menu Windows

To access menu windows, open (click once on) the folder or subfolder containing the menu you want to view and double-click on the corresponding menu button.

As illustrated in the example below, the web-based management GUI presents a virtual representation of the entire Switch in the upper right portion of the browser window. The lower right portion displays the primary CPU management module initially. This view can be changed to display any of the installed functioning modules on the Switch chassis. To view a different module, click on the module you wish to view in the virtual front panel display of the entire Switch. The individual module is displayed in near real time showing LED indicators as they appear on the module. Detailed information about any module may be viewed by accessing the Modules Information menu.

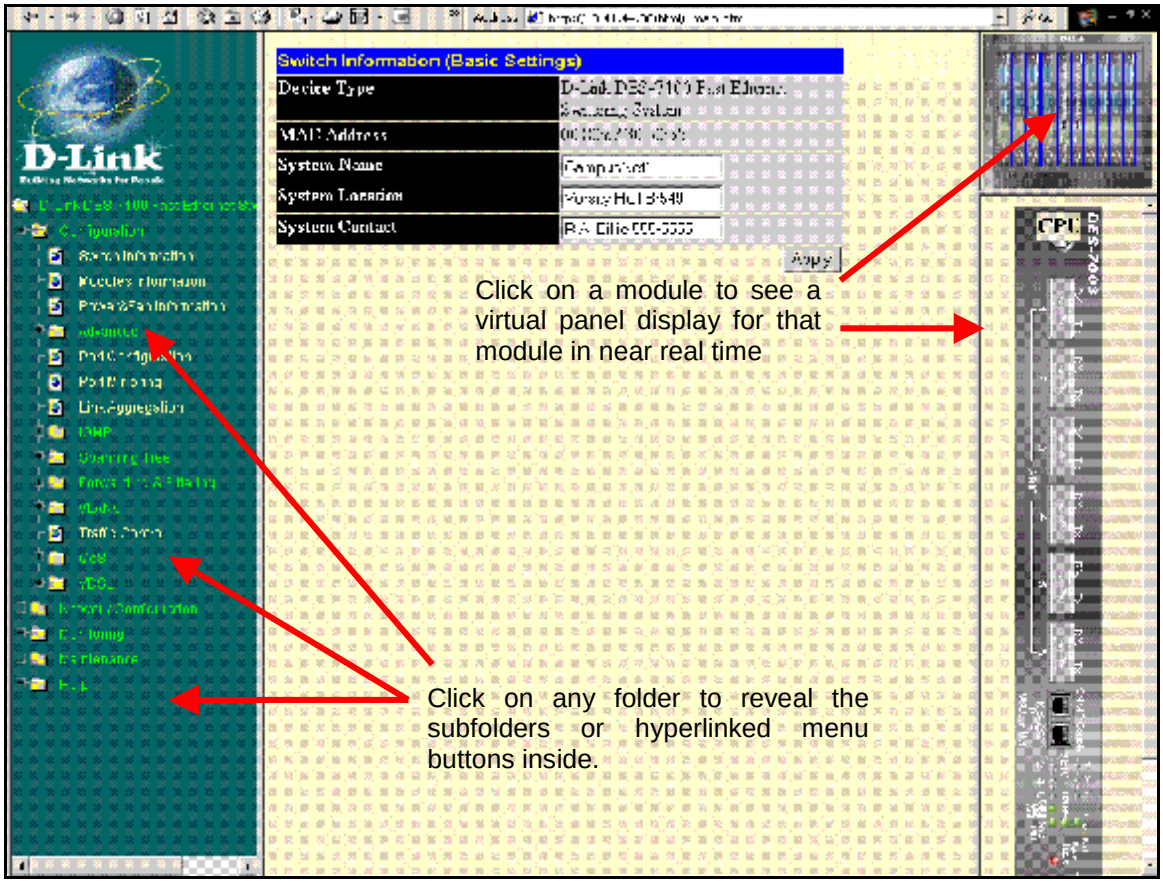


Figure 6- 2. Web Manager Folders and Menus

The various menus available for use in the web manager are organized into four general categories contained in separate folders. The categories (folders) are **Configuration**, **Network Configuration**, **Monitoring** and **Maintenance**. This chapter is organized in the same fashion as the menus in the web manager and presented in the same order.

Commonly Used Buttons

The following buttons are used throughout the web management application on the various menus.

Add	Used to create a new set of parameters for the function or application. For most menus this will bring up a new menu used for configuration.
Modify	Used to change an exiting set of parameters. The menu used to changes configuration settings are very similar to the menus used for creating a new set.
✕	Clicking this will delete the previously created configuration set, such as a VLAN or port trunk group.
Apply	Clicking this will apply the settings as they appear in the menu. This does not save the settings however. Configuration settings must be saved using the save function or they will be lost if the system or relevant switch module is rebooted or powered off.

CLI Reference vs. Web Manager

The web-based management menus presented here are organized somewhat differently than in the CLI Reference Manual. The material in this chapter follows roughly the same order that the menu hyperlinks appear in the left side panel of the web interface. For the purpose of cross referencing, many of the sections describing web manager menus also list the corresponding CLI command or commands in their basic form. The CLI cross-references do not contain the entire syntax for the command. Please read the CLI Reference Manual to view the entire syntax for the CLI commands. Since some command groups are very large, only the section of the CLI Reference Manual that is relevant to the material discussed is referenced instead of listing all the relevant commands.

Configuration

Click on the Configuration folder to reveal the menu buttons used for general information and configuration of the Switch. Included in the Configuration folder are the following menus and sub-folders:

- **Switch Information**
- **Modules Information**
- **Power & Fan Information**
- **Advanced Settings**
- **Port Configuration**
- **Port Monitoring**
- **Port Trunking**
- **IGMP Snooping**

Switch Information

The first page you see when you successfully login displays the System Information menu.

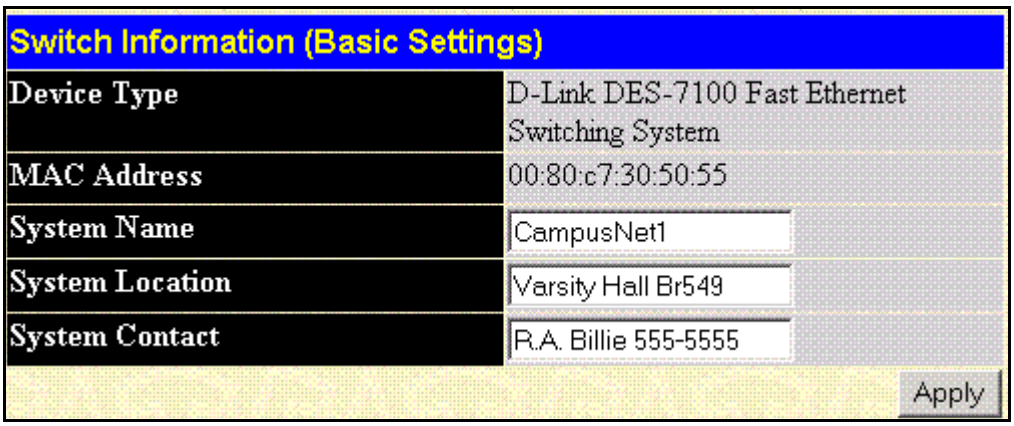


Figure 6- 3. First Menu – Switch Information - Basic

The first window to appear after logging in displays the **System Information (Basic Settings)** menu. The System Information displays general information about the Switch including its MAC Address.

You can also enter a **System Name**, **System Location**, and the name and telephone number of the administrator in the **System Contact**. It is recommended that the person responsible for the maintenance of the network system be listed here. Click on the *Apply* button to make the changes effective.

To view this information using Telnet use CLI command **`show switch`**. To change the name, contact and location information use the CLI commands **`config snmp system_name`**, **`config snmp system_contact`** and **`config snmp system_location`**.

Modules Information

To view this information using Telnet use CLI command **`show unit_information`**.

The Modules Information table lists read-only information about any installed modules.

Modules Information

Slot	UNIT Type	Boot PROM Version	Firmware Version	Hardware Revision
L2				
L3	DES7010 VDSL	0.00.005	0.00.032	0
L4	DES7010 VDSL	0.00.005	0.00.032	0
L5	DES7010 VDSL	0.00.005	0.00.032	0
L6	DES7010 VDSL	0.00.005	0.00.032	0
L7	DES7010 VDSL	0.00.005	0.00.032	0
CPU	DES7003 CPU	0.00.002	0.00.032	1
CPU	DES7003 CPU	0.00.002	0.00.032	1
L8				
L9				
L10				
L11				
L12				

Figure 6- 4. Modules Information

Information about the installed modules includes the type of module, the boot PROM version, the firmware version number and the hardware revision designation. The modules are listed according to the slot name. Slots L7 and L8 are reserved for the primary CPU management module and the optional redundant management module.

Advanced Settings

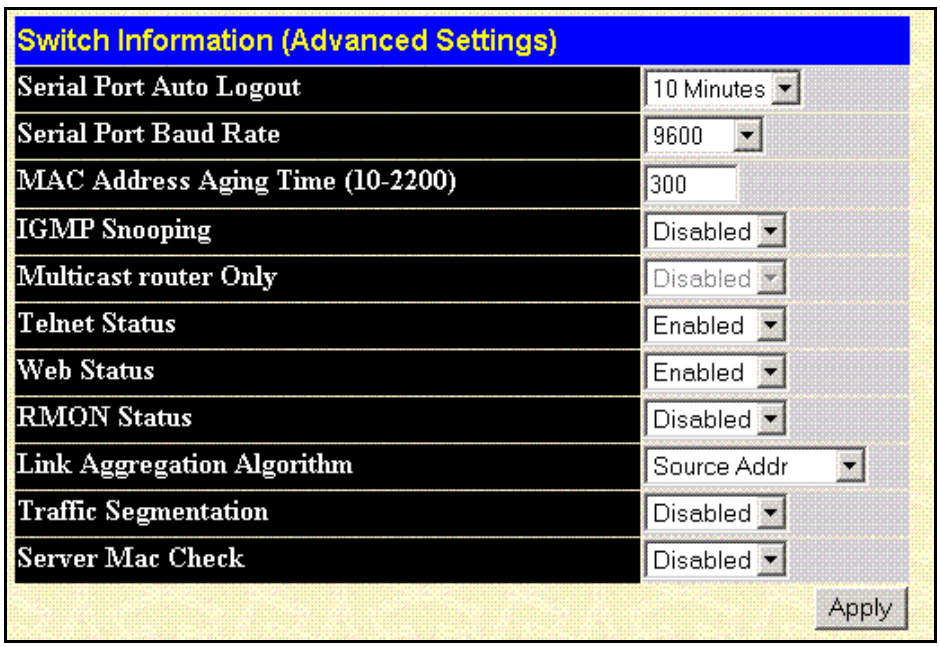


Figure 6- 5. Switch Information – Advanced Settings

The Advanced Settings menu options are summarized in the table below.

Variables in the Advanced Settings menu of the Web Manager and their corresponding CLI command groups are the following:

Serial Port Auto Logout To configure the serial console port auto logout using Telnet use CLI command **config serial_port auto_logout**.	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: *2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes* or *Never.*
Serial Port Baud Rate To configure the serial console port baud rate using Telnet use CLI command **config serial_port baud_rate**.	Select the baud rate used for the console interface. This automatically logs the user out after an idle period of time as defined. Choose from the following options: *9600, 19200, 38400* or *115200*.
MAC Address Aging Time To configure the MAC address aging using Telnet use CLI command **config fdb aging_time**.	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The default age-out time for the Switch is 300 seconds. To change this, type in a different value representing the MAC address age-out time in seconds. The Aging Time can be set to any value between 10 and 2200 seconds.
IGMP Snooping To enable IGMP snooping switch-wide using Telnet use CLI command **enable igmp_snooping**.	To enable system-wide IGMP Snooping capability select *Enabled*. IGMP snooping is *Disabled* by default. Enabling IGMP snooping allows you to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the IGMP Snooping Settings menu (see page 60).
Multicast Router Only To enable Telnet use CLI command **forward_mcrouter_only**.	If this option is enabled and IGMP Snooping is also enabled, the switch forwards all multicast traffic to a multicast-enabled router only. Otherwise, the switch will forward all multicast traffic to any IP router.
Telnet Status Telnet status is configured with CLI commands **enable/disable telnet**.	Telnet configuration is *Enabled* by default. If you do not want to allow configuration of the system through Telnet choose *Disabled*.
Web Status Web-based management is configured with CLI commands **enable/disable web**.	Web-based management is *Enabled* by default. If you choose to disable this by selecting *Disabled*, you will lose the ability to configure the system through the web interface as soon as these settings are applied.
RMON Status RMON status is configured with CLI commands **enable/disable rmon**.	Remote monitoring (RMON) of the switch is *Enabled* or *Disabled* here.
Link Aggregation Algorithm To change the link aggregation algorithm using Telnet use CLI command **config link_aggregation algorithm**.	The algorithm that the switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose *Source Address, Destination Address* or *Both.* (See Link Aggregation)

Management Port Configuration

The DES-7003 CPU module has an RJ-45 UTP Ethernet port on the front panel labeled *Mgmt* that can be used for in-band configuration of the Switch. Use this port to access the management software of the Primary Master CPU blade. Use Telnet or the Web management software just as if you were accessing the Switch through the network. Enter the Switch IP address, user name and password in the same way. This may be a more convenient way to connect to the CPU for some users and it can be used if there are problems on the network that are blocking a connection.

> ***Note:*** *Normally the Management Port is not used for ordinary network data traffic. The exception to this may be if the Switch is configured to receive IP settings assignments from a server via BOOTP or DHCP. In this case, the Management Port should be connected directly to a server, preferably one that is configured to provide only DHCP or BOOTP service. Connecting a DCHP or BOOTP enabled router or Layer 3 switch to the Management Port will allow ordinary network traffic through the port. If this is unavoidable, consider assigning the IP settings manually and configure the network DHCP or BOOTP server to account for the manual assignment.*

The CLI command **`config mgmt_port`** is used for management port configuration.

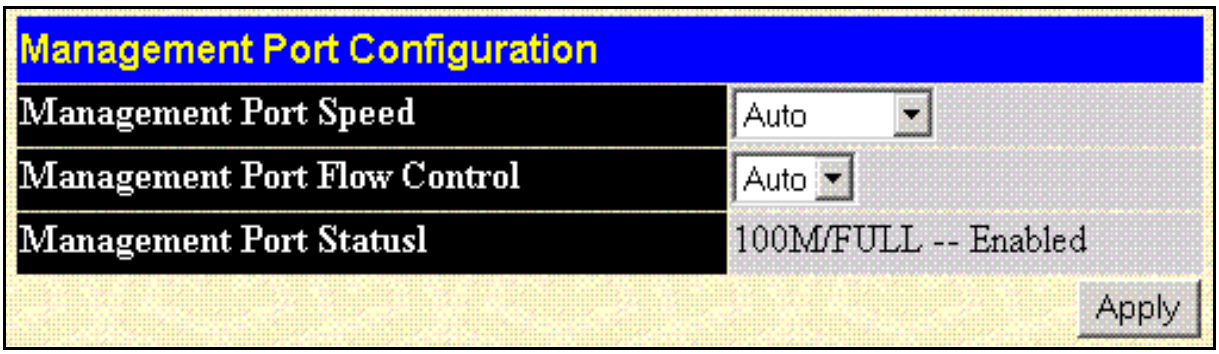


Figure 6- 6. Management Port Configuration

Mgmt Port Speed	Select *Auto* for Auto-negotiation. Or select *100M/Full* for port operation at 100 Mbps and full duplex. Select *100M/Half* for port operation at 100 Mbps and half duplex. Select *10M/Full* for port operation at 10 Mbps and full duplex. Select *10M/Half* for port operation at 10 Mbps and half duplex.
Mgmt Port Flow Control	Selecting *Enabled* in full-duplex mode will implement IEEE 802.3x flow control. Selecting *Enabled* when the port is in half duplex mode will implement normal Ethernet collision-based backpressure flow control. Select *Disabled* for no flow control. When port speed is configured for *Auto* flow control will also be *Auto* and may not be changed.
Mgmt Port Status	Displays the Speed/Duplex and Flow Control status of the Mgmt port.

Port Configuration

The statuses of the module ports are summarized in the Port Information Table. Use the configuration menus at the top of the menu to configure ports individually or a selected range of ports. The example Port Configuration menu pictured below shows the default port settings for the DES-7010 VDSL module.

The options available for port configuration vary according to the type of module in the slot. This is the main difference between the modules, in almost every other respect, ports on the different module types can be thought of as standard ports on a Layer 2 Ethernet switch.

The differences between the module types as far as port configuration is concerned is summarized below:

Type	DES-7003	DES-7005	DES-7006	DES-7010
Speed	Uplink ports for Optical Gigabit Ethernet operate at 1000 Mbps in full duplex only.	10 or 100 Mbps	100 Mbps only	Adjustable for upstream and downstream speed customization
Duplex		Full or Half	Full only	N/A
Flow Control	Enable or Disable per port	Enable or Disable per port	Enable or Disable per port	N/A
Learning	Enabled on all ports.	Enable or Disable per port	Enable or Disable per port	Enable or Disable per port
State	Enable or Disable per port	Enable or Disable per port	Enable or Disable per port	Enable or Disable per port

Unlike standard Ethernet ports, VDSL ports allow customization of upstream and downstream data rates. See the table below for a description. The Rate Adaptive feature for VDSL ports is enabled (or disabled) in a separate menu (see VDSL Port Rate Adaptive section on page 75)

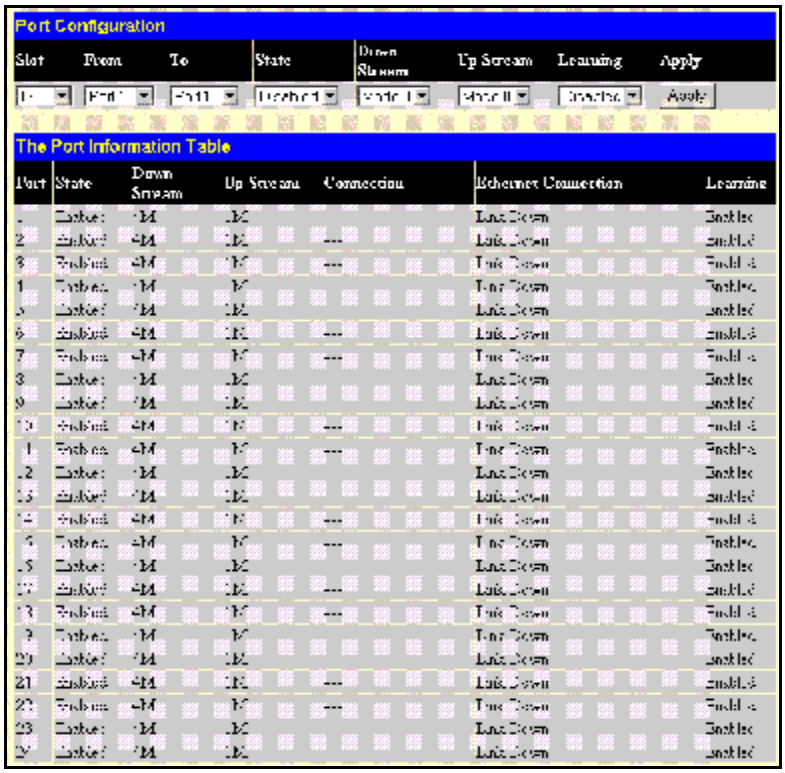


Figure 6- 7. Port Configuration – DES-7010 VDSL Module

To configure port settings for any module, first select the **Slot** from the drop-down menu, then which ports are to be configured in the **From** and **To** drop-down menus. See the table below for a summary of the management options for the available switch modules.

Each port or range of ports can be configured for the following parameters in the Port Configuration menu:

State (all ports on DES-7005, DES-7006 and DES-7010 modules)	Enable or disable the port or ports. If you choose *Disabled* in the **State** field, devices connected to that port cannot use the Switch, and the Switch purges their addresses from its address table after the MAC address aging time elapses.
Speed/Duplex (all ports on DES-7005 module; DES-7006 ports operate at 100 Mbps and full duplex only)	Select *Auto* for Auto-negotiation. This allows the port to select the best transmission speed and duplex mode based on the capabilities of the device at the other end. Select *100M/Full* for port operation at 100 Mbps and full duplex. Select *100M/Half* for port operation at 100 Mbps and half duplex. Select *10M/Full* for port operation at 10 Mbps and full duplex. Select *10M/Half* for port operation at 10 Mbps and half duplex.
Flow Control (all ports on DES-7005 and DES-7006 modules)	Selecting *Enabled* in full-duplex mode will implement IEEE 802.3x flow control. Selecting *Enabled* when the port is in half duplex mode will implement normal Ethernet collision-based backpressure flow control. Select *Disabled* for no flow control.
Learning (all ports on DES-7005, DES-7006 and DES-7010 modules)	Enable or disable learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When learning is *Disabled*, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section titled Forwarding and Filtering on page 65 for information on entering MAC addresses into the forwarding table.
Downstream (all ports on DES-7010 module)	Choose the downstream (Tx) speed for the port (s). To select the port downstream speed in Mbps, choose *Mode 0, 512K, 1M, 2M, 3M, 4M, 5M, 8M, 10M, 15M* from the drop-down menu. The default downstream port speed is *Mode 0.* Mode 0 is the default setting for VDSL ports. It specifies a downstream speed of 4 Mbps.
Upstream (all ports on DES-7010 module)	Choose the upstream (Rx) speed for the port (s). To select the port downstream speed in Mbps, choose *Mode 0, 512K, 1M, 2M, 3M, 4M, 5M, 8M, 10M, 15M* from the drop-down menu. The default downstream port speed is *Mode 0.* Mode 0 is the default setting for VDSL ports. It specifies an upstream speed of 1 Mbps and downstream speed of 4 Mbps.
Rate Adaptive (all ports on DES-7010 module)	The VDSL Rate Adaptive feature automatically senses line condition and adjusts download and upload speeds if a set rate cannot be maintained. The default setting will set speed to *Mode 0* when a rate can no longer be supported. *Optimum* setting sets speed to Mode 0 but then tests raise the download and upload speed incrementally to achieve the best performance level. This function is configured per port using a separate menu in the web manager (see page 75).

The CLI command set **`config ports`** is used for port configuration of ports on the DES-7005 and DES-7006 switch modules. For configuration of VDSL ports on the DES-7010 switch module use the CLI command set **`config vdsl_ports`**.

Uplink Port Configuration

Use the Port Configuration menu to configure settings for the six GBIC ports on the DES-7003 CPU module. It is important to keep in mind that the device connected to the GBIC ports must have compatible speed/duplex and Flow Control settings. Optical fiber connections must operate at 1000 Mbps at full duplex.

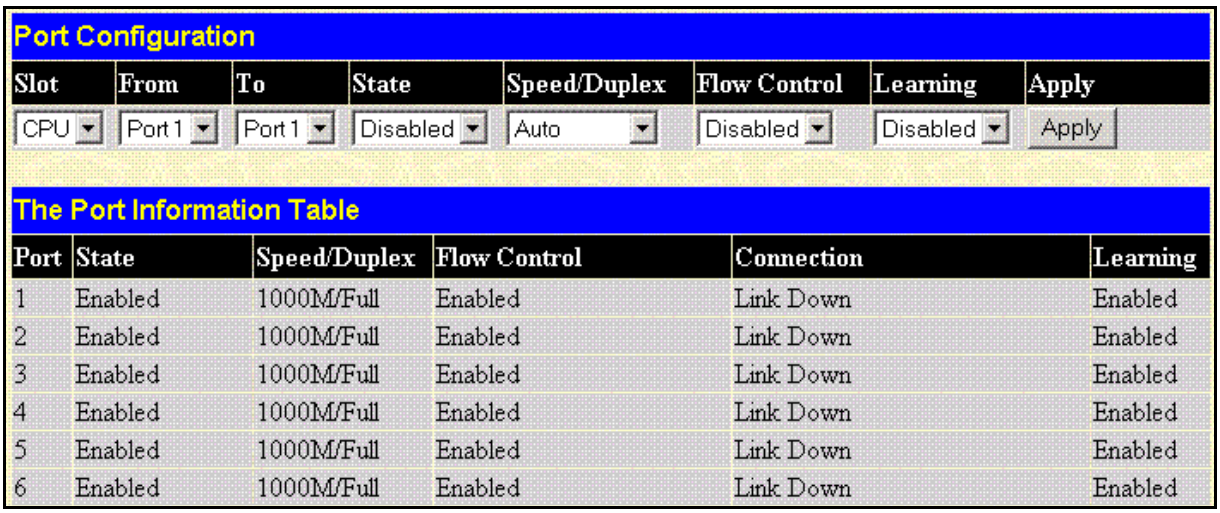


Figure 6- 8. Port Configuration – GBIC Uplink Ports on the DES-7003 CPU module

State	Enable or disable the port or ports. If you choose *Disabled* in the **State** field, devices connected to that port cannot use the Switch, and the Switch purges their addresses from its address table after the MAC address aging time elapses.
Speed/Duplex	GBIC ports supports two speed/duplex modes, *1000M/Full* and *Auto* to support auto-negotiation when connected a device that also supports auto-negotiation. Optical Gigabit Ethernet operates at 1000 Mbps in full duplex only.
Flow Control	Selecting *Enabled* in full-duplex mode will implement IEEE 802.3x flow control when connected to a system that supports IEEE 802.3x.
Learning	Enable or disable learning for the selected ports. When *Enabled*, destination and source MAC addresses are automatically listed in the forwarding table. When learning is *Disabled*, MAC addresses must be manually entered into the forwarding table.

Port Mirroring

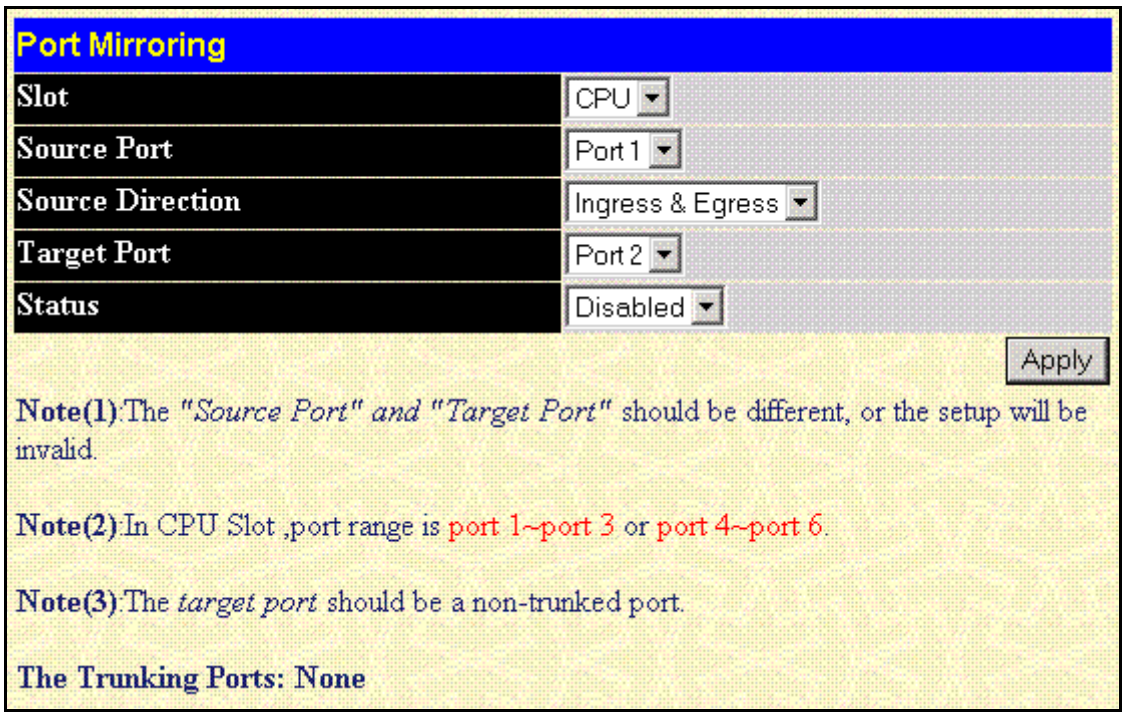


Figure 6- 9. Port Mirroring window

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port.

To configure a mirror port, first select the **Source Port** from where you want to copy frames and the **Target Port**, which receives the copies from the source port. This is the port where you will connect a monitoring/troubleshooting device such as a sniffer or an RMON probe. Next, select the **Source Direction**, *Ingress*, *Egress*, or *Ingress & Egress* and change the *Status* drop-down menu to *Enabled*. Finally, click **Apply** to let the changes take effect.

Relevant CLI command sets for port mirroring are **`config mirror`** and **`enable/disable mirror`**.

Note: *You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunk group. Please note a target port and a source port cannot be the same port.*

Link Aggregation

Link Aggregation allows multiple ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation or port trunking is most commonly used to link a bandwidth intensive network device or devices – such as a server – to the backbone of a network.

Up to 8 links (ports) may form a single trunk group on a switch module and no more than two trunk groups are allowed per module. Each trunk group must reside entirely on a single module. The CPU module allows creation of one or two port trunk groups of up to 3 GBIC uplink ports. Port trunk groups are numbered consecutively. Any member port can be designated as the master of the group. All configuration options – including the VLAN configuration – that can be applied to the master port are applied to the entire trunk group.

Load balancing is automatically applied to the ports in the trunked group and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a trunked port group as a single link, on the switch level. On the port level, the STP will use the port parameters of the master port in the calculation of port cost and in determining the state of the port trunk group. If two redundant trunked groups are configured on the switch, STP will block one entire group – in the same way STP will block a single port that has a redundant link.

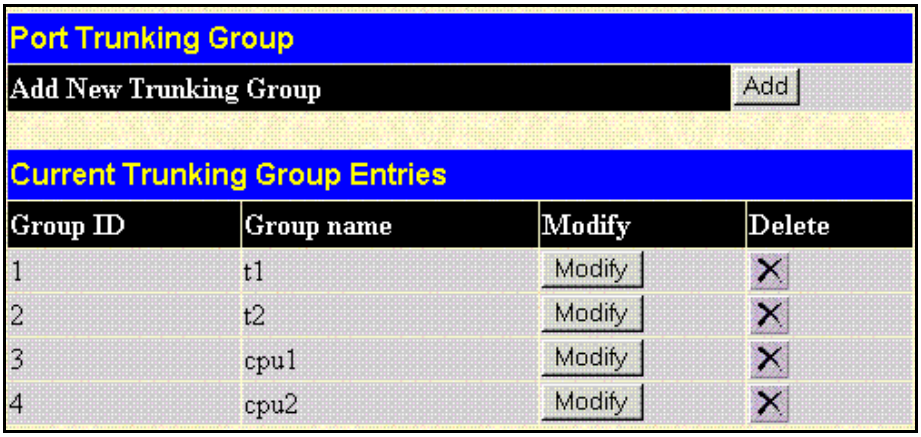


Figure 6- 10. Port Trunking Group Entry Table

To configure port trunk groups, click the Add button to add a new trunk group and use the menu Port Trunking Configuration menu (see example below) to set up trunk groups. To change or delete a port trunk group, click the Modify or Delete option in the Current Trunk Group Entries Table.

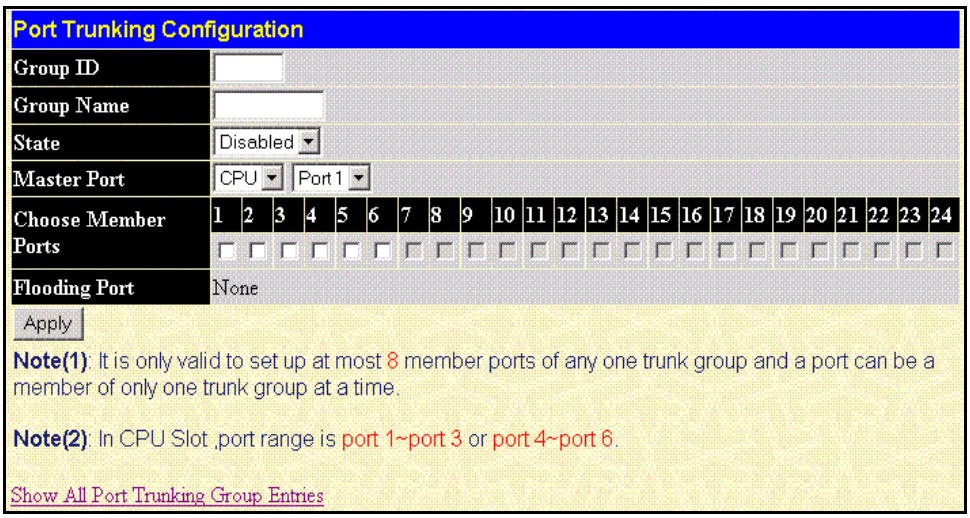


Figure 6- 11. Port Trunking Configuration – Add Menu

The user-changeable parameters in the Switch are as follows:

Select Slot Number	Choose the slot on which you wish to set up a trunk group. Trunk groups must be confined to ports on a single module.
Select Group ID	Select an ID number for the group.
Group Name	Type in a name for the group (optional).
State	Trunk groups can be toggled between *Enabled* and *Disabled*. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Port Member	Choose the members of the trunked group. Up to 8 ports per group can be assigned to a group.

Relevant CLI command sets for link aggregation are **`create/delete link_aggregation`** and **`config link_aggregation`**.

IGMP Snooping Settings

In order to use IGMP Snooping it must first be enabled for the entire Switch (see Advanced Settings on page 52). You may then fine tune the settings for each VLAN using the IGMP Snooping Settings menu. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues multicasts when there are no longer hosts requesting that they continue.

Use the IGMP Snooping Group Entry Table to view IGMP Snooping status. To modify settings, click the Modify button for the VLAN ID you want to change.

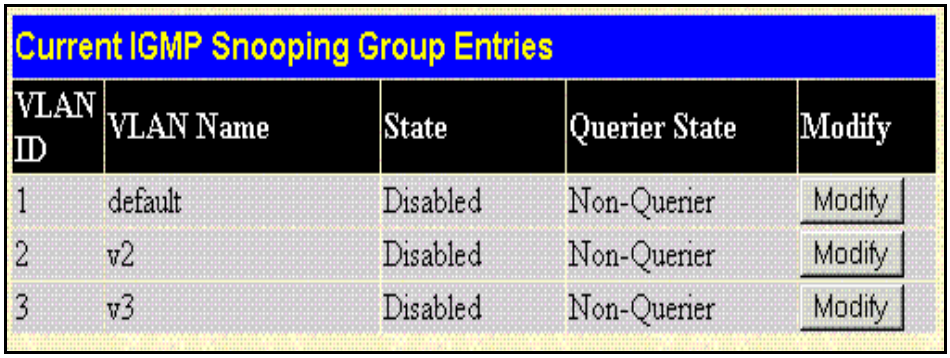


Figure 6- 12. IGMP Snooping Entry Table

Clicking the Modify button will bring up the IGMP Snooping Settings menu.

See IGMP Snooping on page 46 for a description of the protocol.

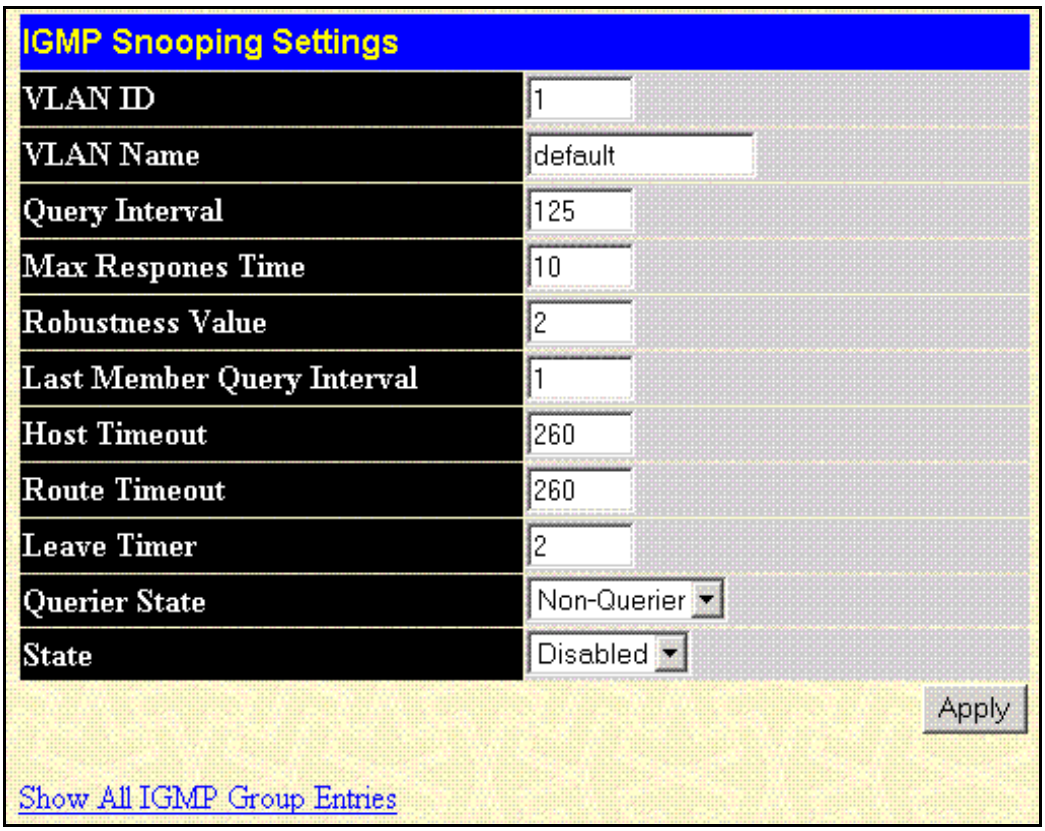


Figure 6- 13. IGMP Snooping Settings Screen

The user-changeable parameters for IGMP Snooping are listed here along with their CLI command strings.

Query Interval **config igmp_snooping querier <vlan_name>/all query_interval <sec>**	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 9,999 seconds are allowed. Default = 125.
Max Response Time **config igmp_snooping querier <vlan_name>/all max_response_time <sec>**	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Variable **config igmp_snooping <vlan_name>/all robustness_variable <value>**	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 2 to 255. Default = 2.
Last Member Query Interval **config igmp_snooping <vlan_name>/all last_member_query_interval <sec>**	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1.
Host Timeout **config igmp_snooping <vlan_name>/all host_timeout <sec>**	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260.
Route Timeout **config igmp_snooping <vlan_name>/all router_timeout <sec>**	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260.
Leave Timer **config igmp_snooping <vlan_name>/all leave_timer <sec>**	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted.
Querier State **config igmp_snooping querier <vlan_name>/all state [enabled/disabled]**	Choose *Querier* to enable transmitting IGMP Query packets or *Non-Querier* to disable. The default value is *Non-Querier*.
State **config igmp_snooping <vlan_name>/all state [enabled/disabled]**	Select *Enabled* to implement IGMP Snooping. This is *Disabled* by default.

Static Router Ports

A static router port is a port through which a connection to a multicast-enabled router has been established. Typically a designated static router port or group of ports is connected directly to such a router. This option is generally used with legacy routers that are not able to generate host membership queries. Use of a static router port means the Switch will forward all packets sent through the port(s) with the multicast-enabled router as the destination. Furthermore the static router port will receive all multicast data for all VLANs.

The Static Router Port Entry hyperlink first presents the Static Router Ports Entry Table.

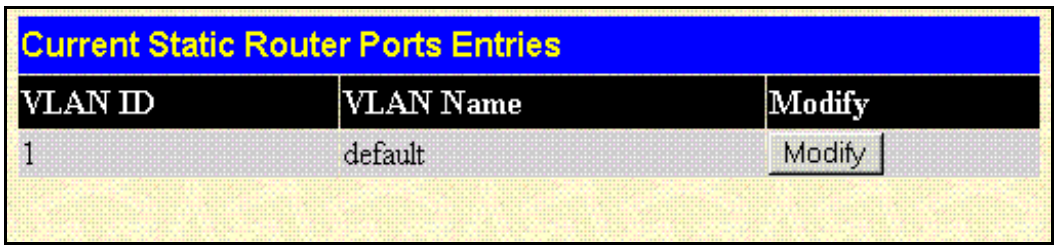


Figure 6- 14. Static Router Ports Entry Table

To designate a new static router port or to change an existing one, click the Modify button for the corresponding VLAN ID number. The Static Router Ports Settings menu appears.

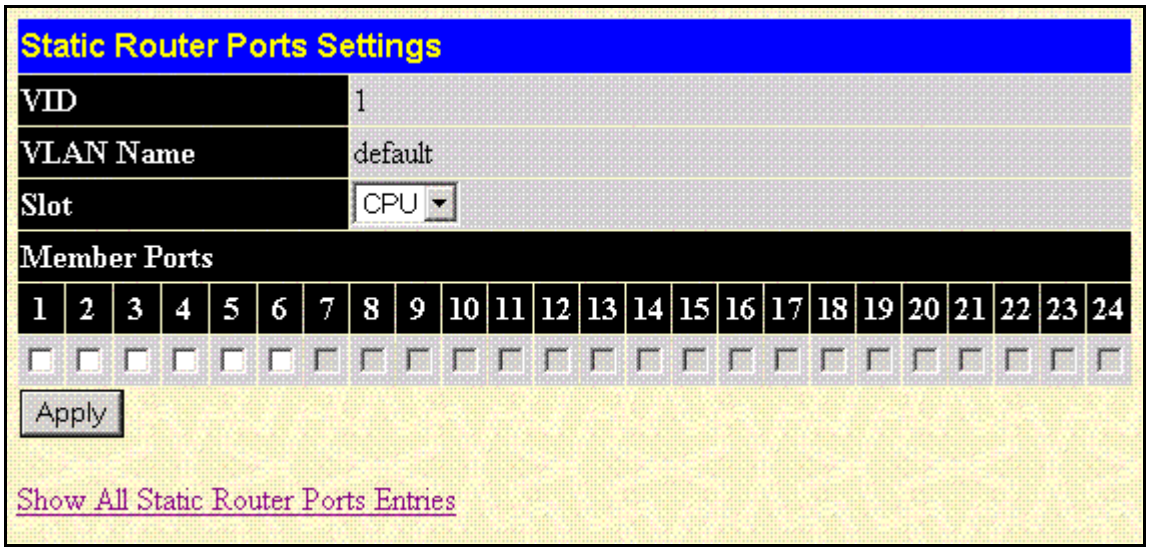


Figure 6- 15. Set Static Router Ports

VID	The VLAN ID number in which the static router port(s) reside.
VLAN Name	The name, if any, given to the VLAN.
Slot	Select the module by name where the static router port(s) are being set up.
Member Ports	Check the port or ports that will be designated as static router ports

Relevant CLI command set for multicast static router ports is **`config router_ports`** (see also **`enable_snooping forward_mcrouter_only`**).

Spanning Tree Protocol Configuration

Spanning Tree Protocol as defined by IEEE 802.1D is disabled by default on the Switch. This is to allow the Switch to progress through the learning more quickly when it is first connected to the network. Use the STP Switch Settings menu to enable and adjust STP settings for Switch. To disable STP for individual ports, use the Port Spanning Tree menu.

STP Switch Settings

The following figures and tables describe the configuration of the Spanning Tree Protocol (STP) on the switch, system-wide. STP must be enabled system-wide in order to effectively enable or disable it on a per port basis (see next section).

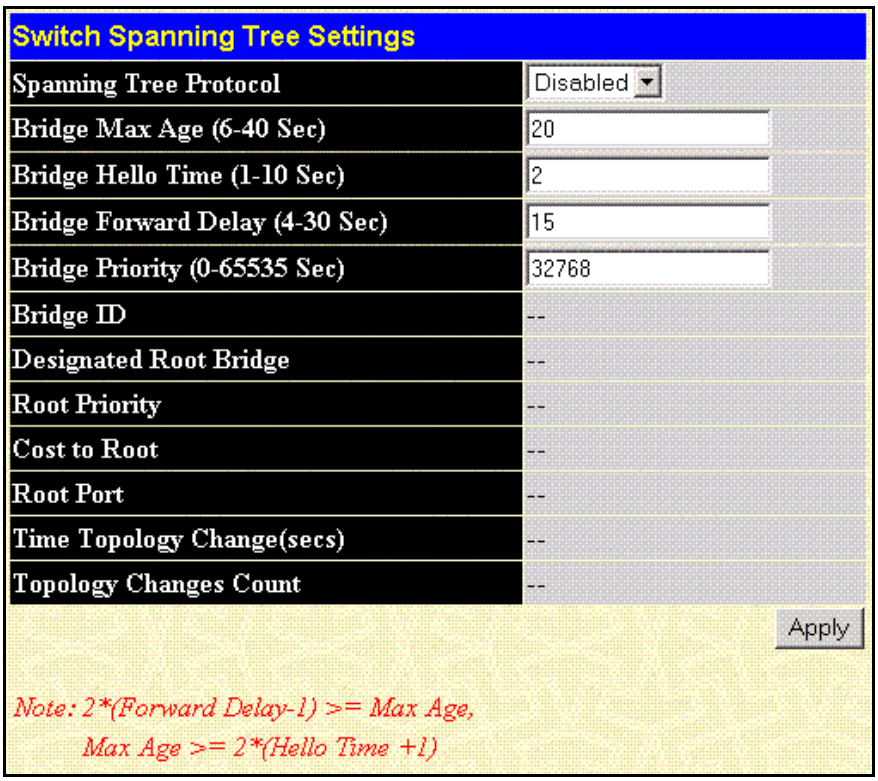


Figure 6- 16. STP Switch Settings Menu

Set the parameters listed below in the STP Switch Settings menu.

Spanning Tree Protocol	Allows the STP to be globally *Enabled* or *Disabled* on the switch. Default = *Disabled*.
Bridge Max Age (6-40 Sec)	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Bridge Hello Time +1)]. The maximum value is the lower of 40 or [2 x (Bridge Forward Delay –1)]. Default = 20 Default = 20
Bridge Hello Time (1-10 Sec)	The time interval (in seconds) at which the root device transmits a configuration message. Default = 2

Switch Spanning Tree Settings continued from previous page	
Bridge Forward Delay (4-30 Sec)	The maximum time (in seconds) the root device will wait before changing states (i.e., from the listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward packets. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. Maximum value is 30 Minimum value is the higher of 4 or [(Max. Age / 2) +1] Default = 15
Bridge Priority (0-65535 Sec)	Device priority used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. The lower the numeric value, the higher the priority. If all devices have the same priority, the device with the lowest MAC address will become the root device. Range 0 to 65535. Default = 32,768

The relevant CLI commands for system-wide STP are **`config stp`**, **`show stp`** and **`enable`**/**`disable stp`**.

Port Spanning Tree

On some networks it may be desirable to disable STP for an individual port. For example, if there is only a single workstation connected to the port or in circumstances where a private client network may be renting a single port, these are circumstances where there is no chance that a redundant loop will exist. STP can be disabled for the port to conserve bandwidth and CPU function, but more importantly to avoid the possible delay of critical frames or packets that could potentially be blocked by STP.

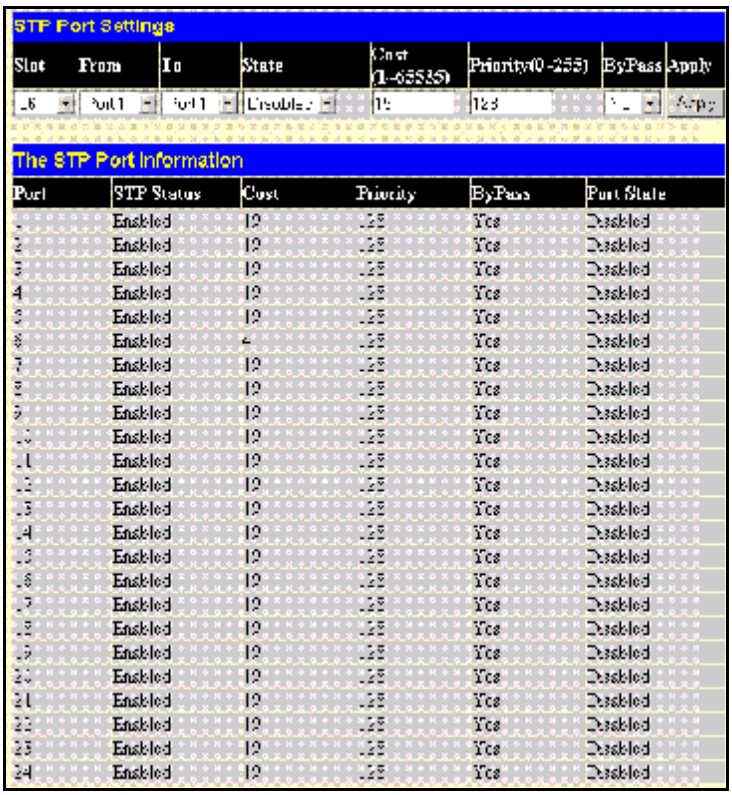


Figure 6- 17. Spanning Tree Port Settings

To configure Port Group STP for any module, first select the **Slot** from the drop-down menu, then choose which ports are to be configured in the **From** and **To** drop-down menus.

The Port Group STP parameters that can be configured are:

State	The STP State for the port or port group can be *Disabled* or *Enabled.* The default setting STP State is *Enabled*.
Port Cost	A Port Cost can be set from 1 to 65535. The lower the number, the greater the probability the port will be chosen to forward packets.
Priority	A Port Priority can be from 0 to 255. The lower the number, the greater the probability the port will be chosen as the Root Port.
By Pass	If you select *No* the forward delay timer is set to zero thus bypassing the waiting time before the listening state. Default settings is *Yes*.

The relevant CLI commands for Port Group STP are **`config stp_ports`** and **`show stp_ports`**.

Forwarding and Filtering

Use these menus to setup Multicast and Unicast forwarding and MAC Address filtering.

For relevant forwarding and filtering CLI commands please read the section titled **Layer 2 FDB Commands** in the CLI Reference Manual.

To configure the MAC address aging time used for the forwarding table, see Advanced Settings (page 52) for web-based configuration or use the CLI command **`config fdb aging_time`**.

Static Unicast Forwarding

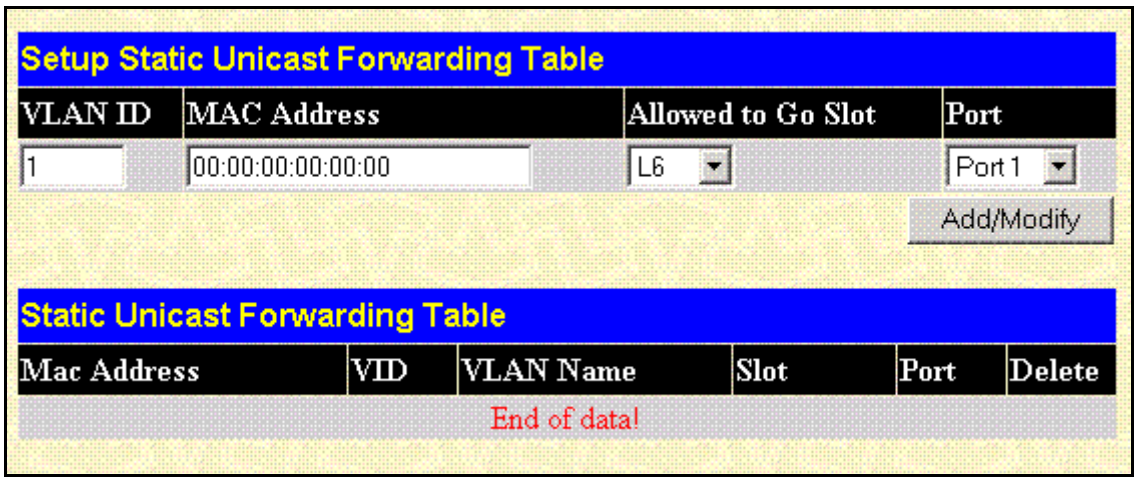


Figure 6- 18. Static Unicast Forwarding Setup

To add an entry, define the following parameters in the **Add an Entry** field:

VLAN ID	The VLAN ID number of the VLAN to which the above MAC address belongs.
MAC Address	The MAC address to which packets will be statically forwarded.
Allowed to Go to Slot	Allows the designation of the module on which the above MAC address resides.
Port	Choose the port where the MAC address resides. Selecting Port 0 means no ports are allowed.

The corresponding CLI commands for the Static Unicast Forwarding menu are **`create fdb`**, **`delete fdb`**, **`clear fdb`** and **`show fdb`**.

Static Multicast Forwarding

The following figure and table describe how to set up Multicast forwarding on the switch. Open the Multicasting folder and click on the 802.1Q Multicast Forwarding button to see the entry screen below:

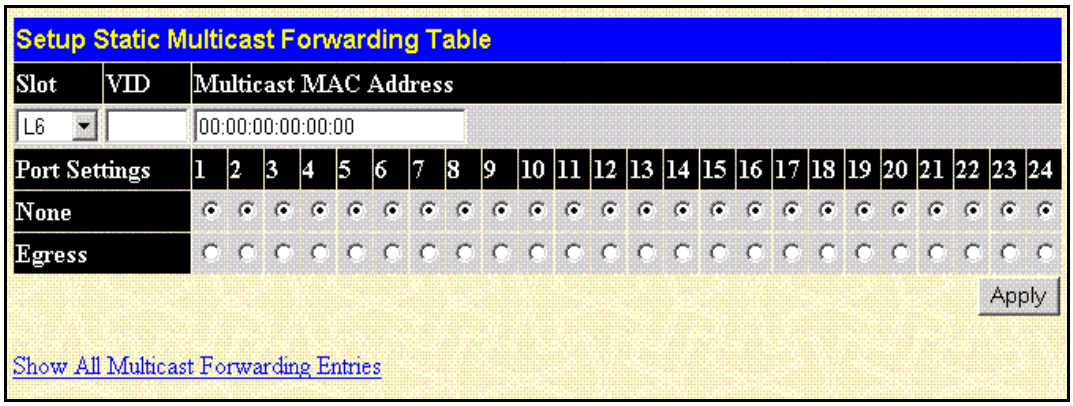


Figure 6- 19. Setup Static Multicast Forwarding Table

Use the Multicast Forwarding Screen to define the following parameters:

MAC Address	The MAC address of the static source of multicast packets.
VID	The VLAN ID of the VLAN the above MAC address belongs to.
Port Settings	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are; None – no restrictions on the port dynamically joining the multicast group, None is chosen, then an end station attached to the port can join the multicast group using GMRP. Egress – the port is a static member of the multicast group.

The corresponding CLI commands for the Multicast Forwarding menu are **`create multicast fdb`**, **`config multicast_fdb`** and **`show multicast_fdb`**.

Static MAC Address Filtering

Filtering based on MAC address is implemented globally for all ports.

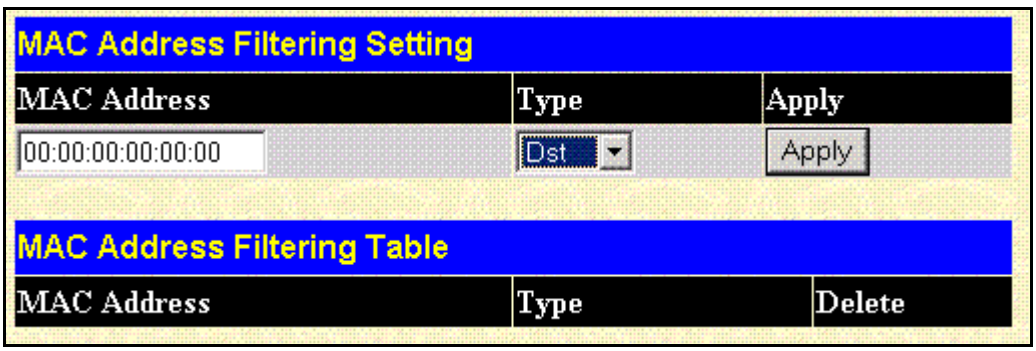


Figure 6- 20. MAC Address Filter Setup

Enter the unicast MAC address in the **MAC Address** field, and specify the **Type** from the drop-down menu, choose *Dst* - Destination, *Src* - Source, or *Either* for a source or destination of packets. Specifying a MAC address entry in the filtering table as a Destination will filter packets with this MAC address as their destination. Source will filter packets with this MAC address as their source, and Either will filter packets with this MAC address as either their source or destination.

The CLI commands used for MAC filtering are **`create fdbfilter`**, **`delete fdbfilter`** and **`show fdbfilter`**.

VLANs

Configure 802.1Q Static VLANs

The following figures and tables describe how to set up 802.1Q VLANs on the switch.

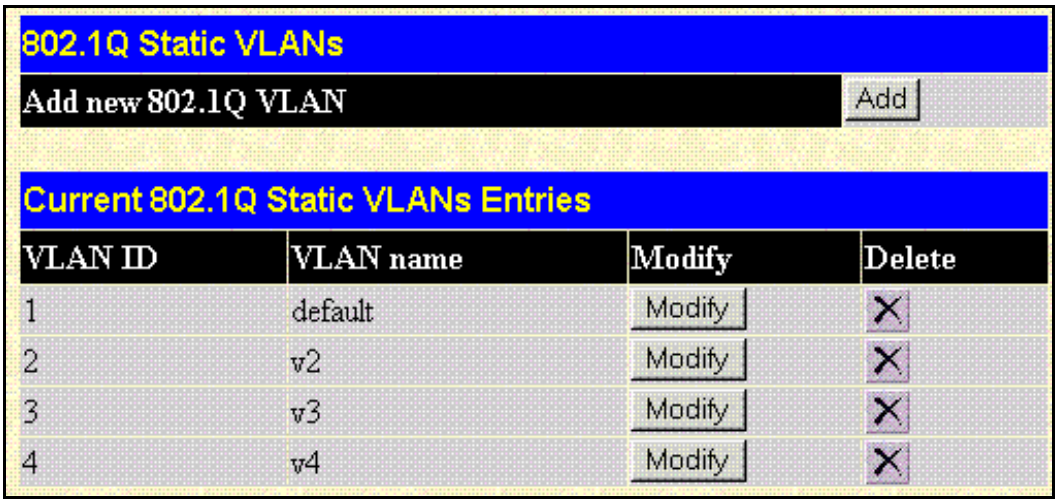


Figure 6- 21. 802.1Q Static VLANs Screen

The Static VLANs menu lists existing VLANs by their VLAN ID (VID) and by name. To create a new VLAN, click on the *New* button in the header row of the table. To edit an existing VLAN, click on the *Modify* button of the VLAN you want to edit. To eliminate an entire VLAN, click on the "*X*" button for the VLAN you wish to delete.

The user configurable settings are the same when you Add or Modify a VLAN. Read the next section for a description of these settings.

The CLI command to delete an existing VLAN is **`delete vlan`**. To view existing VLANs use the **`show vlan`** command.

Add a Static 802.1Q VLAN

The following figure and table describe the parameters that must be configured to add an 802.1Q VLAN on the switch. Click the Show All Static VLAN Entries hyperlink to return to the Current VLAN Entries table.

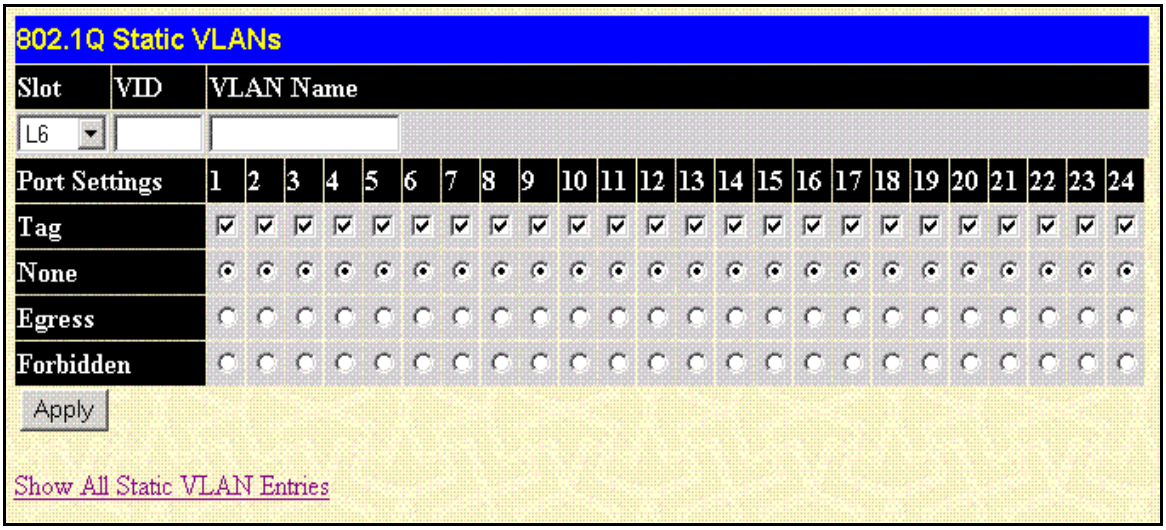


Figure 6- 22. 802.1Q Static VLANs Entry Settings – Add Screen

VLAN ID (VID)	The VLAN ID of the VLAN that is being created.
VLAN Name	The name of the VLAN that is being created.
Slot	Choose the module on which you want to define VLANs. A VLAN may exist on multiple modules.
Port	Corresponds to the ports that will be members of the VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
None	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
Egress	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.

The CLI command to add a new VLAN is **`create vlan`**. To select the member ports with CLI use the **`config vlan`** command.

Edit 802.1Q VLANs

The following figure and table describe how to edit an existing 802.1Q VLAN entry on the switch.

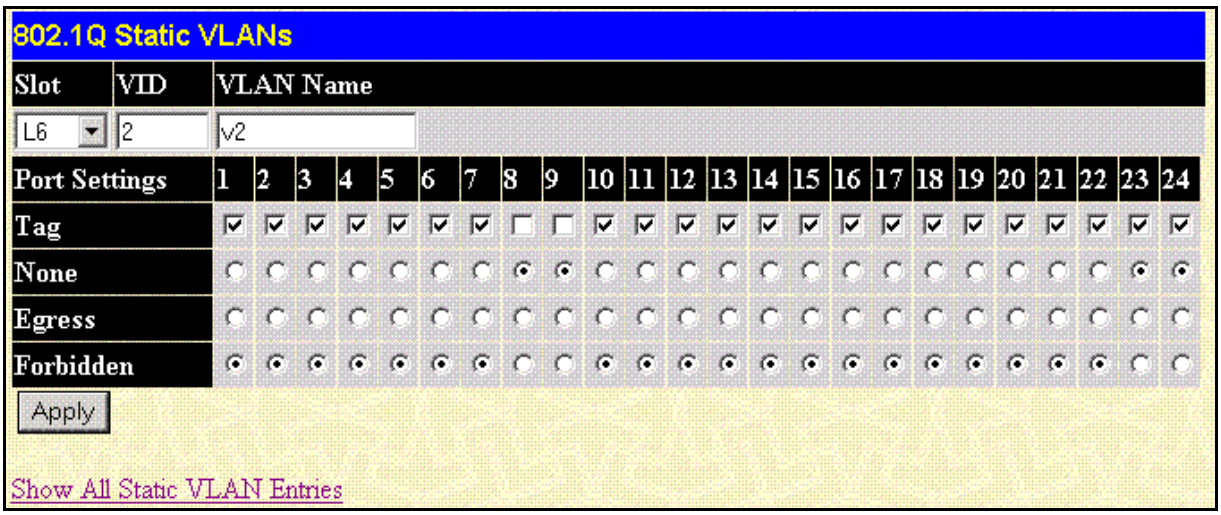


Figure 6- 23. 802.1Q Static VLANs Entry Settings – Edit Screen

The Static VLANs Edit screen presents the current configuration of the VLAN. Use this screen to change settings for the VLAN as described in the table below. Click the Show All Static VLAN Entries hyperlink to return to the Current VLAN Entries table.

VLAN ID (VID)	The VLAN ID of the VLAN to be edited. For editing, VLANs are identified by name.
VLAN Name	The name of the VLAN to be edited.
Slot	Choose the module on which you want to define VLANs. A VLAN may exist on multiple modules.
Port	A list of the ports that are static members of the currently selected VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
None	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
Egress	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.

Click **Apply** to let your changes take effect.

The CLI command to change the configuration of an existing VLAN is **`config vlan`**.

802.1Q Port Settings

Open the 802.1Q Port Settings menu and select the Slot and range of ports to configure. For the selected port or group of ports, choose to enable or disable Ingress checking and establish an acceptable packet rule.

The following figure and table describe how to configure the 802.1Q VLAN port settings for the switch.

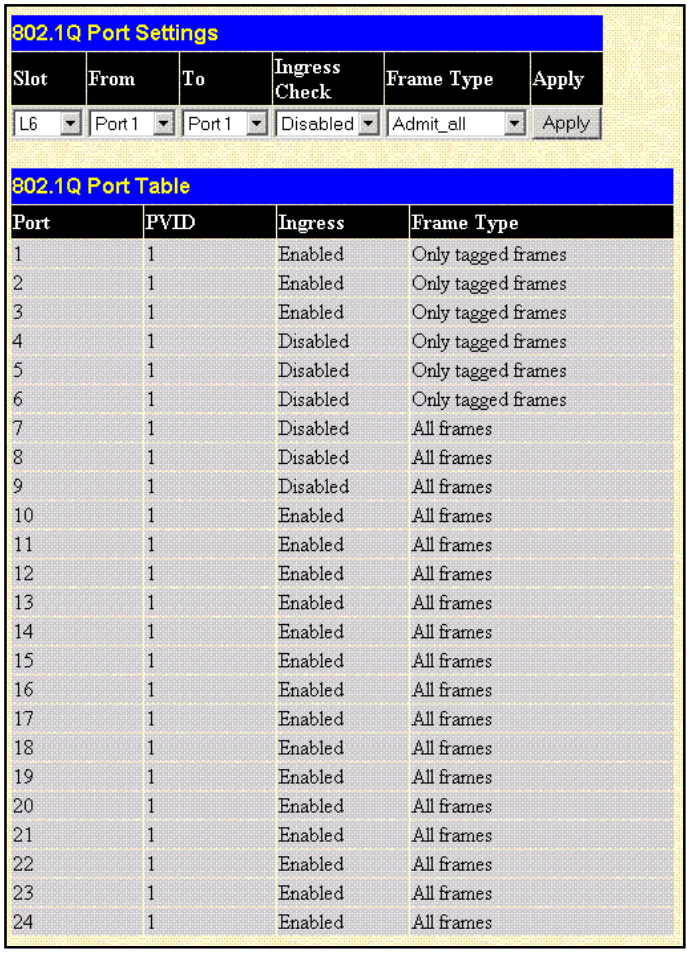


Figure 6- 24. Port VLAN ID (PVID) Screen

PVID	Shows the current PVID assignment for each port. The switch's default is to assign all ports to the Default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames,as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
Ingress Check	Specifies the port to check the VID of incoming packets against its VID or PVID. If the two are equal, the port will receive the packet. It the two are unequal, the port will drop the packet. This is used to limit traffic to a single VLAN.
Frame Type	Select *Admit all* to allow all frame types, tagged or untagged. Select *Tagged only* to allow only tagged frames.

Click **Apply** to let your changes take effect.

The CLI command used to view port VLAN settings is **`show 802.1q port`**. To configure 802.1Q port settings use the command group **config 802.1q port.**

Defined Router

Use this to create a list of servers or routers that are allowed to communicate with other ports on the switch module using VLAN ID and MAC addresses. This will limit communication between ports on a switch module to only specified servers as defined by VLAN and MAC address. This form of traffic segmentation is used for security and efficiency.

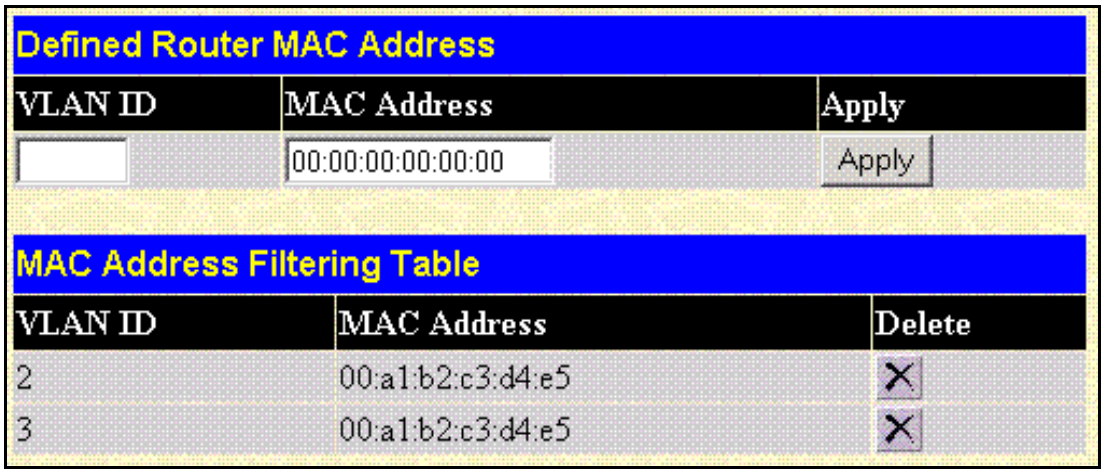


Figure 6- 25. Defined Router MAC Address Entry Table

VLAN ID	Enter the VID in which the router or server resides.
MAC Address	Specify the router or server by typing its MAC address.

The relevant CLI information can be found in the CLI Reference manual in the section titled Traffic Segmentation. The commands used to designate a router or server for communication between segmented ports are **`config server-mac-list`**, **`enable server-mac-check`** and **`disable server-mac-check`**.

Traffic Control (Broadcast/Multicast Storm Control)

Use the Traffic Control Setting menu to enable or disable storm control and adjust the threshold for multicast and broadcast storms, as well as DLF (Destination Look Up Failure). Traffic control settings are applied to individual Switch modules.

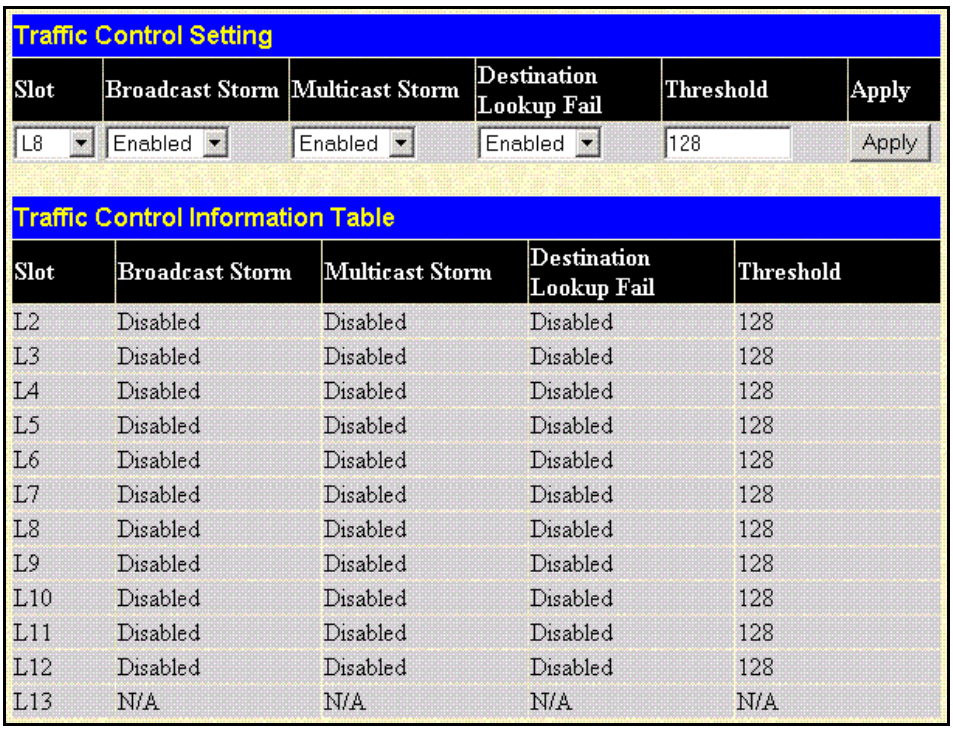


Figure 6- 26. Traffic Control Settings

Traffic or storm control is used to stop broadcast, multicast or ARP request storms that may result when a loop is created. The Destination Look Up Failure control is a method of shutting down a loop when a storm is formed because a MAC address cannot be located in the Switch's forwarding database and it must send a packet to all ports or all ports on a VLAN.

To configure Traffic Control, select the **Slot** you want to configure. **Broadcast Storm**, **Multicast Storm** and **Destination Look Up Failure** may be *Enabled* or *Disabled*. The **Threshold** value is the upper threshold at which the specified traffic control is switched on. This is the number of Broadcast, Multicast or DLF packets, in Kbps, received by the switch that will trigger the storm traffic control measures. The Threshold value can be set from 0 to 255 packets. The Default setting is 128.

To configure these settings using CLI, use the command group **`config traffic control`**. To view the Traffic Control status of the Switch modules use the CLI command **`show traffic control`**.

Quality of Service (QoS)

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. The IEEE 802.1p Priority specification uses 8 priority levels to classify data packets. In 802.1p compliant devices, a tag inserted into the packet header is used to identify the priority level of data packets.

The Switch implements 802.1p priority using 4 hardware queues instead of 8. Therefore the Switch must have a means of mapping the 8 levels specified in the IEEE 802.1p standard to the 4 hardware queues used in the Switch. This is done using the Class of Service menu explained below. Further customization of priority classification can be done with the Output Scheduling menu, also explained below.

Individual ports may still be assigned priority using the 8 levels as defined by the 802.1p standard.

It is important to note that changes in a networks QoS scheme should be carefully considered, planned for and if possible tested for efficiency. When set up properly, it QoS can allow efficient and timely delivery of data for video conferencing or IP telephony without causing unacceptable delays of other network traffic. If QoS is not well set up however, significant delays and excessive packet loss may result for data assigned to lower priority queues.

Port Priority

This window allows you to set a default 802.1p priority to each port on the switch for packets that have not already been assigned a priority value. The default priority is applied to packets transmitted and received that do not have a priority tag already.

The 802.1p priority queues are numbered from 0 – the highest priority – to 7 – the lowest priority. If you change the default priority settings so that ports do not have a uniform default priority, the highest priority 0 should be reserved only for video conferencing or similar applications that cannot tolerate latency. A port given a default priority of 0 should be used only for such purposes; for example, one port might be dedicated for IP telephony services or video conferencing applications and not used for anything else.

To configure Port Default Priority for any module, first select the **Slot** from the drop-down menu, then choose which ports are to be configured in the **From** and **To** drop-down menus. Choose the level of **Priority** level for the port; select 0 – 7.

Click **Apply** to let your changes take effect.

The relevant CLI commands for default 802.1p Priority assignment are **`config 802.1p default_priority`** and **`show 802.1p default_priority`**.

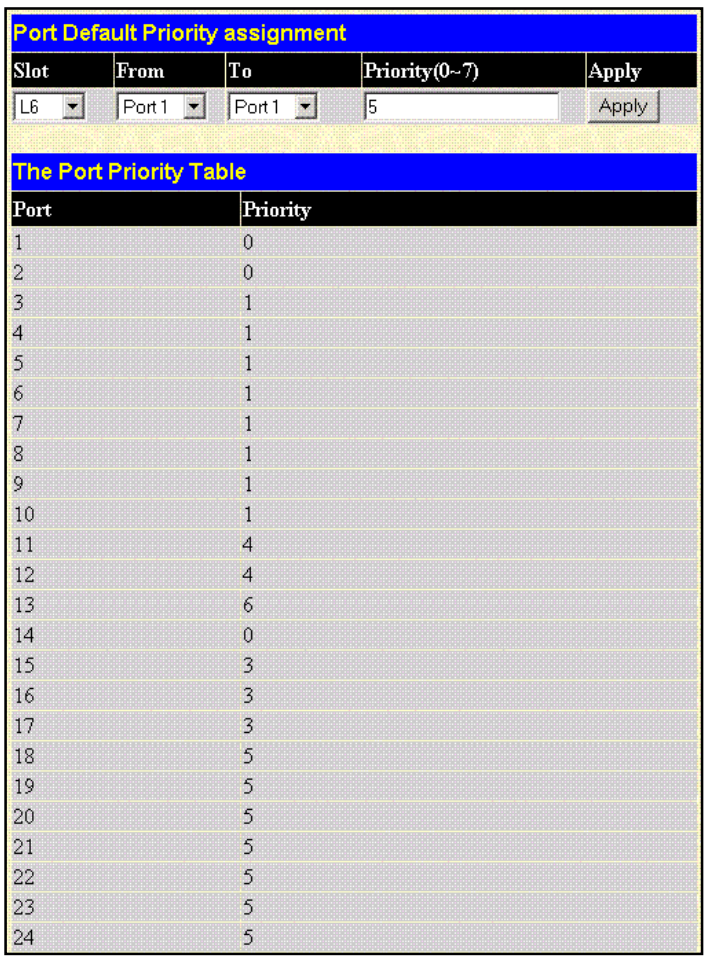


Figure 6- 27. Port Default Priority

Traffic Class Configuration

The Traffic Class Configuration menu is used to map incoming packets with 802.1p priority tags to one of the 4 hardware queues used on the Switch.

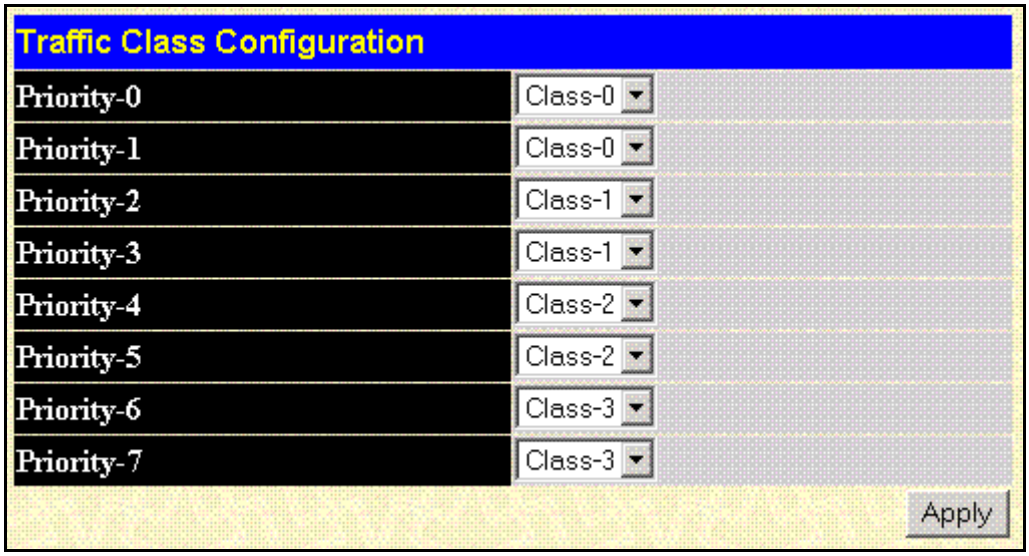


Figure 6- 28. Traffic Class Configuration window

This window allows you to configure traffic class priority by specifying the class value, from 0 to 3, of the Switch's eight levels of priority.

Click **Apply** to let your changes take effect.

Traffic class configuration uses the CLI command **`config 802.1p user_priority`**. To view the existing configuration use the CLI command **`show 802.1p user_priority`**.

QoS Output Scheduling Configuration

QoS can be customized by changing the output scheduling used for the hardware queues in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues are affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If you choose to customize this setting, it is important to monitor network performance, especially during peak demand as bottlenecks can quickly develop if the QoS settings are not suitable.

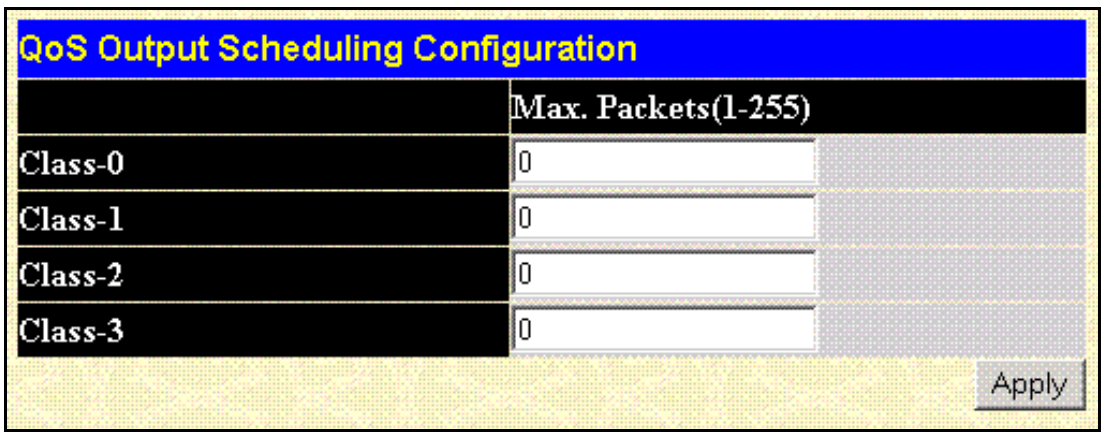


Figure 6- 29. QoS Output Scheduling Configuring

The MAX. Packets field specifies the number of packets that a queue will transmit before surrendering the transmit buffer to the next lower priority queue in a round-robin fashion.

Click **Apply** to let your changes take effect.

Use the CLI command **`config scheduling`** for customizing QoS scheduling.

VDSL Configuration and Monitoring

(DES-7010 Modules Only)

For DES-7010 module installations there are four menus available to enable the VDSL Rate Adaptive feature per port, monitor transmission power and perform a loop back test to check end-to-end connectivity. To configure available upstream and downstream bandwidth for individual ports, see the Port Configuration section on page 55.

VDSL Port Rate Adaptive

The VDSL Rate Adaptive function can be enabled or disabled o a per port basis. It is disabled by default on all ports of the DES-7010 VDSL module. When the VDSL rate adaptive mode is enabled, the switch automatically senses line condition and adjusts downstream and upstream speeds if the set rate cannot be maintained.

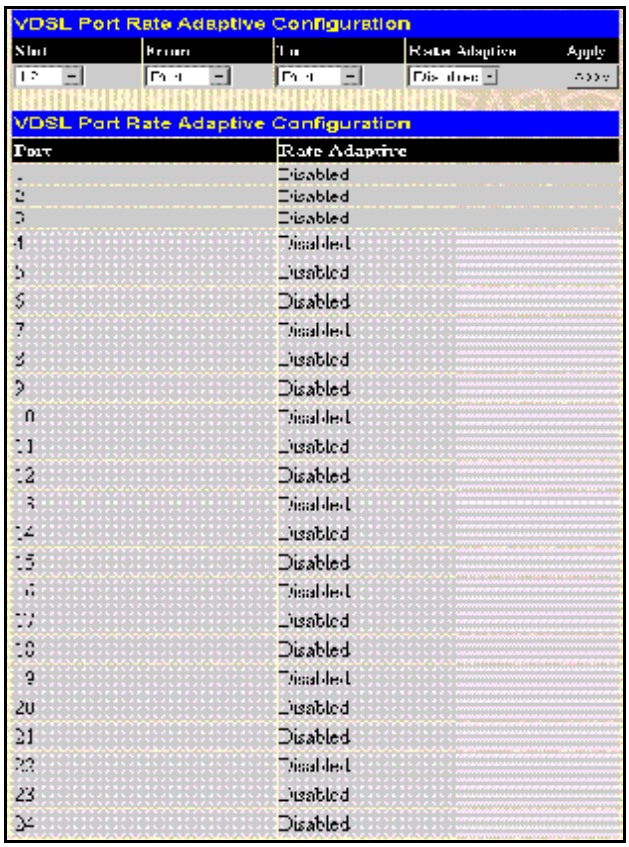


Figure 6- 30. VDSL Port Rate Adaptive Configuration

To configure Port Rate Adaptive for any VDSL module, first select the **Slot** from the drop-down menu, then choose which ports are to be configured in the **From** and **To** drop-down menus. Choose the **Rate Adaptive** mode from the drop-down menu. Choose options *Disabled*, *Default* or *Optimum*.

The setting *Default* will set speed to *Mode 0** when a rate can no longer be supported. The *Optimum* setting will set speed to Mode 0 and test the downstream and upstream speeds. It then raises the speed incrementally to achieve the best performance level.

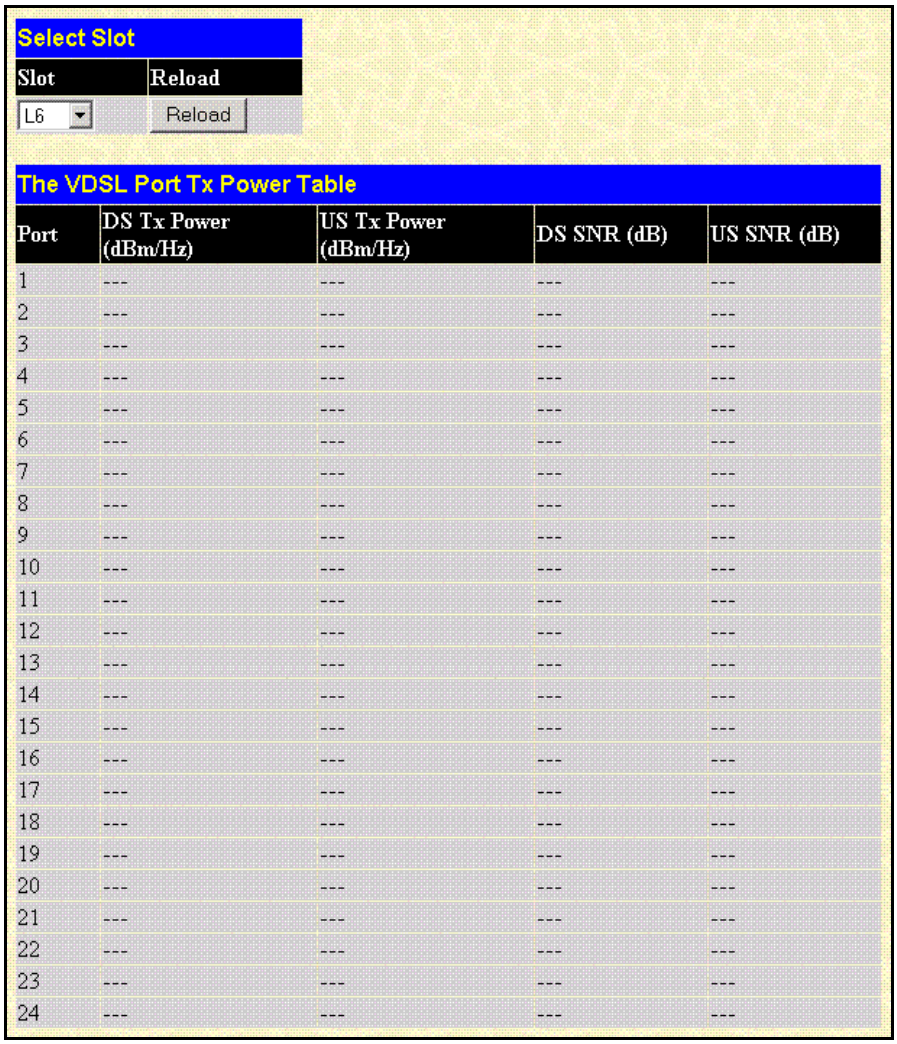
Click **Apply** to let your changes take effect.

You may also use the CLI command **`config vdsl_port rate adaptive mode`** to change this setting.

* Mode 0 is the default setting for VDSL ports. It specifies an upstream speed of 1 Mbps and downstream speed of 4 Mbps. See Port Configuration on page 55 for details on how to manually configure upstream and downstream port speeds on the DES-7010 VDSL Module.

View VDSL Transmission Power and SNR

Use this table to monitor the transmission power and Signal-to-Noise (SNR) ratio for VDSL ports. This is sometime useful for troubleshooting and monitoring VDSL ports. Power levels may be subject to local or regional regulatory restrictions.



Select Slot

Slot	Reload
L6	Reload

The VDSL Port Tx Power Table

Port	DS Tx Power (dBm/Hz)	US Tx Power (dBm/Hz)	DS SNR (dB)	US SNR (dB)
1	---	---	---	---
2	---	---	---	---
3	---	---	---	---
4	---	---	---	---
5	---	---	---	---
6	---	---	---	---
7	---	---	---	---
8	---	---	---	---
9	---	---	---	---
10	---	---	---	---
11	---	---	---	---
12	---	---	---	---
13	---	---	---	---
14	---	---	---	---
15	---	---	---	---
16	---	---	---	---
17	---	---	---	---
18	---	---	---	---
19	---	---	---	---
20	---	---	---	---
21	---	---	---	---
22	---	---	---	---
23	---	---	---	---
24	---	---	---	---

Figure 6- 31. VDSL Port Tx Power Table

DS Tx Power	Downstream Transmission Power dBm/Hz
US Tx Power	Upstream transmission Power dBm/Hz
DS SNR	Downstream Signal to Noise Ratio dB
US SNR	Upstream Signal to Noise Ration dB

VDSL Loopback Test

The loopback test for VDSL ports is used like a Ping test to check connectivity. Connectivity is checked for the Local loop or internal path, that is from the Switch CPU to the to the VDSL chip set for the selected VDSL module. The Line loopback test is used to test connectivity from the VDSL module port to the end user's CPE.

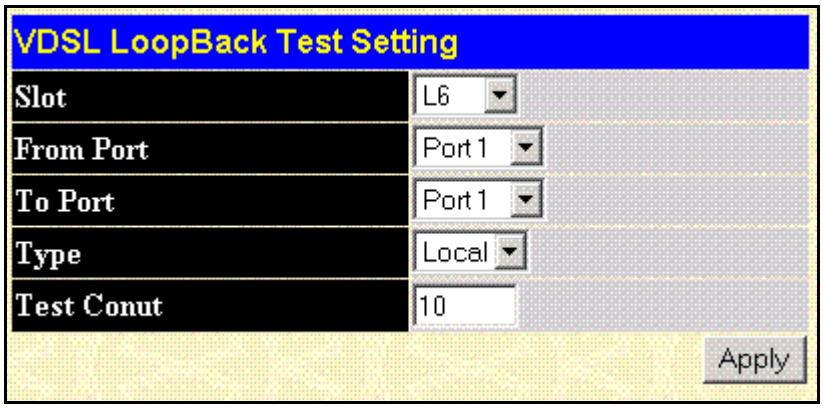


Figure 6- 32. Local Loopback Test Screen

To perform a local loopback test, select the VDSL **Slot** number of the port(s) you want to test.Select the **Type** of test you want to conduct, and type in the number of repetitions for the test. Click **Apply** to initiate the test. A *Local* test tests connectivity from the CPU to the VDSL controller chip on the VDSL module. A *Line* test checks connectivity to the CPE for the port(s). To see the results of a loopback test, click the View LoopBack Test Results button. The corresponding CLI command for this function is **`config vdsl_port_loopback_test`**.

View LoopBack Test Results

The results of the VDSL Loopback test can be viewed for all the ports on a single module. Results are listed for each port. The information includes the **State** of the test, the **Count Fail/Total** ratio of the test packets sent and the **Type** of test.

To view loopback test result with CLI the command is **`show vdsl_loopback_test`**.

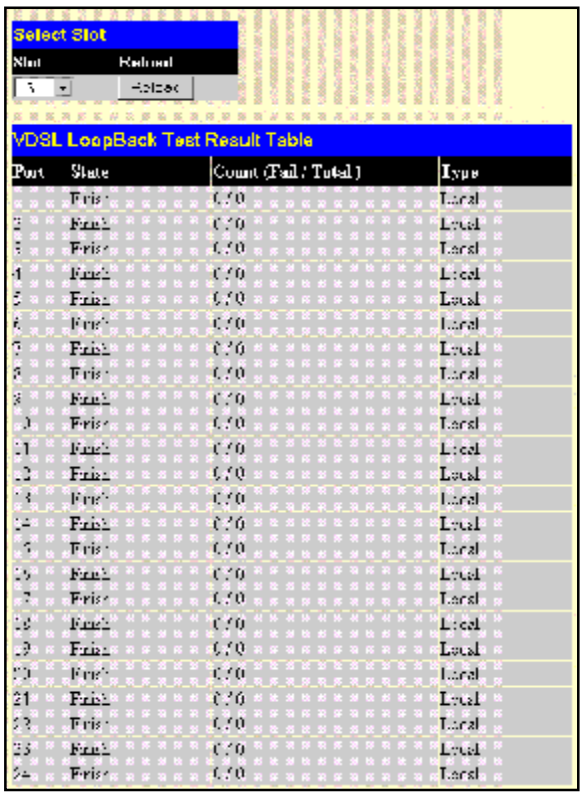


Figure 6- 33. Loopback Test Results Screen

Network Configuration

Network configuration settings include the IP settings for the Switch, SNMP settings, settings up user accounts and configuring system time settings.

IP Address

Use this to view or change Switch IP settings.

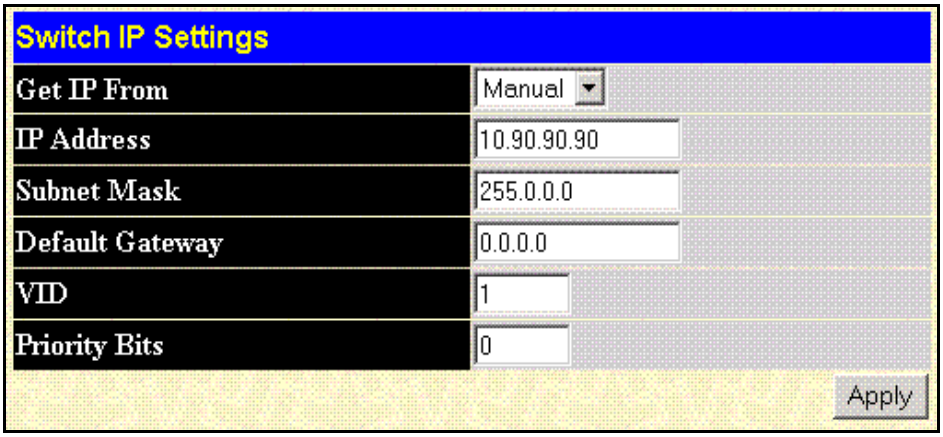


Figure 6- 34. IP Settings Window

In the IP Settings window, read-only information includes the **Switch MAC Address** and the current IP settings (listed under **Current Settings**). Change IP settings under **New Settings**. The CLI command set for Switch IP settings is **`config ip`**.

To change IP settings:

1. Select *Manual*, *BOOTP* or *DHCP* in the **Get IP From** menu.*
2. If you are assigning IP settings manually, type in the IP settings for *IP Address*, *Subnet Mask* and *Default Gateway*.
3. Change the Management VLAN ID number in the **Management VID** box (default Management VID = 1). CLI command = **`config ip vlan`**.
4. Click **Apply** to let your changes take effect.

**** Important Note:*** *The GBIC uplink ports on the DES-7003 CPU module are currently not compatible with BOOOTP and DHCP client modes. The Switch can receive BOOTP or DHCP settings instructions through the Management Port on the Primary Master CPU module. However, since this port is not intended for routine network traffic and should not be used to uplink the Switch to the network, it should be connected directly to a non-networked DHCP or BOOTP server with the function limited to providing service only to the Switch.*

Security IP Address

Use the Security IP Settings screen to choose one to three management stations.

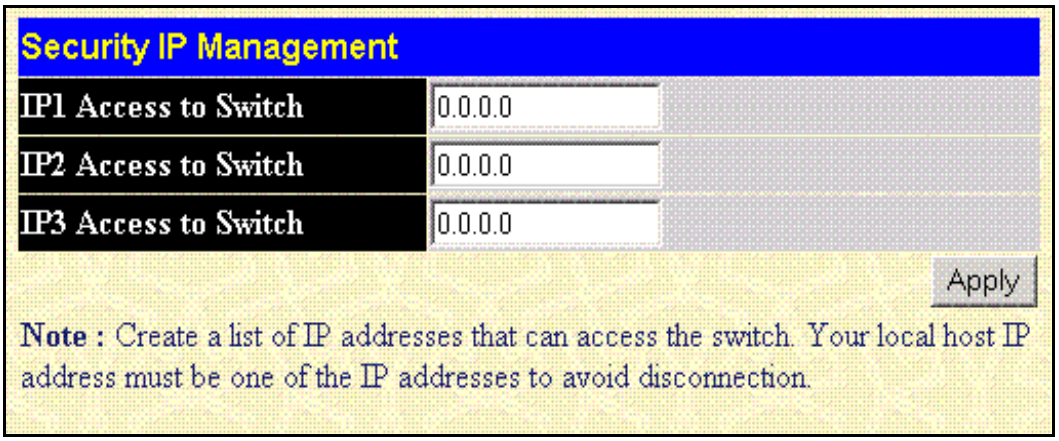


Figure 6- 35. Management Station IP Address Screen

Use the Management Station IP Settings to select up to three management stations used to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address in the area provided and click on the *Apply* button. CLI commands = **`config trusted_host`**, **`delete trusted_host`** and **`show trusted_hosts`**.

Note: *If you are not currently running the web manager from one of the IP addresses defined in the Management Station IP Settings screen, you will lose access to the web manager when you click on Apply.*

SNMP Manager

Use the Community Strings menu to define up to four community strings. Community strings are used to verify who can receive SNMP information from the switch.

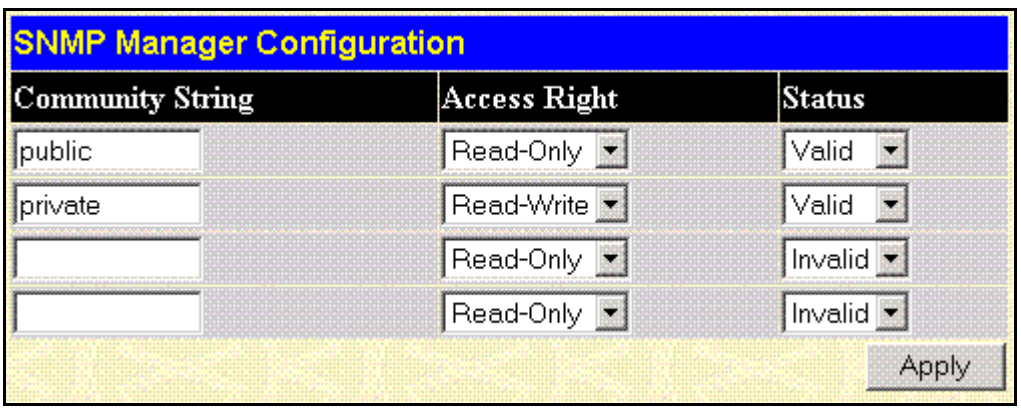


Figure 6- 36. Community Strings Menu

Type in the Community String in any of the four entry fields. Use the drop-down menu to define the Access Right and Status of the corresponding string. For the Access Right, select Read-Write or Read Only. Under Status, choose Valid to enable the string or Invalid to disable it.

The relevant CLI commands for SNMP manager settings are **`create snmp community`**, **`delete snmp community`**, **`config snmp community`** and **`show snmp`**.

Trap Manager

The following menu allows the user to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 4 trap managers may be entered.

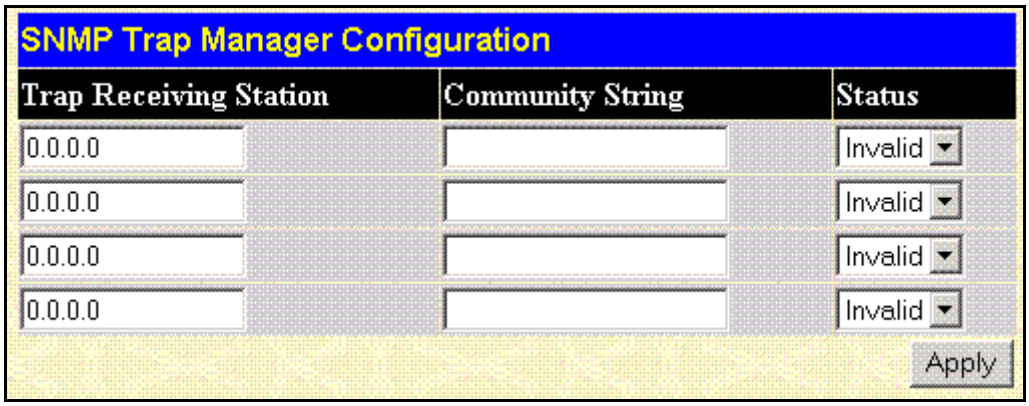


Figure 6- 37. Trap Receivers Menu

To set up trap receivers, define the following:

Trap Receiving Station	Type in the IP address of the trap recipient, i.e. the IP address of the management station that will receive traps generated by the switch.
Community String	Type in a string of up to 20 characters used for authentication of users wanting to receive traps from the switch's SNMP agent.
Status	Choose Valid or Invalid for the string. This is used to temporarily limit the receipt of traps generated by the switch.

The CLI commands used to manage trap receivers are **`create snmp trap_receiver`**, **`config snmp trap_receiver`**, **`delete snmp trap_receiver`**, **`disable snmp traps`** and **`enable snmp traps`**.

Date & Time and SNTP Configuration

System time and date used for the Switch can be adjusted and defined according to time zone and seasonal variations. The Switch may also use SNTP to update date and time information.

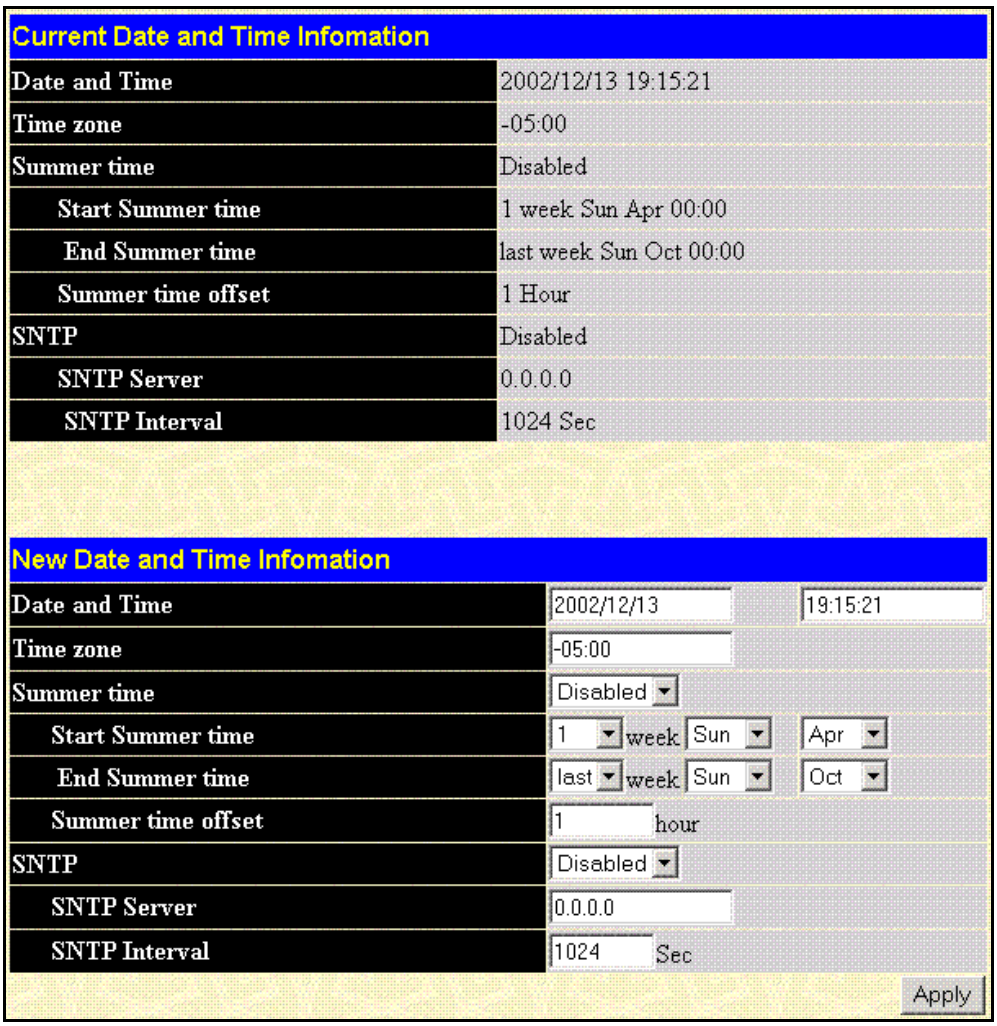


Figure 6- 38. Current Date and Time Information

To configure **Date and Time**, type in the correct date in the form YEAR/MONTH/DAY. Type in the local time in the form HOUR:MINUTE:SECOND.

Time Zone information uses the standard GMT (Greenwich Mean Time) as the reference base. Type in the time zone information in the form +/- HOUR:MINUTE.

Summer Time settings may be *Enabled* or *Disabled* according to local practice. To define the end of Daylight Savings Time (DST) and the beginning of Summer (Standard Time) where applicable, choose the week (1 = 1st week of month, 2 = 2nd week etc.), day of the week and month Standard Time normally begins and DST ends. Likewise define the end of Standard Time (beginning of DST) according to normal local practice. Summer time offset is the number of hours that clocks are adjusted when the seasonal time changes occur.

Date and time settings allow for use of Simple Network Time Protocol (SNTP) or use the internal system clock. To enable NTP service, select *Enabled* from the NTP drop-down menu and type in an IP address of the chosen **SNTP Server**. **SNTP Interval** controls the frequency of NTP updates, that is, the amount of time in seconds between NTP update requests.

Click the **Apply** button to set the system time and date.

The CLI commands work a bit differently for date and time settings on the Switch. Please refer to the CLI Reference Manual in the section on Date and Time for details.

User Accounts

Use the User Accounts Control Table to control user privileges. To view existing account using CLI use the command **show account**.

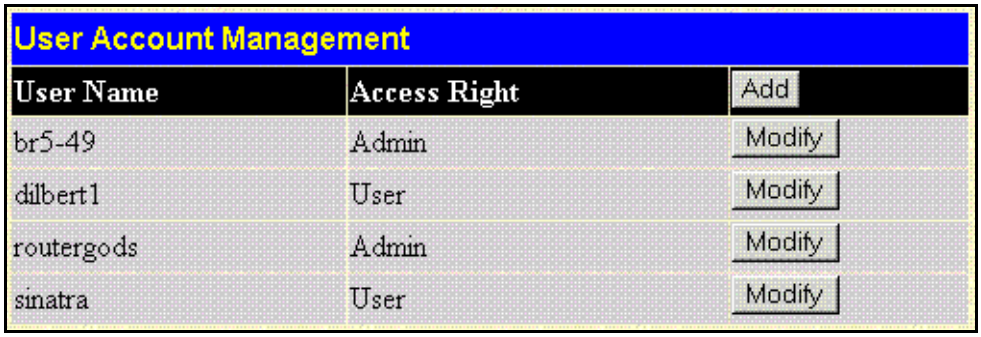


Figure 6- 39. User Accounts Control Table

To add a new user, click on the *Add* button. To modify or delete an existing user, click on the *Modify* button for that user.

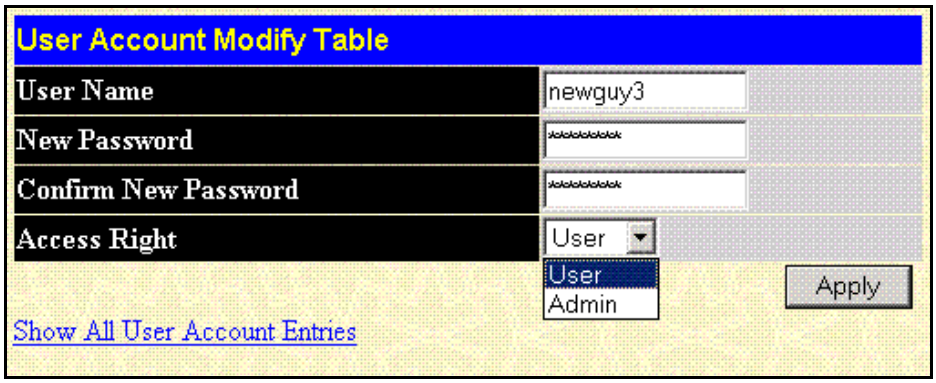


Figure 6- 40. Add User Accounts Control

Add a new user by typing in a **User Name**, and **New Password** and retype the same password in the **Confirm New Password**. Choose the level of privilege (*Admin* or *User*) from the **Access Right** drop-down menu. To add a user account using the CLI commands use **create account** and **config account**.

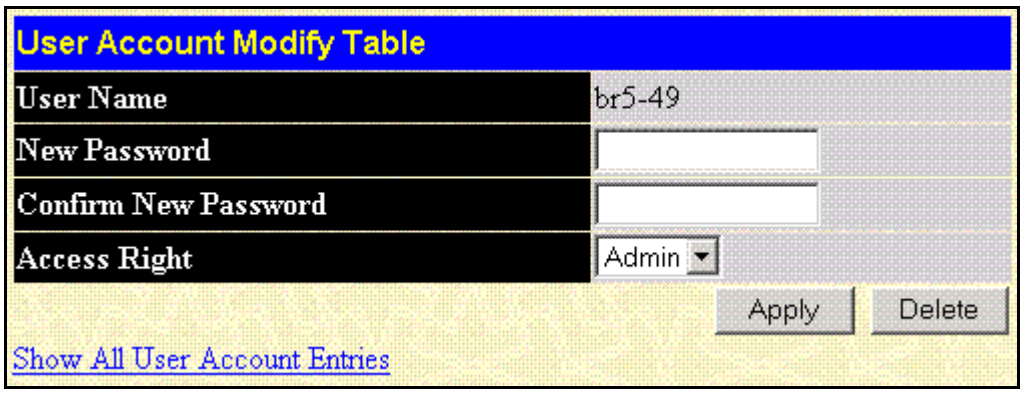


Figure 6- 41. Modify User Accounts

Modify or delete an existing user account in the User Account Control Table – Edit. To delete the user account, click on the *Delete* button. To change the password, type in the **New Password** and retype it in the **Confirm New Password** entry field. Choose the level of privilege (*Admin* or *User*) from the **Access Right** drop-down menu. To delete a user account using CLI use the command **delete account**. To change an existing account use **config account**.

Monitoring

This category includes: Power and Fan Information, Port Utilization, Packets (Received (RX), UMB_cast (RX), and Transmitted (TX)), Errors (Received (RX) and Transmitted (TX)), Size (Received (RX)), MAC Address, IGMP Snooping and Port Access Control, as well as secondary screens.

Power and Fan Information

To view this information using Telnet use CLI command **`show power_fan_information`**.

The Power and Fan Information table lists the current status of all system fans and power modules.

Power Information	
Power Number	**Power Status**
1	Normal
2	Normal
3	Not exist
4	Not exist

Fan Information	
Fan Number	**Fan Status**
1	Normal
2	Normal
3	Normal
4	Normal
5	Abnormal
6	Abnormal
7	Abnormal
8	Abnormal

Figure 6- 42. Power & Fan Information

The Power Information in the top section of the table lists the status of the power supply and redundant power supply. Fan Information displays the status of the 8 system fans numbered as follows: Fans 1-4 are the fans located on the back-plane and Fans 5-8 are located in the slide in fan module of the DES-7000 chassis.

Port Utilization

The Switch can display the utilization percentage of a specified port in the window below.

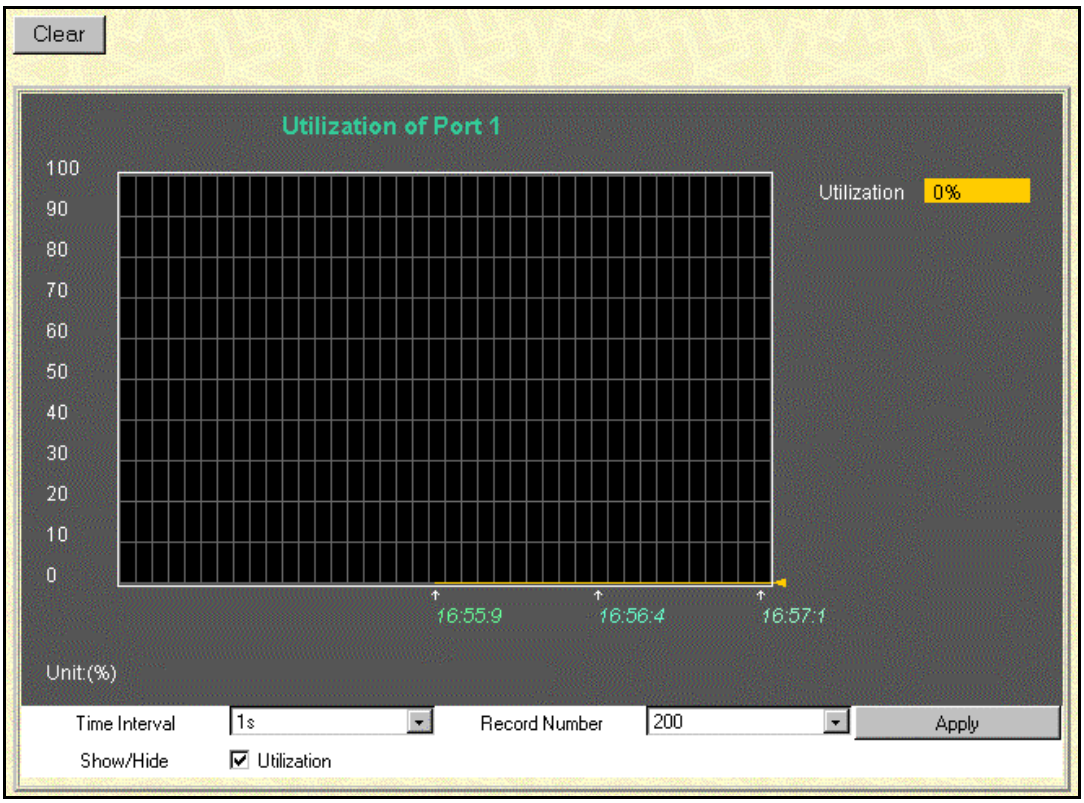


Figure 6- 43. Utilization window

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 20.
Show/Hide	Check whether or not to display Utilization.
Clear	Clicking this button clears all statistics counters on this window.

To view port utilization information with Telnet or a console emulator use the command **`show utilitzation`**.

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. The six windows offered are as follows:

Received (RX)

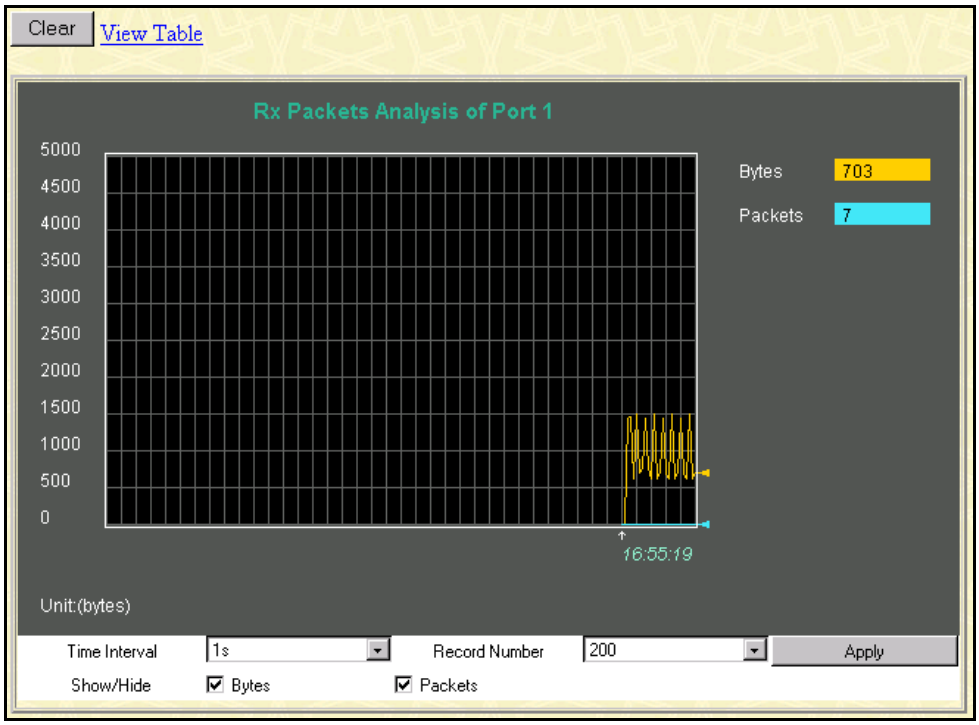
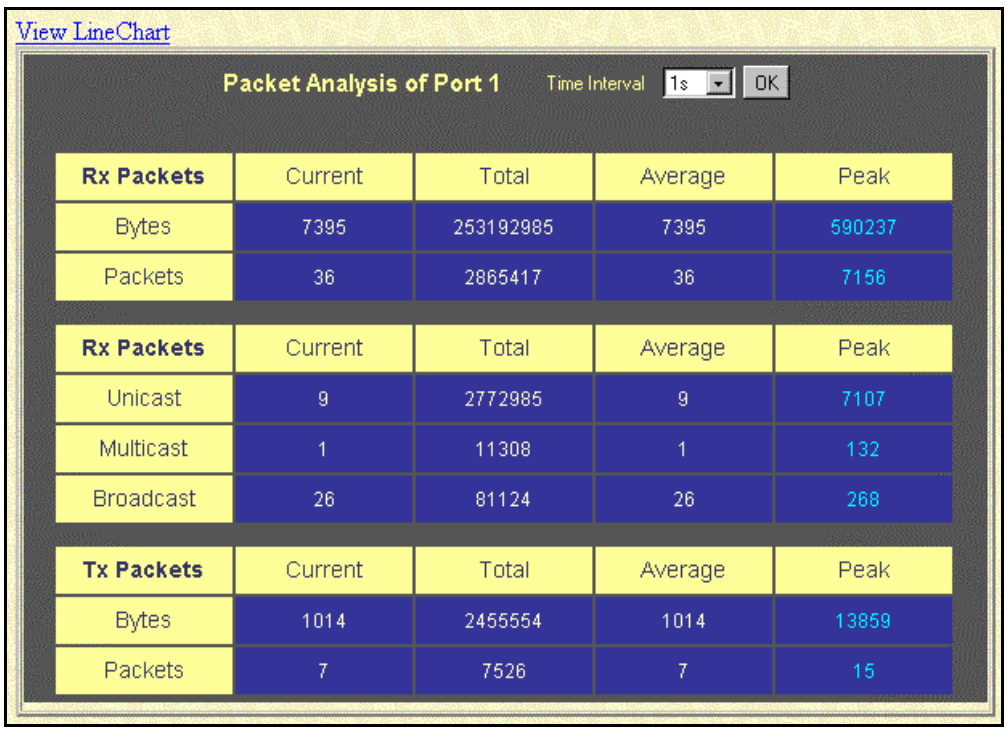


Figure 6- 44. Rx Packets Analysis window (Line Chart)



Rx Packets	Current	Total	Average	Peak
Bytes	7395	253192985	7395	590237
Packets	36	2865417	36	7156

Rx Packets	Current	Total	Average	Peak
Unicast	9	2772985	9	7107
Multicast	1	11308	1	132
Broadcast	26	81124	26	268

Tx Packets	Current	Total	Average	Peak
Bytes	1014	2455554	1014	13859
Packets	7	7526	7	15

Figure 6- 45. Rx Packets Analysis window (Table)

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is 20.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

The CLI command to view packet statistics is **`show packet ports`**.

UMB-cast (RX)

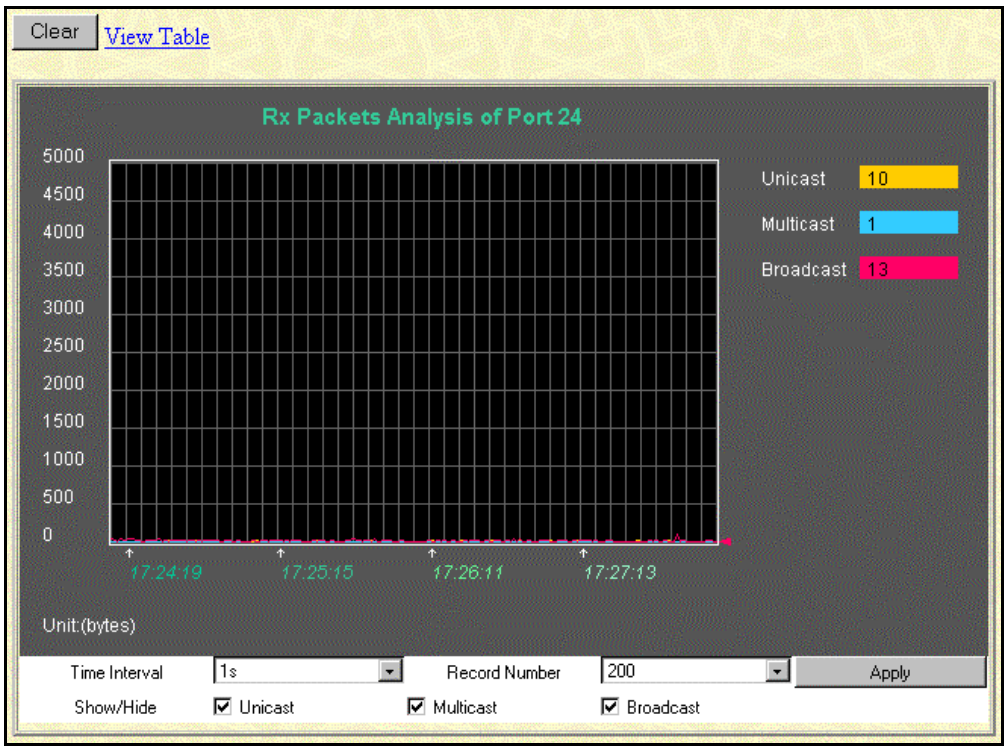


Figure 6- 46. Rx Packets Analysis window for UMB (Line Chart)

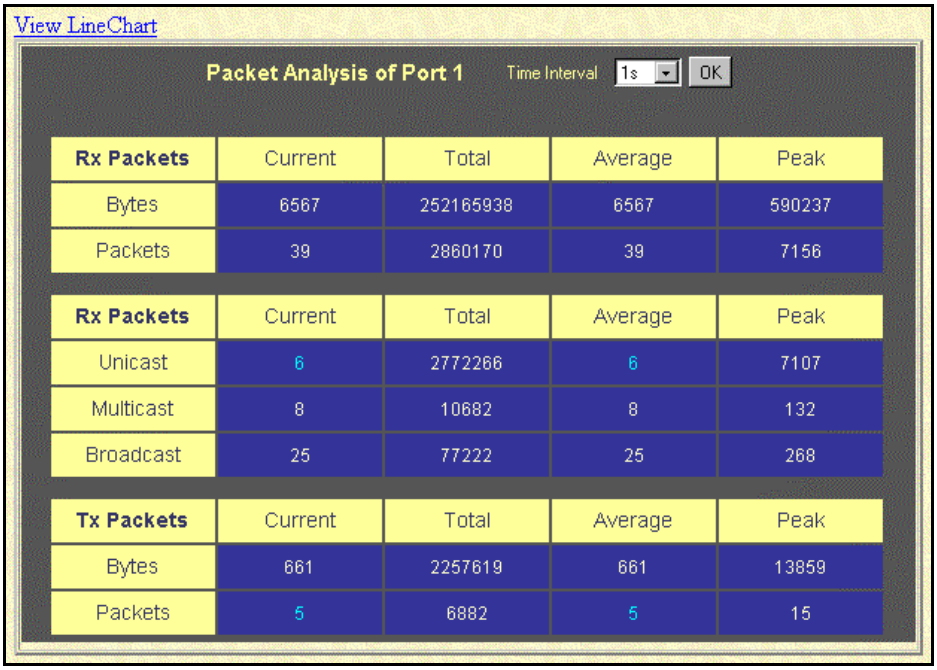


Figure 6- 47. Rx Packets Analysis window for MBU (Table)

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds.
Record Number	Select number of times the Switch will be polled between *20* and *200*.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

The CLI command to view packet statistics is **`show packet ports`**.

Transmitted (TX)

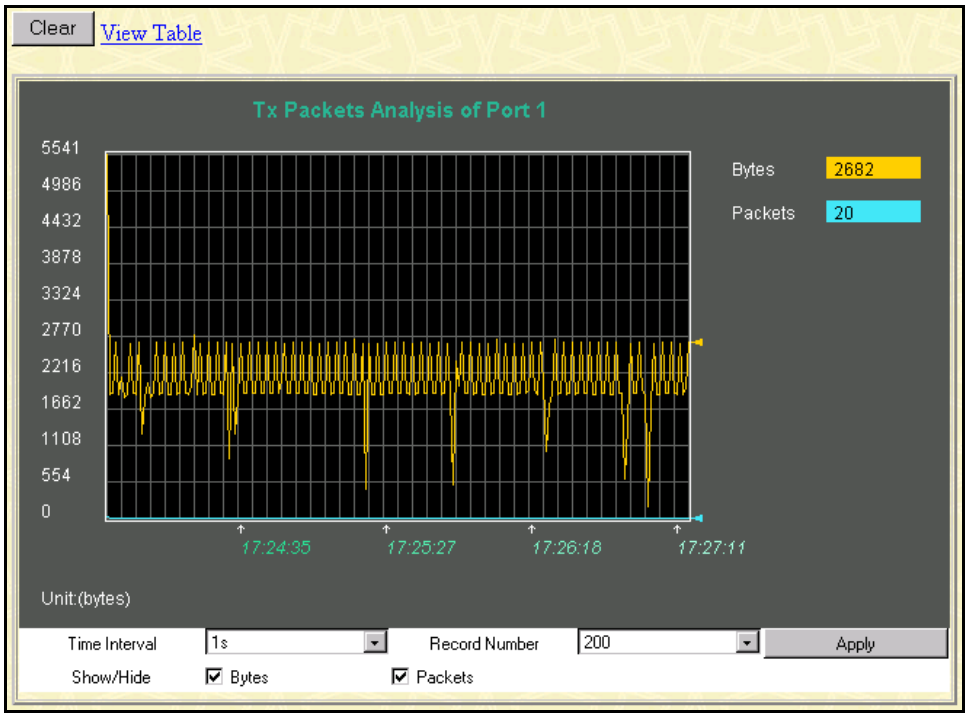
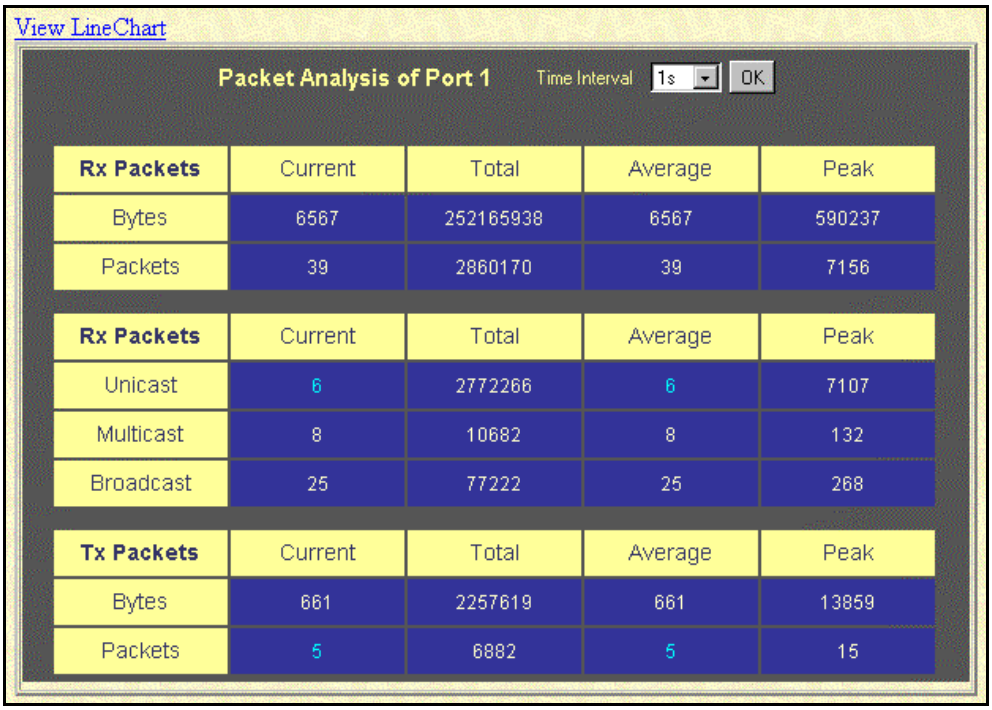


Figure 6- 48. Tx Packets Analysis window (Line Chart)



Rx Packets	Current	Total	Average	Peak
Bytes	6567	252165938	6567	590237
Packets	39	2860170	39	7156

Rx Packets	Current	Total	Average	Peak
Unicast	6	2772266	6	7107
Multicast	8	10682	8	132
Broadcast	25	77222	25	268

Tx Packets	Current	Total	Average	Peak
Bytes	661	2257619	661	13859
Packets	5	6882	5	15

Figure 6- 49. Tx Packets Analysis window (Table)

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *20*.
Bytes	Counts the number of bytes successfully sent from the port.
Packets	Counts the number of packets successfully sent on the port.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

The CLI command to view packet statistics is **`show packet ports`**.

Error Statistics

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. The four windows offered are as follows:

Received (RX)

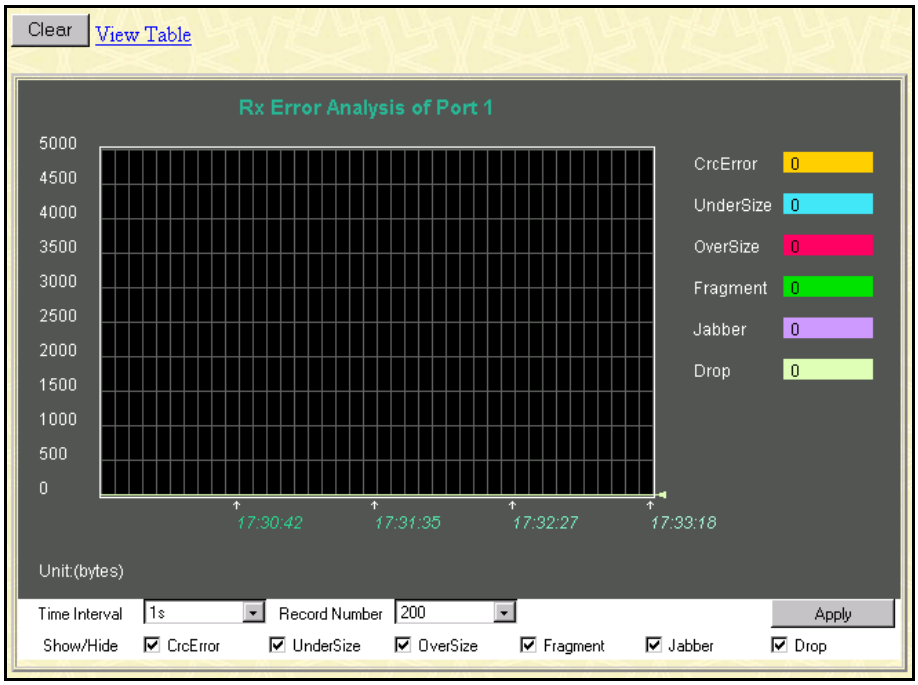


Figure 6- 50. Rx Error Analysis window (Line Chart)

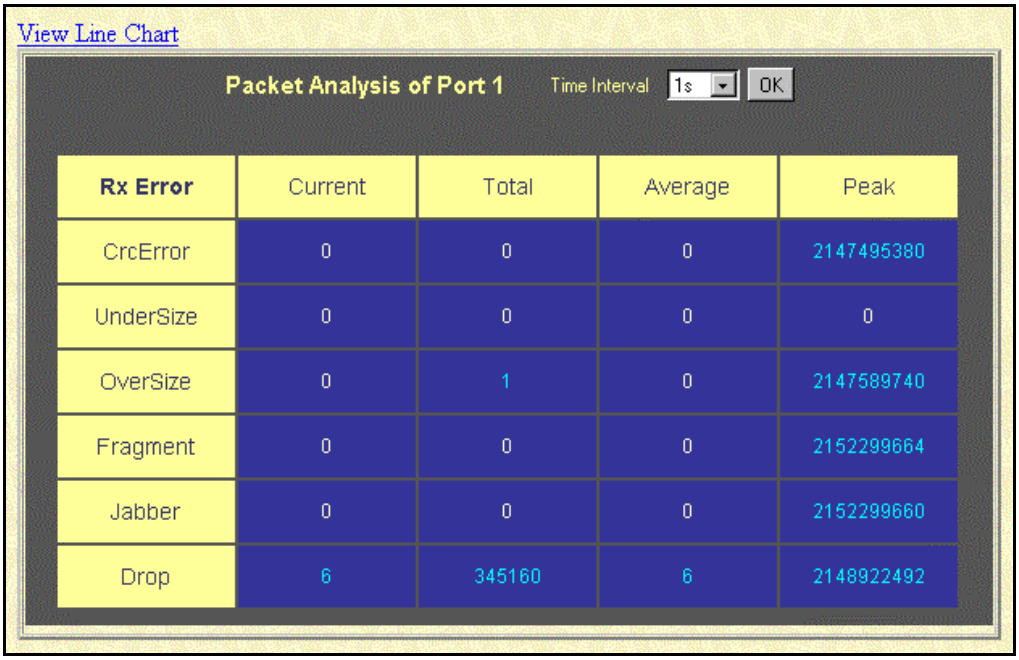


Figure 6- 51. Rx Error Analysis window (Table)

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *20*.
CRCError	Counts otherwise valid frames that did not end on a byte (octet) boundary.
UnderSize	The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network occurrence.
OverSize	Counts packets received that were longer than 1518 octets, or if a VLAN frame, 1522 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	The number of frames with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522
Drop	The number of frames which are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display CrcError, UnderSize, OverSize, Fragment, Jabber, and Drop errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

The CLI command to view packet error statistics is **`show error ports`**.

Transmitted (TX)

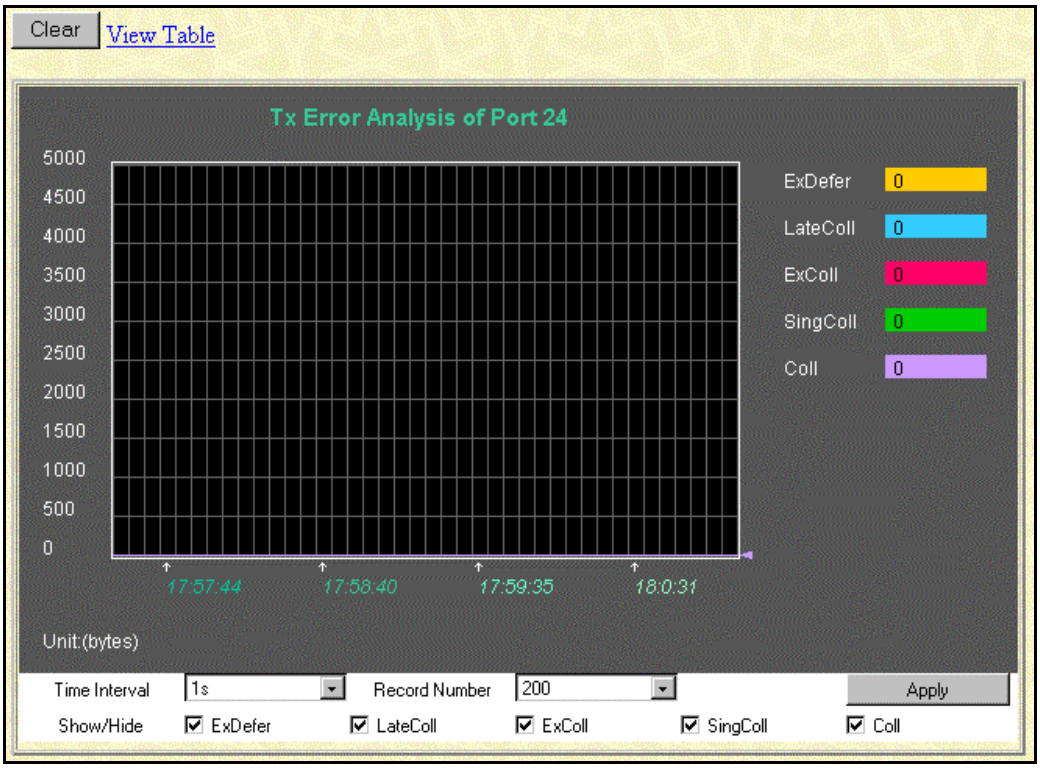
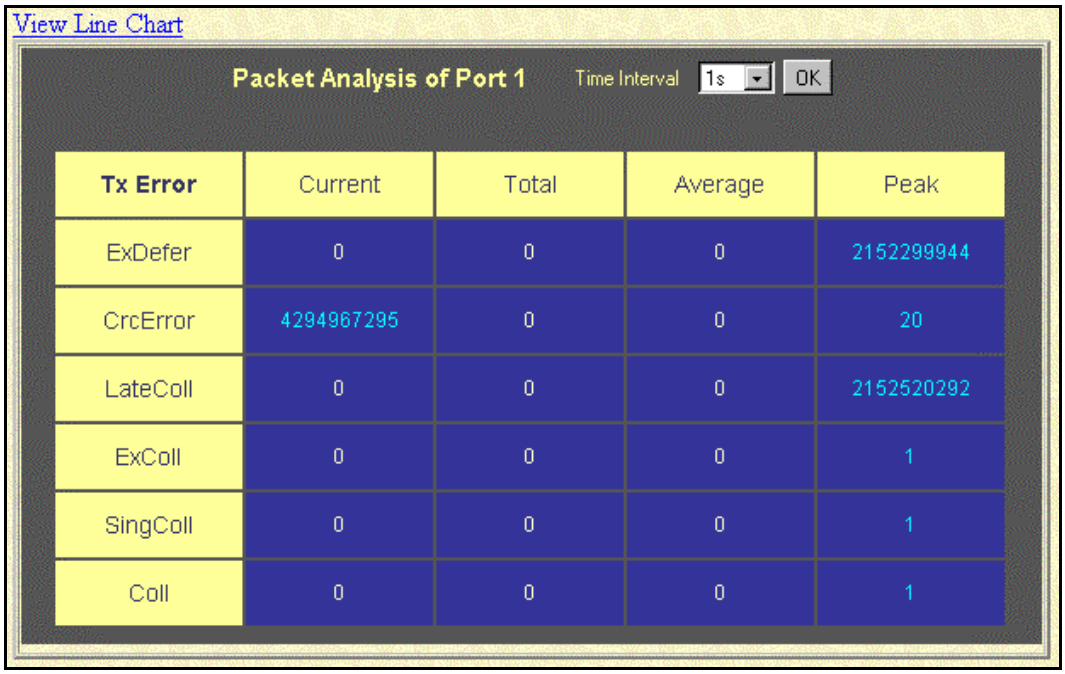


Figure 6- 52. Tx Error Analysis window (Line Chart)



Tx Error	Current	Total	Average	Peak
ExDefer	0	0	0	2152299944
CrcError	4294967295	0	0	20
LateColl	0	0	0	2152520292
ExColl	0	0	0	1
SingColl	0	0	0	1
Coll	0	0	0	1

Figure 6- 53. Tx Error Analysis window (Table)

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *20*.
ExDefer	Counts the number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRCError	Counts otherwise valid frames that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Show/Hide	Check whether or not to display ExDefer, CrcError, and LateColl errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

The CLI command to view packet error statistics is **`show error ports`**.

Packet Size Statistics

The Web Manager allows packets received by the Switch, arranged in six groups, to be viewed as either a line graph or a table. The two windows offered are as follows:

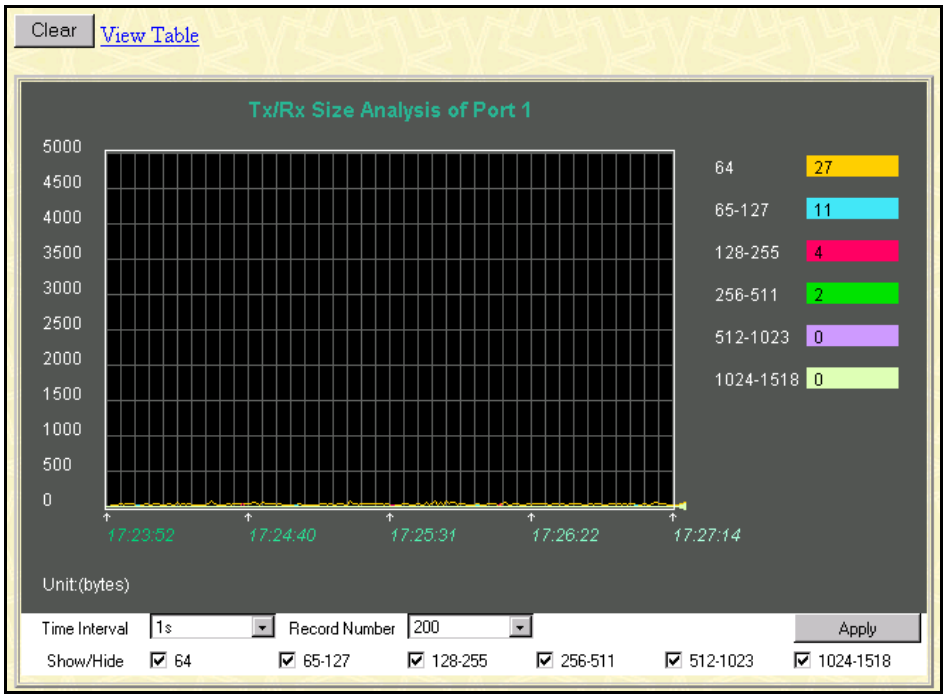


Figure 6- 54. Tx/Rx Size Analysis window (Line Chart)

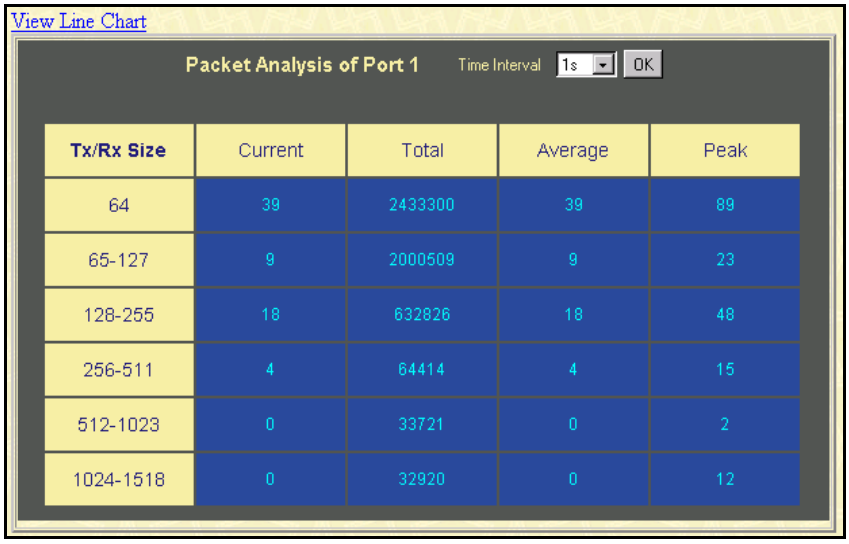


Figure 6- 55. Packet Analysis window (Table)

The information is described as follows:

Time Interval	Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between *20* and *200*. The default value is *20*.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128–255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

The CLI command to view packet size statistics is **`show packet ports`**.

MAC Address Table (Forwarding Data Base)

This menu is used to view the Switch's dynamic MAC address forwarding table. When the switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the switch. The Switch's MAC address table is referred to as the Forwarding Data Base in the CLI Reference Manual. To view the MAC address table using CLI the command is **`show fdb`**.

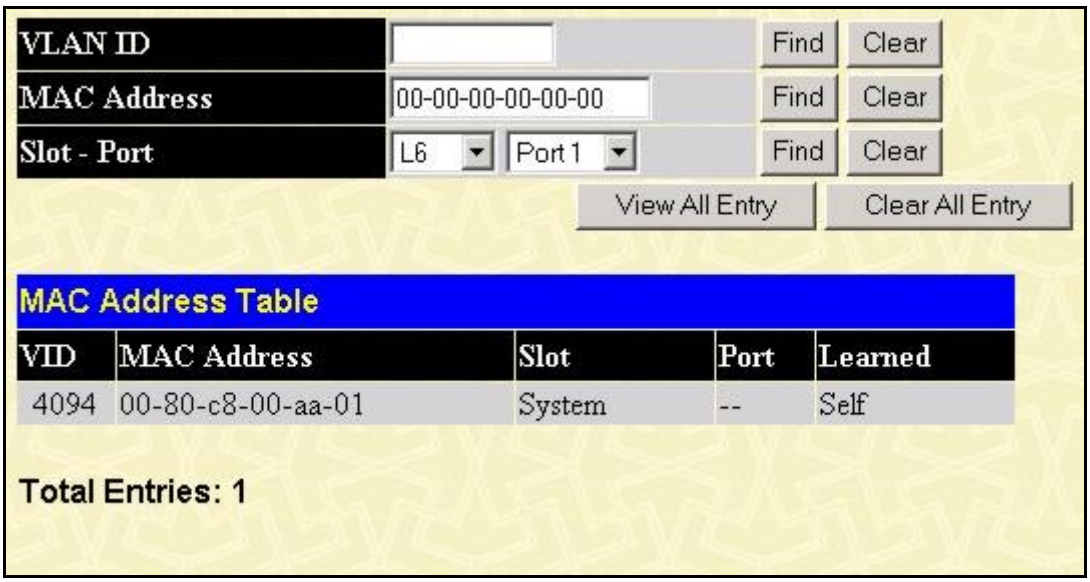


Figure 6- 56. MAC Address Table window

The information is described as follows:

Search by:	
VLAN ID	Allows the forwarding table to be browsed by VLAN ID (VID).
MAC Address	Allows the forwarding table to be browsed by MAC Address.
Slot - Port	Allows the forwarding table to be browsed by port number.
Find	Click the icon to find the data entry.
Clear	Clears all static and dynamic forwarding table entries for the VLAN ID, MAC Address or Port number. Only one of these three options (VLAN ID, MAC Address or Port) can be cleared at a time.
View All Entries	Lists all entries for the forwarding table.
Clear All Entries	Clears all entries for the forwarding table.
VID	The VLAN ID associated with the port or MAC address listed.
MAC Address	The MAC address entered into the address table.
Port	The port associated with the MAC address.
Learned	How the switch discovered the MAC address. The possible entries are *Dynamic*, *Self*, and *Static*.
Next	Click this button to view the next page of the address table.

IGMP Snooping

The Switch's IGMP snooping table can be browsed using the Web Manager. The table is displayed by VLAN ID (VID).

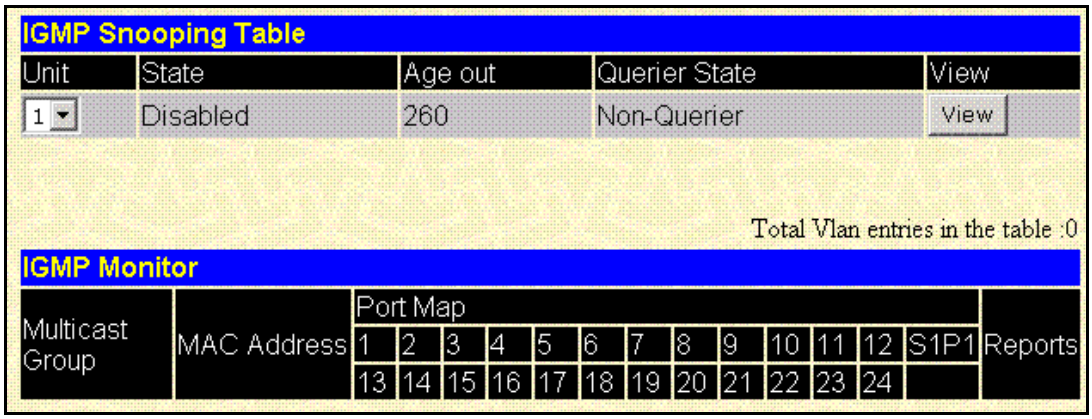


Figure 6- 57. IGMP Snooping Table window

The information is described as follows:

Unit	Select the Switch unit in a stacked group.
VID	VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.
Search	Click on the View button to display the IGMP Snooping Table for the current VID.
Multicast Group	The IP address of a multicast group learned by IGMP snooping.
MAC Address	The corresponding MAC address learned by IGMP snooping.
Port Map	Displays the ports that have forwarded multicast packets.
Reports	The number of IGMP reports for the listed source.

To view this information using CLI, use the command **`show igmp snooping group`**.

Maintenance

This category includes TFTP Services (Update Firmware, Configuration File, Save Settings, and Save History Log), Switch History, Ping Test, Local Loopback, Line Loopback, Save Changes, Factory Reset, Restart System.

TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch firmware to be upgraded by downloading a new firmware file from a TFTP server to the Switch. A configuration file can also be loaded into the Switch, and switch settings can be saved to a TFTP server. In addition, the Switch's history log can be uploaded from the Switch to a TFTP server.

Please note that TFTP server software must be running on the management station for the TFTP services listed here to work.

To use the TFTP services with CLI, use the **upload** / **download** CLI command set.

Download Firmware

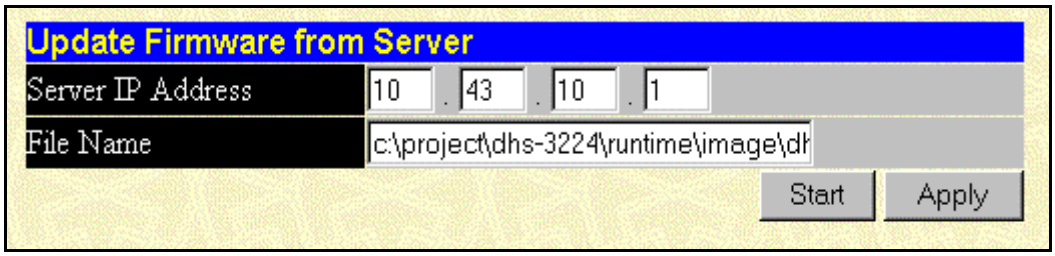


Figure 6- 58. Update Firmware from Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the Switch. Click **Apply** to enter the server's IP address into the Switch's RAM (use Save Changes to enter the address into the Switch's non-volatile RAM). Click **Start** to initiate the file transfer.

The information is described as follows:

Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the new firmware file on the TFTP server.

Configuration File

A configuration file can be downloaded from a TFTP server to the Switch. This file is then used by the Switch to configure itself.

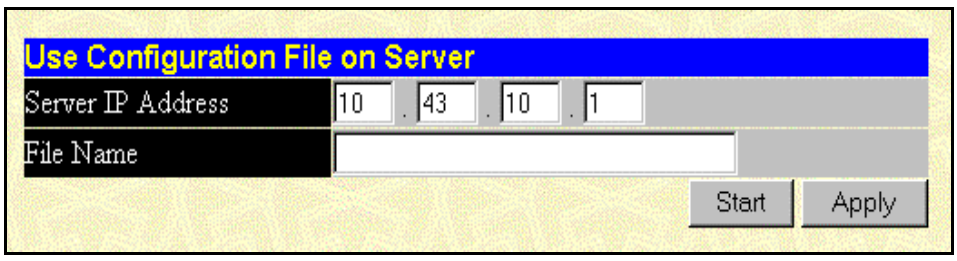


Figure 6- 59. Use Configuration File on Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the Switch. Click **Apply** to enter the server's IP address into the Switch's RAM (use Save Changes to enter the address into the Switch's non-volatile RAM). Click **Start** to initiate the file transfer.

The information is described as follows:

Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the new firmware file on the TFTP server.

Save Settings

The Switch's current settings can be uploaded to a TFTP Server by the Switch's management agent.

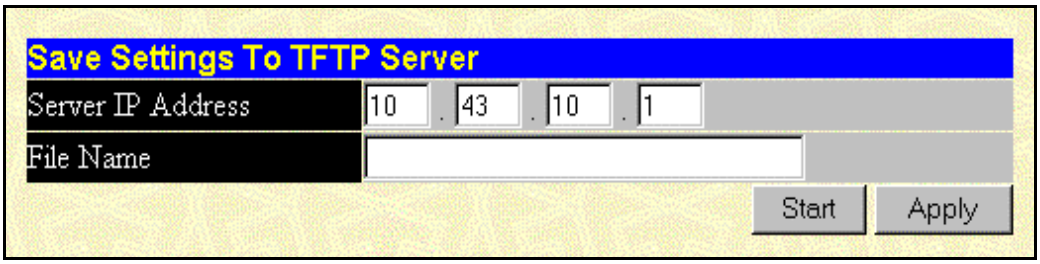


Figure 6- 60 Save Settings To TFTP Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the Switch. Click **Apply** to enter the server's IP address into the Switch's RAM (use Save Changes to enter the address into the Switch's non-volatile RAM). Click **Start** to initiate the file transfer.

Please note that if the user does not save configurations to NV-RAM, the configurations the user is uploading to a TFTP server will not be saved correctly.

The information is described as follows:

Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the new firmware file on the TFTP server.

Save History Log

The Switch's management agent can upload its history log file to a TFTP server.

Please note that an empty history file on the TFTP server must exist on the server before the Switch can upload its history file.

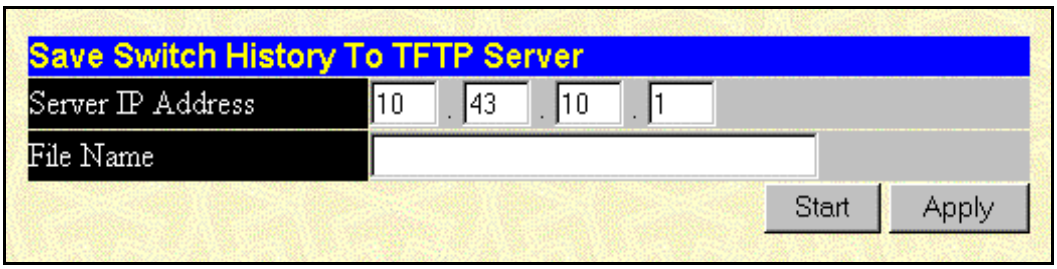


Figure 6- 61. Save Switch History To TFTP Server window

Enter the IP address of the TFTP Server in the **Server IP Address** field and the complete path and file name of the firmware file for the Switch. Click **Apply** to enter the server's IP address into the Switch's RAM (use Save Changes to enter the address into the Switch's non-volatile RAM). Click **Start** to initiate the file transfer.

The information is described as follows:

Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the new firmware file on the TFTP server.

Switch History

The Web Manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

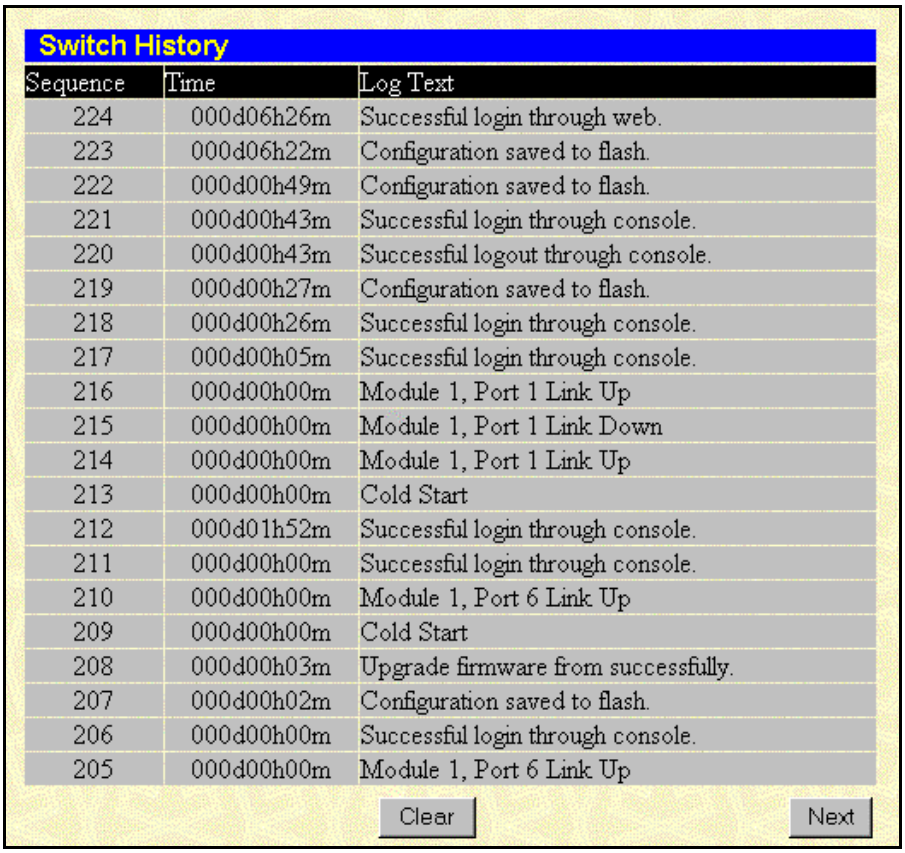


Figure 6- 62. Switch History window

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Clicking **Next** at the bottom of the window will allow you to display all the Switch Trap Logs. Clicking **Clear** will reset this log.

The information is described as follows:

Sequence	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Displays the time in days, hours, and minutes since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

The relevant CLI commands to view and delete the Switch history log are **`show log`** and **`clear log`**.

Ping Test

The Switch is able to test the connection with another network device using Ping.

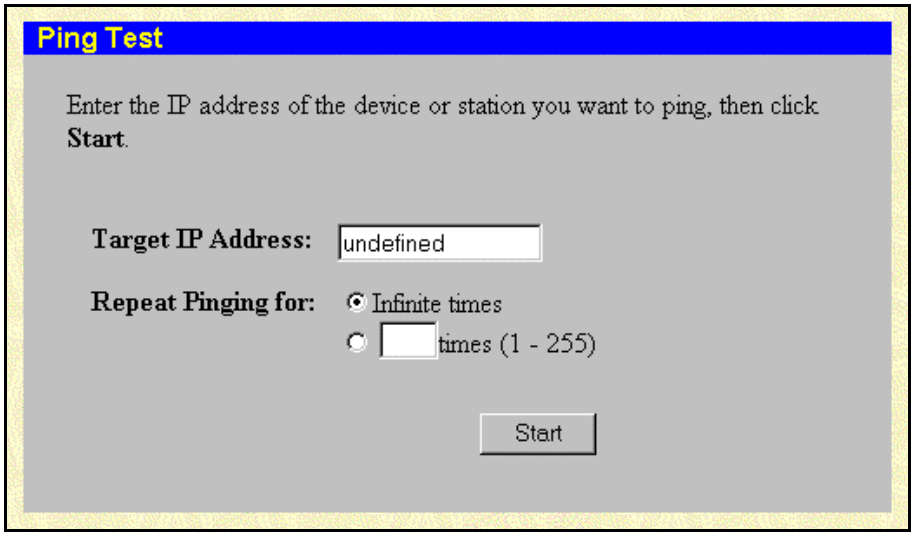


Figure 7- 1. Ping Test window

Enter the IP address of the network device to be Pinged in the first field and select the number of test packets to be sent (3 is usually enough). Click **Start** to initiate the Ping program.

The CLI command for a Ping test is simply **`ping`**.

Save Changes

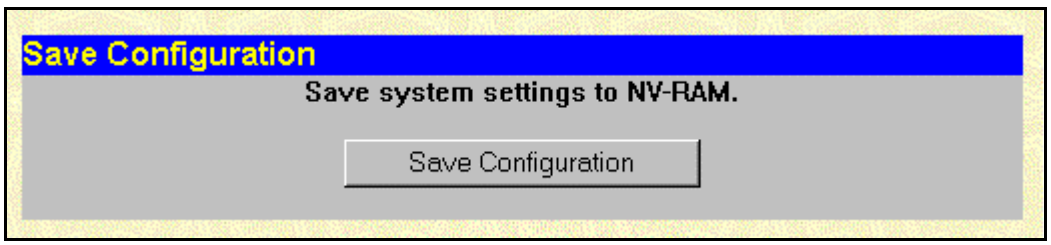


Figure 6- 63. Save Configuration window

To save all the changes made in the current session to the Switch's flash memory, click the **Save Configuration** button.

To save settings using CLI the command is **`save`**.

Factory Reset

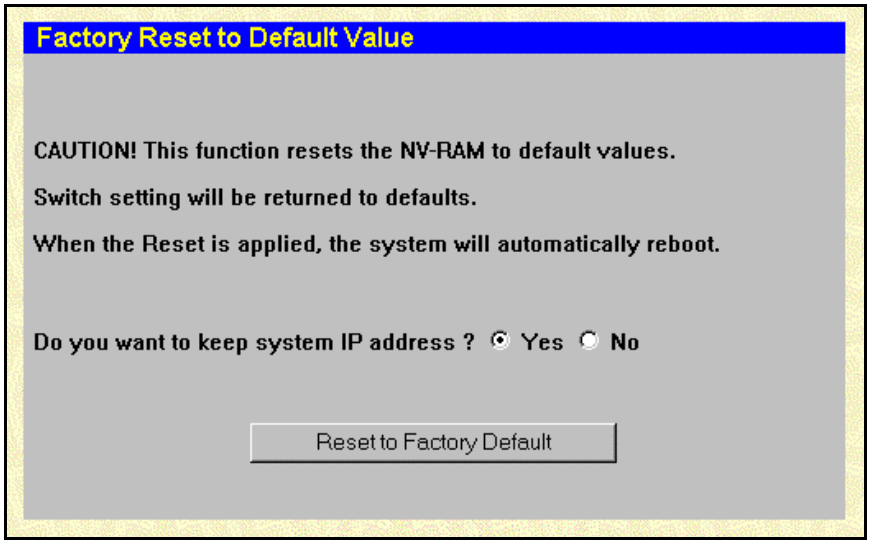


Figure 6- 64. Factory Reset to Default Value window

A remote reset returns the Switch to the initial parameters set at the factory. You may opt to save the current IP settings for the Switch. Click **Reset to Factory Default** to reset the Switch. The default IP settings for the Switch are 10.90.90.90/255.0.0.0 and are configured for manual setting.

The CLI command to reset Switch configuration to the default settings is **`reset`**.

Restart System

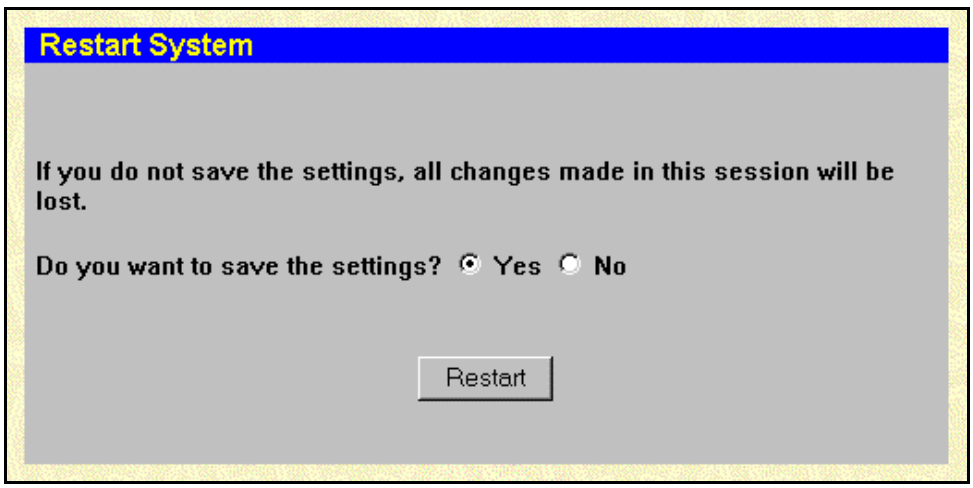


Figure 6- 65. Restart System window

To perform a reboot of the Switch, which resets the system, click the **Restart** button.

The CLI command to restart is **`reboot`**, CLI allows the option of restarting an individual slot.

A

Technical Specifications

General		
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX/LX Gigabit Ethernet IEEE 802.1ab 1000BASE-T Gigabit Ethernet IEEE 802.1p/q IEEE 802.3x RFC 1123, RFC 2236 RFC1493, RFC 951 RFC2131, RFC1058 RFC1723, RFC 1389 RFC1253, RFC1583 RFC2178, RFCRFC 1850 RFC 1112, RFC 2236	
Management	MIB II, RMON, SNMP,	
Protocol	CSMA/CD	
Data Transfer Rate Ethernet Fast Ethernet: Gigabit Ethernet:	**Half-duplex** 10 Mbps 100 Mbps n/a	**Full-Duplex** 20 Mbps 200 Mbps 2000 Mbps
Topology	Star	
Network Cables 10BASE-T: 100BASE-TX: 1000BASE-T	2-pair Category 3/4/5 UTP (max. 100 m) EIA/TIA-568 100-ohm STP (max. 100 m) 2-pair Category 5 UTP (max. 100 m) EIA/TIA-568 100-ohm STP (max. 100 m) 2-pair Category 5 UTP (max. 100 m) EIA/TIA-568 100-ohm STP (max. 100 m)	

Physical and Environmental	
AC Input	90 to 264 VAC, 47-63 Hz (auto-adjusting internal power supply)
AC Output	3.3V, 4A~80A
DC Fans	Two built-in 60 x 60 mm fans per power supply unit
Temperature	Operating: 0° to 40° C (32° to 104° F) Storage: -25° to 55° C (-13° to 131° F)
Relative Humidity	Operating: 5% to 95% (non-condensing) Storage: 0% to 95% (non-condensing)
Dimensions	DES-7000 H: 70cm(27.56in) W: 44.5cm(17.52in) D: 47cm(18.50in) DES-7100 H: 35.6cm(14.02in) W: 44.5cm(17.52in) D: 29.4cm(11.57in)
EMI	CE Class A
Safety	CSA international

Index

D-Link Offices

Australia
D-Link Australasia
1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia
TEL: 61-2-8899-1800 FAX: 61-2-8899-1868
TOLL FREE (Australia): 1300 766 868
TOLL FREE (New Zealand): 0800-900900
URL: www.dlink.com.au
E-MAIL: support@dlink.com.au & info@dlink.com.au

Brazil
D-Link Brasil Ltda.
Rua Tavares Cabral 102 - Conj. 31 e 33
05423-030 Pinheiros, Sao Paulo, Brasil
TEL: (5511) 3094 2910 to 2920 FAX: (5511) 3094 2921
URL: www.dlink.com.br

Canada
D-Link Canada
2180 Winston Park Drive, Oakville,
Ontario, L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223
BBS: 1-965-279-8732 FTP: ftp.dlinknet.com
TOLL FREE: 1-800-354-6522
URL: www.dlink.ca E-MAIL: techsup@dlink.ca

Chile
D-Link South America (Sudamérica)
Isidora Goyenechea 2934
Oficina 702, Las Condes, Santiago, Chile
TEL: 56-2-232-3185 FAX: 56-2-232-0923
URL: www.dlink.com.cl

China
D-Link Beijing
Level 5,Tower W1,The Tower,Oriental Plaza
No.1,East Chang An Ave., Dong Cheng District
Beijing,100738,China
TEL: (8610) 85182529/30/31/32/33
FAX: (8610) 85182250
URL: www.dlink.com.cn E-MAIL: webmaster@dlink.com.cn

Denmark
D-Link Denmark
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL: 45-43-969040 FAX: 45-43-424347
URL: www.dlink.dk E-MAIL: info@dlink.dk

Egypt
D-Link Middle East
7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt
TEL: 202-624-4615 FAX: 202-624-583
URL: www.dlink-me.com
E-MAIL: support@dlink-me.com & dlinkegypt@dlink-me.com

Finland
D-Link Finland
Pakkalankuja 7A, 01510 Vantaa, Finland
TEL: 358-9-2707-5080 FAX: 358-9-2707-5081
URL: www.dlink-fi.com

France	D-Link France Le Florilege, No. 2, Allée de la Fresnerie, 78330 Fontenay-le-Fleury, France TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr
Germany	D-Link Central Europe (D-Link Deutschland GmbH) Schwalbacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 BBS: 49-(0) 6192-971199 (analog) & BBS: 49-(0) 6192-971198 (ISDN) INFO: 00800-7250-0000 (toll free) & HELP: 00800-7250-4000 (toll free) REPAIR: 00800-7250-8000 & HELP: support.dlink.de URL: www.dlink.de & E-MAIL: info@dlink.de
India	D-Link India Plot No.5, Kurla -Bandra Complex Rd., Off Cst Rd., Santacruz (East), Mumbai, 400 098 India TEL: 91-022-2652-6696/6788/6623 FAX: 91-022-2652-8914/8476 URL: www.dlink.co.in E-MAIL: service@dlink.co.in & tushars@dlink.co.in
Italy	D-Link Mediterraneo Srl/D-Link Italia Via Nino Bonnet n. 6/B, 20154, Milano, Italy TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it
Japan	D-Link Japan 10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp
Netherlands	D-Link Benelux Lichtenauerlaan 102-120, 3062 ME Rotterdam, Netherlands TEL: +31-10-2045740 FAX: +31-10-2045880 URL: www.d-link-benelux.nl & www.dlink-benelux.be E-MAIL: info@dlink-benelux.com
Norway	D-Link Norway Karihaugveien 89, 1086 Oslo TEL: 47-22-309075 FAX: 47-22-309085 SUPPORT: 800-10-610 & 800-10-240 (DI-xxx) URL: www.dlink.no
Russia	D-Link Russia 129626 Russia, Moscow, Graphskiy per., 14, floor 6 TEL/FAX: +7 (095) 744-00-99 URL: www.dlink.ru E-MAIL: vl@dlink.ru
Singapore	D-Link International 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-6774-6233 FAX: 65-6774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com

South Africa
D-Link South Africa
Einstein Park II, Block B
102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion, Gauteng, Republic of South Africa
TEL: +27-12-665-2165 FAX: +27-12-665-2186
URL: www.d-link.co.za E-MAIL: attie@d-link.co.za

Spain
D-Link Iberia S.L.
Sabino de Arana, 56 bajos, 08028 Barcelona, Spain
TEL: 34 93 409 0770 FAX: 34 93 491 0795
URL: www.dlink.es E-MAIL: info@dlink.es

Sweden
D-Link Sweden
P. O. Box 15036, S-167 15 Bromma, Sweden
TEL: 46-8-564-61900 FAX: 46-8-564-61901
URL: www.dlink.se E-MAIL: info@dlink.se

Taiwan
D-Link Taiwan
2F, No. 119, Pao-chung Road, Hsin-tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw E-MAIL: dssqa@dlinktw.com.tw

Turkey
D-Link Turkiye
Beybi Giz Plaza, Ayazaga Mah. Meydan Sok. No. 28
Maslak 34396, Istanbul-Turkiye
TEL: 90-212-335-2553 (direct) & 90-212-335-2525 (pbx)
FAX: 90-212-335-2500 E-MAIL: dlinkturkey@dlink-me.com
E-MAIL: support@dlink-me.com

U.A.E.
D-Link Middle East FZCO
P.O. Box18224 R/8, Warehouse UB-5
Jebel Ali Free Zone, Dubai – United Arab Emirates
TEL: (Jebel Ali): 971-4-883-4234
FAX: (Jebel Ali): 971-4-883-4394 & (Dubai): 971-4-335-2464
E-MAIL: dlinkme@dlink-me.com & support@dlink-me.com

U.K.
D-Link Europe (United Kingdom) Ltd
4th Floor, Merit House, Edgware Road, Colindale, London
NW9 5AB United Kingdom
TEL: 44-020-8731-5555 SALES: 44-020-8731-5550
FAX: 44-020-8731-5511 SALES: 44-020-8731-5551
BBS: 44 (0) 181-235-5511
URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A.
D-Link U.S.A.
53 Discovery Drive, Irvine, CA 92618, USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
INFO: 1-800-326-1688 URL: www.dlink.com
E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms _____
Organization: _____ Dept. _____
Your title at organization: _____
Telephone: _____ Fax:_____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____
Telephone: _____ Fax:_____
Reseller's full address: _____
_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
o Home o Office o Travel o Company Business o Home Business o Personal Use

2. How many employees work at installation site?
o 1 employee o 2-9 o 10-49 o 50-99 o 100-499 o 500-999 o 1000 or more

3. What network protocol(s) does your organization use ?
o XNS/IPX o TCP/IP o DECnet o Others_____

4. What network operating system(s) does your organization use ?
o D-Link LANsmart o Novell NetWare o NetWare Lite o SCO Unix/Xenix o PC NFS o 3Com 3+Open
o Banyan Vines o DECnet Pathwork o Windows NT o Windows NTAS o Windows '95
o Others_____

5. What network management program does your organization use ?
o D-View o HP OpenView/Windows o HP OpenView/Unix o SunNet Manager o Novell NMS
o NetView 6000 o Others_____

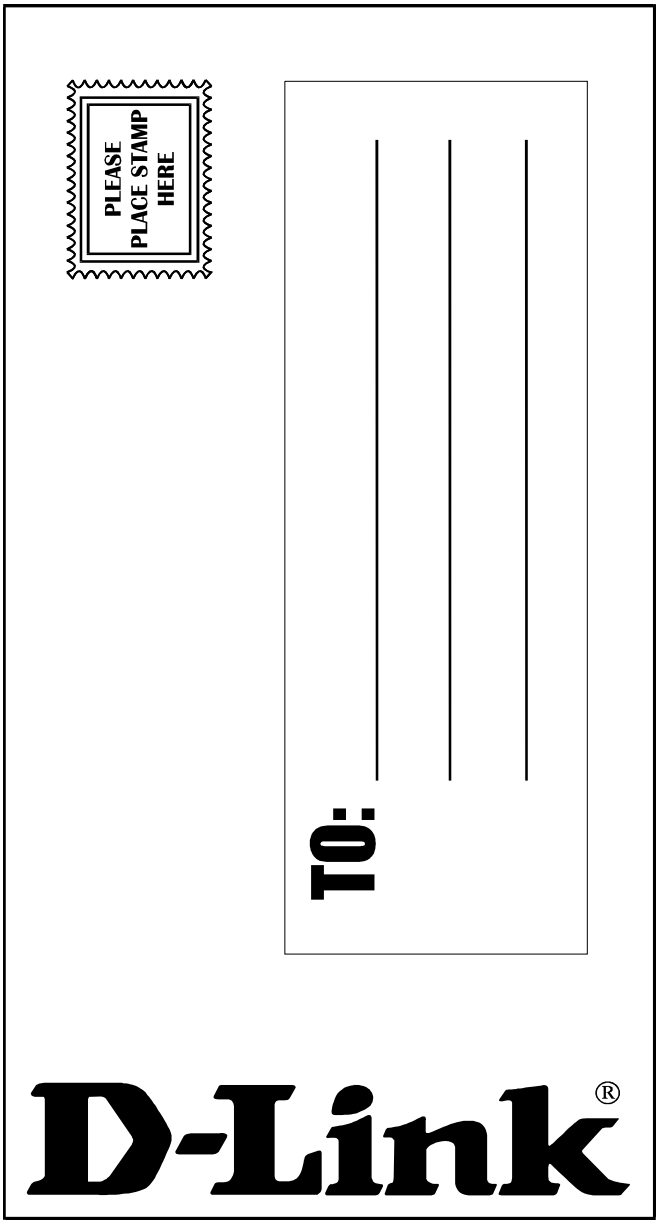
6. What network medium/media does your organization use ?
o Fiber-optics o Thick coax Ethernet o Thin coax Ethernet o 10BASE-T UTP/STP
o 100BASE-TX o 100BASE-T4 o 100VGAnyLAN o Others_____

7. What applications are used on your network?
o Desktop publishing o Spreadsheet o Word processing o CAD/CAM
o Database management o Accounting o Others_____

8. What category best describes your company?
o Aerospace o Engineering o Education o Finance o Hospital o Legal o Insurance/Real Estate o Manufacturing
o Retail/Chainstore/Wholesale o Government o Transportation/Utilities/Communication o VAR
o System house/company o Other_____

9. Would you recommend your D-Link product to a friend?
o Yes o No o Don't know yet

10.Your comments on this product?
_____


PLEASE
PLACE STAMP
HERE
TO:
D-Link®