D-Link®
Building Networks for People

User Guide

Product Model: DPN-3012-E /RU

OLT

Release A1

September 2008 P/N 651PN3012035G

Table of Contents

Preface

The *DPN-3012-E Gigabit Ethernet Passive Optical Network (GE-PON) OLT CO Switch User Manual* is divided into sections that describe the system installation and operating instructions with examples.

Section 1, Introduction – Describes the Switch and its features.

Section 2, Installation – Helps you get started with the basic installation of the Switch and also describes the front panel, rear panel, side panels, and LED indicators of the Switch.

Section 3, Connecting the Switch – Tells how you can connect the Switch to the GE-PON network

Section 4, Introduction to Switch Management – Introduces basic Switch management features, including password protection, SNMP settings, IP address assignment, connecting devices to the Switch, and using the Reset, Reboot System, and Logout windows.

Section 5, Introduction to Web-based Switch Management – This section talks about connecting to and using the Web-based switch management feature on the Switch.

Section 6, Administration – A detailed discussion about configuring the basic functions of the Switch, including Device Information, IP Address, Port Configuration, User Accounts, Port Mirroring, System Log Settings, System Severity Settings, SNTP Settings, MAC Notification Settings, TFTP Services, FTP Services, Multiple Image Services, Ping Test, Safeguard Engine, Static ARP Settings, Routing Table, DHCP Auto Configuration, SNMP Manager, DHCP Server Screening, and Single IP Management Settings.

Section 7, Layer 2 Features – A discussion of Layer 2 features of the Switch, including VLAN, Protocol VLAN, Trunking, IGMP Snooping, IGMP Snooping, Loopback Detection, Spanning Tree, and Forwarding & Filtering.

Section 8, QoS – Features information on QoS, including Bandwidth Control, QoS Scheduling Mechanism, QoS Output, Scheduling, 802.1p Default Priority, 802.1p User Priority, WRED Settings and Browse WRED Settings.

Section 9, ACL – Discussion on the ACL function of the Switch, including Access Profile Table, ACL Flow Meter and CPU Interface Filtering.

Section 10, Security – A discussion on the Security functions on the Switch, including Authorization Network State Settings, Traffic Control, Port Security, Port Lock Entries, IP-MAC-Port Binding, 802.1x, Web Authentication, Trust Host, Access Authentication Control, MAC-based Access Control, Traffic Segmentation, SSL, and SSH.

Section 11, Monitoring – Features information on Monitoring including Device Status, CPU Utilization, Port Utilization, Packets, Errors, Packet Size, Browse Router Port, VLAN Status, Port Access Control, MAC Address Table, IGMP Snooping Group, Switch Log, Browse ARP Table, Session Table and MAC-based Access Control Authentication Status.

Section 12, Save Services – A discussion of how to use Save Changes, Configure Information, and Config Current Setting.

Appendix A, Technical Specifications – Technical specifications for the 3012-E Gigabit Ethernet Passive Optical Network (GE-PON) OLT CO Switch

Appendix B, Cables and Connectors – Describes the RJ-45 receptacle/connector, straight through and crossover cables and standard pin assignments.

Appendix C, Cable Lengths – Information on cable types and maximum distances.

Intended Readers

The *DPN-3012-E Gigabit Ethernet Passive Optical Network (GE-PON) OLT CO Switch User Manual* contains information for setup and management of the Switch. The term, "the Switch" will be used when referring to the DPN-3012-E switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[ ]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
`Boldface Typewriter Font`	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Italics	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type filename means that you should type the actual filename instead of the word shown in italic.
Menu Name > Menu Option	**Menu Name > Menu Option** Indicates the menu structure. **Device > Port > Port Properties** means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions

A **NOTE** indicates important information that helps you make better use of your device.

A **NOTICE** indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

A **CAUTION** indicates a potential for property damage, personal injury, or death.

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this document, the caution icon ( ) is used to indicate cautions and precautions that you need to review and follow.

Safety Cautions

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

- Observe and follow service markings.
  - Do not service any product except as explained in your system documentation.
  - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
  - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage on the power supply is set to match the power available at your location:
  - 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
  - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
  - 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

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

- Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.
- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

NOTE: A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local, regional or national codes and practices.

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

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

CAUTION: Do not replace the battery with an incorrect type. The risk of explosion exists if the replacement battery is not the correct lithium battery type. Dispose of used batteries according to the instructions.

Protecting Against Electrostatic Discharge

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

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

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

Section 1

Introduction

The following manual describes the installation, maintenance and configurations concerning members of the D-Link DPN-3012-E (GE-PON) switch. For the remainder of this document, we will refer to the D-Link DPN-3012-E (GE-PON) switch as the Switch for examples, configurations and explanations.

Switch Description

The Gigabit Ethernet Passive Optical Network (GE-PON) OLT CO Switch is designed for point to multi-point FTTH applications.

The GE-PON service delivers up to 1Gbps speed over fiber optic cabling, enabling next-generation simultaneous voice, video and data services including high-speed Internet access and video streaming. The DPN-3012-E/RU is a cost-effective, easy-to-deploy technology ideal for multi-unit buildings (MxU), like departments, hotels, etc…

The OLT provides the function to convert the GEPON (Giga-bit Ethernet Passive Optical Network) interface conforming to IEEE802.3ah to trunk interface. The OLT provides 4 1000BASE-T/SFP Combo interfaces as the trunk interface, and supported L2 SW function. One OLT has three open slots, and each open slot support one module with 4 GEPON (Giga Bit Ether Passive Optical Network) interfaces and each GEPON interface accommodates up to 32 ONU through the optical splitter.

Software Features

- Supports the following IEEE 802.3ah Ethernet in the First Mile features:
  - Auto Discovery / Grant Allocation/ Ranging/ Report Handling
  - Alarm Report (Dying Gasp/ Remote link down/ Temperature abnormal)
  - OAM Information
  - FEC
  - Downstream bandwidth control policing
  - Following Upstream Bandwidth controls by DBA
    - Fixed Bandwidth
    - Assured Bandwidth
    - Best Effort Bandwidth
    - Max and Min Bandwidth
  - Remote diagnostic (Loop back / Ping)
  - Peer to peer management (Access Control/ traffic limitation.)
- ONU remote management (Link speed/Link enable, disable)
- ONU remote firmware upgrade
- Port lock for each ONU.
- QoS Support:
  - 8 queues per port
  - 802.1p support
  - CoS based on TOS
  - CoS DSCP
  - Strict Priority Scheduling
- Supports following L2 features:
  - 802.1Q VLAN for up to 4000 VLANs
  - 802.1ad Double-tagging, (PON handle)
  - L2 FDB (Address learning)
  - 802.3ad (strict/dynamic) Trunking support on uplink ports
  - Port Mirroring
  - IGMP snooping v1/v2 (non-query mode) for up to 255 groups
  - IGMP proxy
  - Multicast VLAN
  - 802.1D Spanning-Tree support on uplink ports
  - 802.1W Rapid Spanning-Tree support on uplink ports
  - 802.S Multiple Spanning-Tree support on uplink ports
- Supports following security features:
  - MAC Authentication
  - AES Encryption
- Supports following Management features:
  - ACL
  - Performance statistics
  - Telnet
  - SYSLOG
  - SNMP v1
  - SNMP v2c
  - CLI for RS-232 console
  - MIB/Trap
  - SNTP
  - RTC
  - TFTP Client

- Firmware upgradeable via TFTP
- Configuration download/upload via TFTP
- Dual Runtimes
- Dual Configurations
- Supports both in-band and out-band management
- Support for D-Link D-View
- Web Interface

- Compatible with following devices:
  - Backward compatible with all functions on DPN-3012 V.B1/A1 platform
  - Compatible to the ONU with the DPN-301/RU and DPN-304/RU models

Ports

The following ports are present within the Base Unit of the Switch:

- Supports up to 3 x 4 port Downlink OLT modules
- 4x 1000 Base-T / SFP Combo Uplink ports
- Female DCE RS-232 DB-9 console port in front panel for out-of-band configuration of the software features
- RJ-45 Connector console port in front panel for out of band configuration of the software features.

1000Base-T / SFP combo mini-GBIC ports comply with the following standards:

- Fully compliant with IEEE 802.3
- Fully compliant with IEEE 802.3u
- Fully compliant with IEEE 802.3z
- Fully compliant with IEEE 802.3ab
- Support Full-Duplex operations
- IEEE 802.3x Flow Control support for Full-Duplex mode

All SFP ports support the following transceivers:

- DEM-310GT (1000Base-LX, Single-mode, 10Km)
- DEM-311GT (1000Base-SX, Multi-mode, 500m)
- DEM-312GT (1000Base-SX, Multi-mode, 2Km)
- DEM-314GT (1000Base-LH, Single-mode, 50Km)
- DEM-315GT (1000Base-ZX, Single-mode, 80Km)

Front-Panel Components

The front panel of the DPN-3012-E supports up to three DPN-3012-E-01/ 4 port OLT modules, 4x 1000 Base-T / SFP Combo Uplink ports, Female DCE RS-232 DB-9 console port and an RJ-45 Connector console port for out of band configuration. The hardware components of the DPN-3012-E-01 4 port OLT modules appear in the next section.

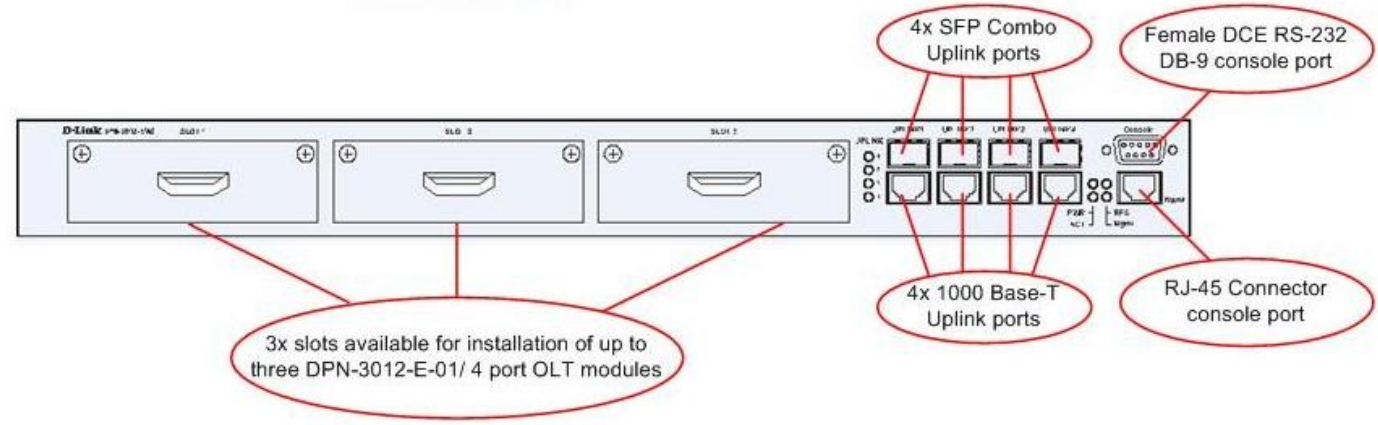


Figure 1- 1. Front Panel of the DPN-3012-E

Rear-Panel Components

The rear panel of the DPN-3012-E consists of an internal power supply, connector for an optional Redundant Power Supply (RPS) and a Power Switch.

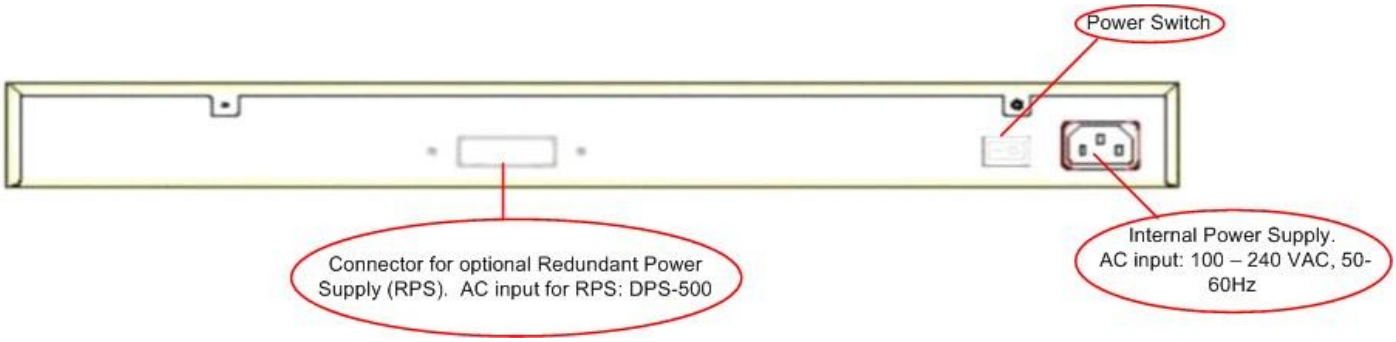


Figure 1- 2. Rear Panel of the DPN-3012-E

The rear panel includes an outlet for an optional external redundant power supply. When power fails, the optional external RPS will take over all the power immediately and automatically. The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. The Switch automatically adjusts its power setting to any supply voltage in the range from 100 ~ 240 VAC at 50 ~ 60 Hz.

LEDs

The front panel of the DPN-3012-E has LED indicators for power, OLT Equipment Active Status, Redundant Power Supply Status, Control LAN port and for the four combo 1000BASE-T/SFP ports.

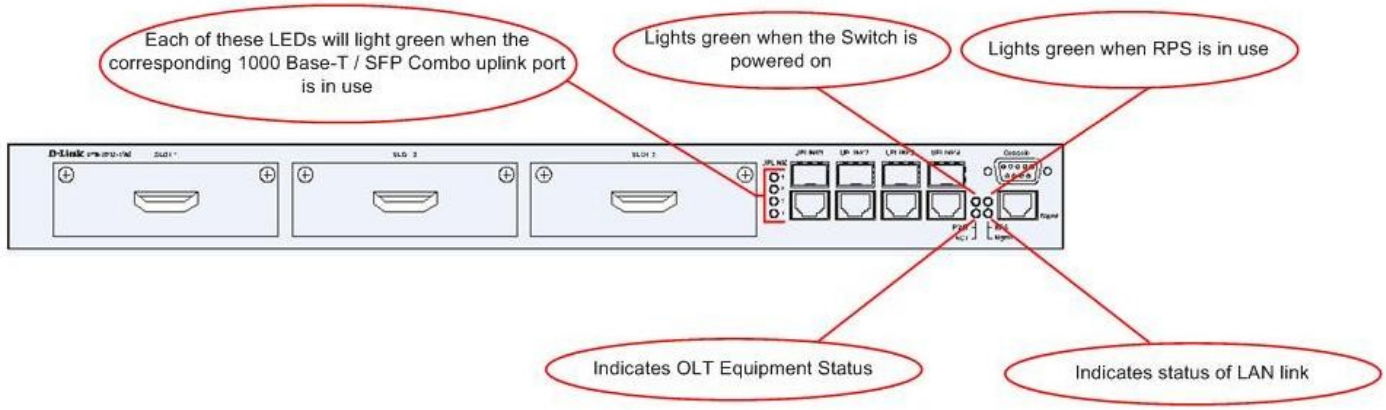


Figure 1- 3. LED Indicators for the DPN-3012-E

The following table describes the LEDs for the DPN-3012-E:

LED	Description
Power	Off – Power Off Solid Green – Power On
Status	Solid Green – Self test passed Blinking Green – System booting Blinking Red – Switch controller failed / PON chip set initialization failed / FAN failed
RPS	Off – RPS off Solid green – RPS in use
Console	Solid Green – Control LAN link up Blinking Green – Transmitting or receiving data Off – Control LAN link down
1000 Base-T / SFP Combo Uplink ports	These four LEDs represent the connection status of each 1000BASE-T/SFP combo port, with LED 1 representing Uplink 1, LED 2 representing Uplink 2, LED 3 representing Uplink 3 and LED 4 representing Uplink 4. • Solid Green – Uplink up • Blinking Green – Uplink transmitting or receiving data. • Off – Uplink down

DPN-3012-E-01 4 port OLT modules

The DPN-3012-E supports up to three DPN-3012-E-01/ 4 port OLT modules. Each module provides 4 OLT ports for the DPN-3012-E/RU and complies with IEEE802.3ah standards.

The DPN-3012-E module has the following features:

- 4 SFF SC type OLT ports
- Fully compliant with IEEE 802.3ah
- Each OLT port supports up to 32 ONUs
- Single Mode Fiber cables
- Upstream (ONU→OLT) wavelength: 1310nm
- Downstream (OLT→ONU) wavelength: 1490nm
- Optical power budget: 28dB minimum
- Maximum distance: 20Km
- Four PON port active LEDs

DPN-3012-E-01/ 4 port OLT module Front Panel View

The front panel of the DPN-3012-E-01 / 4 port OLT module has four SFF SC type OLT ports and four PON port active LEDs.

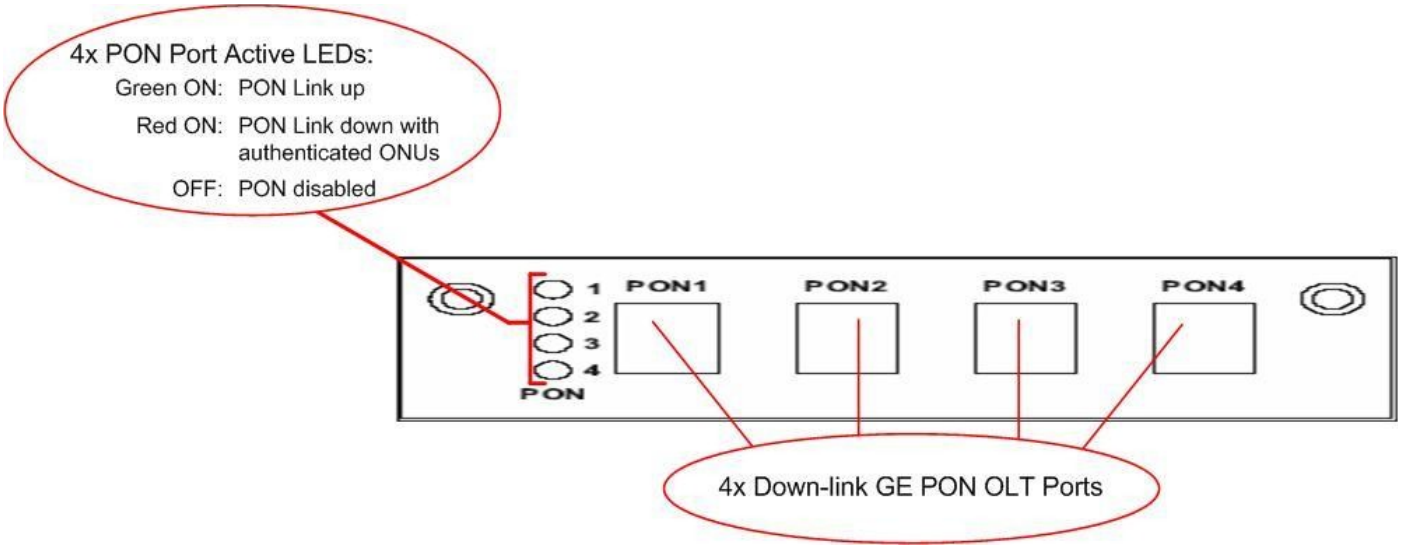


Figure 1- . Front Panel view of DPN-3012-E-01/ 4 port OLT module

SECTION 2

Installation

Package Contents

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

- One Stand-alone Switch
- One AC power cord
- This Manual on CD
- Mounting kit (two brackets and screws)
- RS-232 console cable

If any item is missing or damaged, please contact your local D-Link Reseller for replacement.

Before You Connect to the Network

The site where you install the Switch may greatly affect its performance. Please follow these guidelines for setting up the Switch.

- Install the Switch in a rack that can support at least 5.614kg of weight. Do not place heavy objects on the Switch.
- The power outlet should be within 1.82 meters (6 feet) of the Switch.
- Visually inspect the power cord and see that it is fully secured to the AC/DC power port.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation.
- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.

Installing the Switch in a Rack

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

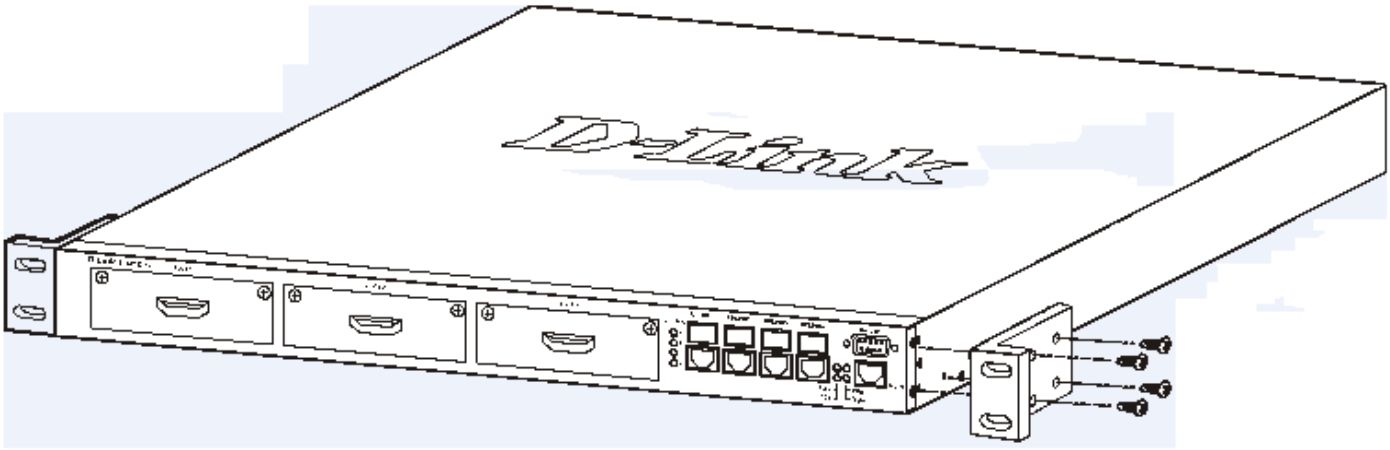


Figure 2- . Fasten mounting brackets to the DPN-3012-E RU

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figures 2-5 and 2-6 below.

Mounting the Switch in a Standard 19" Rack

CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing components in a rack, do not pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in injury.

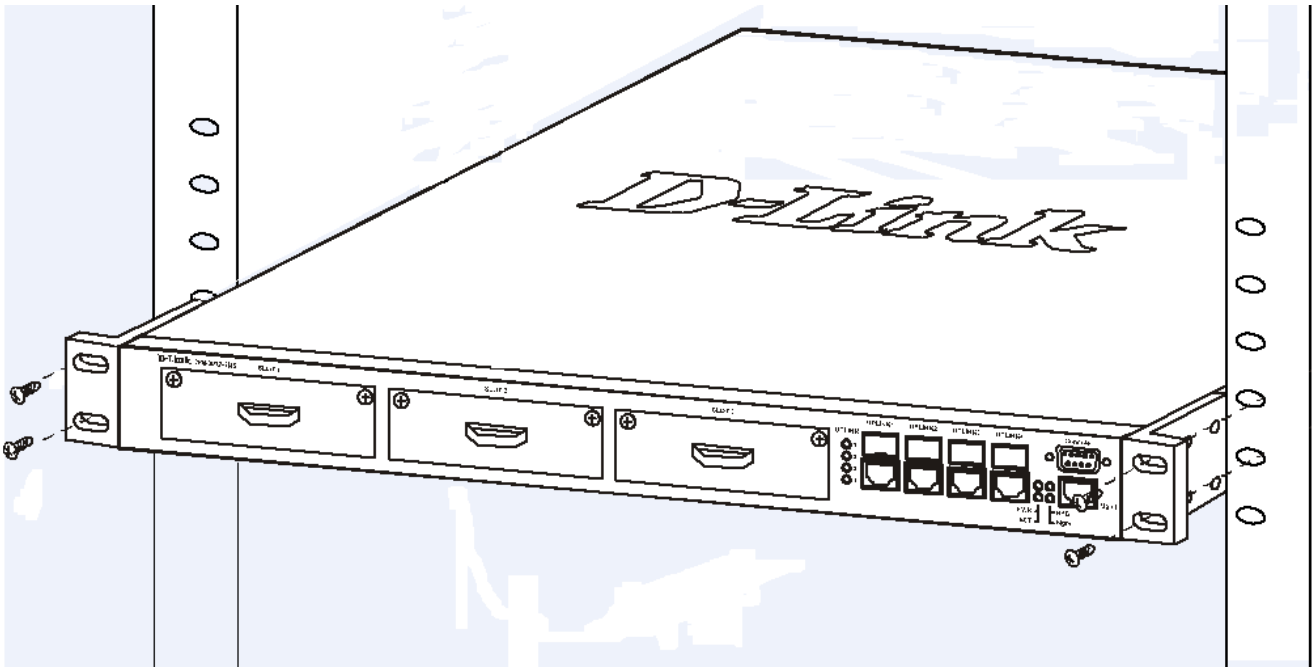


Figure 2- . Installing the DPN-3012-E RU in a rack

Power on AC Power

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet. Turn On the power switch on the back of the DPN-3021-E.

After the Switch is powered on, the Uplink LED indicators will illuminate momentarily, the OLT Equipment Status LED will flash green. When POST completes all LED's

Power Failure

For AC power supply units, as a precaution, in the event of a power failure, unplug the Switch. When power has resumed, plug the Switch back in.

RPS Installation

Follow the instructions below to connect an RPS power supply to the Switch. The DPS-500 is a redundant power-supply unit designed to conform to the voltage requirements of the switches being supported. The DPS-500 can be installed into a DPS-900, or DPS-800 rack mount unit.

CAUTION: The AC power cord for the Switch should be disconnected before proceeding with installation of the DPS-500.

DPS-900

The DPS-900 is a standard-size rack mount (5 standard units in height) designed to hold up to eight DPS-500 redundant power supplies.

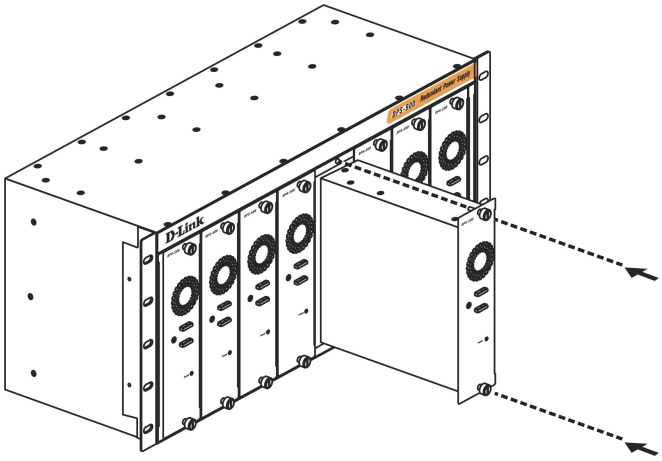


Figure 2- . Installing the DPS-500 into the DPS-900

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

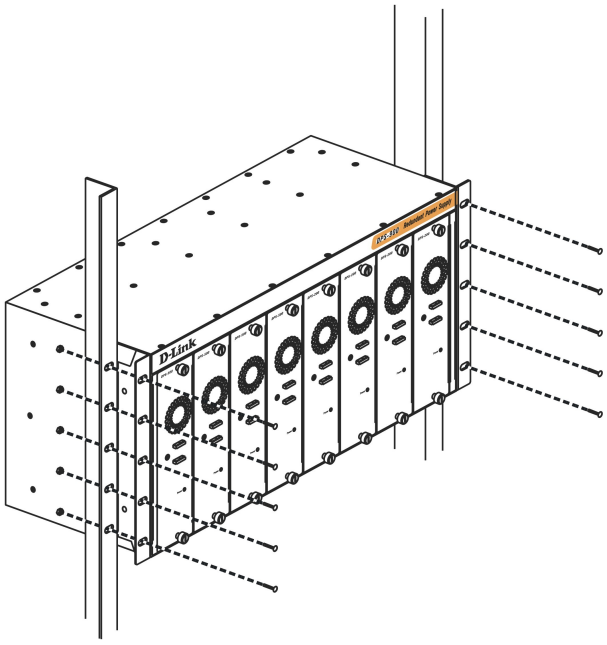


Figure 2- . Installing the DPS-900 into the equipment rack

CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing components in a rack, do not pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in injury.

DPS-800

The DPS-800 is a standard-size rack mount (1 standard unit in height) designed to hold up to two DPS-500 redundant power supplies.

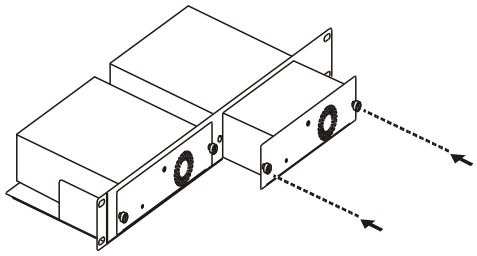


Figure 2- . Install DPS-500 in DPS-800

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

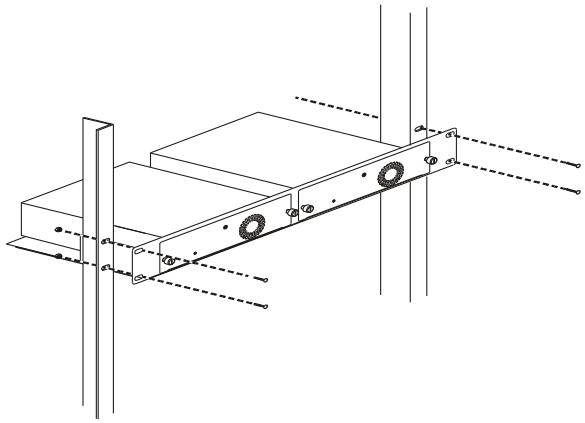


Figure 2- . Install DPS-800 in an Equipment Rack

Connect to RPS

The DPS-500 is connected to the Master Switch using a 14-pin DC power cable. A standard, three-pronged AC power cable connects the redundant power supply to the main power source.

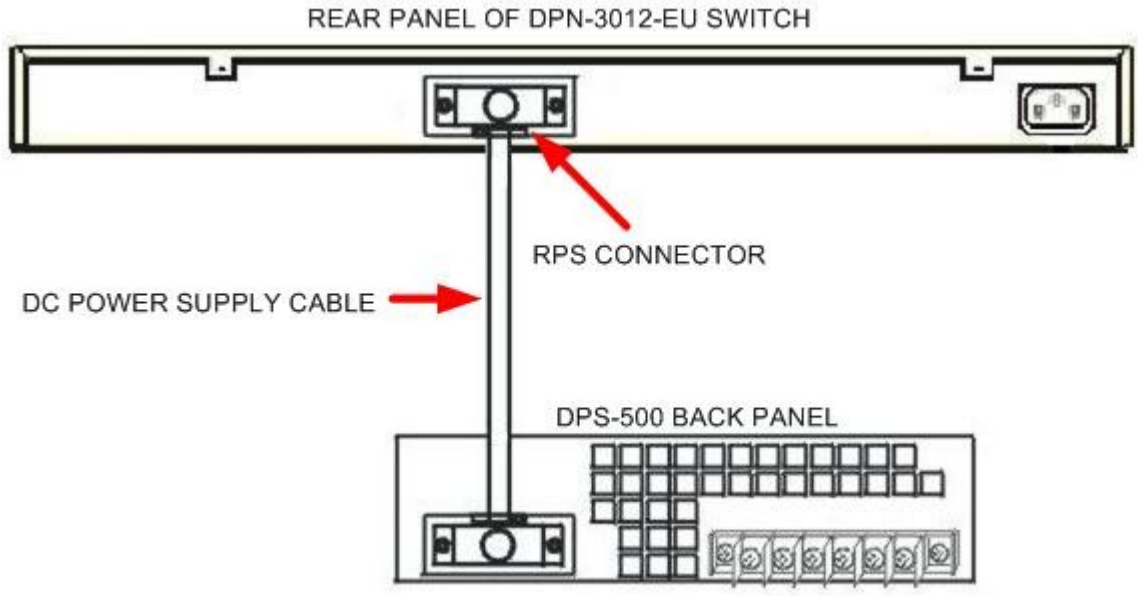


Figure 2- . DPN-3012-EU with the DPS-500 chassis RPS

1. Insert one end of the 14-pin DC power cable into the receptacle on the switch and the other end into the redundant power supply.
2. Using a standard AC power cable, connect the redundant power supply to the main AC power source. A green LED on the front of the DPS-200 will glow to indicate a successful connection.
3. Re-connect the switch to the AC power source. On certain switches, such as the DHS-3628/DHS-3628F, an LED indicator will show that a redundant power supply is now in operation.
4. No change in switch configuration is necessary for this installation.

NOTE: See the DPS-500 documentation for more information.

CAUTION: Do not use the Switch with any redundant power system other than the DPS-500.

Section 3

Connecting the Switch

GPON Topology

GPON Topology

The following diagram shows the DPN-3012-E RU connected to a typical GPON network.

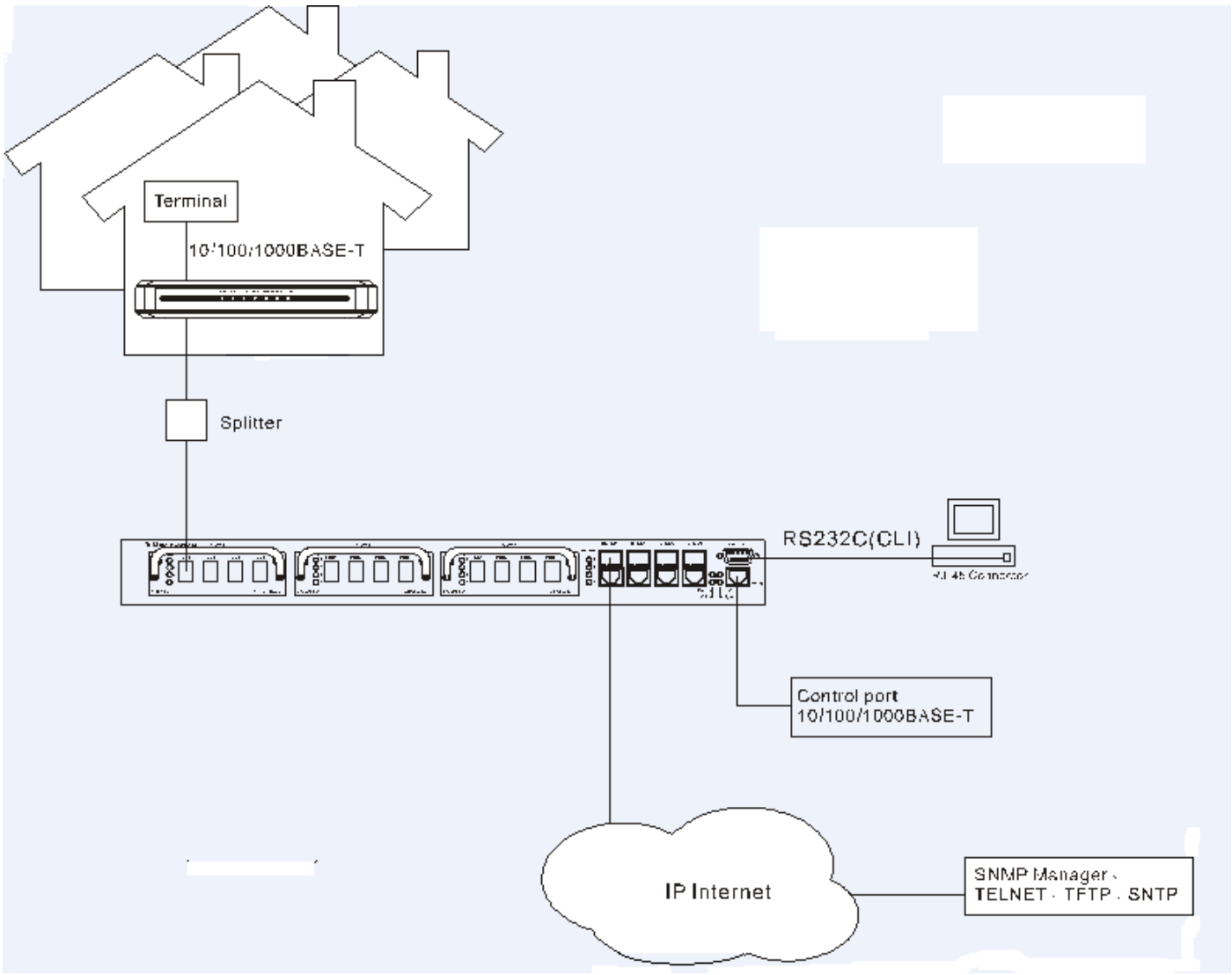


Figure 3- . DPN-3012-E RU connected to a GPON network

Section 4

Introduction to Switch Management

Management Options

This system may be managed out-of-band through the console port on the front panel or in-band using Telnet. The user may also choose the web-based management, accessible through a web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser, such as Netscape Navigator (version 6.2.3 and higher) or Microsoft® Internet Explorer (version 6.0 and higher).

SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1 and version 2c. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Connecting the Console Port (RS-232 DCE)

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a female DB-9 connector, implemented as a Data Terminal Equipment (DTE) connection.

To use the console port, you need the following equipment:

- A terminal or a computer with both a serial port and the ability to emulate a terminal.
- A null modem or straight-through RS-232 cable with a female DB-9 connector for the console port on the Switch.

To connect a terminal to the console port:

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
3. Select the appropriate serial port (COM port 1 or COM port 2).
4. Set the data rate to 115200 baud.
5. Set the data format to 8 data bits, 1 stop bit, and no parity.
6. Set flow control to none.
7. Under Properties, select VT100 for Emulation mode.
8. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that you select Terminal keys (not Windows keys).

NOTE: When you use HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 allows you to use arrow keys in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

9. After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
10. After the boot sequence completes, the console login screen displays.
11. If you have not logged into the command line interface (CLI) program, press the Enter key at the User name and password prompts. There is no default user name and password for the Switch. The administrator must first create user names and passwords. If you have previously set up user accounts, log in and continue to configure the Switch.
12. Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the ***DPN-3012-E GE-PON CLI Manual*** on the documentation CD for a list of all commands and additional information on using the CLI.
13. When you have completed your tasks, exit the session with the logout command or close the emulator program.
14. 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 PC, make sure the emulation is set to VT-100. You will be able to set the emulation by clicking on the **File** menu in you HyperTerminal window, clicking on **Properties** in the drop-down menu, and then clicking the **Settings** tab. This is where you will find the **Emulation** options. If you still do not see anything, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear on your console screen. This is where the user will enter commands to perform all the available management functions. The Switch will prompt the user to enter a user name and a password. Upon the initial connection, there is no user name or password and therefore just press enter twice to access the command line interface.

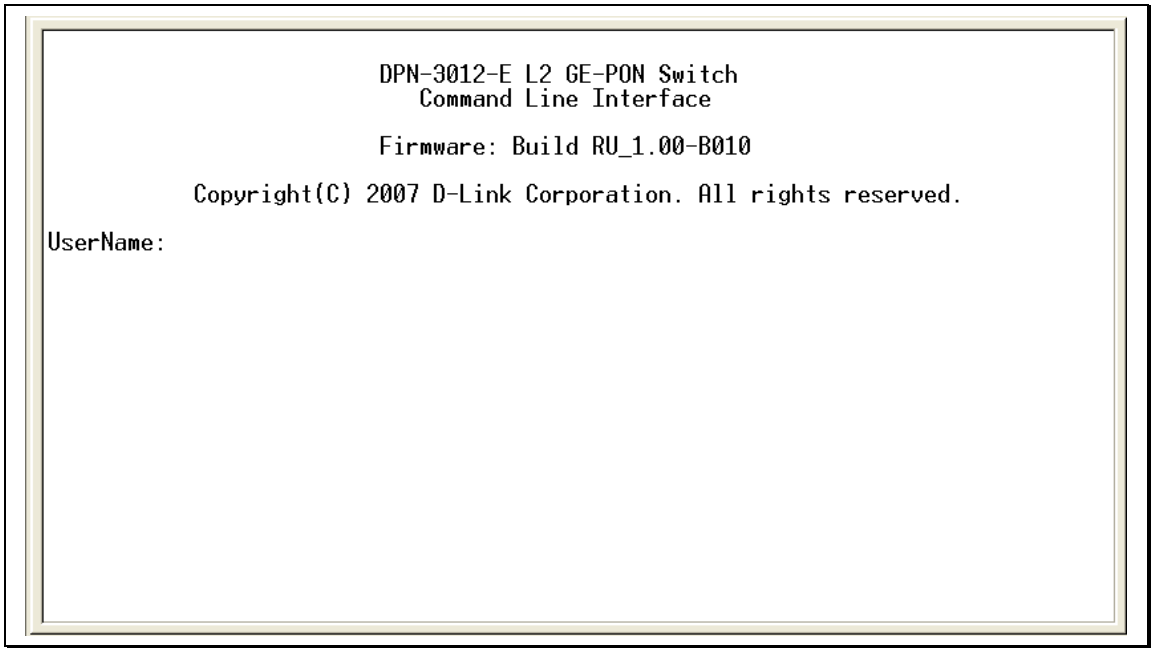


Figure 4- . Initial screen after first connection

First Time Connecting to the Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

NOTE: The passwords used to access the Switch are case-sensitive; therefore, "S" is not the same as "s."

When you first connect to the Switch, you will be presented with the first login screen.

NOTE: Press Ctrl+R to refresh the screen. This command can be used at any time to force the console program in the Switch to refresh the console screen.

Press **Enter** in both the Username and Password fields. You will be given access to the command prompt **DHS-3628GF:4#** shown below:

There is no initial username or password. Leave the Username and Password fields blank.

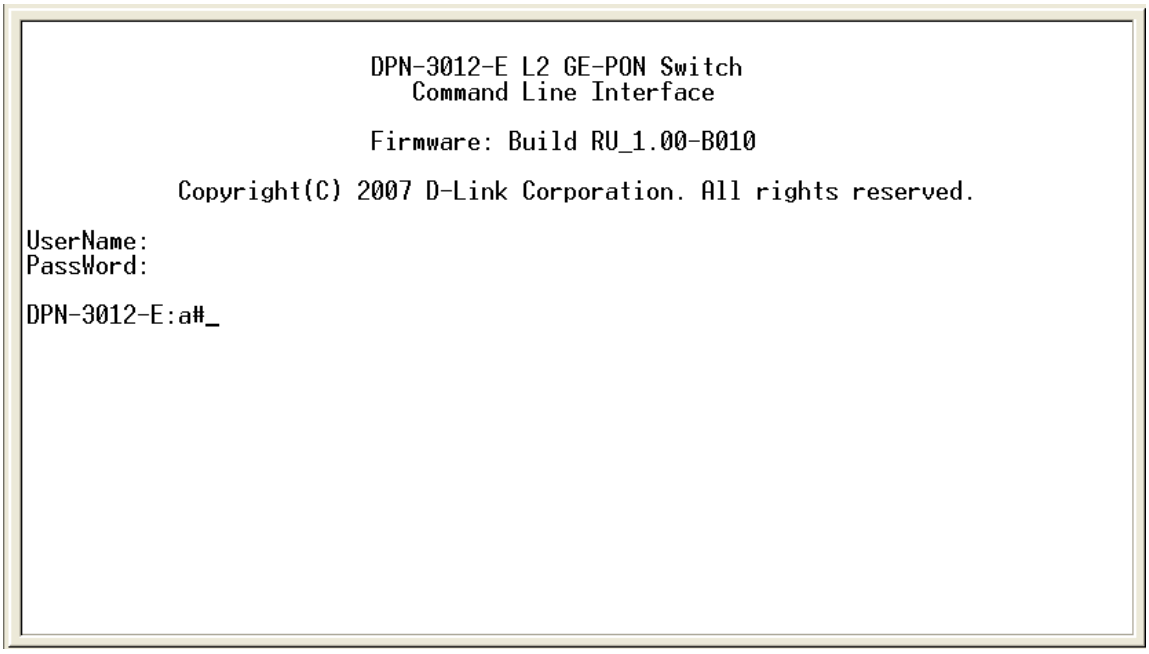


Figure 4- . Command prompt

NOTE: The first user automatically gets Administrator-level privileges. It is recommended to create at least one Admin-level user account for the Switch.

Password Protection

The Switch does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If you log in using a predefined administrator-level user name, you have privileged access to the Switch's management software.

After your initial login, define new passwords for both default user names to prevent unauthorized access to the Switch, and record the passwords for future reference.

To create an administrator-level account for the Switch, follow these steps:

- At the CLI login prompt, enter **create account admin** followed by the <*user name*> and press the Enter key.
- You will be asked to provide a password. Type the <*password*> used for the administrator account being created and press the Enter key.

- You will be prompted to enter the same password again to verify it. Type the same password and press the Enter key.
- Successful creation of the new administrator account will be verified by a Success message.

NOTE: Passwords are case sensitive. User names and passwords can be up to 15 characters in length.

The sample below illustrates a successful creation of a new administrator-level account with the user name "newmanager".

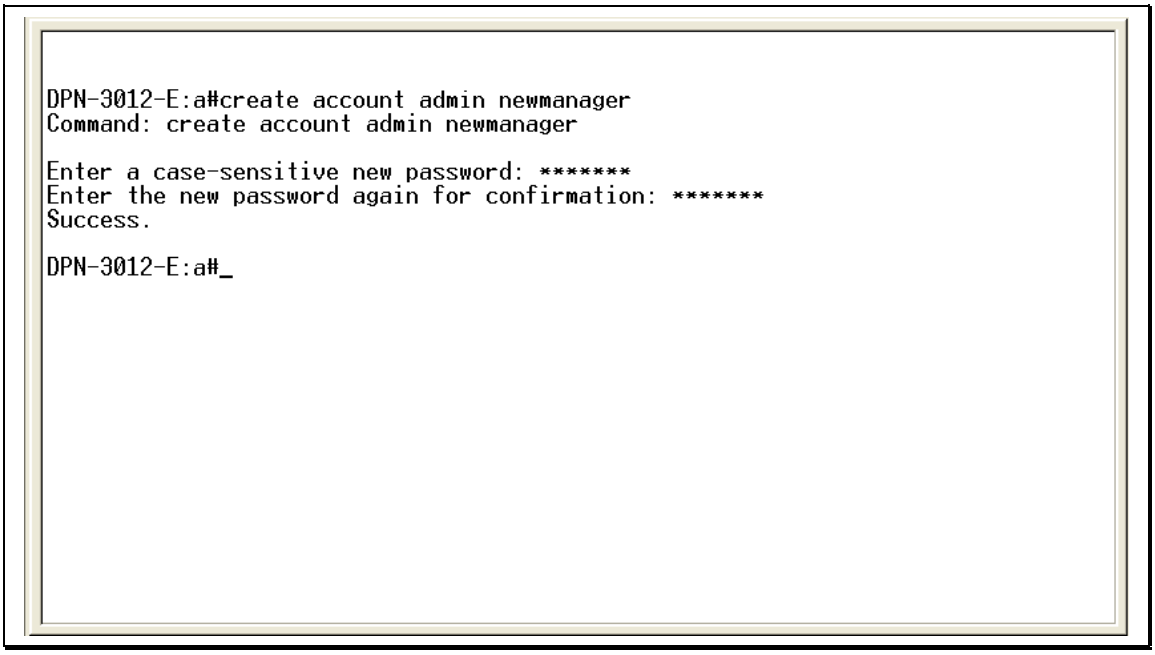


Figure 4- . Create account admin manager

NOTICE: CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all your configuration changes in nonvolatile storage, you must use the save command to copy the running configuration file to the startup configuration.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

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

The Switch supports SNMP versions 1 and 2c. You can specify which version of SNMP you want to use to monitor and control the Switch.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

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

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

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

IP Address Assignment

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 192.168.0.1. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "**show switch**" into the command line interface, as shown below:

```
DPN-3012-E:a#show switch
Command: show switch

Device Type       : DPN-3012-E
Module-1 Status   : Available
Module-2 Status   : Available
Module-3 Status   : Available
MAC Address       : 00-17-9A-0D-37-19
IP Address        : 192.168.0.1
VLAN Name         : default
Subnet Mask       : 255.255.255.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build RU_1.00-B003
Firmware Version  : Build RU_1.00-B010
Hardware Version  : A1
System Name       :
System Location   :
System Contact    :
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
Clipaging         : Enabled
Dual Image        : Supported
Last Reboot Status: ColdStart

DPN-3012-E:a#
```

Figure 4- . Show switch command

The Switch's MAC address can also be found from the Web management program on the **Device Information** window that appears after successfully logging onto the Switch.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands:

config ipif ipaddress *xxx.xxx.xxx.xxx* subnet_mask *yyy.yyy.yyy.yyy* gateway_address *zzz.zzz.zzz.zzz*

Where the x's represent the IP address to be assigned to the IP interface, the y's represent the corresponding subnet mask and the z's represent the default-gateway.

Once the Switch has been assigned an IP address, subnet mask and default-gateway it can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

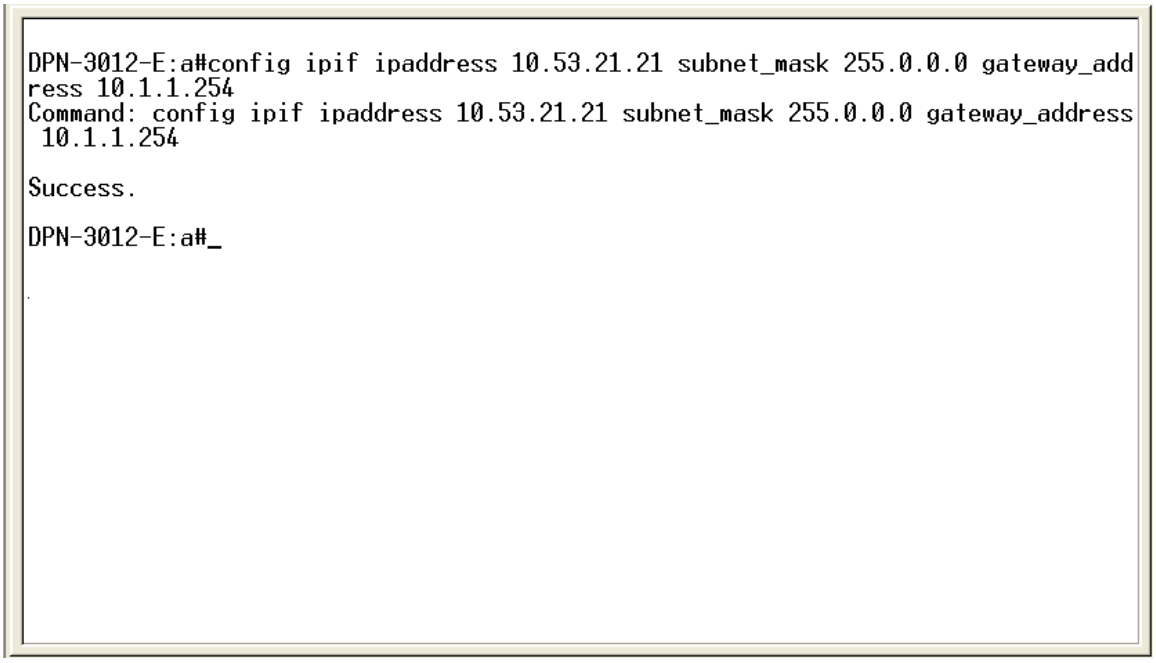


Figure 4- . Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.53.21.21 with a subnet mask of 255.0.0.0 and a default-gateway of 10.1.1.254. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

Section 5

Web-based Switch Configuration

Introduction

All software functions of the Switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Opera, Netscape Navigator/Communicator, or Microsoft Internet Explorer. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Login to Web Manager

To begin managing your Switch, simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the Switch.

NOTE: The Factory default IP address for the Switch is 192.168.0.1.

This opens the management module's user authentication window, as seen below.

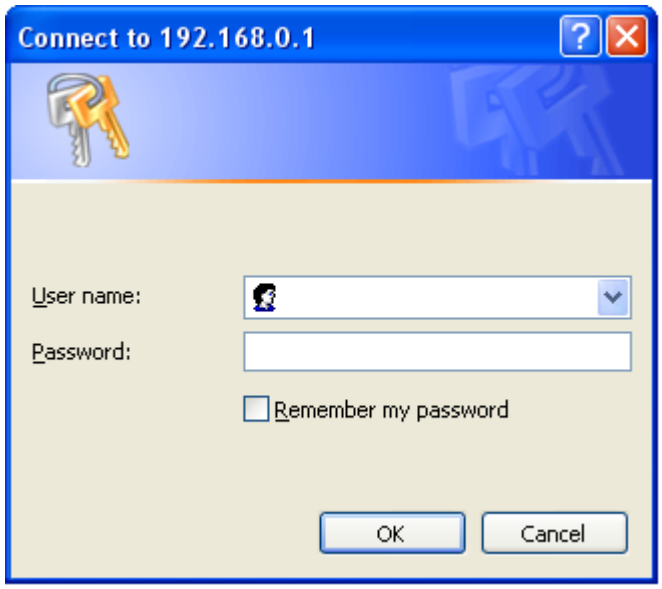


Figure 5- . Enter Network Password window

Leave both the User Name field and the Password field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into three distinct areas as described in the table.

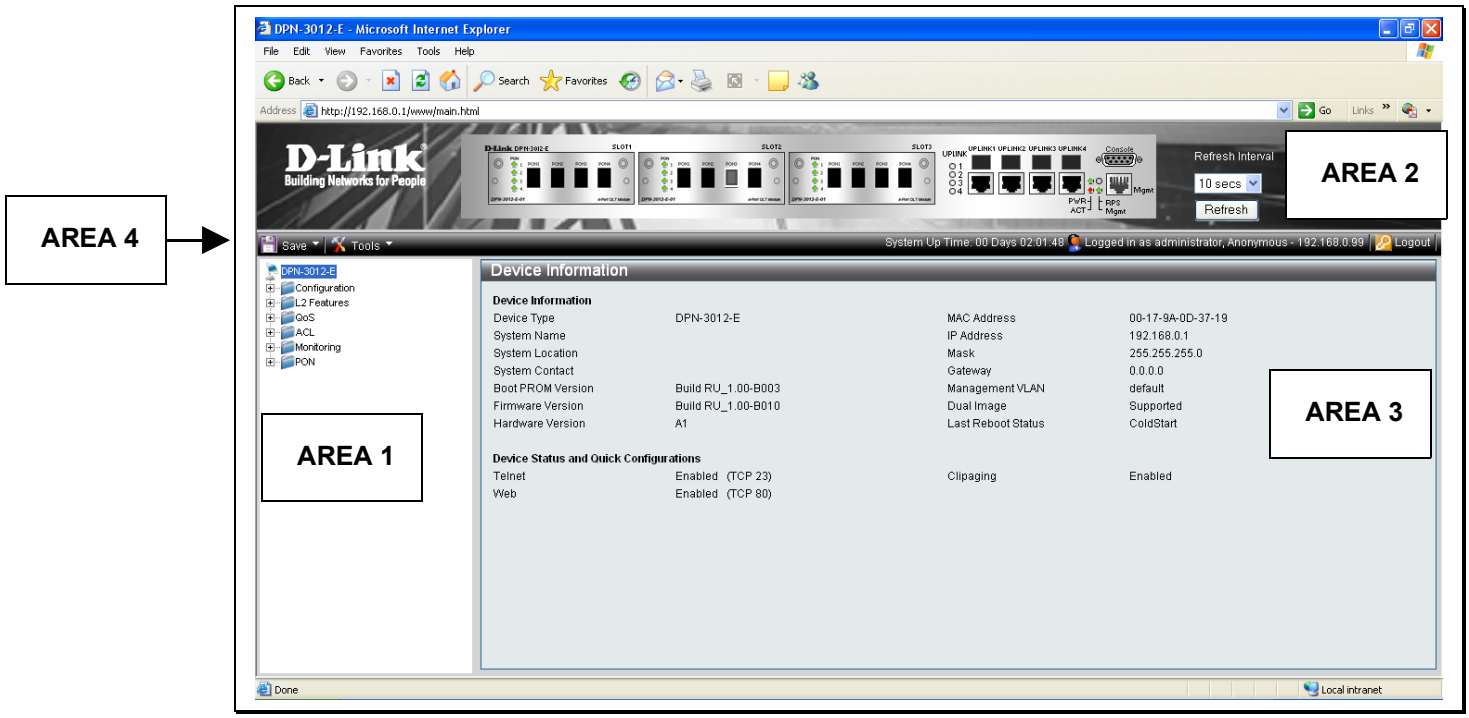


Figure 5- . Main Web-Manager page

Area	Function
Area 1	Select the window to be displayed. The folder icons can be opened to display the hyperlinked menu buttons and subfolders contained within them.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. Also includes a drop-down menu that allows you to set the Refresh Interval.
Area 3	Presents switch information based on your selection and the entry of configuration data.
Area 4	Select from the following options on the toolbar. Choose one of the following options from the **Save** drop-down menu: ▪ Click *Save Configuration ID 0* from the drop-down menu to save the current configuration to *Configuration ID 0* in the Switch's flash memory. ▪ Click *Save Configuration ID 1* from the drop-down menu to save the current configuration to *Configuration ID 1* in the Switch's flash memory. ▪ Click *Save Log* from the drop-down menu to save the *Log* to the Switch's flash memory. ▪ Click *Save All* from the drop-down menu to save the *Configuration ID 0*, *Configuration 1* and *Log* to the Switch's flash memory. Choose one of the following options from *Tools* drop-down menu *Configuration File Backup & Restore*, *Upload Log File*, *Reset*, *Download Firmware* and *Reboot System*. An explanation of how to carry use the **Tools** options, appears in the **Tools Menu** section.

NOTICE: Any changes made to the Switch configuration during the current session must be saved in the Save Changes web window (explained below) or use the command line interface (CLI) command save.

Tools Menu

The Tools Menu allows you to carry out the following functions:

- Configuration File Backup & Restore
- Upload Log File
- Reset
- Download Firmware
- Reboot System

Configuration File Backup & Restore

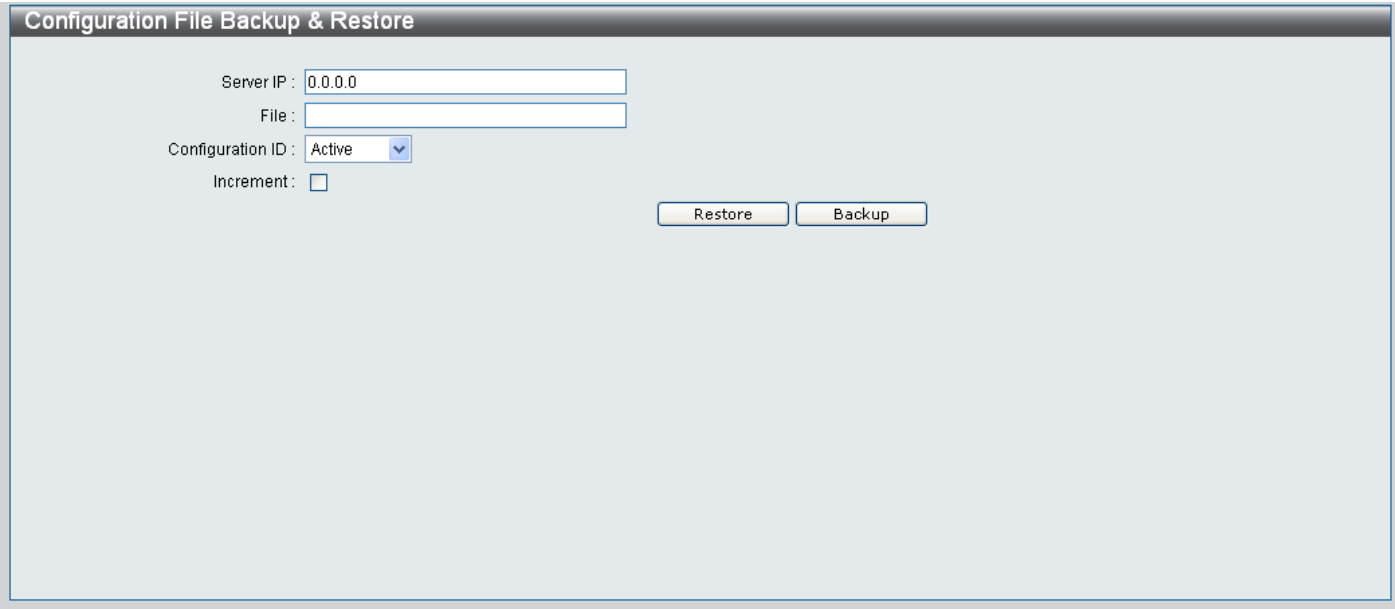


Figure 5- 3. Configuration File Backup & Restore page

Configure the parameters as explained below:

Parameter	Description
Server IP	Type the *TFTP IP Address* of the Server that you want the *Configuration File* backed up/restored to.
File	Type the *File Name* of the *Configuration File* you want to Backup or Restore.
Configuration ID	Use the drop-down menu to choose the *Image ID* that will be backed up/restored to. Choose *Active* to backup/restore the image to the active Image ID, choose *1* to backup/restore the image to *Configuration ID 1 and* choose *2* to backup/restore the configuration to *Configuration ID 2*.
Increment	Tick the checkbox to specify that the current configuration will not be cleared before applying the new configuration.

Restoring the Configuration File

To restore the configuration file, click the **Restore** button.

Backup the Configuration File

To backup the configuration file, click the **Backup** button.

Upload Log File

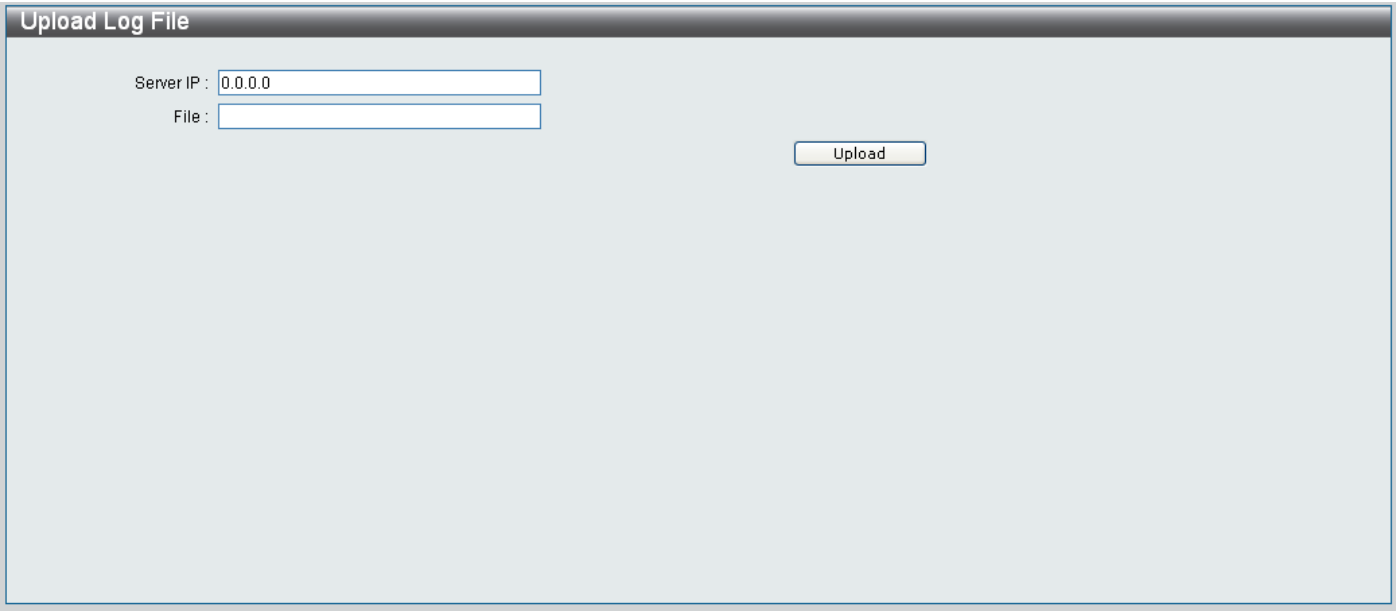


Figure 5- 4. Upload Log File page

Configure the parameters as explained below:

Parameter	Description
Server IP	Type the IP address of the TFTP Server you want to upload the log file to.
File	Type the filename that the log file will be saved as on the TFTP server.

Click the **Upload** button to start the upload.

Reset

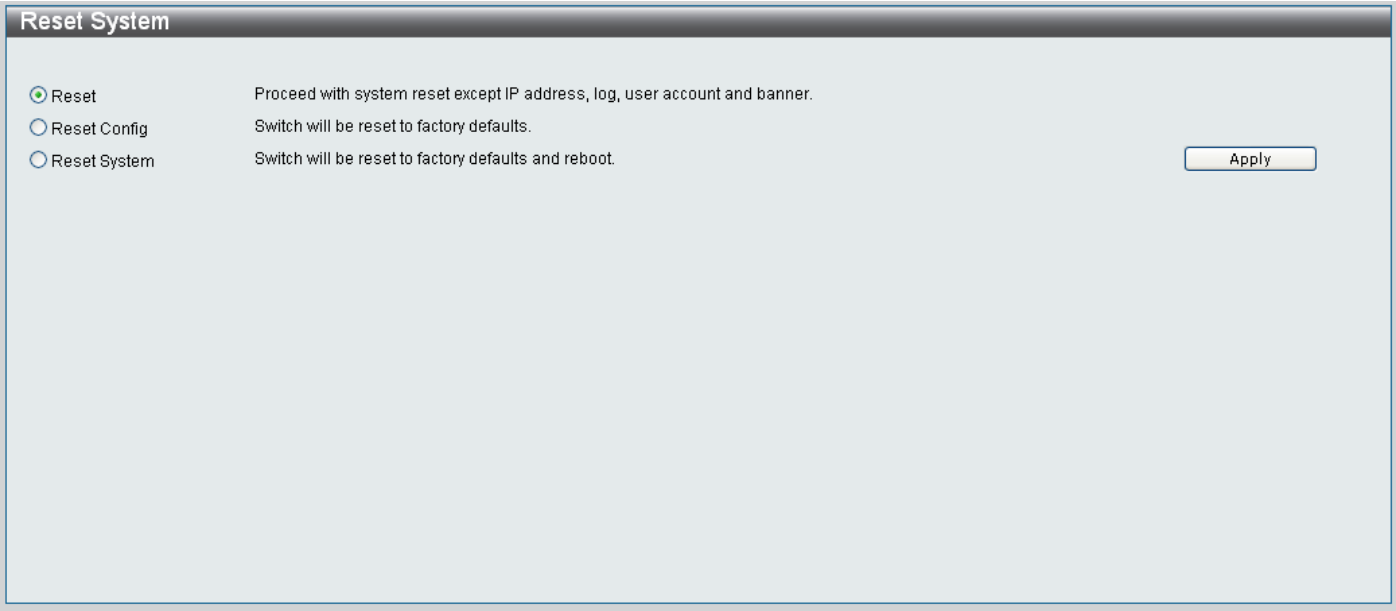


Figure 5- 5. Reset page

Configure the radio buttons as explained below:

Parameter	Description
Reset	Click the **Reset** radio button to reset the system configuration, with the exception of *IP Address, Log, User Account* and *Banner* information.
Reset Config	Click the **Reset Config** radio button to reset the system to factory defaults.
Reset System	Click the **Reset System** radio button to reset the system to factory defaults and reboot the Switch.

Click the **Apply** button to carry out the *Reset Method* specified.

Download Firmware

Use the **Download Firmware** menu to download a new Firmware image from a TFTP server.

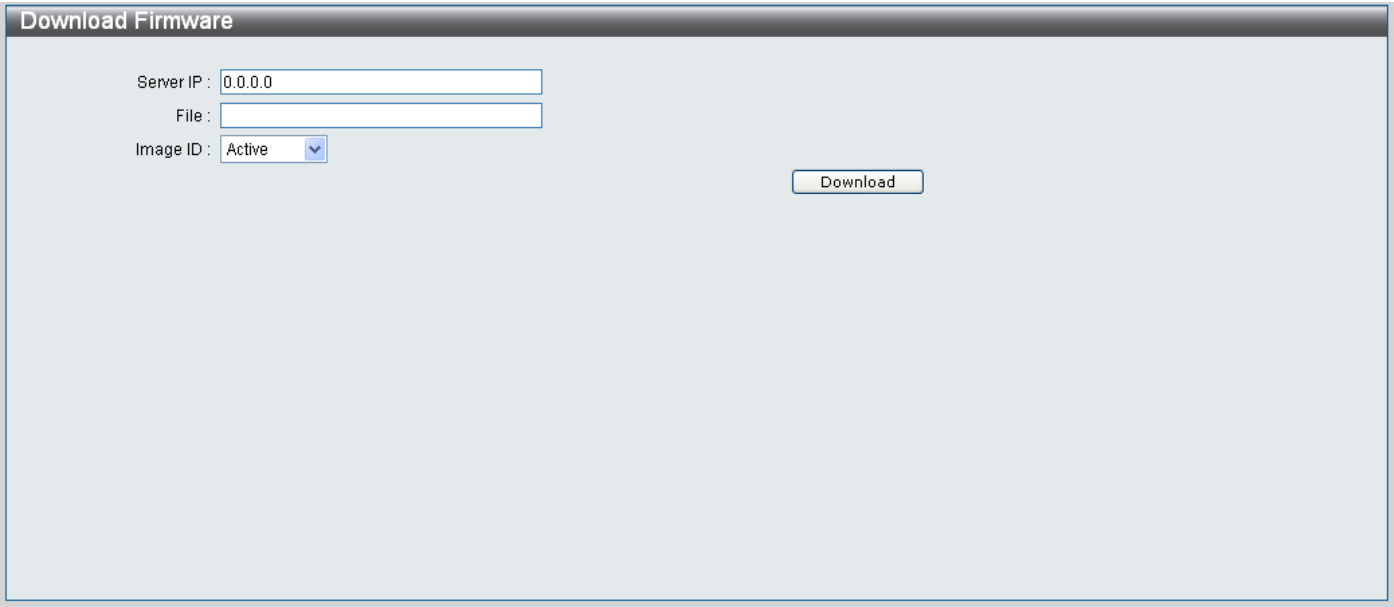


Figure 5- 6. Download Firmware page

Configure the parameters as explained below to download a new Firmware image:

Parameter	Description
Server IP	Type the IP address of the TFTP server that has the Firmware image you want to download.
File	Type the *file name* of the firmware file you want to download.
Image ID	Use the drop-down menu to choose which *Image ID* the downloaded *Firmware Image* will be written to. Choose *Active* to write the image to the active Image ID, choose *1* to write the image to *Configuration ID 1 and* choose *2* to write the configuration to *Configuration ID 2*.

Click the **Download** button start downloading the firmware image.

Reboot System

Use the **Reboot System** option to reboot the Switch.

- Click the **Yes** radio button to save the settings before restarting the Switch.
- Click the **No** radio button to restart the Switch, without saving the settings first.
- Click the **Reboot** button to reboot the Switch.

Figure 5- 7. Reboot System page

Web Pages

When you connect to the management mode of the Switch with a web browser, a login window is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list and description of the main folders available in the web interface:

Configuration – Contains windows concerning the configuration of the Switch, including Device Information, IP Address, Port Configuration, User Accounts, System Log Configurations, Web Settings, Telnet Settings, Clipaging Settings, Firmware Information, MAC Address Aging Time, Dual Configuration Settings, SNTP Settings and SNMP Settings.

Layer 2 Features – Contains windows concerning including 802.1Q VLAN, VLAN Ports Settings, QinQ, Port Trunking, LACP Port Settings, Traffic Segmentation, IGMP Snooping, Spanning Tree and Forwarding & Filtering.

QoS – Contains windows concerning Bandwidth Control, Traffic Control, 802.1p Default Priority, 802.1p User Priority and QoS Scheduling Mechanism

ACL – Contains the window for the ACL Configuration Wizard, Access Profile List and ACL Finder.

Monitoring – Contains windows for Device Status, CPU Utilization, Port Utilization, OLT Port Utilization, Packet Size, Packets, Errors, Browse ARP Table, Browse VLAN, Show VLAN Ports, Browse Session Table, IGMP Snooping Group and MAC Address Table.

PON – Contains windows for PON ONU firmware upgrade, ONU Information, Reboot OLT & ONU, OLT Port Settings, MAC Authentication, PON Bandwidth Control, ONU FEC Settings, ONU UNI Port Settings, ONU Encryption Settings, Diagnostic Test, ONU IGMP Snooping Settings, ONU IGMP Snooping Groups, OLT VLAN, ONU 802.1Q VLAN PVID Settings, ONU 802.1Q VLAN Settings, ONU Port Base VLAN Settings, P2P, OLT FDB Address Limitation, ONU MAC Address Table, Policing Queue Bandwidth Settings, Policing Queue Size Settings, ONU Default Filter Settings, ONU Classifier Filter Settings, ONU Default VLAN Rule Settings, ONU VLAN Rule Settings, ONU Priority Map Settings and PON Profile Settings.

NOTE: Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Section 6

Configuration

Device Information

IP Address

Port Configuration

User Accounts

System Log Configurations

Web Settings

Telnet Settings

Clipaging Settings

Firmware Information

MAC Address Aging Time

Dual Configuration Settings

SNTP Settings

SNMP Settings

Device Information

The **Device Information** displays the main settings for all major functions for the Switch and appears automatically when you log on. To return to the **Device Information** window, click the **DPN-3012-E** icon (the first item on the Web Manager's menu).

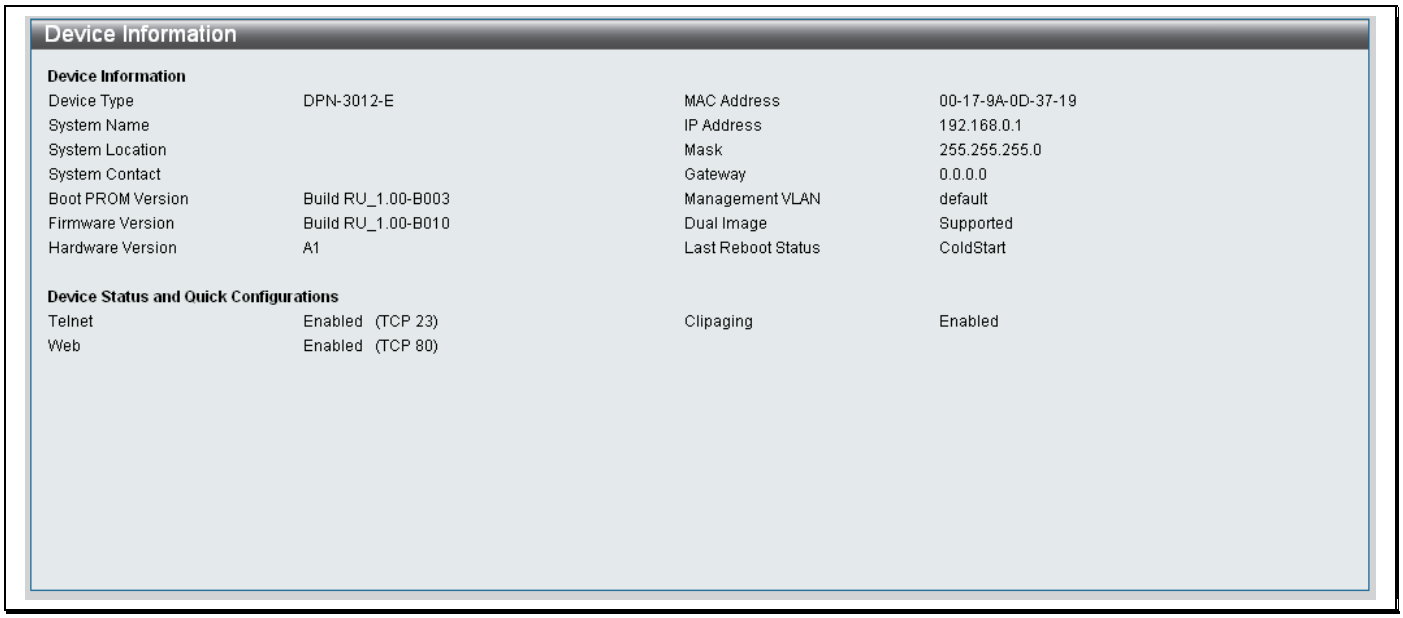


Figure 6- . Device Information window

The **Device Information** window is divided into two main sections, *Device Information* and *Device Status and Quick Configurations*.

Descriptions for each of the items displayed on the *Device Information* section are explained below:

Parameter	Description
Device Type	Displays the model name of the device.
System Name	Displays the System Name set in the SNMP configuration.
System Location	Displays the System Location set in the SNMP configuration.
System Contact	Displays the System Contact set in the SNMP configuration.
Boot PROM Version	Displays the Boot PROM Version loaded onto the Device.
Firmware Version	Displays the Firmware Version loaded onto the Device.
Hardware Version	Displays the Hardware Version of the Device.
MAC Address	Displays the MAC Address of the Device.
IP Address	Displays the IP Address configured on the Device.
Mask	Displays the Subnet Mask configured on the Device.
Gateway	Displays the Default Gateway configured on the Device.
Management VLAN	Displays the name of the Management VLAN configured on the Device.
Dual Image	Displays if the Switch supports two separate Firmware images concurrently.
Last Reboot Status	Displays the last time the Switch was rebooted.

Descriptions for each of the items displayed on the *Device Status and Quick Configuration* section are explained below:

Parameter	Description
Telnet	Displays the status of the Telnet Interface and the port number used to access the interface.
Web	Displays the status of the Web Interface and the port number used to access the interface.
Clipaging	Displays the Clipaging Status.

IP Address

The IP Address of the Switch can be changed through the CLI or the Web Interface. To change IP settings using the web manager you must access the IP Address menu located in the Administration folder.

To configure the Switch's IP address:

Click the **Configuration** > **IP Address** menu link. The web manager will display the Switch's current IP settings in the IP configuration menu, as seen below.

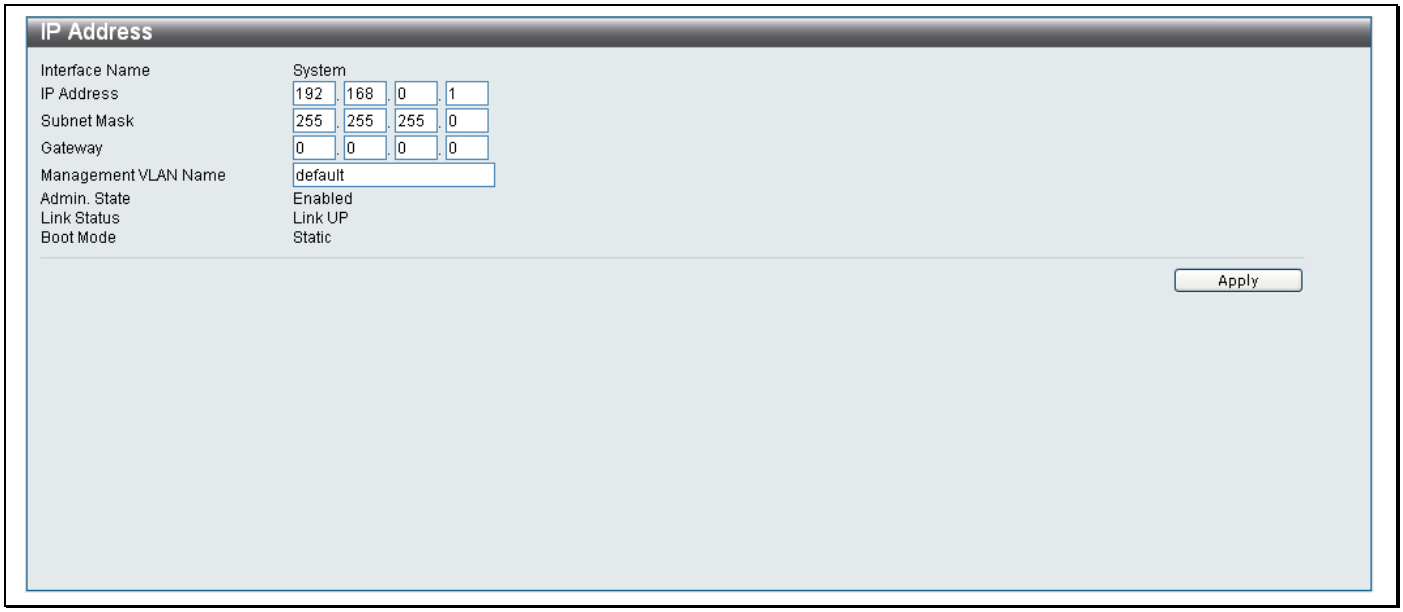


Figure 6- . IP Address window

To configure the Switch's IP address, subnet mask, and default gateway address:

1. Enter the appropriate IP Address and Subnet Mask.
2. If you want to access the Switch from a different subnet from the one it is installed on, enter the IP address of the Default Gateway. If you will manage the Switch from the subnet on which it is installed, you can leave the default address (0.0.0.0) in this field.
3. If no VLANs have been previously configured on the Switch, you can use the *default* Management VLAN Name. The *default VLAN* contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, you will need to enter the *VLAN ID* of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.

NOTE: The Switch's factory default IP address is 192.168.0.1 with a subnet mask of 255.255.255.0 and a default gateway of 0.0.0.0.

The following parameters appear in the IP Address window:

Parameter	Description
Interface Name	Displays the name of the Interface that the IP address is being configured on.
IP Address	The Switch is configured with an IP address of 192.168.0.1 by default. Type the IP address you want to assign to the interface in the textboxes.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Default Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gate-

	way. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
Management VLAN Name	This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management menu. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned.
Admin. State	This field displays the status of the IP Interface. The IP Interface can not be disabled by an administrator.
Link Status	This field displays the link status of the IP interface.
Boot Mode	Static indicates that the Switch only supports Static IP address configuration.

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

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager of other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 192.168.0.1. You can change the default Switch IP address to meet the specification of your networking address scheme.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the following command:

`config ipif ipaddress` ***`xxx.xxx.xxx.xxx`*** **`subnet_mask`** ***`yyy.yyy.yyy.yyy`*** **`gateway_address`** ***`zzz.zzz.zzz.zzz`***

Where the x's represent the IP address to be assigned to the interface and y's represent the corresponding subnet mask.

The IP address and subnet mask set on the Switch can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

Serial Port Settings

Use the **Serial Port Settings** window to change the amount of time a serial connection console session needs to be idle before the Switch automatically logs out the serial connection.

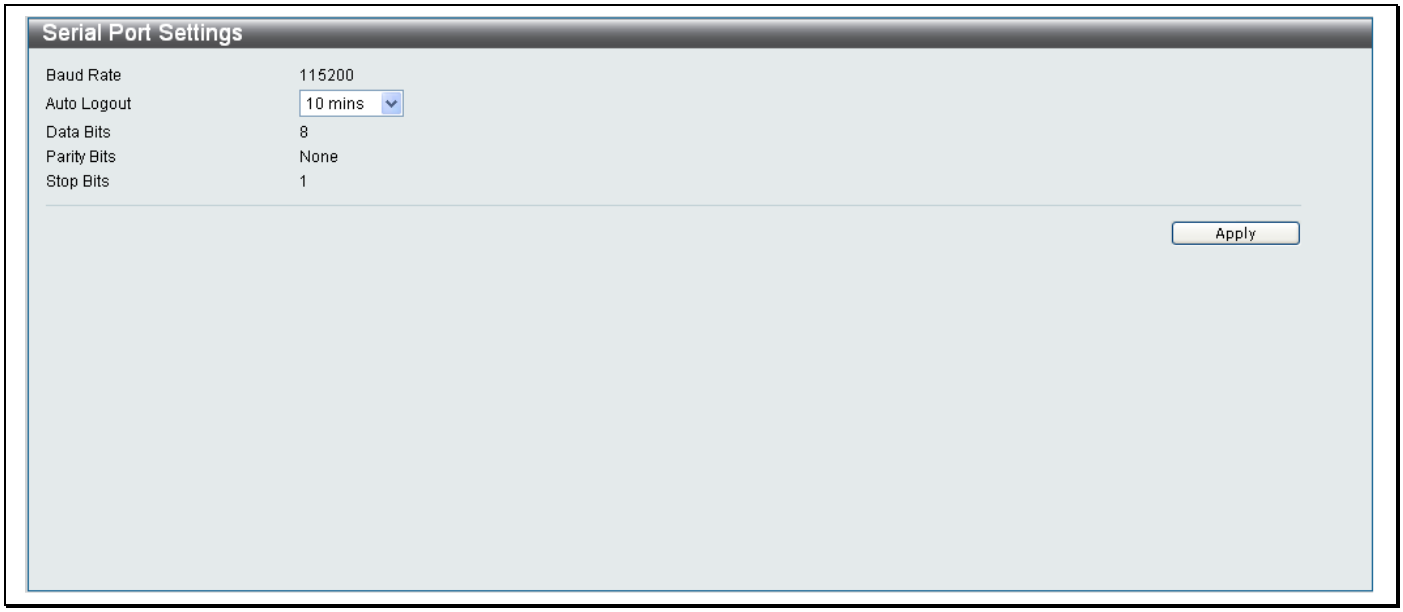


Figure 6- . Serial Port Settings window

The following parameters are displayed in this window:

Parameter	Description
Baud Rate	Displays the Baud Rate of the Serial Port.
Auto Logout	Use the drop-down menu to change the amount of time a serial connection console session needs to be idle before the Switch automatically logs out the serial connection.
Data Bits	Displays the Data Bits of the Serial Port.
Parity Bits	Displays the Parity Bits of the Serial Port.
Stop Bits	Displays the Stop Bits of the Serial Port.

Click **Apply** to implement the new settings on the Switch.

Port Settings

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and flow control.

Click **Configuration > Port Settings** to display the following window:

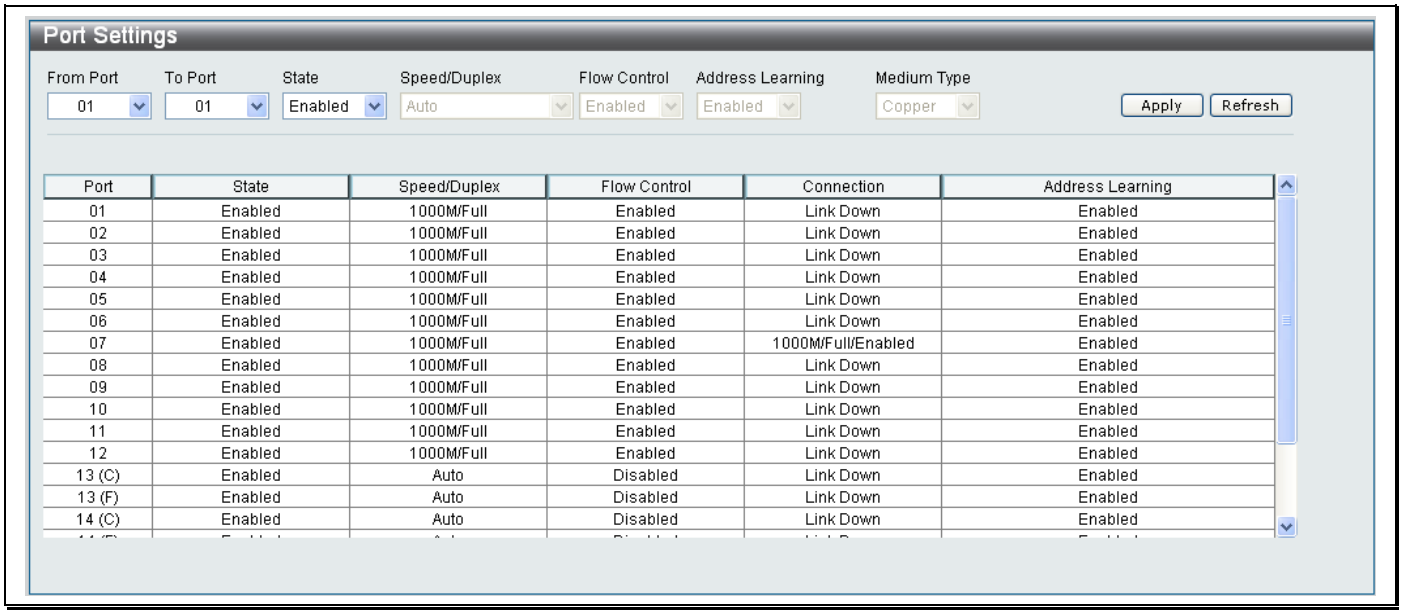


Figure 6- 4. Port Settings window

To configure switch ports:

1. Choose the port or sequential range of ports using the **From Port / To Port** drop-down menus.
2. Use the remaining drop-down menus to configure the parameters as described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to select the port or range of ports to be configured.
State	Toggle this field to either enable or disable a given port or group of ports.
Speed/Duplex	Toggle the **Speed/Duplex** field to either select the speed and full-duplex/half-duplex state of the port. The available options are *Auto*, *10M Half*, *10M Full*, *100M Half*, *100M Full*, *1000M Full_Master*, *1000M Full_Slave* and *1000M Full.* There is no automatic adjustment of port settings with any option other than Auto. *Auto*- This denotes auto-negotiation between 10 and 100 Mbps devices, in full-duplex or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. *10M Half*- This parameter specifies that the port will be operate at 10 Mbps Half-duplex *10M Full*- This parameter specifies that the port will be operate at 10 Mbps Full-duplex *100M Half*- This parameter specifies that the port will operate at 100 Mbps Half-duplex *100M Full*- This parameter specifies that the port will operate at 100 Mbps Full-duplex *1000M Full_Master*- This parameter allows the port to advertise capabilities related to duplex, speed and physical layer type. The 1000M Full_Master option determines that the port has a 1000 Mps master relationship with the gigabit port at the other end of the link. This relationship is necessary for establishing the timing control between the two physical layers. On a master physical layer the timing control is set by a local source. *1000M Full_Slave*- This parameter allows the port to advertise capabilities related to duplex,

	speed and physical layer type. The 1000M Full_Slave option determines that the port has a 1000 Mps slave relationship with the gigabit port at the other end of the link. This relationship is necessary for establishing the timing control between the two physical layers. The slave physical layer uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for *1000M Full_Master,* the other side of the connection must be set for *1000M Full_Slave*. Any other configuration will result in a link down status for both ports. *1000M Full*- Choose this parameter to automatically determine if the port should operate as a 1000 Mbps Full Slave or 1000 Mbps Full Master connection, in order for this to work the other end of the link must be set to automatically determine if the other end is operating at 1000 Mbps Full Slave or 1000 Mbps Full Master.
Flow Control	Use the drop-down menu to set the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control and *Auto* ports use an automatically choose from the two settings. The default is *Disabled*.
Address Learning	Use the drop-down menu to specify if MAC address learning for the selected ports should be *Enabled* or *Disabled*. 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 security or efficiency. The default setting is *Disabled*.
Medium Type	Choose *Copper* to configure the copper combo port connection. Choose *Fiber* to configure the fiber combo port connection.

Click **Apply** to implement the new settings on the Switch.

User Accounts

Use the **User Accounts** window to create new user accounts and control user privileges. The Switch supports up to 10 User Accounts, which can have different Access Right levels: *Admin*, *Operator* or *User*.

To view existing User Accounts, open the **Configuration** folder and click on the **User Accounts** link. This will open the User Accounts window, as shown below:

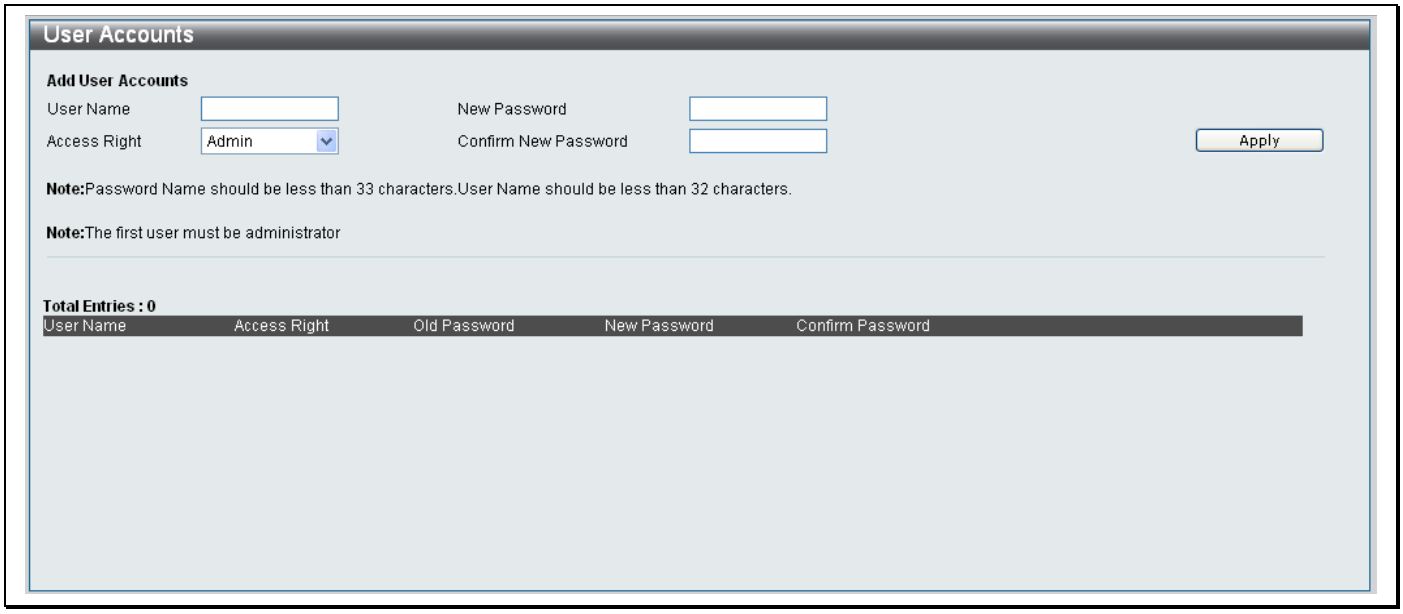


Figure 6- 5.User Accounts window

The following parameters are displayed:

Parameter	Description
User Name	Type in a User Name for the new account. User Name's can be between 1 and 32 characters.
Access Right	Choose if the new user should have *Admin*, *Operator* or *User* privileges from the drop-down menu.
New Password	Type in a password for the new user. The password should be no more than 32 characters and spaces can't be used.
Confirm New Password	Re-type the password for the new user.

Click **Apply** to add the new User Account to the Switch.

System Log Configuration

System Log Settings

To configure the level of System Log messages that the Switch will send to a SYSLOG Server , click **Configuration** > **System Log Configuration** > **System Log Settings**, to reveal the following window:

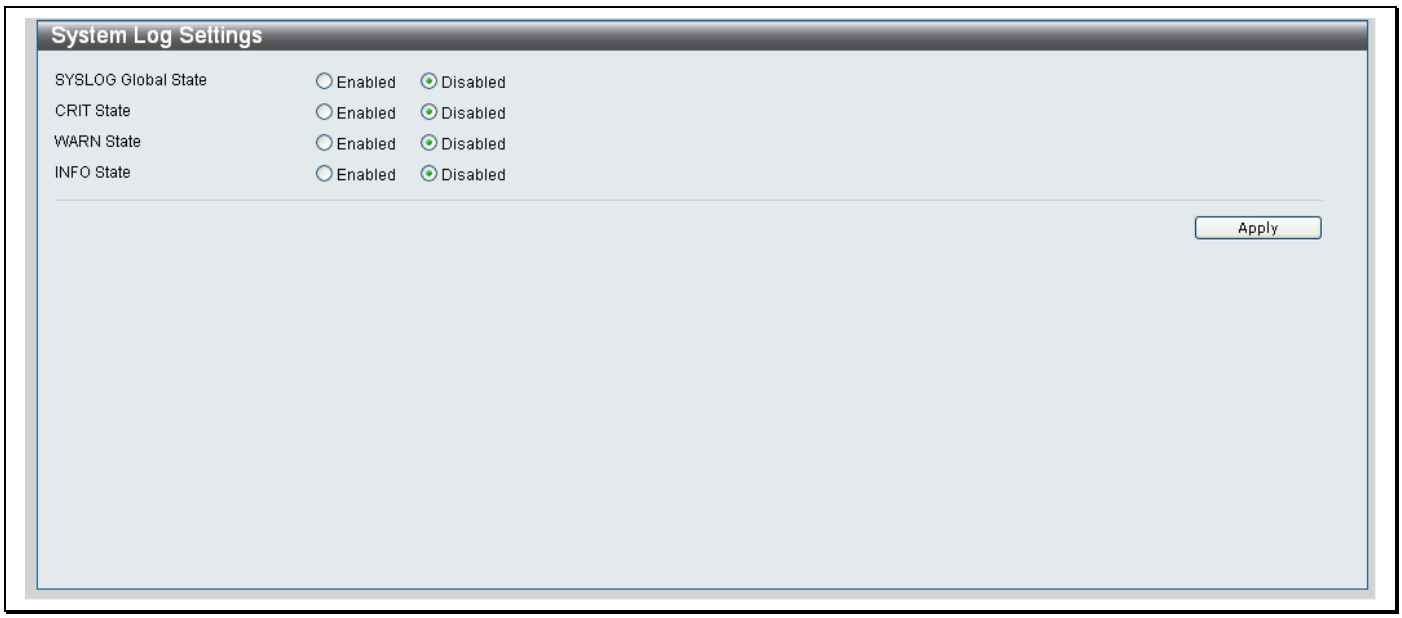


Figure 6- 6.System Log Settings window

The following parameters are displayed:

Parameter	Description
SYSLOG Global State	Click the **Enabled** radio button to enable all SYSLOG Messages.
CRIT State	Click the **Enabled** radio button to enable Critical Level SYSLOG Messages.
WARN State	Click the **Enabled** radio button to enable Warning Level SYSLOG Messages.
INFO State	Click the **Enabled** radio button to enable Informational Level SYSLOG Messages.

Click **Apply** to implement the new Syslog settings on the Switch.

System Log Host

The Switch supports up to five System Log Hosts. To add and configure the System Log Hosts for the Switch, click **Configuration** > **System Log Configuration** > **System Log Host**, to reveal the following window:

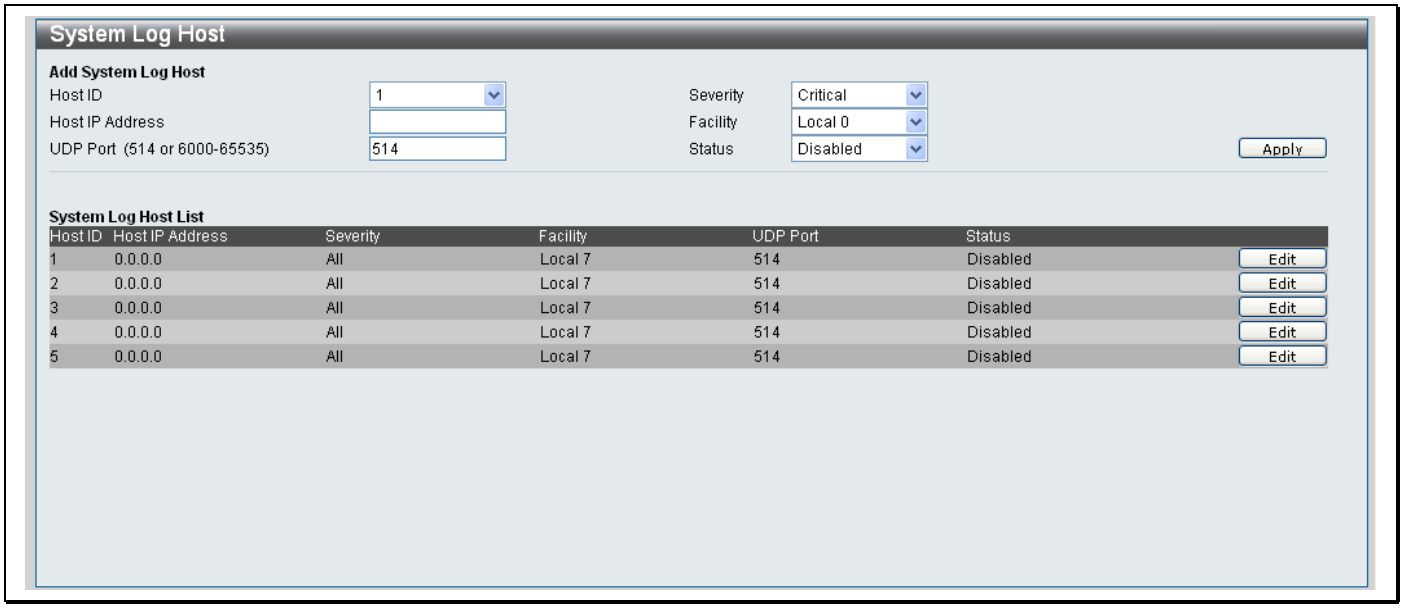


Figure 6- 7.System Log Host window

The following parameters are displayed:

Parameter	Description
Host ID	Choose the index number of the Syslog Server from the drop-down menu.
Host IP Address	Type in the IP address of the Syslog Server.
Severity	Use the drop-down menu to select the level of messages that will be sent. The options are *Critical*, *Warning*, *Informational* and *All*.

Facility

Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility.

The following list shows all the facility values that have been designated, the numerical codes in Bold font are facility values that the Switch currently supports:

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	**local use 0 (local0)**
17	**local use 1 (local1)**
18	**local use 2 (local 2)**
19	**local use 3 (local 3)**
20	**local use 4 (local 4)**
21	**local use 5 (local 5)**
22	**local use 6 (local 6)**
23	**local use 7 (local 7)**

Use the **Facility** drop-down menu to choose one of the following supported facility values:

	local0 – Specifies that local use 0 messages will be sent to the remote host. This corresponds to number 16 from the list above. *local1* – Specifies that local use 1 messages will be sent to the remote host. This corresponds to number 17 from the list above. *local2* – Specifies that local use 2 messages will be sent to the remote host. This corresponds to number 18 from the list above. *local3* – Specifies that local use 3 messages will be sent to the remote host. This corresponds to number 19 from the list above. *local4* – Specifies that local use 4 messages will be sent to the remote host. This corresponds to number 20 from the list above. *local5* – Specifies that local use 5 messages will be sent to the remote host. This corresponds to number 21 from the list above. *local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above.
UDP Port	Type in the UDP Port number used for sending Syslog messages. The default is 514.
Status	Choose *Enabled* or *Disabled* from the drop-down menu to activate or deactivate the Syslog host.

Click **Apply** to add the new Syslog host.

Web Settings

To configure the Web Settings for the Switch, click **Configuration** > **Web Settings** to reveal the following window:

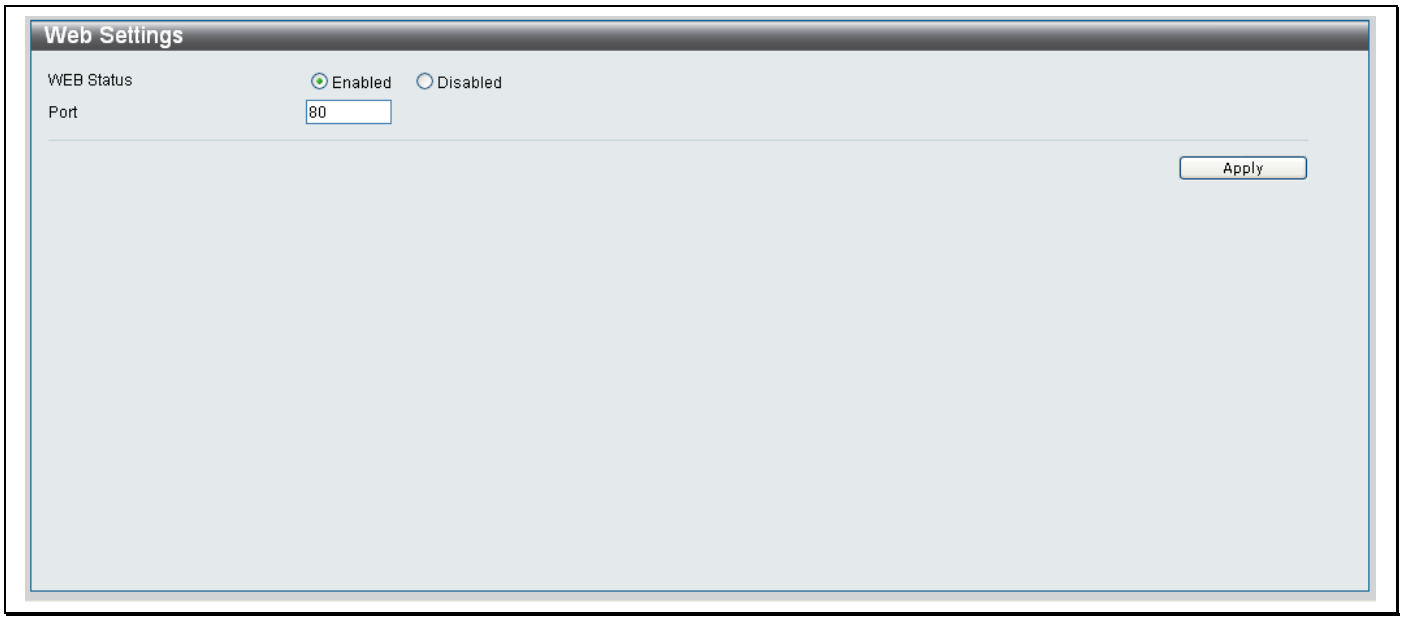


Figure 6- 8.Web Settings window

The following parameters are displayed:

Parameter	Description
WEB Status	Click the **Enabled** radio button to enable the Web Interface. Click the **Disabled** radio button to disable the Web Interface.
Port	Type in the port number that will be used to access the Web Interface. The default is 80.

Click **Apply** to implement the new settings on the Switch.

Telnet Settings

To configure the Telnet Settings for the Switch, click **Configuration** > **Telnet Settings** to reveal the following window:

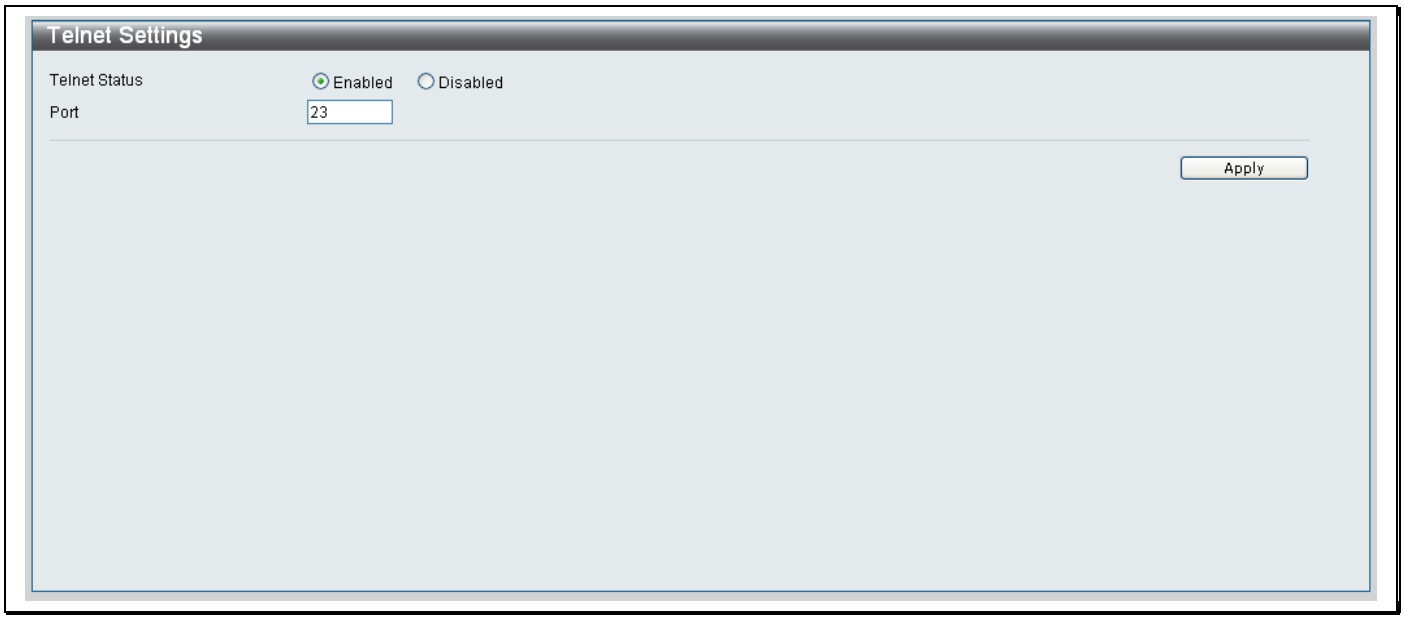


Figure 6- 9. Telnet Settings window

The following parameters are displayed:

Parameter	Description
TELNET Status	Click the **Enabled** radio button to enable Telnet connections to the Switch. Click the **Disabled** radio button to disable Telnet connections.
Port	Type in the port number that will be used to access the Telnet Interface. The default is 23.

Click **Apply** to implement the new settings on the Switch.

Clipaging Settings

The **Clipaging Settings** window is used to enable or disable the function in the Command Line Interface (CLI) that pauses the scrolling of the console screen when an issued **show** command displays more than one page. The default setting is enabled.

To configure the Clipaging Settings for the Switch, click **Configuration** > **Clipaging Settings** to reveal the following window:

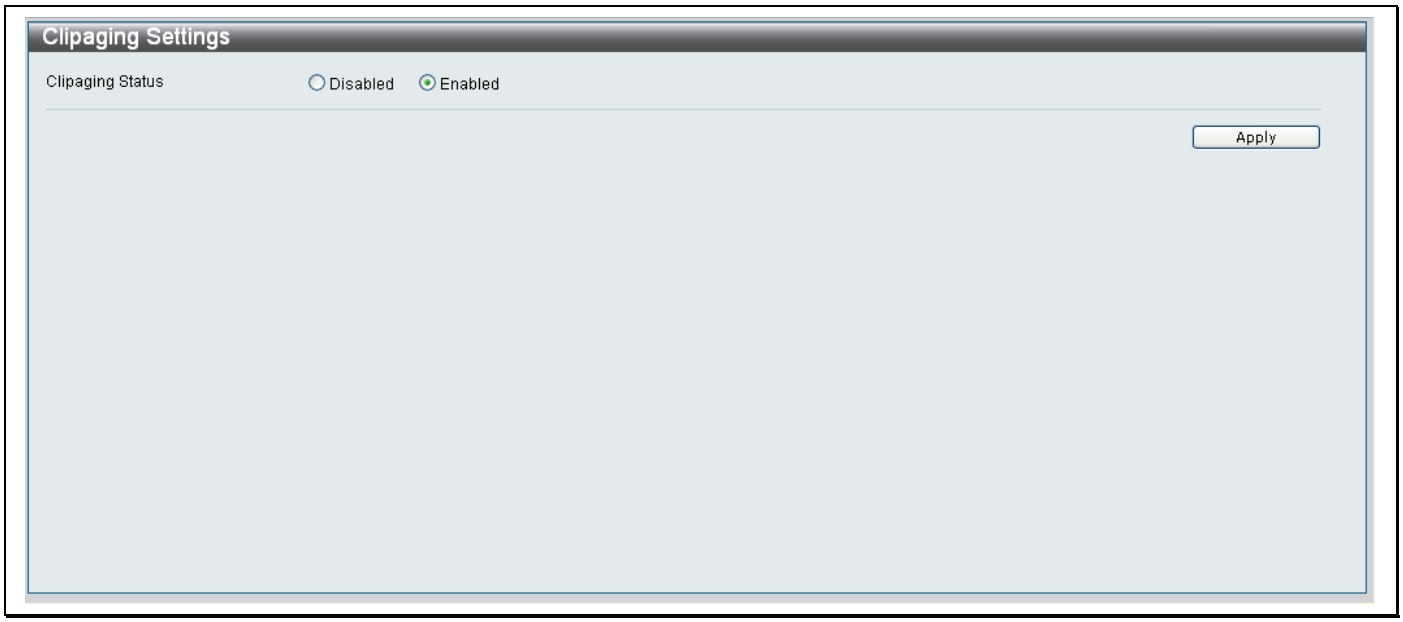


Figure 6- 10. Clipaging Settings window

To enable the Clipaging function, click the **Enabled** radio button, click the **Disabled** radio button to disable the Clipaging function.

Click **Apply** to save the Clipaging setting.

Firmware Information

The Firmware Information window displays the different firmware versions loaded on the Switch. The Switch supports two Firmware Image versions. To access the **Firmware Information** window, click **Configuration** > **Firmware Information** to reveal the following window:

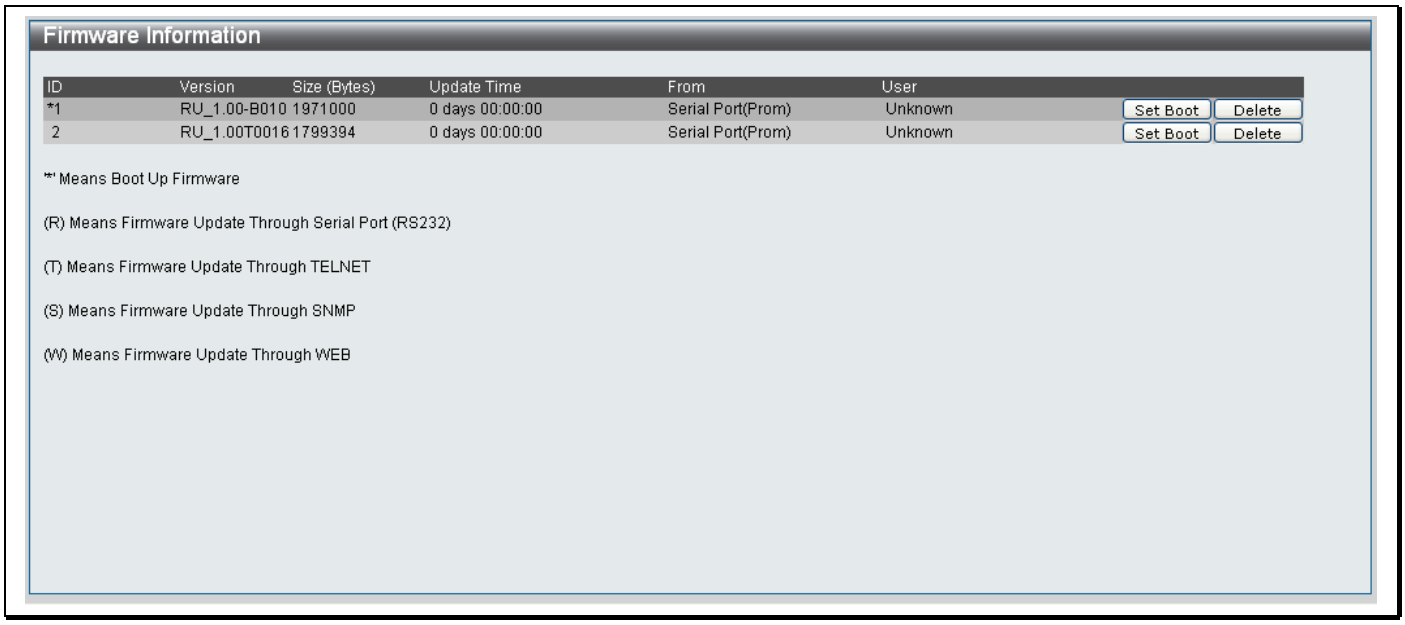


Figure 6- 11. Firmware Information window

The following parameters are displayed:

Parameter	Description
ID	Displays the ID number of the Firmware, an asterix next to the number indicates that the Switch will boot up with this version of firmware.
Version	Displays the Version number of the Firmware.
Size (Bytes)	Displays the Size of the Firmware in bytes.
Update Time	Indicates the date and time the Firmware was loaded onto the Switch. If the **Update Time** field displays *0 days 00:00:00* the firmware update was carried out through the Switch Console port in Prom Mode.
From	Indicates the IP Address and the method used to update the Firmware. If the **From** field displays *Serial Port (Prom)* the firmware update was carried out through the Switch Console port in Prom Mode.
User	Indicates the User Name that loaded the Firmware. If the **User** field displays *Unknown* the firmware update was carried out through the Switch Console port in Prom Mode.
Set Boot	To set the Firmware version that will load when the Switch boots-up, click the **Set Boot** button next to the corresponding Firmware image.
Delete	To delete a Firmware version on the Switch, click the **Delete** button next to the corresponding Firmware image.

MAC Address Aging Time

The **MAC Address Aging Time** window specifies the amount 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).

To access the MAC Address Aging Time window, click **Configuration** > **MAC Address Aging Time** to reveal the following window:

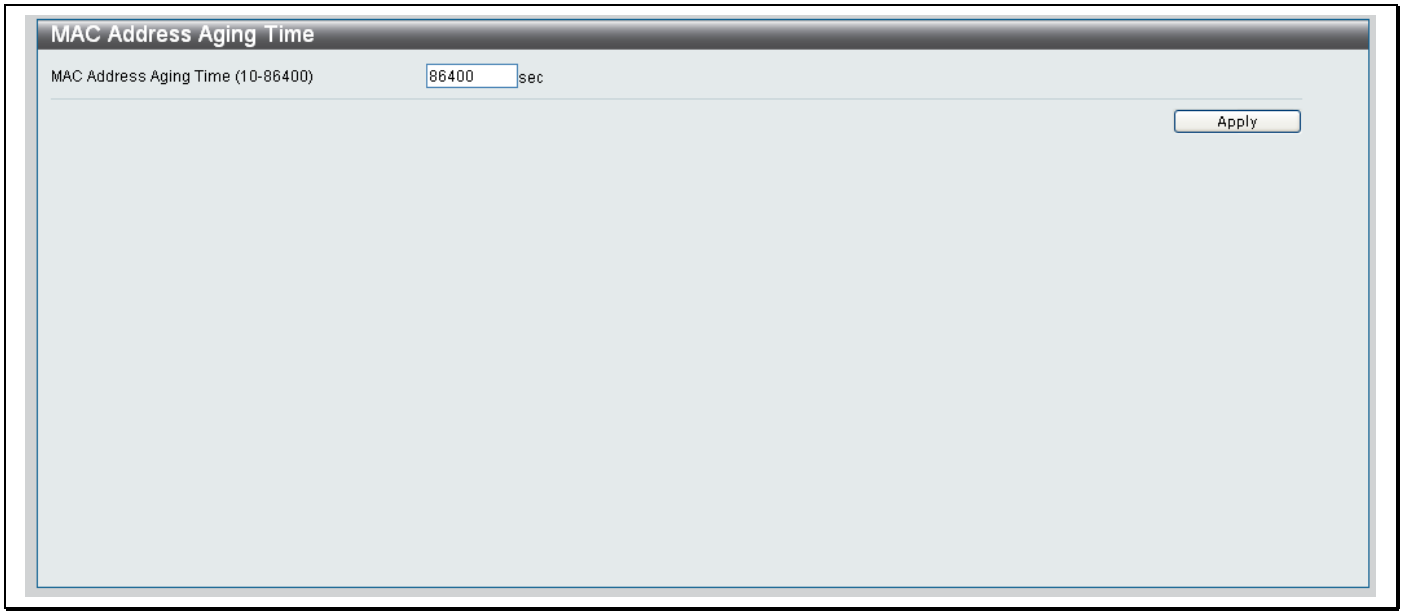


Figure 6- 12. MAC Address Aging Time window

To change the MAC Address Aging Time:

1. Type in a value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between *10* and *8,640* seconds.
2. Click **Apply** to implement the new settings on the Switch.

Dual Configuration Settings

The Switch can store up to two separate configurations. Use the **Dual Configuration Settings** window to set the configuration that the Switch will use when it is booting up. To access the Dual Configuration Settings window, click **Configuration** > **Dual Configuration Settings** to reveal the following window:

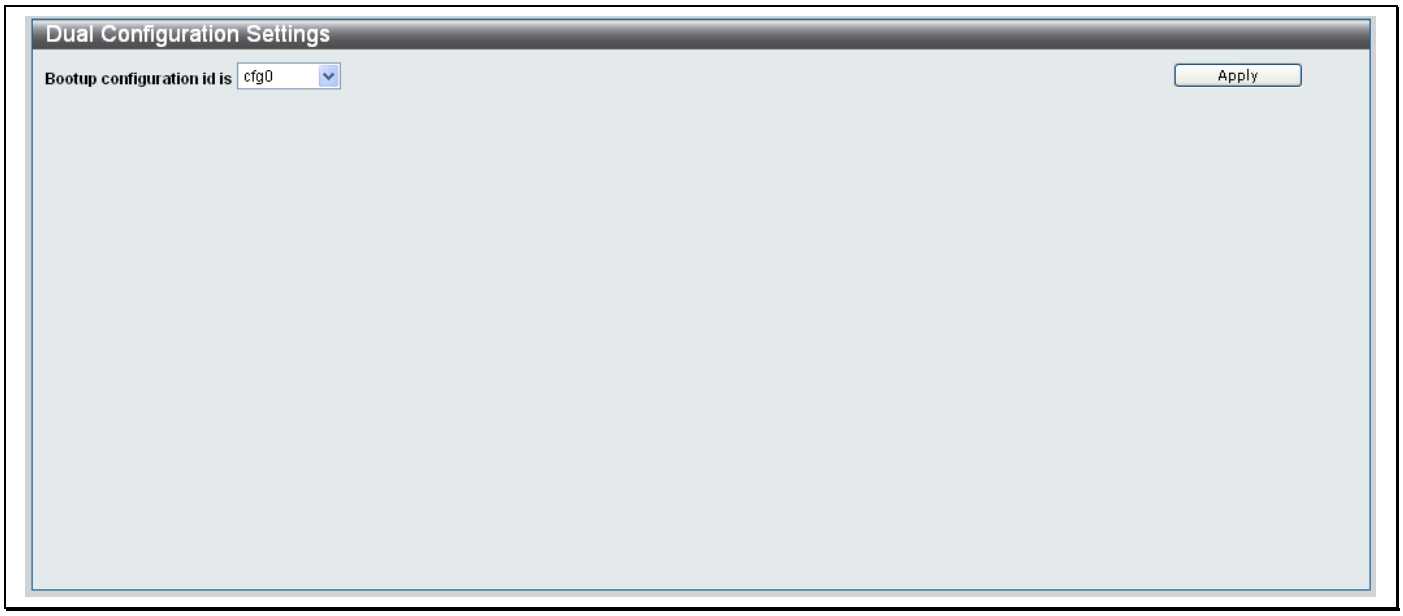


Figure 6- 13. Dual Configuration Settings window

To Set the Bootup Configuration ID:

1. Use the drop-down menu to specify the configuration file that will be loaded at bootup. Choose *cfg0* to specify that **Configuration ID 0** should be used. Choose *cfg1* to specify that **Configuration ID 1** should be used.
2. Click **Apply** to set the Bootup Configuration file ID.

SNTP Settings

Time Settings

The Time Settings window displays and configures the time set on the device and the source used to obtain the time. The Time of the Switch can be set automatically using Simple Network Time Protocol (SNTP) or manually. To configure the Time settings for the Switch, click **Configuration** > **SNTP Settings** > **Time Settings**, to reveal the following window:

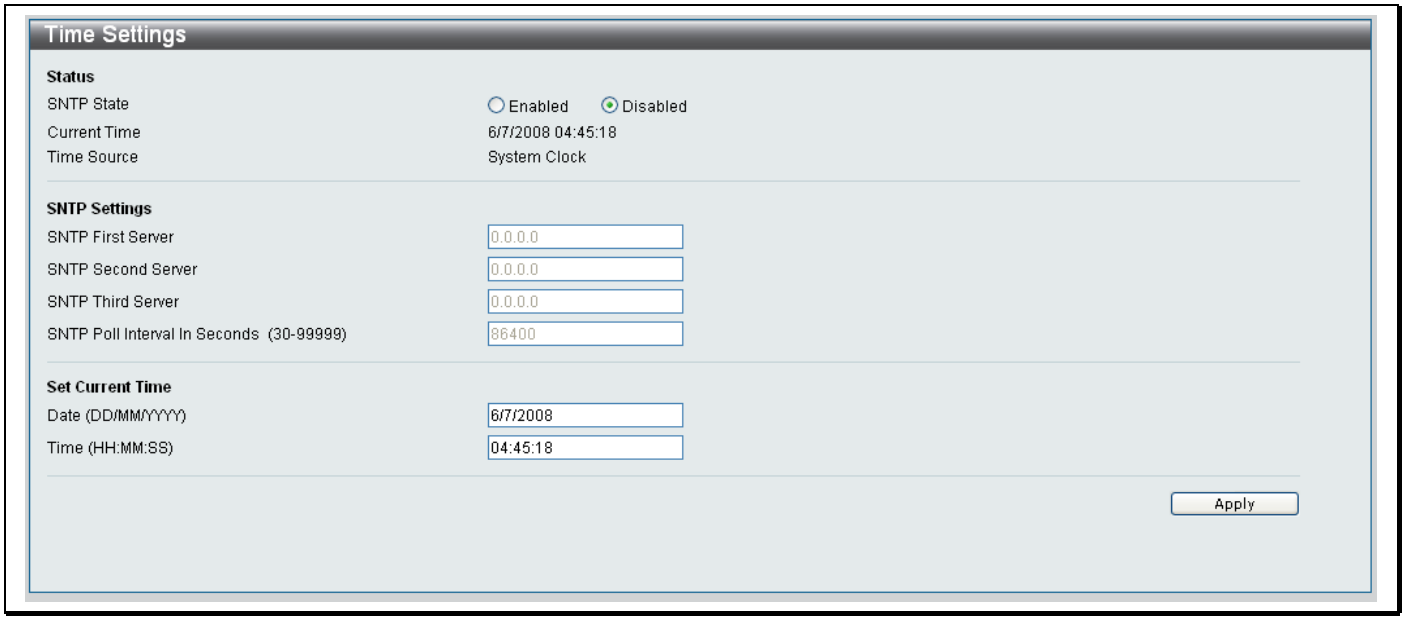


Figure 6- 14. Time Settings window

To Set the Time using SNTP:

1. In the *Status* section, click the **Enabled** radio button.
2. In the *SNTP Settings* section, type in the IP addresses of the SNTP **First**, **Second** and **Third** servers that the SNTP information will be taken from in their respective textboxes.
3. Type in the interval, in seconds, between requests for updated SNTP information.
4. Click **Apply** when you have finished setting the SNTP information.

To Set the Time manually:

1. In the *Status* section, click the **Disabled** radio button.
2. In the *Set Current Times* section, enter the current date in the *Date* field in the following format: *DD/MM/YYYY*, where DD equals the day of the month, MM equals month and YYYY equals the year.
3. In the *Time* field enter the current time in *hours*, *minutes* and *seconds*. Type in the interval, in seconds, between requests
4. Click **Apply** when you have finished setting the time manually.

TimeZone Settings

To configure the Time Zone settings for the Switch, click **Configuration** > **SNTP Settings** > **TimeZone Settings**, to reveal the following window:

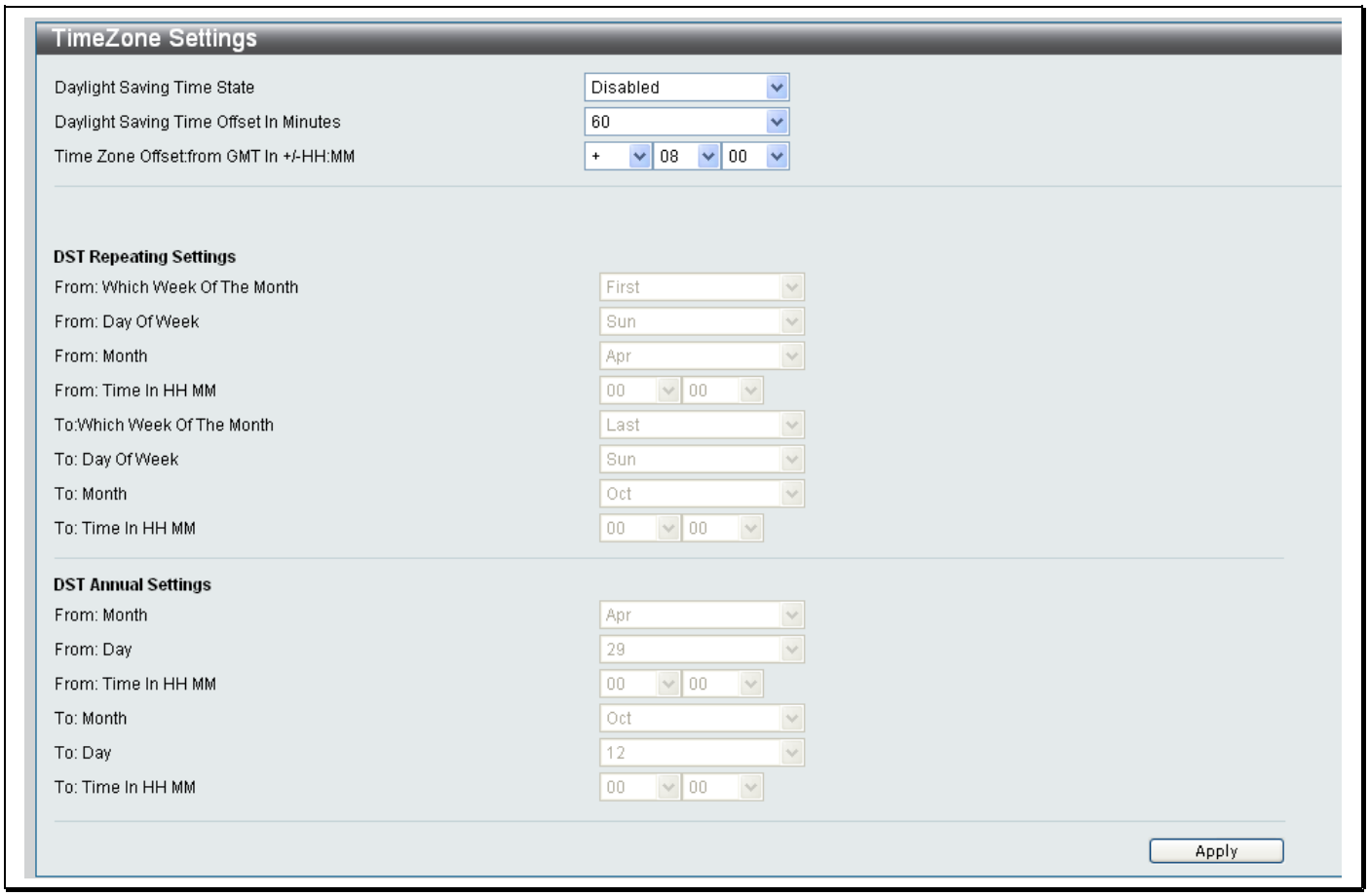


Figure 6- 15. Time Zone settings window

The following parameters can be set:

Parameter	Description
TimeZone Settings	
Daylight Saving Time State	Use this drop-down menu to enable or disable the Daylight Saving Times (DST) State.
Daylight Saving Time Offset in Minutes	Use this drop-down menu to specify the amount of time that will constitute your local DST offset - *30*, *60*, *90*, or *120* minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)

DST Repeating Settings	
Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From: Which Week Of the Month	Use the drop-down menu to select the week of the month that DST will start on.
From: Day of Week	Use the drop-down menu to select the day of the week that DST will start on.
From: Month	Use the drop-down menu to select the month DST will start on.
From: Time in HH MM	Use the drop-down menus to select the time of day that DST will start on.
To: Which Week Of The Month	Use the drop-down menu to select the week of the month the DST will end.
To: Day of Week	Use the drop-down menu to select the day of the week that DST will end.
To: Month	Use the drop-down menu to select the month that DST will end.
To: Time in HH:MM	Use the drop-down menus to select the time DST will end.
DST Annual Settings	
Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.	
From: Month	Use the drop-down menu to select the month DST will start on, each year.
From: Day	Use the drop-down menu to select the day of the week DST will start on, each year.
From: Time in HH MM	Use the drop-down menu to select the time of day DST will start on, each year.
To: Month	Use the drop-down menu to select the month DST will end on, each year.
To: Day	Use the drop-down menu to select the day of the week DST will end on, each year.
To: Time in HH:MM	Use the drop-downs menu to select the time of day that DST will end on, each year.

Click **Apply** to implement changes made to the **Time Zone and DST** window.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

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

The Switch supports the SNMP versions 1 and 2c. In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

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

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv2.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

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

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 windows to select the SNMP version used for specific tasks.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1 and 2c. The administrator can specify the SNMP version used to monitor and control the Switch. The two versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP Community Table

To configure the SNMP Community settings for the Switch, click **Configuration** > **SNMP Settings** > **SNMP Community Table**, to reveal the following window:

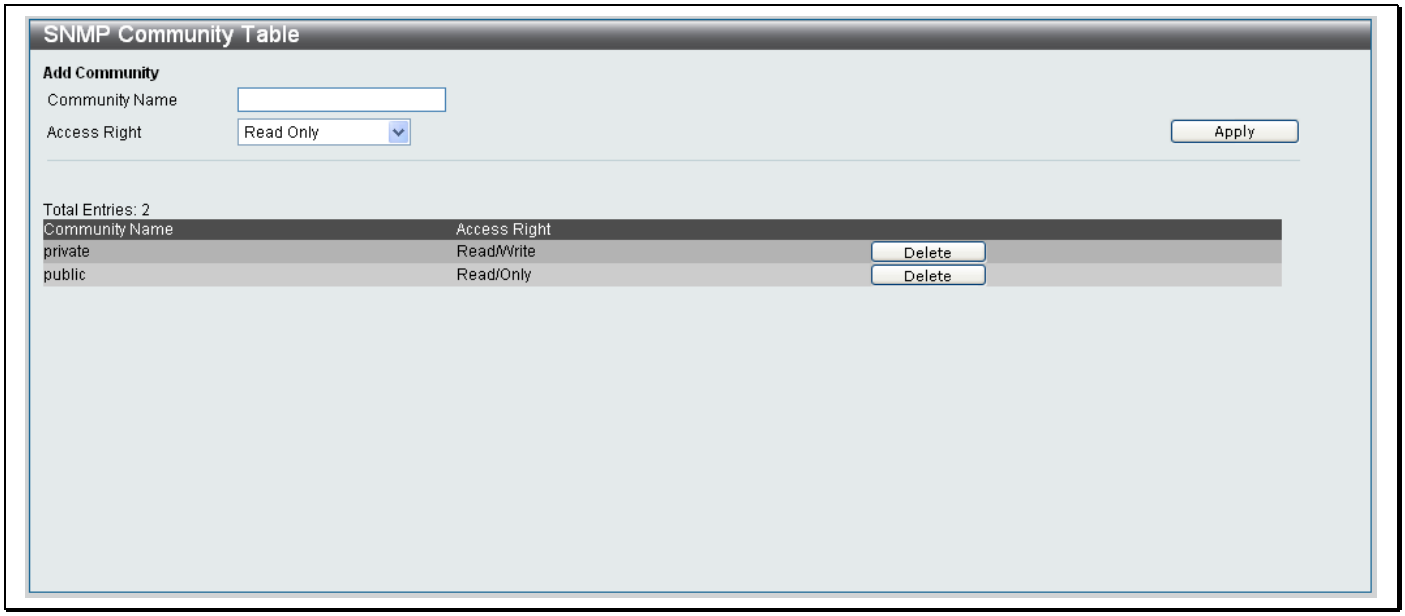


Figure 6- 16. System Log Settings window

The following parameters are displayed:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
Access Right	Use the drop-down menu to select an access right for the Community: *Read Only* – Specifies that the SNMP community members using the community string created can only read the contents of the MIBs on the Switch. *Read Write* - Specifies that the SNMP community members using the community string created can read from and write to the contents of the MIBs on the Switch.

Click **Apply** to implement the new settings on the Switch.

To delete an entry from the SNMP Community Table:

Click the **Delete** button next to the corresponding entry.

SNMP Host Table

Use the **SNMP Host Table** window to setup SNMP trap recipients. To configure the SNMP Host Table on the Switch, click **Configuration** > **SNMP Settings** > **SNMP Host Table**, to reveal the following window:

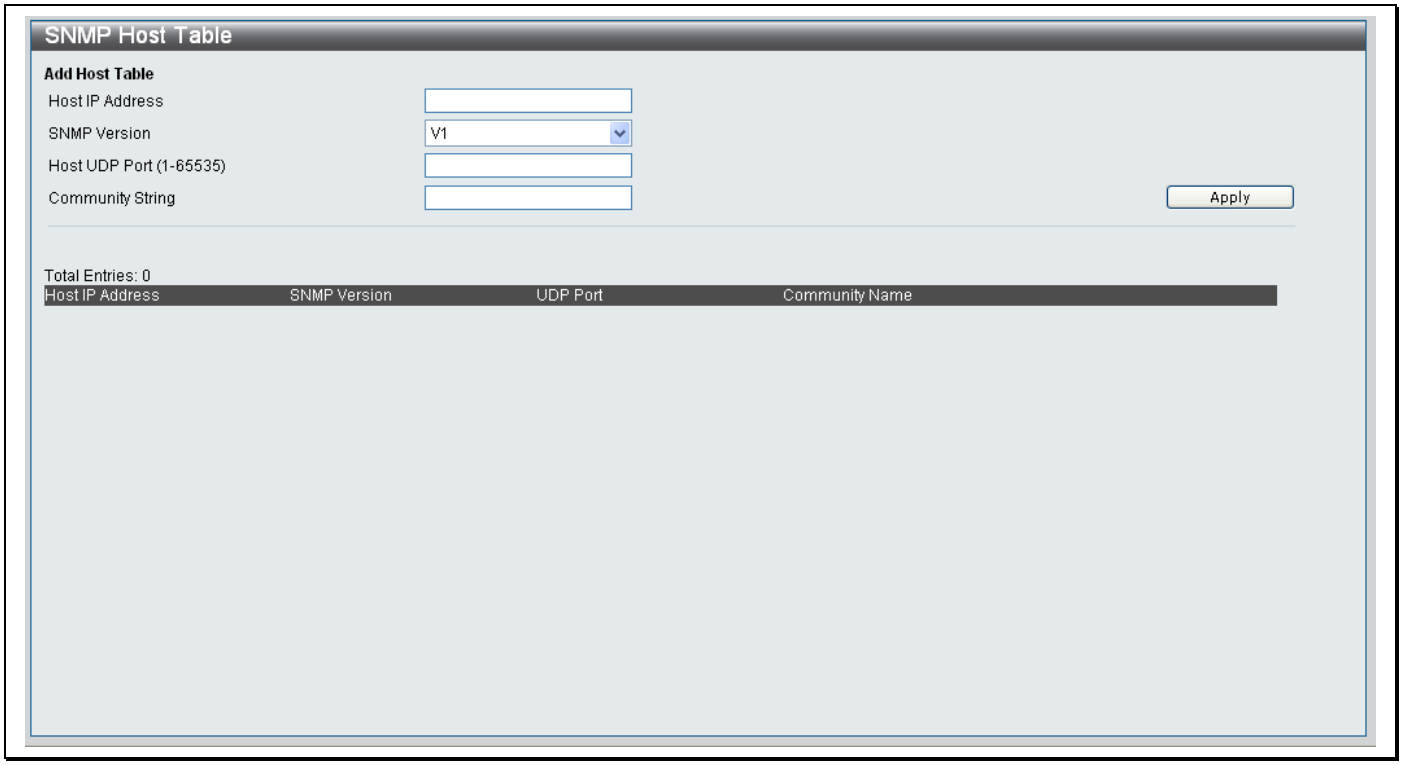


Figure 6- 17. SNMP Host window

To add a new host, configure the parameters as displayed below:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will receive the SNMP traps.
SNMP Version	Choose one of the following SNMP versions from the drop-down menu: *V1*- Select V1 to specify that SNMP version 1 will be used. *V2c*- Select V2c to specify that SNMP version 2c will be used.
Host UDP Port (1-65535)	Type in the UDP Port number that the host will use to receive SNMP traps.
Community String	Type in the community string.

Click **Apply** to implement the new settings on the Switch.

SNMP Manager Table

To configure the SNMP Manager settings for the Switch, click **Configuration** > **SNMP Settings** > **SNMP Manager Table**, to reveal the following window:

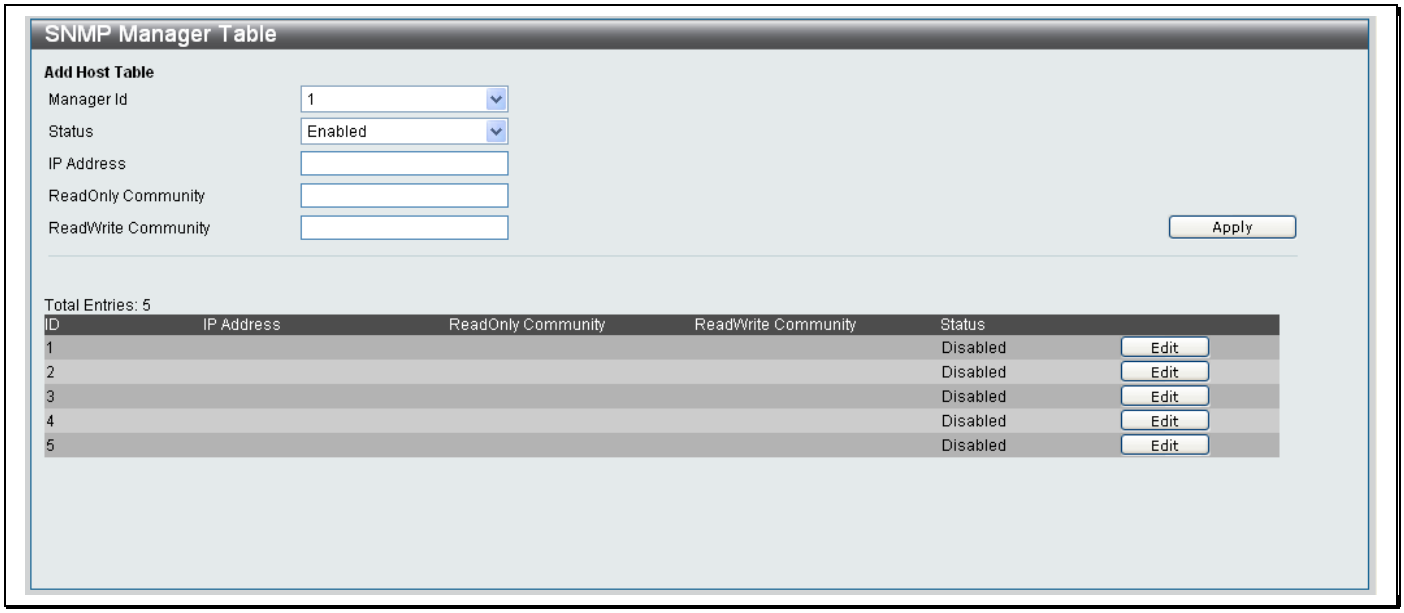


Figure 6- 18. SNMP Manager Table window

The following parameters are displayed:

Parameter	Description
Manager ID	Use the drop-down menu to set a Manager ID for the new remote SNMP manager. The valid ID's are from *1* to *5* .
Status	Choose *Enabled* or *Disabled* from the drop-down menu to Enable or Disable the SNMP Manager.
IP Address	Type in the IP address of the remote SNMP management station.
Read/Only Community	Type in the string of the Read/Only community that the SNMP manager will use. A Read/Only community string can only read the contents of the MIBs on the switch
Read/Write Community	Type in the alphanumeric string of the Read/Write community that the SNMP manager will use. This string is used like a password to give remote SNMP managers read/write access to MIB objects in the Switch's SNMP agent.

Click **Apply** to implement the new settings on the Switch.

SNMP Trap Configuration

To configure the SNMP Trap settings for the Switch, click **Configuration** > **SNMP Settings** > **SNMP Trap Configuration**, to reveal the following window:

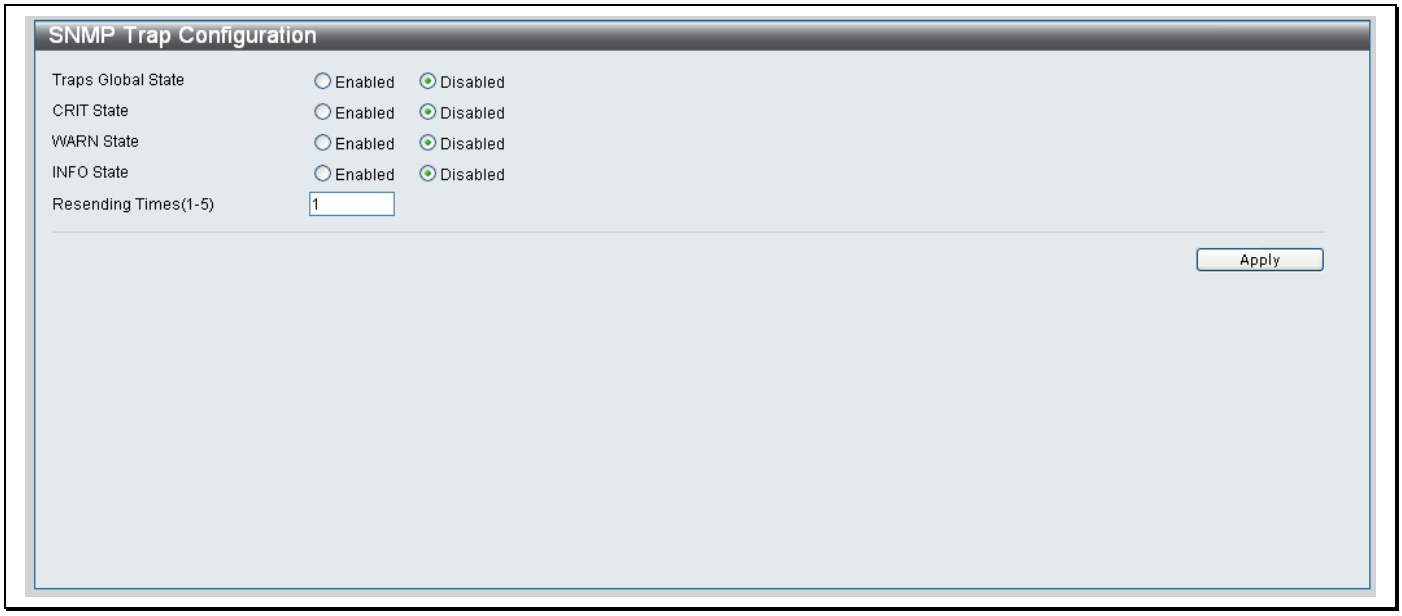


Figure 6- 19. SNMP Trap Configuration window

The following parameters are displayed:

Parameter	Description
Traps Global State	Click the *Enabled* radio button to enable all available of SNMP Trap types.
CRIT State	Click the *Enabled* radio button to enable Critical State SNMP Traps.
WARN State	Click the *Enabled* radio button to enable Warning State SNMP Traps.
INFO State	Click the *Enabled* radio button to enable Information State SNMP Traps.
Resending Times(1-5)	Type in the SNMP trap resend time you want to set on the Switch. The available time is between 1 and 5 seconds.

Click **Apply** to implement the new SNMP Trap Configuration on the Switch.

Section 7

Layer 2 Features

The following section will discuss the Layer 2 features of the Switch. The Switch includes various functions for 802.1Q VLAN, VLAN Ports Settings, QinQ, Port Trunking, LACP Ports Settings, Traffic Segmentation, IGMP Snooping, Spanning Tree and Forwarding & Filtering, all discussed in detail in the following section.

802.1Q VLAN

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

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 that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is 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.

IEEE 802.1Q VLANs

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information 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 allows 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 IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN of which the receiving port is a member.

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 VLAN Packet Forwarding
- 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 whether to filter or forward the packet.
- Egress rules - determines if the packet must be sent tagged or untagged.

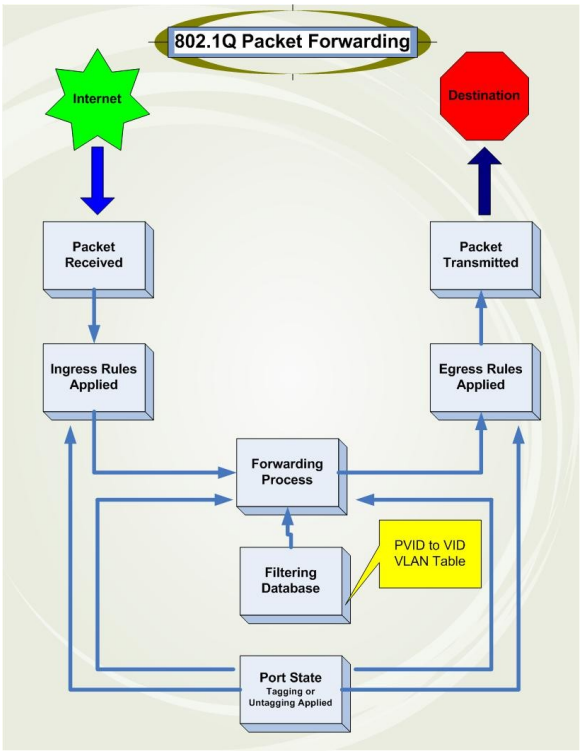


Figure 7- . IEEE 802.1Q Packet Forwarding

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 originally contained in the packet is retained.

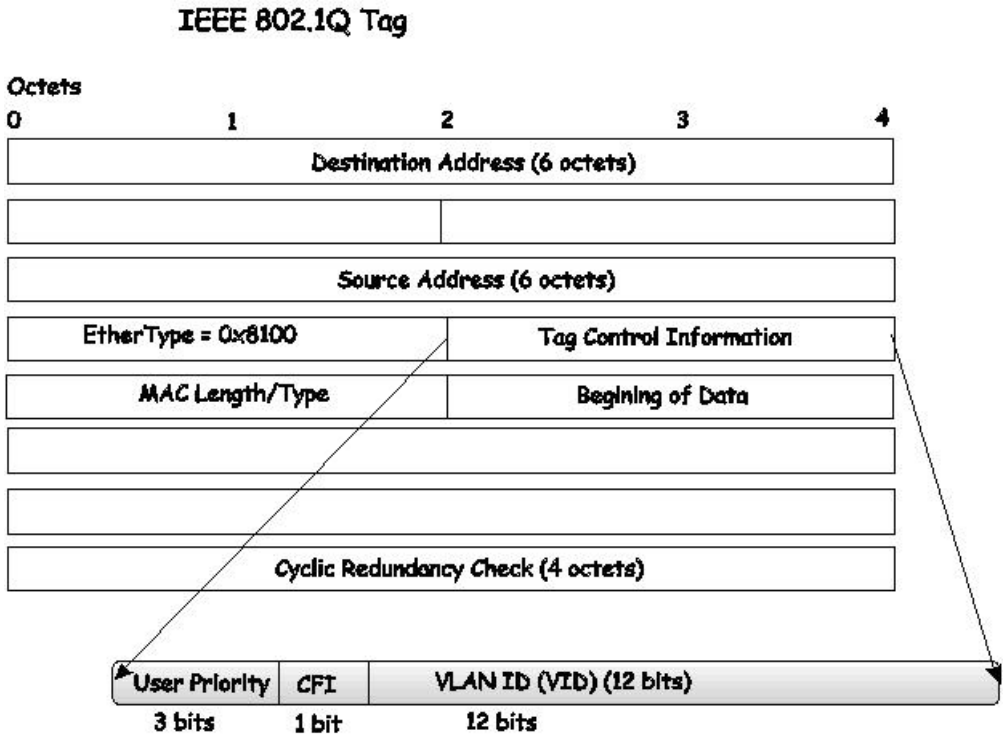


Figure 7- . IEEE 802.1Q Tag

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.

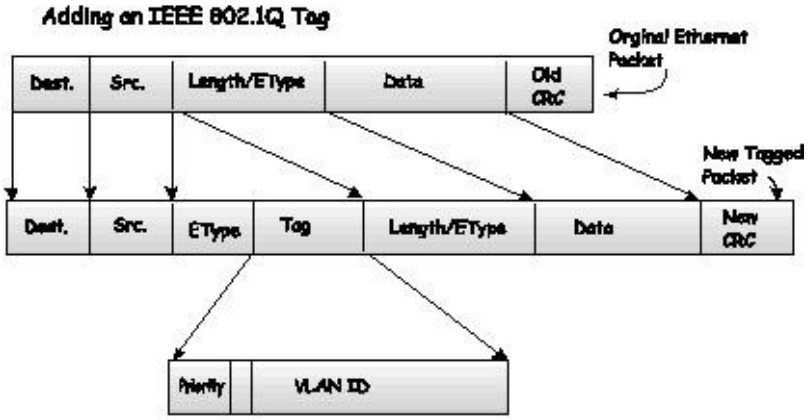


Figure 7- . Adding an IEEE 802.1Q Tag

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 of 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 (or switch stack).

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

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. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

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.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

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

NOTE: If no VLANs are configured on the Switch, then 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.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Figure 7- . VLAN Example - Assigned Ports

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Network resources such as printers and servers however, can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs to two VLAN groups. Ports 8, 9, and 10 are not configured to any VLAN group. This means ports 8, 9, and 10 are in the same VLAN group.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.

NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, you can first set the port trunk group(s), and then you may configure VLAN settings. If you wish to change the port trunk grouping with VLANs already in place, you will not need to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

To access the 802.1Q VLAN settings for the Switch, click **L2 Features** > **802.1Q VLAN**, to reveal the following window:

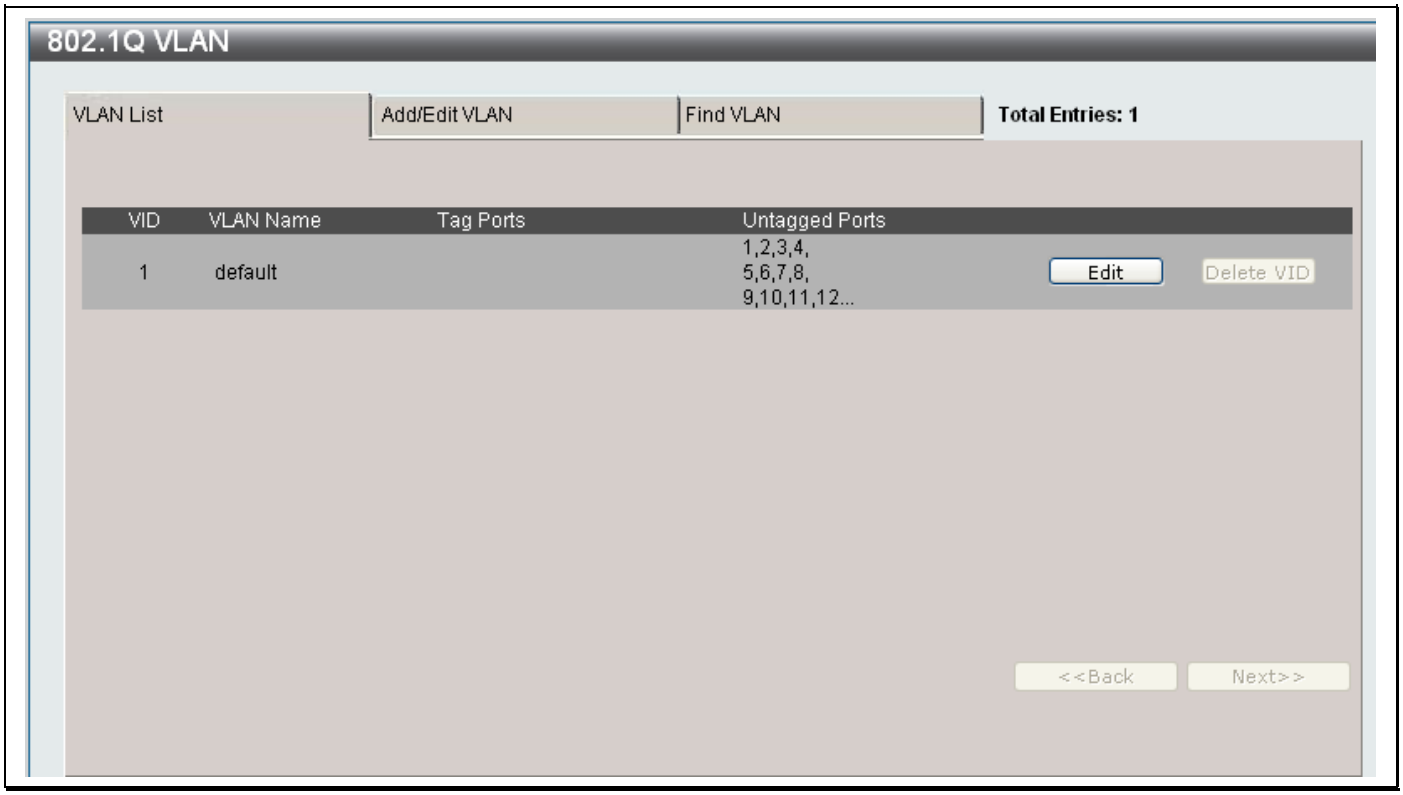


Figure 7- 5. 802.1Q VLAN window

The VLAN List window summarizes the different VLAN's that have been created on the Switch and also allows you to edit the different VLAN's on the Switch. A description of the different parameters displayed in the VLAN List window appears below:

Parameter	Description
VID	Displays the *VID* number of the VLAN.
VLAN Name	Displays the name of the VLAN.
Tag Ports	Displays the tagged ports of this VLAN.
Untagged Ports	Displays the untagged ports of this VLAN.

Editing Existing VLAN

1. Click the **Edit** button next to the VLAN that requires editing to reveal the following window:

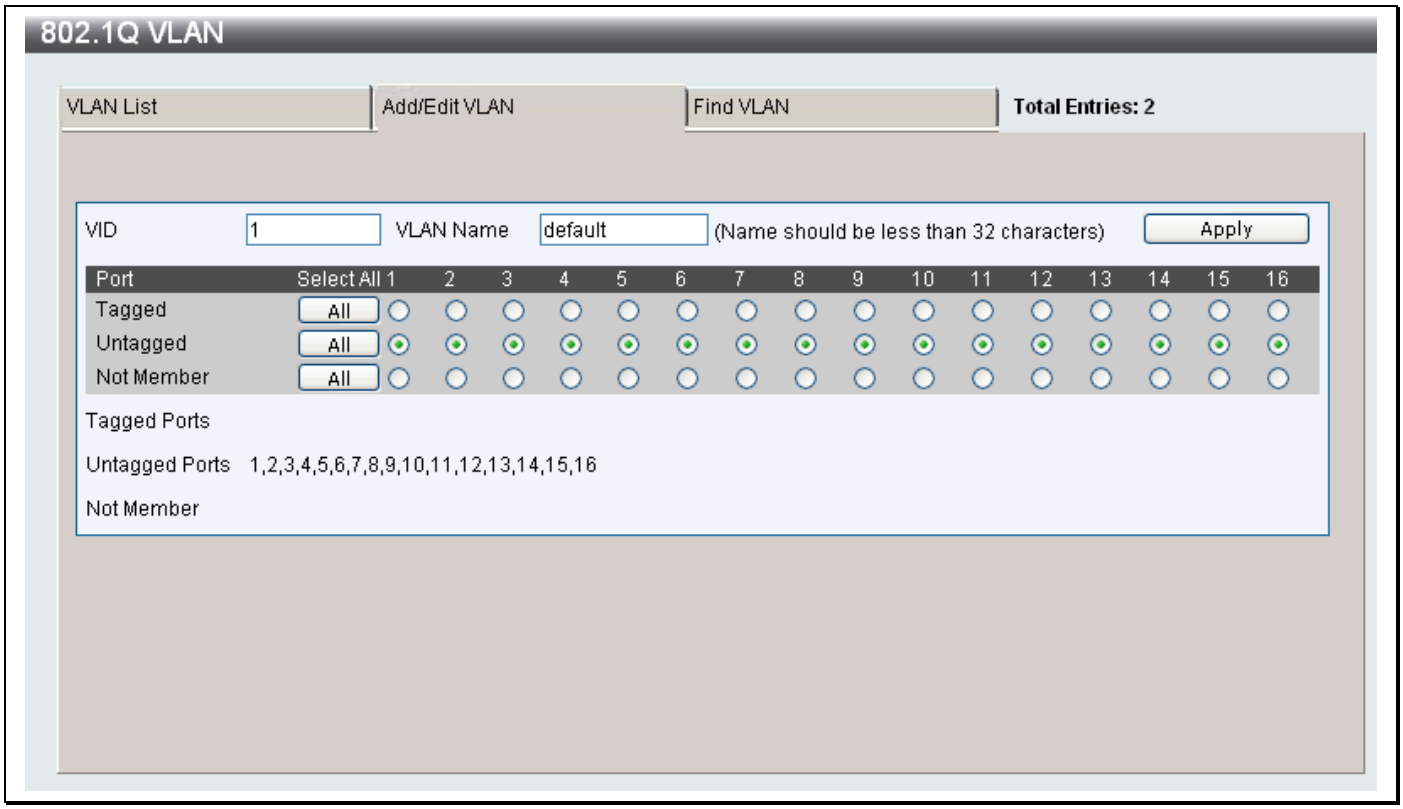


Figure 7- 6. Add/Edit VLAN window

2. The *VLAN Name* can be modified if required.
3. Click the radio buttons to choose the role of each of the ports in the VLAN.
4. When you have finished editing the VLAN, click the **Apply** button to save the changes.
5. A **Success** message indicates that the change has been made successfully.

Deleting a VLAN

1. To delete a VLAN, click the **Delete VID** button next to the VLAN you want to delete.
2. A **Success** message indicates that the VLAN has been deleted.

Creating New VLAN

1. Click the **Add/Edit VLAN** tab at the top of the 802.1Q VLAN window to reveal the following window:

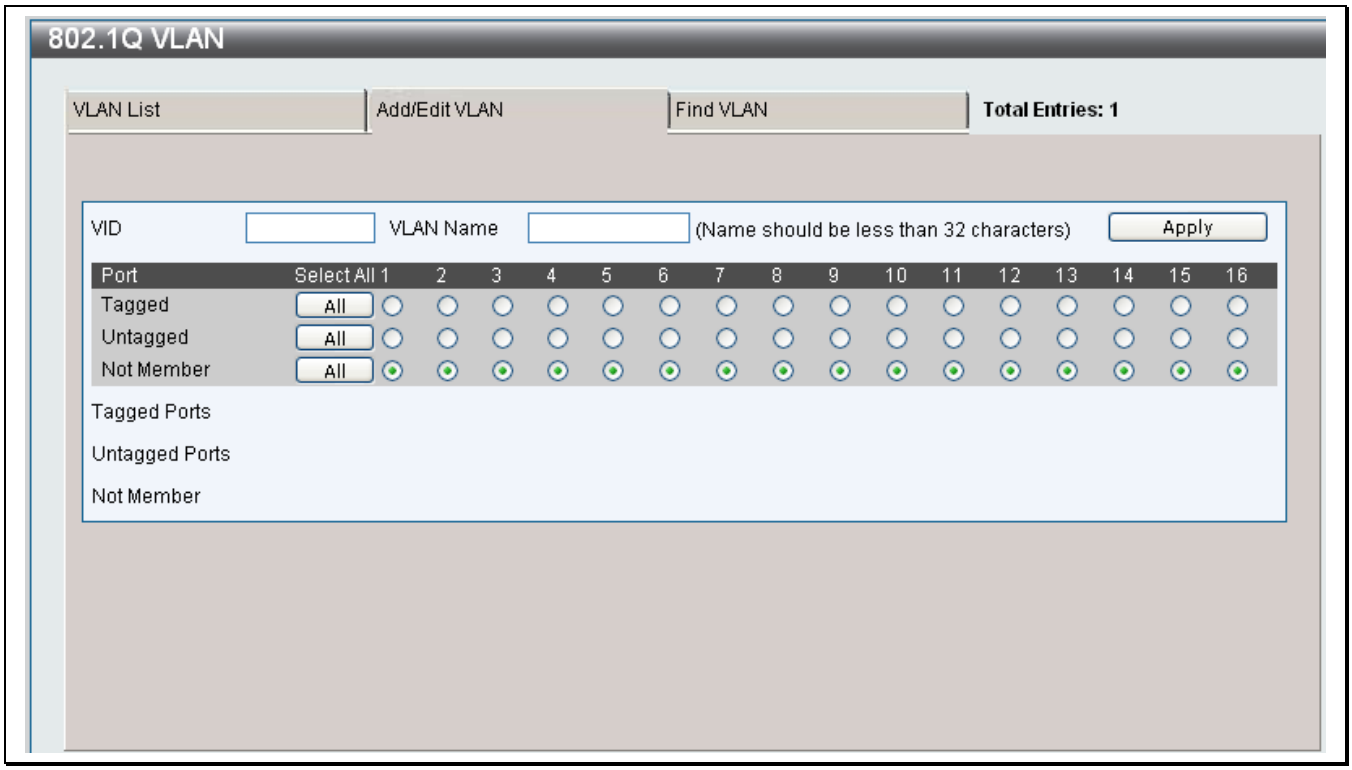


Figure 7- 7. Adding a new VLAN window

2. Type in a *VID* number in the **VID** field.
3. Type in a *VLAN Name* in the **VLAN Name** field. The VLAN name should be alphanumeric with no spaces and be less than 32 characters.
4. Click the radio buttons to choose the role of each of the ports in the VLAN.
5. When you have finished creating the VLAN, click the **Apply** button.
6. A **Success** message indicates that the VLAN has been deleted.

Finding a VLAN

1. Click the **Find VLAN** tab at the top of the 802.1Q VLAN window to reveal the following window:

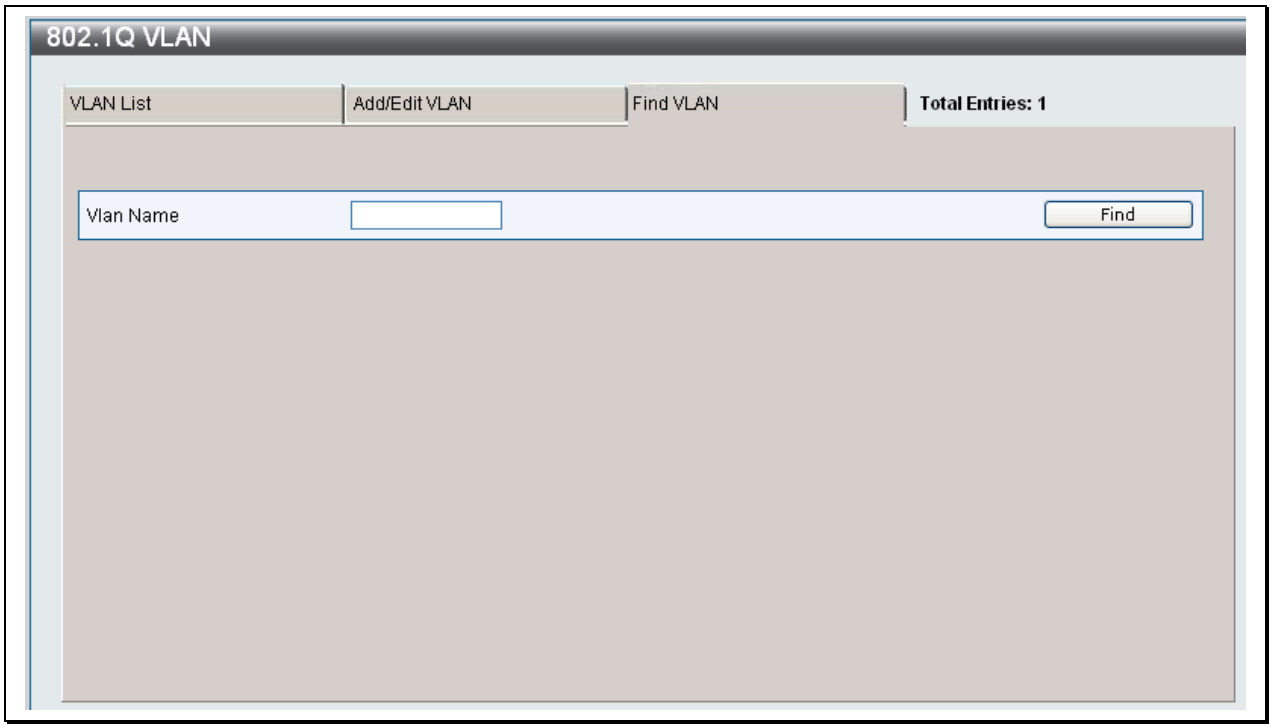


Figure 7- 8. Find VLAN window

2. Type in the *VLAN Name* that you are searching for.
3. Click the **Find** button.
4. If a VLAN matching the name specified in the *VLAN Name* field is found, the **VLAN List** window will open displaying information about the VLAN.

5. The VLAN will display in the **VLAN List** window, the window allows you to edit or delete the VLAN by clicking the **Edit** or **Delete VID** button.

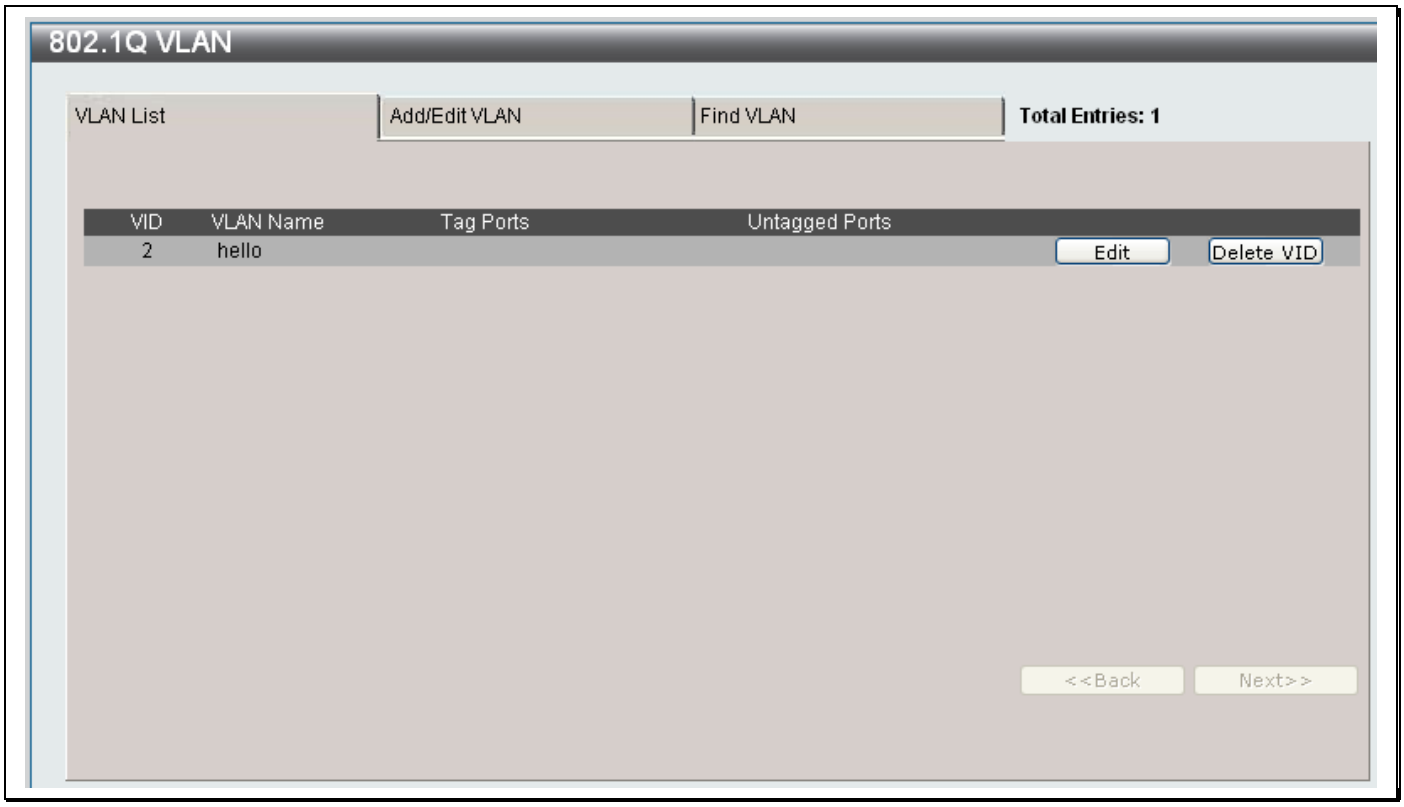


Figure 7- 9. VLAN List window

VLAN Ports Settings

The **VLAN Ports Settings** window is used to set the ingress checking status of each port.

To access the VLAN Ports settings for the Switch, click **L2 Features** > **VLAN Ports Settings**, to reveal the following window:

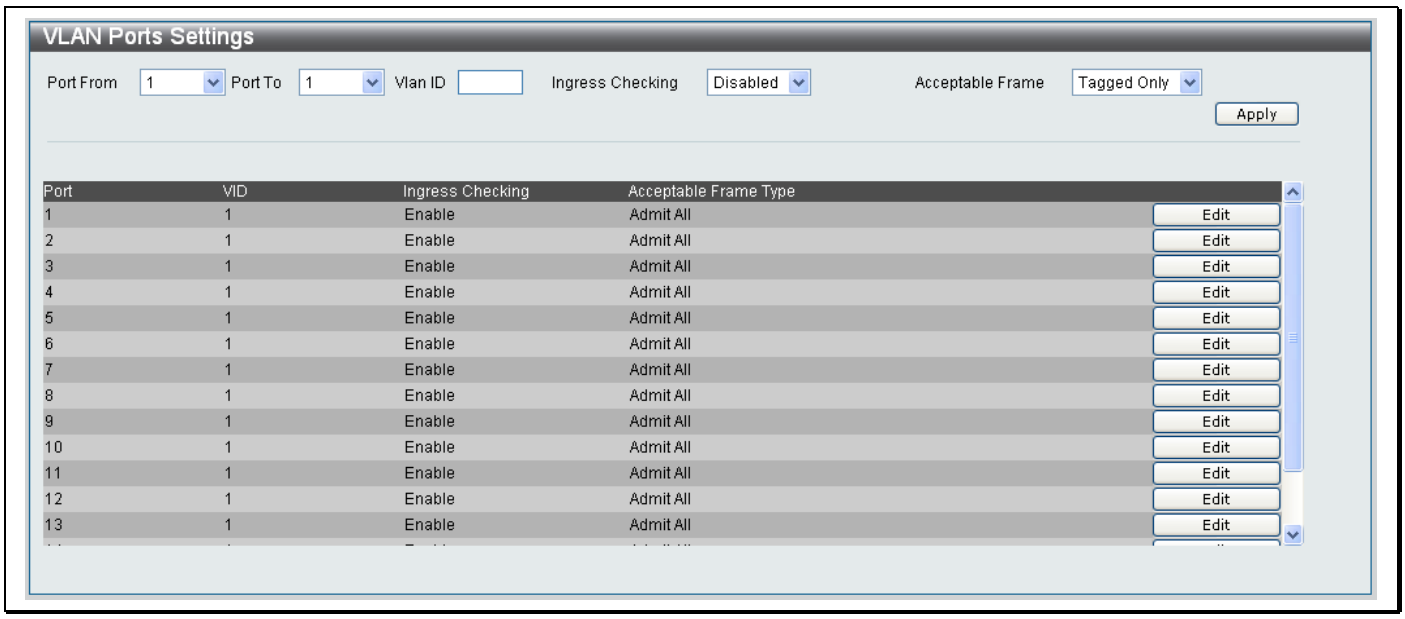


Figure 7- 10. VLAN Ports Settings window

Configure the drop-down menus at the top of the screen as described below:

Parameter	Description
Port From / To	Use the drop-down menus to select the range of ports that you want to enable Ingress checking on.
Vlan ID	Type the ID of the VLAN that will be associated with the specified port(s).
Ingress Checking	Select *Enabled* from the drop-down menu to enable Ingress Checking on the specified ports. Select *Disabled* to disable Ingress Checking.
Acceptable Frame	Choose the type of frame that will be accepted by the port from the drop-down menu: *Tagged Only*- Only tagged frames will be accepted by the port. *Untagged Only*- Only untagged frames will be accepted by the port. *Admit All*- Only Both tagged and untagged frames will be accepted by the port.

Editing a VLAN Port Setting

1. Click the **Edit** button next to the VLAN port you want to edit.
2. The **VID**, **Ingress Checking** and **Acceptable Frame Type** fields can be altered, as shown below:

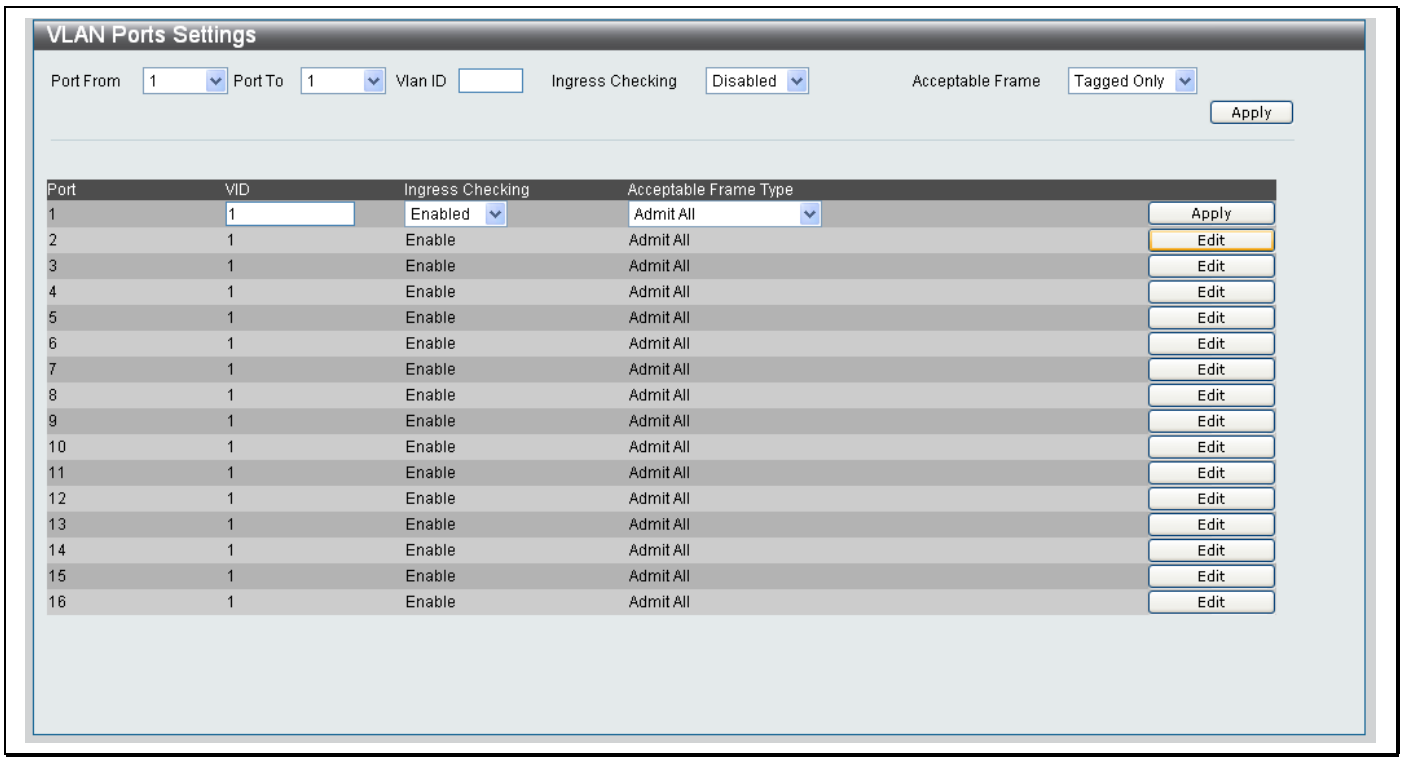


Figure 7- 11. Editing existing VLAN in VLAN Ports Settings window

3. Make the required changes and click the **Apply** button.
4. A **Success** message indicates that the change was successful.

QinQ

Q-in-Q or Double VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This basically lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

QinQ's are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example QinQ VLAN tagged packet.

Destination Address	**Source Address**	**SPVLAN (TPID + Service Provider VLAN Tag)**	**802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)**	**Ether Type**	**Payload**

Consider the example below:

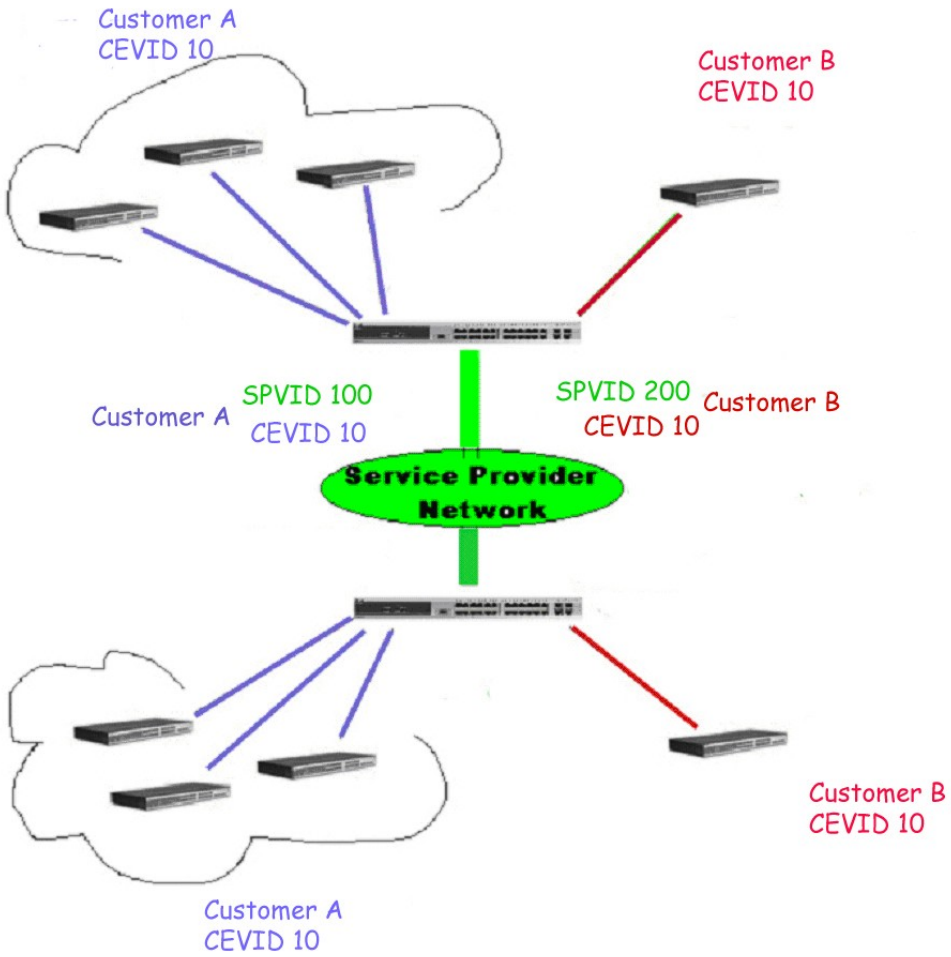


Figure 7- 12. QinQ VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs with different SPVIDs for specific customers (say Customer A and Customer B). Both CEVLANs (Customer VLANs), CEVLAN 10 are tagged with the SPVID 100 (for Customer A) and SPVID 200 (for Customer B) on the Service Provider Access Network, thus being a member of two VLANs on the Service Provider's network. In this way, the Customer can retain their normal VLAN ID's and the Service Provider can separate multiple Customer VLANs using SPVLANs, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for QinQ's

Some rules and regulations apply with the implementation of the QinQ procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both double and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Once Double VLANs are enabled, GVRP must be disabled.
7. All packets sent from the CPU to the Access ports must be untagged.
8. The following functions will not operate when the switch is in QinQ mode:
    - Guest VLANs
    - Web-based Access Control
    - IP Multicast Routing
    - GVRP
    - All Regular 802.1Q VLAN functions

QinQ Settings

To access the QinQ settings for the Switch, click **L2 Features** > **QinQ >QinQ Settings**, to reveal the following window:

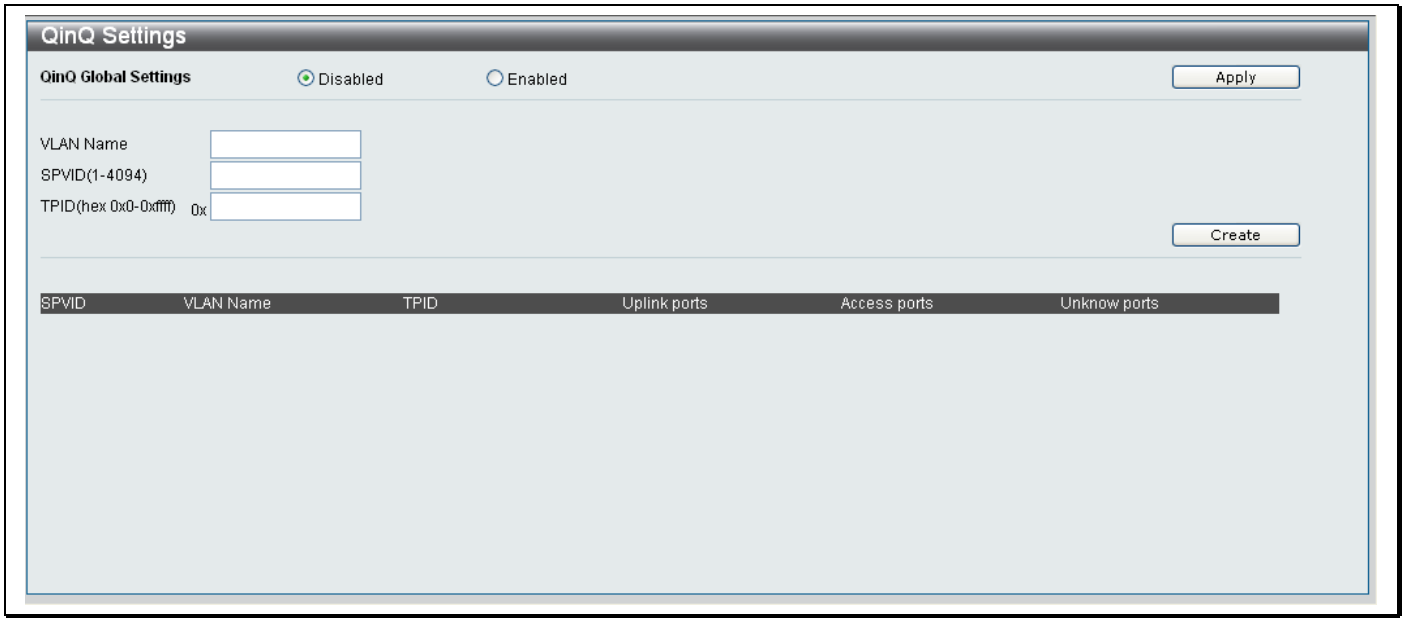


Figure 7- 13. QinQ Settings Window

Enabling the QinQ feature

1. Click the ***Enabled*** radio button.
2. Click the **Apply** button.

Adding a new QinQ VLAN

1. Configure the following parameters as described below:

Parameter	Description
VLAN Name	Type a name for the new QinQ VLAN.
SPVID (1-4094)	Type in the Service Provider VLAN ID for the VLAN to be created. The range is 1-4094.
TPID (hex 0x0-0xffff)	Type in the Tag Protocol Identifier (TPID) for the VLAN to be created.

2. Click the **Create** button.
3. A **Success** message indicates that the QinQ VLAN was added successfully.

4. The new QinQ VLAN will appear in the list at the bottom of the window, as shown below:

Figure 7- 14. QinQ Settings Window displaying new VLAN

The following parameters are displayed in the table at the bottom of the window:

Parameter	Description
SPVID	Displays the Service Provider VLAN ID of the QinQ VLAN.
VLAN Name	Displays the name of the QinQ VLAN.
TPID	Displays the Tag Protocol Identifier (TPID) of the VLAN.
Uplink ports	Displays the port numbers that are configured as Uplink ports.
Access ports	Displays the port numbers that are configured as Access ports.
Unknown ports	Displays the port numbers where the Uplink or Access configuration status is unknown.

Deleting a QinQ VLAN

1. Click the **Delete** button next to the QinQ VLAN you want to delete.
2. A **Success** message indicates that the QinQ VLAN was deleted successfully.

QinQ Port Settings

Use the QinQ Port Settings to define the role of the ports in the QinQ VLAN.

To access the QinQ Port Settings for the Switch, click **L2 Features** > **QinQ >QinQ Port Settings**, to reveal the following window:

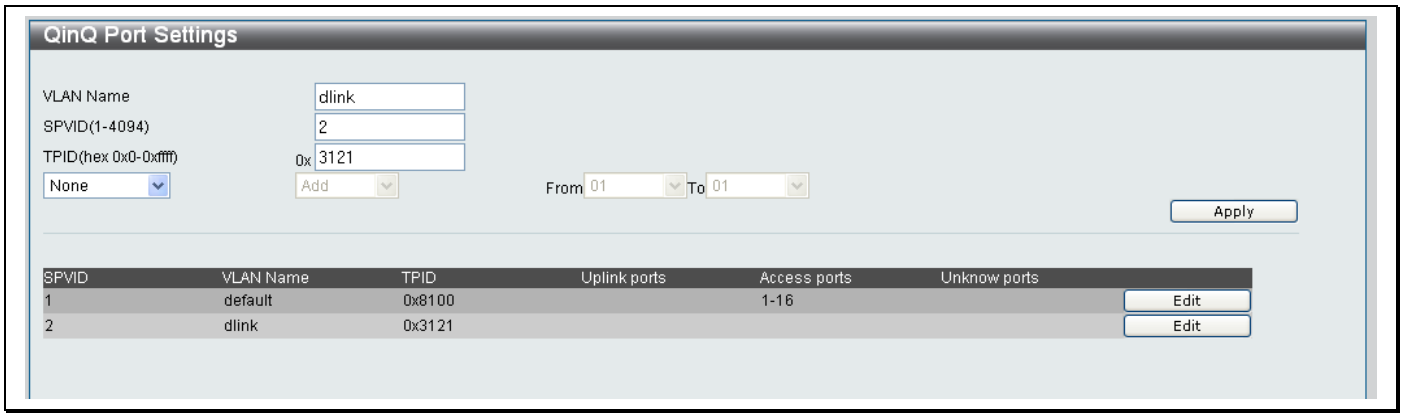


Figure 7- 15. QinQ Ports Settings Window displaying new VLAN

Editing the QinQ Port Settings

1. Click the **Edit** button next to the QinQ VLAN you want to Edit.
2. Edit the required parameters as described below:

Parameter	Description
VLAN Name	Type a name to identify the new VLAN.
SPVID (1-4094)	Type a number between 1 and 4094 to assign a unique SPVID.
TPID (hex 0x0-0xffff)	Type a TPID in hexadecimal format for the VLAN
Uplink ports / Access ports	Choose to make the specified ports *Uplink Ports* or *Access Ports* from the drop-down menu. Choose *None* to specify that the port is not a member.
Add / Delete	Select *Add* from the drop-down menu to add the QinQ VLAN setting. Select *Delete* to delete.
From / To	Use the drop-down menu to specify the port numbers that will be part of the VLAN.

Click the **Apply** button to save the changes.

Port Trunking

The Port Trunking window contains the settings that configure the VLAN Trunk ports and their link aggregation.

To access the Port Trunking window, click **L2 Features** > **Port Trunking** to reveal the following window:

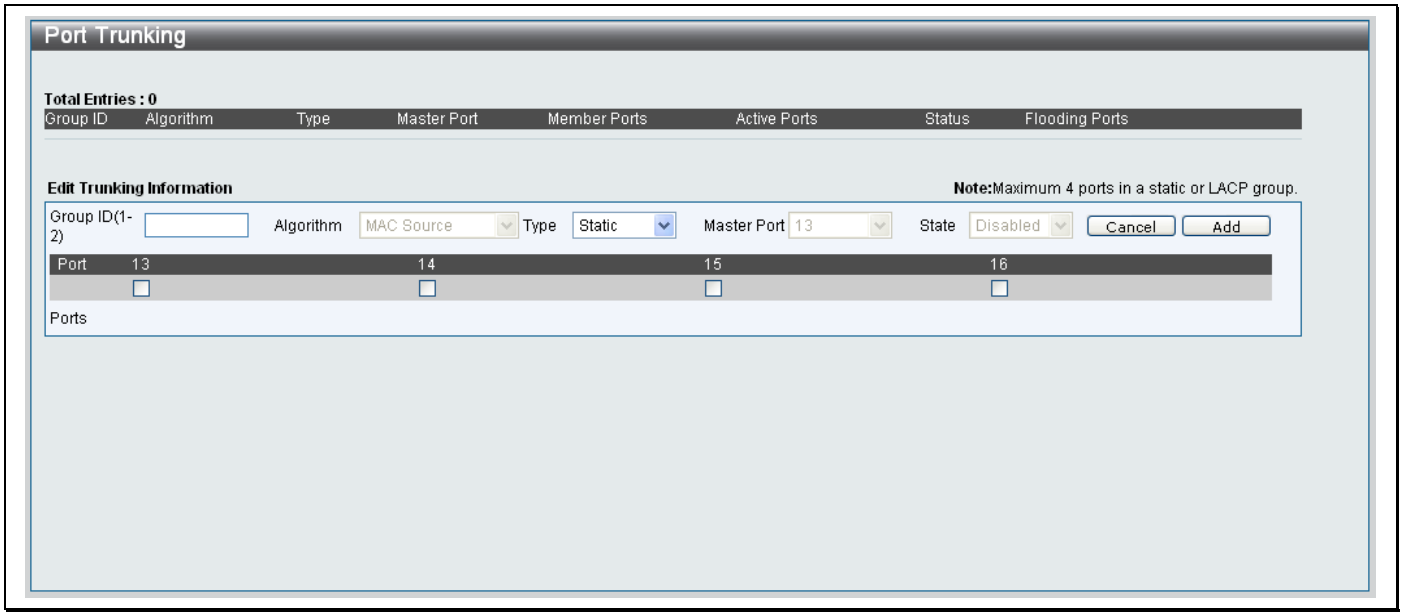


Figure 7- 16. Port Trunking window

Adding a new Port Trunk

To add a new Port Trunk, configure the parameters as described below:

Parameter	Description
Group ID (1 - 2)	Type a value of *1* or *2* to identify the port trunk group. The Switch supports two link aggregation groups.
Algorithm	Use the drop-down menu to choose the time of algorithm that will be used on the link aggregation.
Type	Use the drop-down menu to specify if the group type will be *Static* or use *LACP*. The default setting is *Static*.
Master Port	Use the drop-down menu to select a master port for the entire trunk group. The master port is the reference port for the entire trunk group. When a trunk group is formed any changes that effect this trunk group, such as a VLAN setting, must be changed through the Master Port.
State	Select *Enabled* or *Disabled* from the drop-down menu to enable or disable the Port Trunk.
Port	Tick the port numbers that will be members of the Port Trunk Entry.

Click the **Add** button to add the new Port Trunk.

Editing an existing Port Trunk

To edit an existing Port Trunk, click the **Edit** button next to the Port Trunking entry you want to modify:

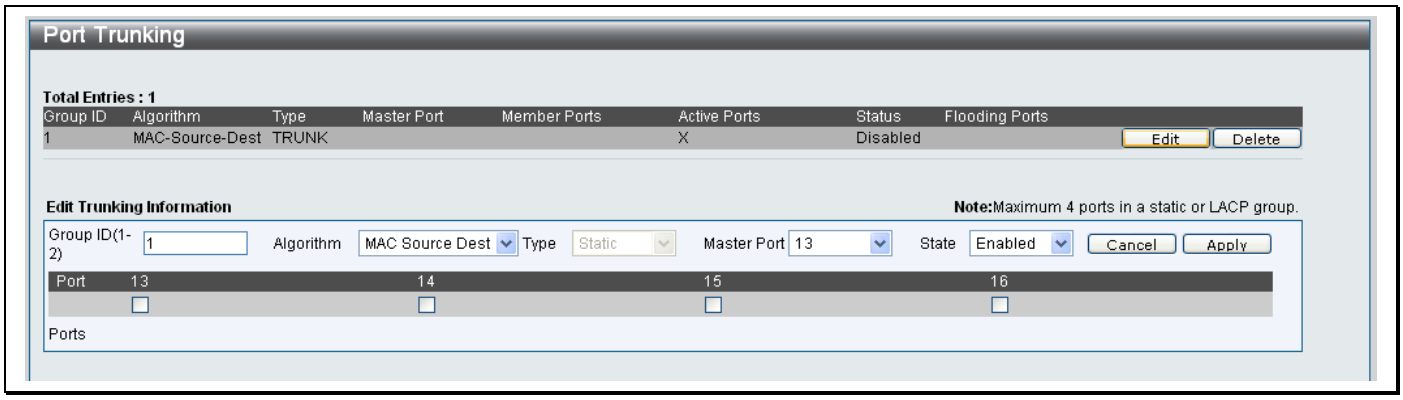


Figure 7- 17. Editing an existing Port Trunk in Port Trunking window

Configure the parameters as described below:

Parameter	Description
Group ID (1 - 2)	Type a value of *1* or *2* to identify the port trunk group. The Switch supports two link aggregation groups.
Algorithm	Use the drop-down menu to choose the time of algorithm that will be used on the link aggregation.
Type	Use the drop-down menu to specify if the group type will be *Static* or use *LACP*. The default setting is *Static*.
Master Port	Use the drop-down menu to select a master port for the entire trunk group. The master port is the reference port for the entire trunk group. When a trunk group is formed any changes that effect this trunk group, such as a VLAN setting, must be changed through the Master Port.
State	Select *Enabled* or *Disabled* from the drop-down menu to enable or disable the Port Trunk.
Port	Tick the port numbers that will be members of the Port Trunk Entry.

Click the **Apply** button to save the change to the Port Trunk configuration.

Deleting a Port Trunk

To delete an existing Port Trunk, click the **Delete** button next to the Port Trunking entry you want to delete.

LACP Port Settings

The LACP Port Settings window configures the Link Aggregation Control Protocol settings for the compliant ports on the Switch.

To access the LACP Port Settings window, click **L2 Features** > **LACP Port Settings** to reveal the following window:

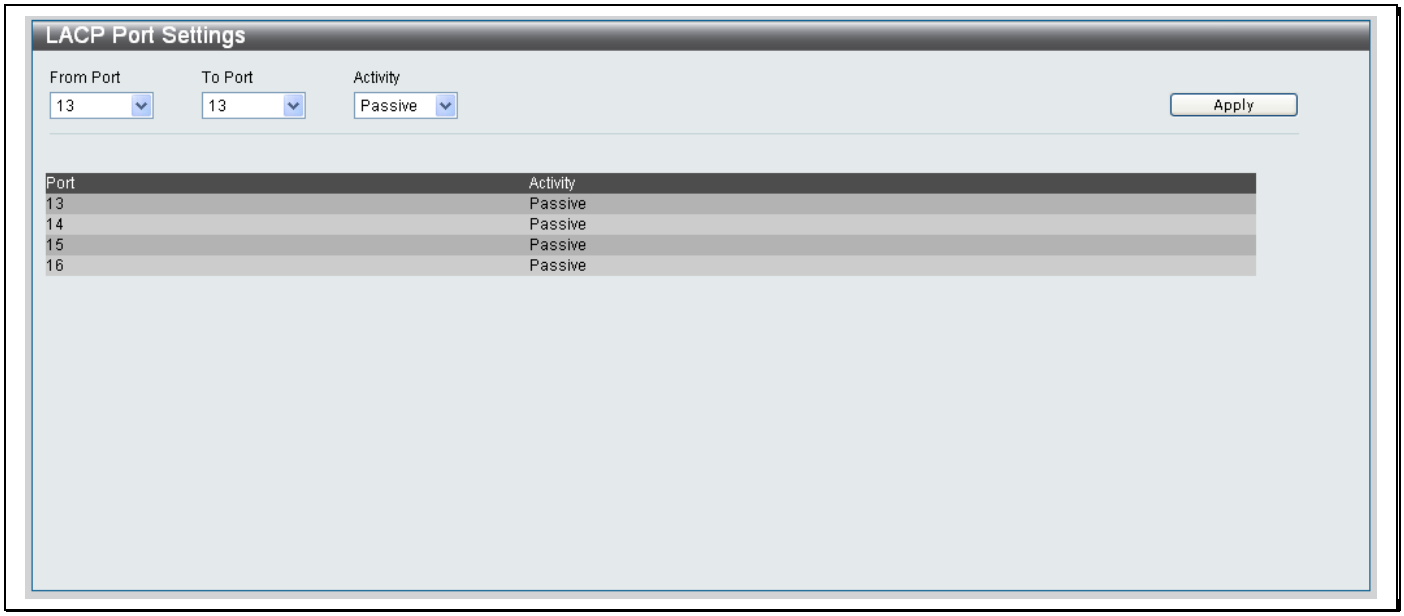


Figure 7- 18. LACP Port Settings window

- Choose the range of ports you want to control the LACP settings for from the **From Port** and **To Port** from the drop-down menus.
- Choose one of the following modes from the drop-down menu to determine if the LACP ports will process LACP control frames:

  Active- Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

  Passive- LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.

- Click the **Apply** to save the changes.

Traffic Segmentation

The Traffic Segmentation window configures the Traffic Segmentation settings. The primary purpose of the traffic segmentation function is to limit the traffic flow from a single port to a group of ports. The traffic segmentation function can provide security based on the ports in a VLAN. These ports can not to forward to some ports in the same VLAN, if these ports are not in the forwarding list of the source port. Each port has its own individual forwarding list. This port can only forward packets to one or several ports which are in the forwarding list. The traffic segmentation can only be used in a VLAN. The port can not forward packets to the ports which are members of another VLAN, even if these ports are in the forwarding list of the source port.

To access the Traffic Segmentation window, click **L2 Features** > **Traffic Segmentation** to reveal the following window:

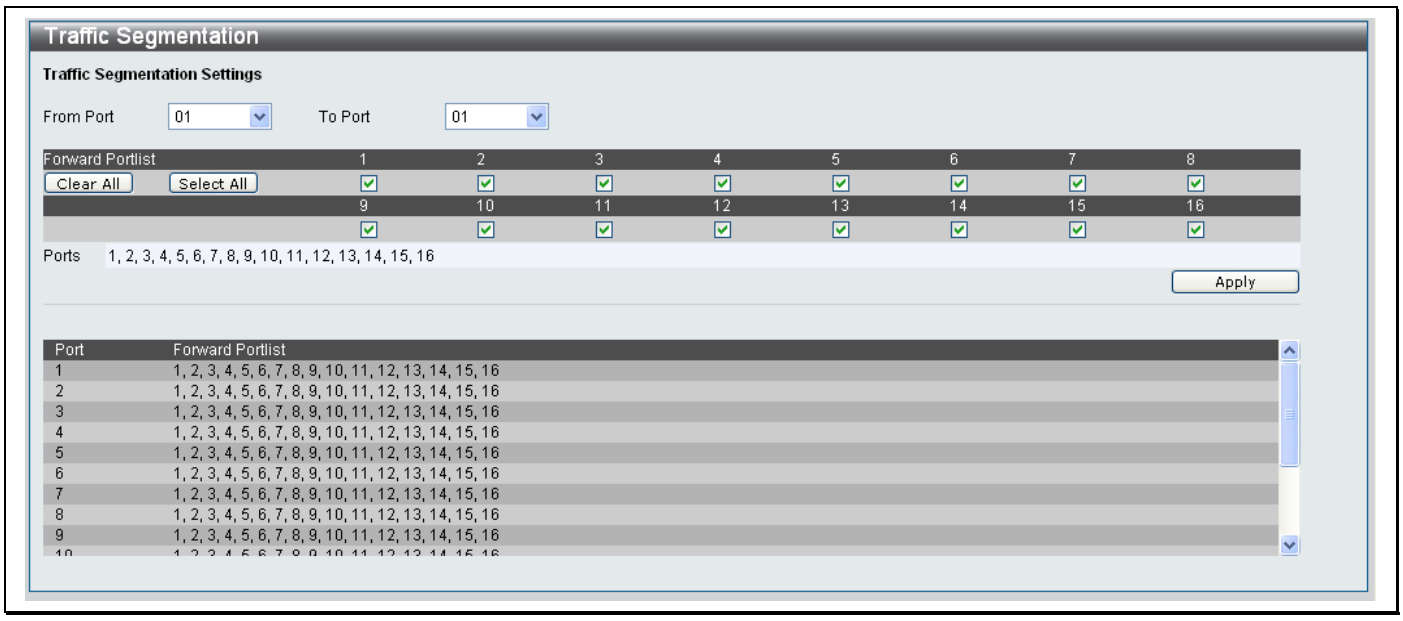


Figure 7- 19. Traffic Segmentation window

- Choose the range of ports you want to control the LACP settings for from the **From Port** and **To Port** from the drop-down menus.
- In the *Forward Portlist* tick the ports that the source port can forward to. The forwarding list of all the ports can be set by the traffic segmentation function. The default value of the forwarding list is all ports. This value only works with ports within the same VLAN.
- Click the **Clear All** button to de-select all the **Forward Portlist** entries. Click the **Select All** button to select all the **Forward Portlist** entries.
- Click the **Apply** to save the changes.

The table at the bottom of the screen displays all the configured *Forward Portlist* entries on the Switch.

IGMP Snooping

IGMP Snooping Settings

The IGMP Snooping Settings window is used to enable/disable IGMP Snooping. To access the IGMP Snooping Settings window, click **L2 Features** > **IGMP Snooping > IGMP Snooping Settings**.

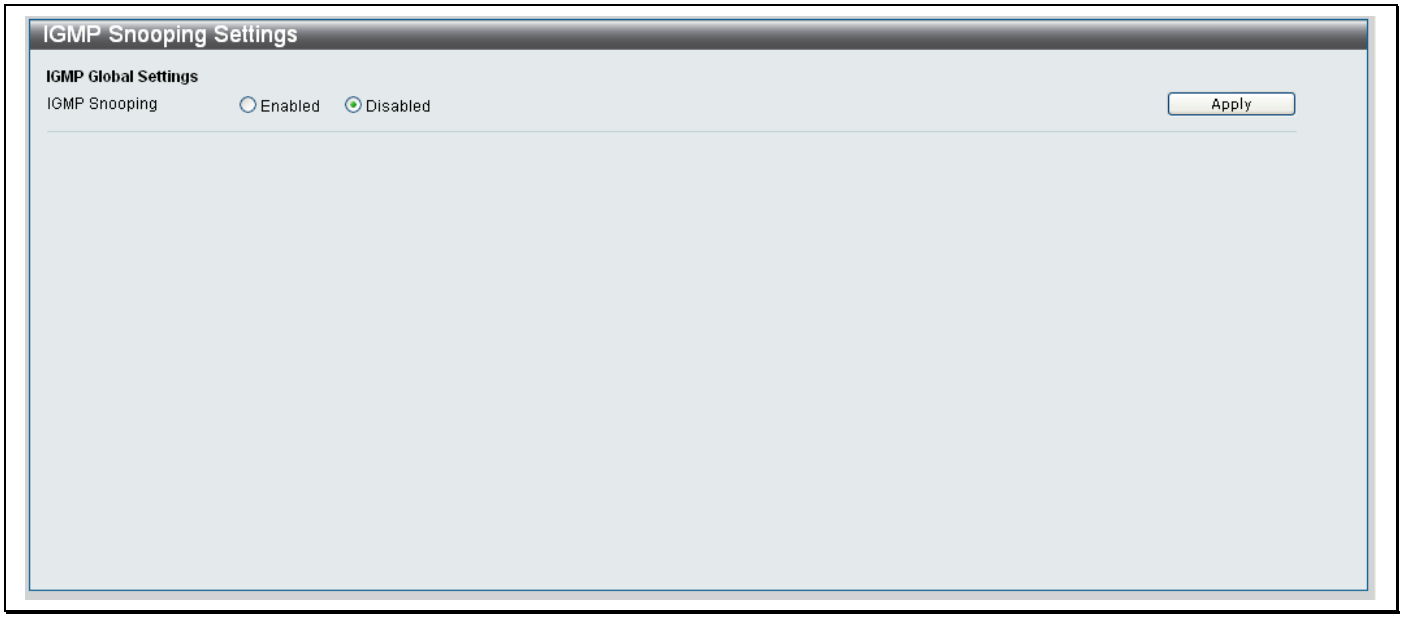


Figure 7- 20. IGMP Snooping Settings window

Click the **Enabled** radio button to enable IGMP Snooping. Click the **Disabled** button to disable IGMP Snooping.

IGMP Snooping Multicast VLAN Settings

The IGMP Snooping Multicast VLAN Settings window is used to create and modify IGMP Snooping Multicast VLAN's.

To access the IGMP Snooping Multicast VLAN Settings window click **L2 Features** > **IGMP Snooping > IGMP Snooping Multicast VLAN Settings**.

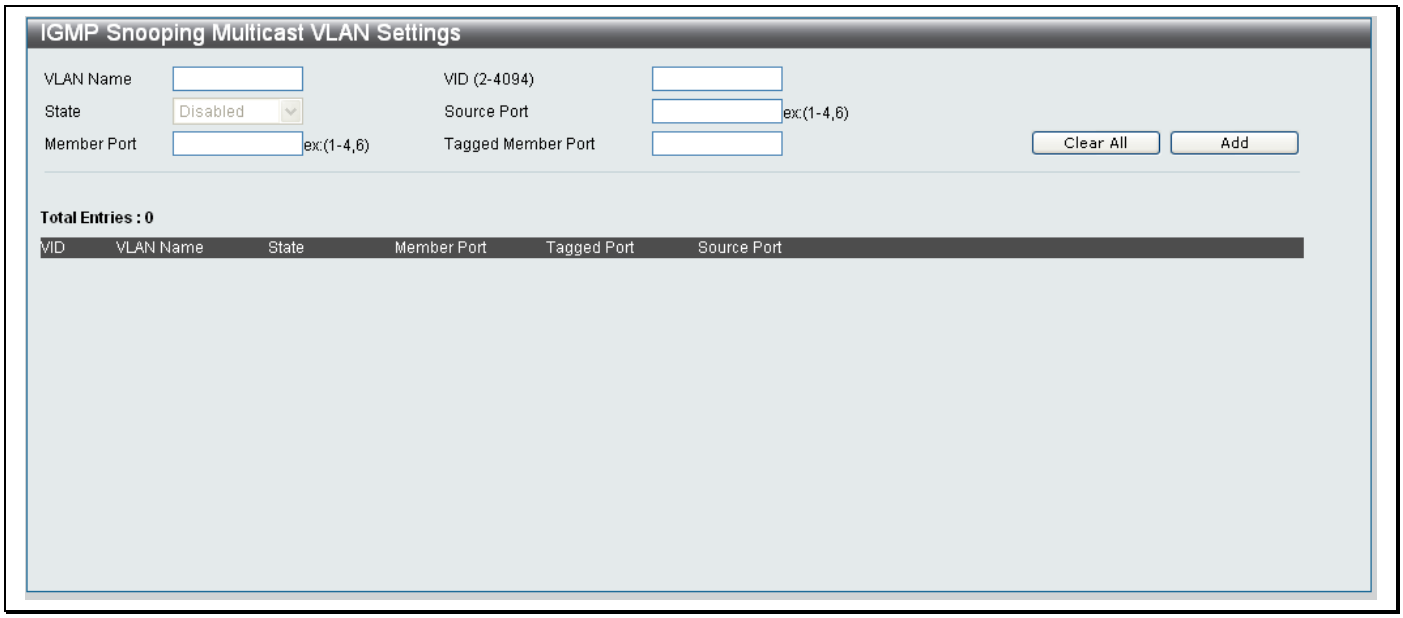


Figure 7- 21. IGMP Snooping Multicast VLAN Settings window

Configure the parameters as described below:

Parameter	Description
VLAN Name	Type the VLAN name of the VLAN that the IGMP Snooping Multicast VLAN will belong to.
VID (2-4094)	Type VID number of the VLAN that the IGMP Snooping Multicast VLAN will belong to.
State	Use the drop-down menu to specify if the IGMP Snooping Multicast VLAN settings should be *Enabled* or *Disabled* on the specified VLAN.
Source Port	Use the drop-down menu to specify if the IGMP Snooping Multicast VLAN Settings should be Enabled or Disabled on the specified VLAN.
Member Port	Type the *Member Port* numbers in this field.
Tagged Member Port	Type the *Tagged Member Port* numbers in this field.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 802.1s MSTP. 802.1d STP will be familiar to most networking professionals. However, since 802.1w RSTP and 802.1s MSTP has been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1d STP, 802.1w RSTP and 802.1s MSTP.

802.1s MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4096-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field).
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **STP Instance Settings** window when configuring an MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1w Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1s, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1d and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-1 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are

sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

802.1s MSTP	802.1w RSTP	802.1d STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
Discarding	Discarding	Blocking	No	No
Discarding	Discarding	Listening	No	No
Learning	Learning	Learning	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

Figure 7- 22. Comparing Port States

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1d/802.1w/802.1s Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1d format when necessary. However, any segment using 802.1d STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per user-defined group of ports basis.

STP Bridge Global Settings

To access the STP Bridge Global Settings window, click **L2 Features** > **Spanning Tree > STP Bridge Global Settings**

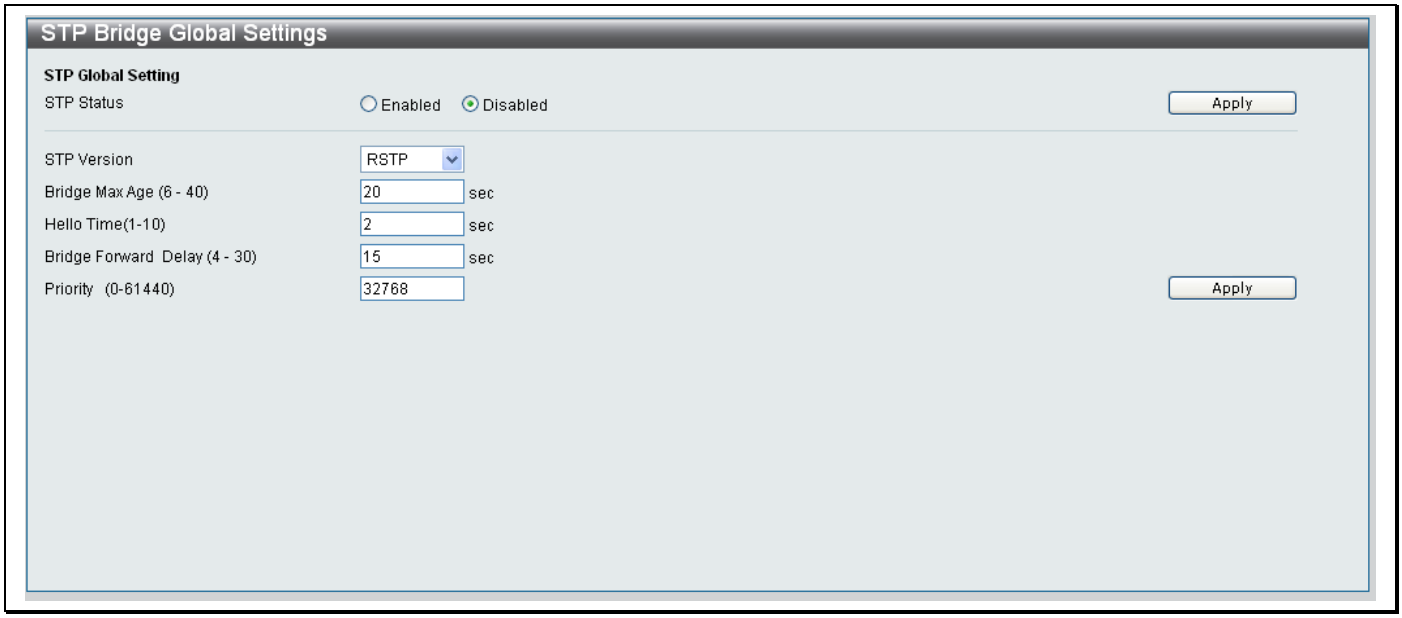


Figure 7- 23. STP Bridge Global Settings window

NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. 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)

Configure the parameters as described below:

Parameter	Description
STP Status	Click the **Enabled** radio button to enable Spanning-Tree Protocol. Click **Disabled** to disable. Click the **Apply** button next to **STP Status** to change the status.
STP Version	Use the drop-down menu to choose the desired version of STP to be implemented on the Switch. There are two choices: *STP* - Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. *RSTP* - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch.
Bridge Max Age (6-40)	This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20.
Hello Time (1-10)	This value can be set 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.
Bridge Forward Delay (4-30)	This value can be from *4* to *30* seconds. Any port on the Switch spends this time in

	the listening state while moving from the blocking state to the forwarding state.
Priority (0-61440)	Type in a numerical value between 0 and 61440 that is used to determine the root device, root port and designated port. The device with the highest priority becomes the root device. The lower the numerical value, the higher the priority. The default value is 32768.

Click the **Apply** button at the bottom of the window to apply the new Spanning-Tree configuration.

STP Port Settings

To access the STP Port Settings window, click **L2 Features** > **Spanning Tree > STP Port Settings**

The STP Port Settings window is divided into two main sections. The top section of the window is used to configure the STP Port Settings. The bottom section displays a table showing the current STP Ports Settings configuration.

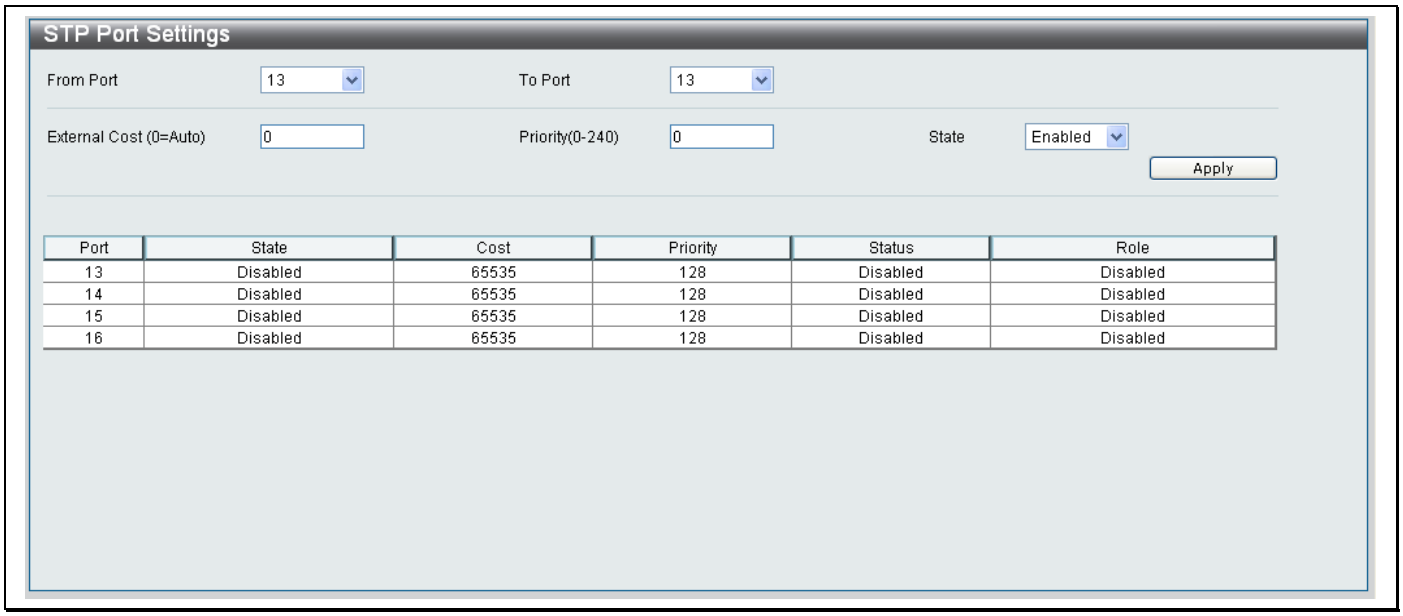


Figure 7- 24. STP Port Settings window

Configure the parameters as described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to select the range of ports that you want to configure the STP Ports settings for.
External Cost (0=Auto)	Type a value in this field to define the metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or manually as described below: *Automatically*- Inputting *0* in this field automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. *Manually*- Inputting a value between 1 and 65535 determines the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Priority (0-240)	Type in a Priority value between 0 and 240. The lower the number, the greater the probability the port will be chosen to forward packets.
State	Choose *Enabled* from the drop-down menu to enable STP for the specified ports. Choose *Disabled* to disable.

Click the **Apply** button at the bottom of the window to apply the new STP Port Settings.

Forwarding & Filtering

This folder contains windows for Unicast Forwarding and Multicast Forwarding.

Unicast Forwarding

The following figure and table describe how to set up **Unicast Forwarding** on the Switch and ONU. To access the Unicast Forwarding window, click **L2 Features> Forwarding & Filtering> Unicast Forwarding**.

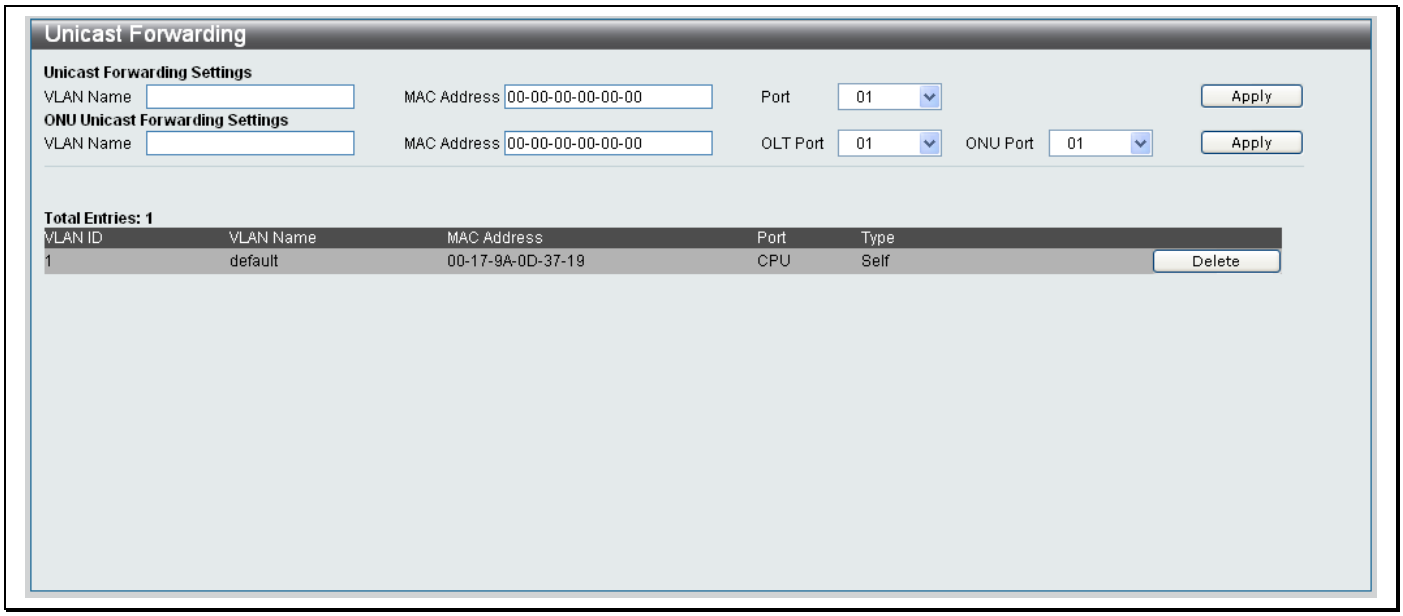


Figure 7- 25. Unicast Forwarding window

Configure the Switch Unicast Forwarding Settings in the parameters below the **Unicast Forwarding Settings** section:

Parameter	Description
VLAN Name	Type the VLAN name of the VLAN where the MAC Address resides.
MAC Address	Type the MAC address to which the packets need to be statically forwarded to. This must be a Unicast MAC Address.
Port	Use the drop-down menu to select the port number where the MAC Address entered above resides.

Click the **Apply** button to add the Switch Unicast Forwarding entry.

Configure the ONU Unicast Forwarding Settings in the parameters below the **ONU Unicast Forwarding Settings** section:

Parameter	Description
VLAN Name	Type the VLAN name of the VLAN where the MAC Address resides.
MAC Address	Type the MAC address to which the packets need to be statically forwarded to. This must be a Unicast MAC Address.
OLT Port	Use the drop-down menu to select the OLT port number where the MAC Address entered above resides.
ONU Port	Use the drop-down menu to select the ONU port number where the MAC Address entered above resides.

Click the **Apply** button to add the ONU Unicast Forwarding entry.

Multicast Forwarding

The following figure and table describe how to set up **Multicast Forwarding** on the Switch and ONU. To access the **Multicast Forwarding** window, click **L2 Features> Forwarding & Filtering> Multicast Forwarding**.

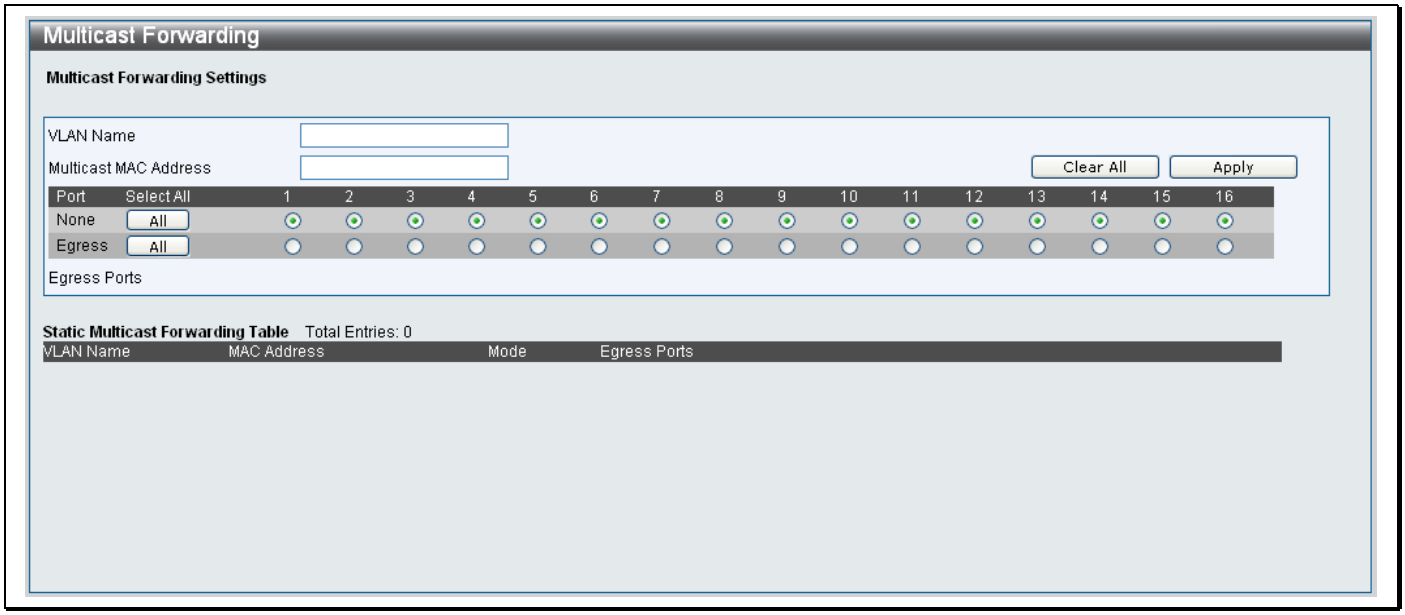


Figure 7- 26. Multicast Forwarding window

The Multicast Forwarding window is divided into two sections. The top half of the window is used to add a new Multicast Forwarding entry and the bottom half is used to display the existing entries in the Switch's Static Multicast Forwarding Table.

Adding a new Multicast Forwarding Entry

To add a new Multicast Forwarding Entry, configure the parameters as described below:

Parameter	Description
VLAN Name	The VLAN Name of the VLAN to which the corresponding MAC address belongs.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port 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. When None is chosen, the port will not be a member of the Static Multicast Group. *Egress* - The port is a static member of the multicast group.

Click the **Apply** button to add the new Multicast Forwarding entry.

Section 8

QoS

Bandwidth Control

Traffic Control

802.1p Default Priority

802.1p User Priority

QoS Scheduling Mechanism

The Switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (Voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the Switch implements 802.1P priority queuing.

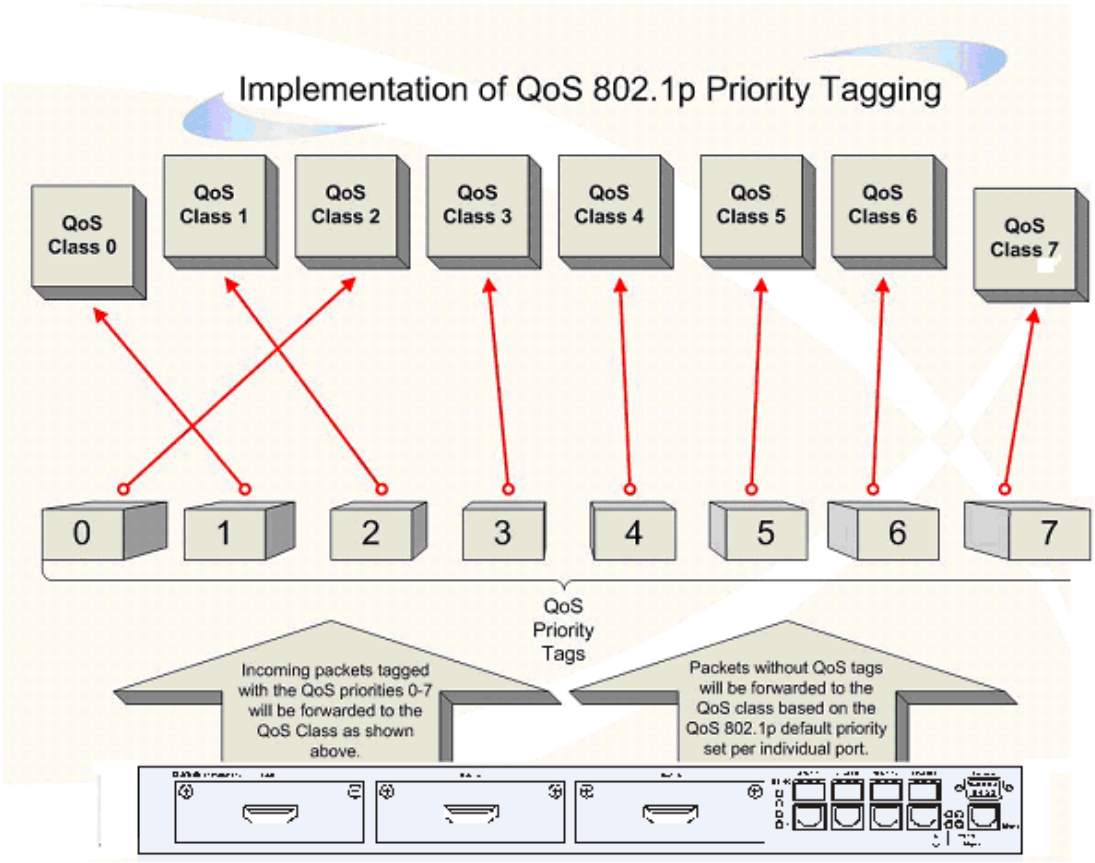


Figure 8- . Mapping QoS on the Switch

The picture above shows the default priority setting for the Switch. Class-7 has the highest priority of the eight priority queues on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag tagged. Then the user may forward these tagged packets to designated queues on the Switch where they will be emptied, based on priority.

For example, let's say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the

administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This result's in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has eight priority queues. These priority queues are labeled as 7, the high queue to 0, the lowest queue. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority tags as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

For strict priority-based scheduling, any packets residing in the higher priority queues are transmitted first. Multiple strict priority queues empty based on their priority tags. Only when these queues are empty, are packets of lower priority transmitted.

For weighted round robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the Switch has eight priority queues (and eight Classes of Service) for each port on the Switch.

Bandwidth Control

The **Bandwidth Control** window is used to place a ceiling on the transmitting and receiving data rates for any selected port. Click **QoS> Bandwidth Control** to access the **Bandwidth Control** window:

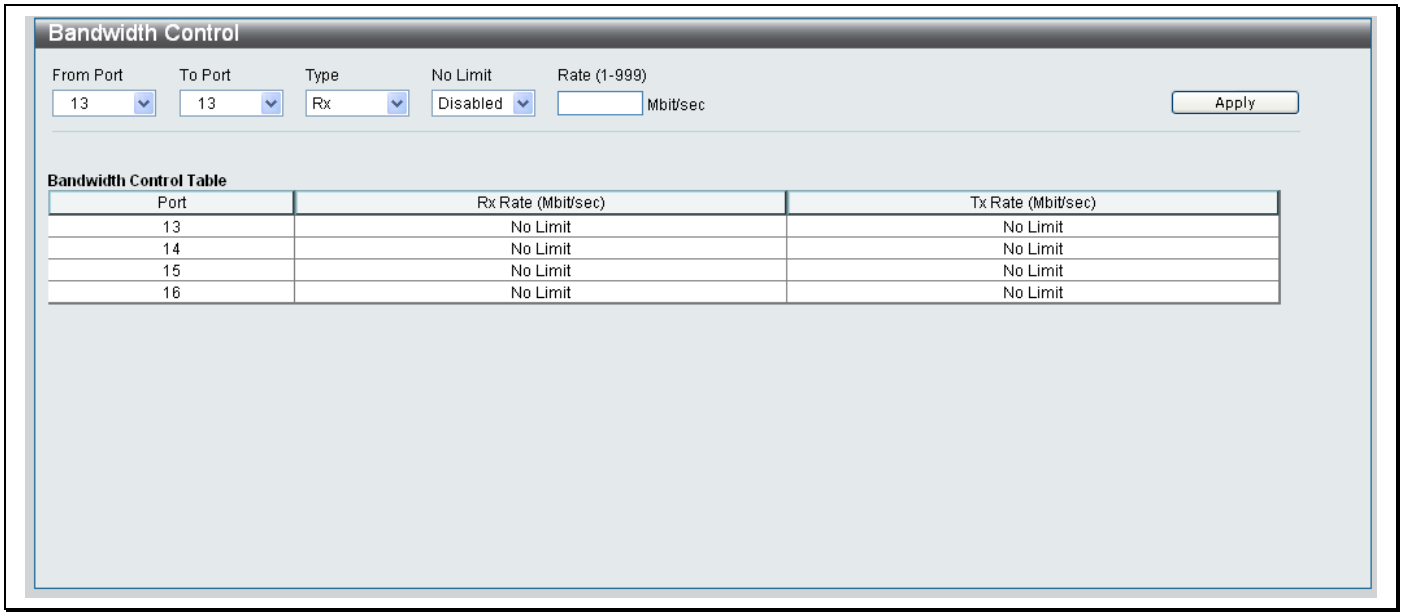


Figure 8- 2. Bandwidth Control window

Configure the parameters as described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to choose a consecutive group of ports that need be configured.
Type	Use the drop-down menu to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	Use the drop-down menu you to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.
Rate (1-156249)	Type the data rate in this field, in Mbits per second that will be the limit for the selected port. The value must be between *1* and 999 Mbit/sec.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured Bandwidth Settings will be displayed in the **Bandwidth Contol Table** at the bottom of the window.

Traffic Control

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as part of a normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recoup it using the **Port Settings** window in the **Configuration** folder and selecting the disabled port and returning it to an Enabled status.

To view the following window to configure Traffic Control, click **QoS > Traffic Control**.

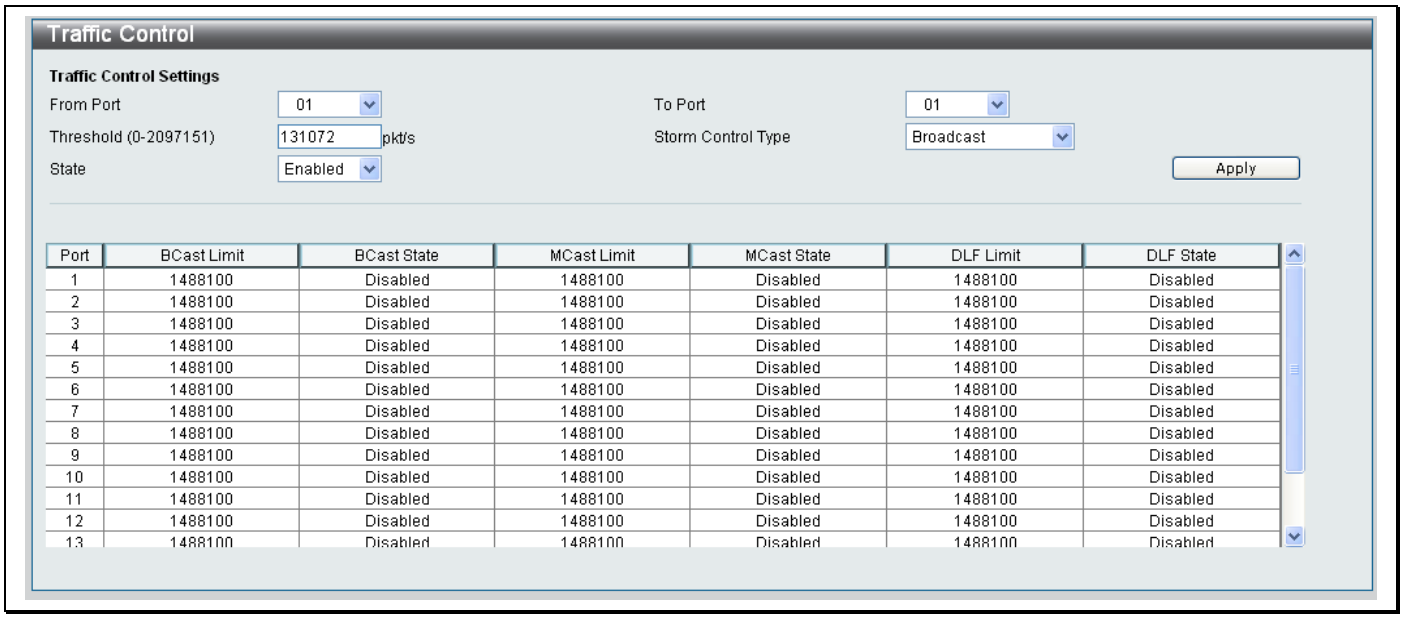


Figure 8- 3. Traffic Control window

Configure the parameters as described below:

Parameter	Description
From Port / To Port	Use the drop-down menus to choose a consecutive group of ports that need be configured.
Threshold (0-2097151)	Type a value to define the upper threshold at which the specified traffic control is switched on. The value defines the number of *Broadcast* / *Multicast* / *Unknown Unicast* packets received by the Switch that will trigger the storm traffic control measures.
Storm Control Type	Use the drop-down menu to choose if the ports should use *Broadcast*, *Multicast* or *Unknown Unicast* Storm Control Type.
State	Choose *Enabled* from the drop-down menu to enable the Traffic Control Setting. Choose *Disabled* to disable.

Click **Apply** to set the Traffic Control for the selected ports. Results of configured Traffic Control Settings will be displayed in the table at the bottom of the window.

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. To access the **802.1p Default Priority** window, click **QoS**> **802.1p Default Priority**.

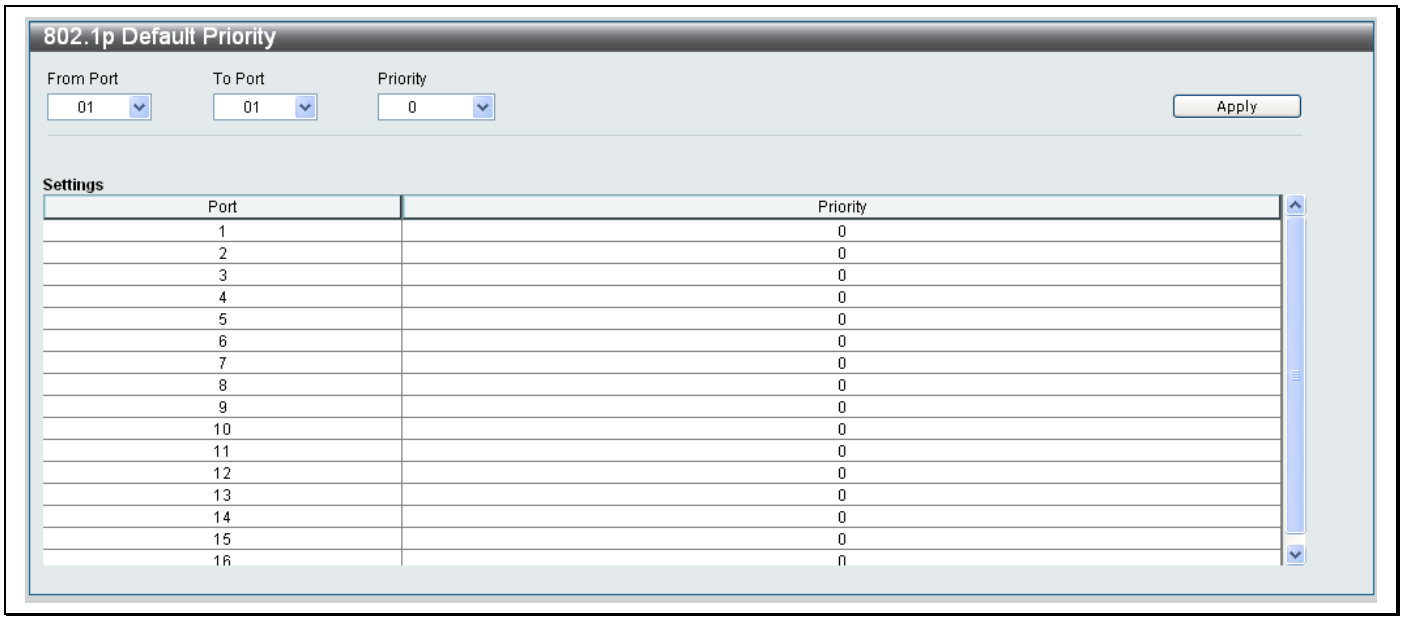


Figure 8- 4. 802.1p Default Priority window

Use the drop-down menus at the top of the window to assign a default 802.1p priority to any give port of the Switch. The priority queues are numbered from 0, the lowest priority, to 7, the highest priority. Click **Apply** to implement the changes.

802.1p User Priority

The Switch allows the assignment of a user priority to each of the 802.1p priorities. To access the **802.1p User Priority** window, click **QoS**> **802.1p User Priority**.

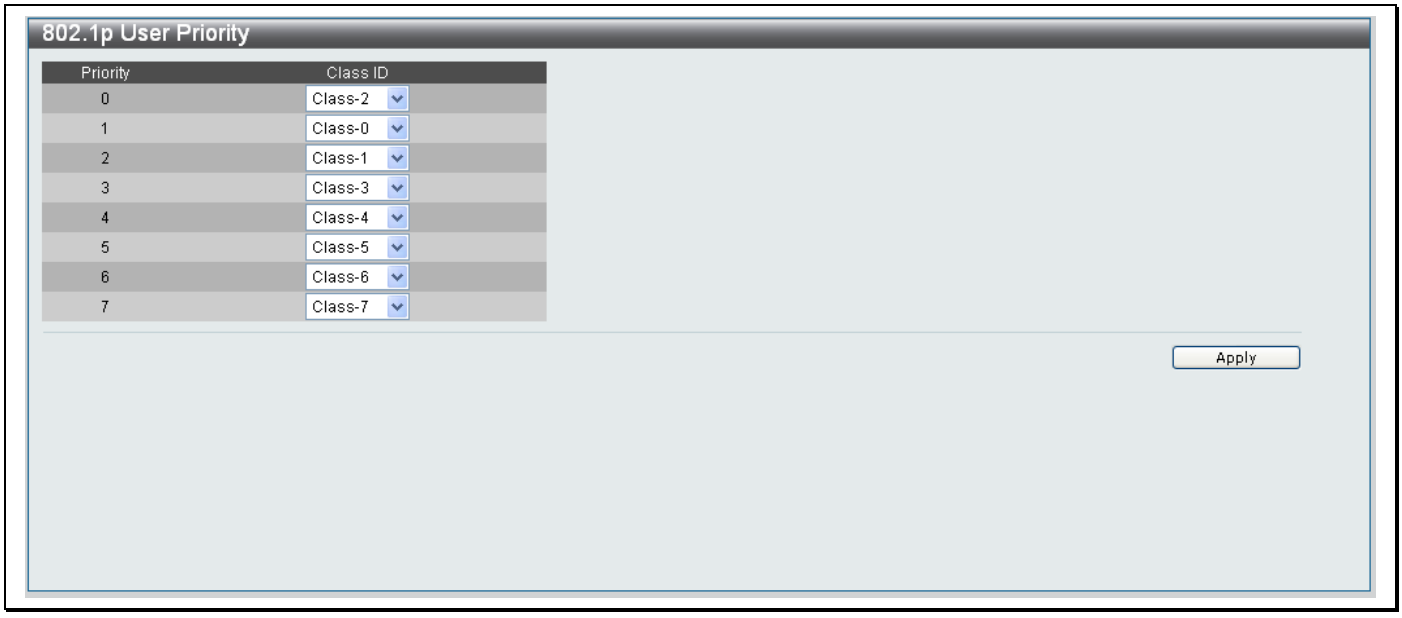


Figure 8- 5. 802.1p User Priority window

Use the drop-down menus to assign a *Class* to each of the eight levels of the 802.1p priorities.

Click **Apply** to implement the changes.

QoS Scheduling Mechanism

The **QOS Scheduling Mechanism** window displays the traffic scheduling mechanism. To access the **QOS Scheduling Mechanism** window, click **QoS > QoS Scheduling Mechanism**.

The Scheduling Mechanism that is supported by the DPN-3012-E RU is *strict*, as shown below:

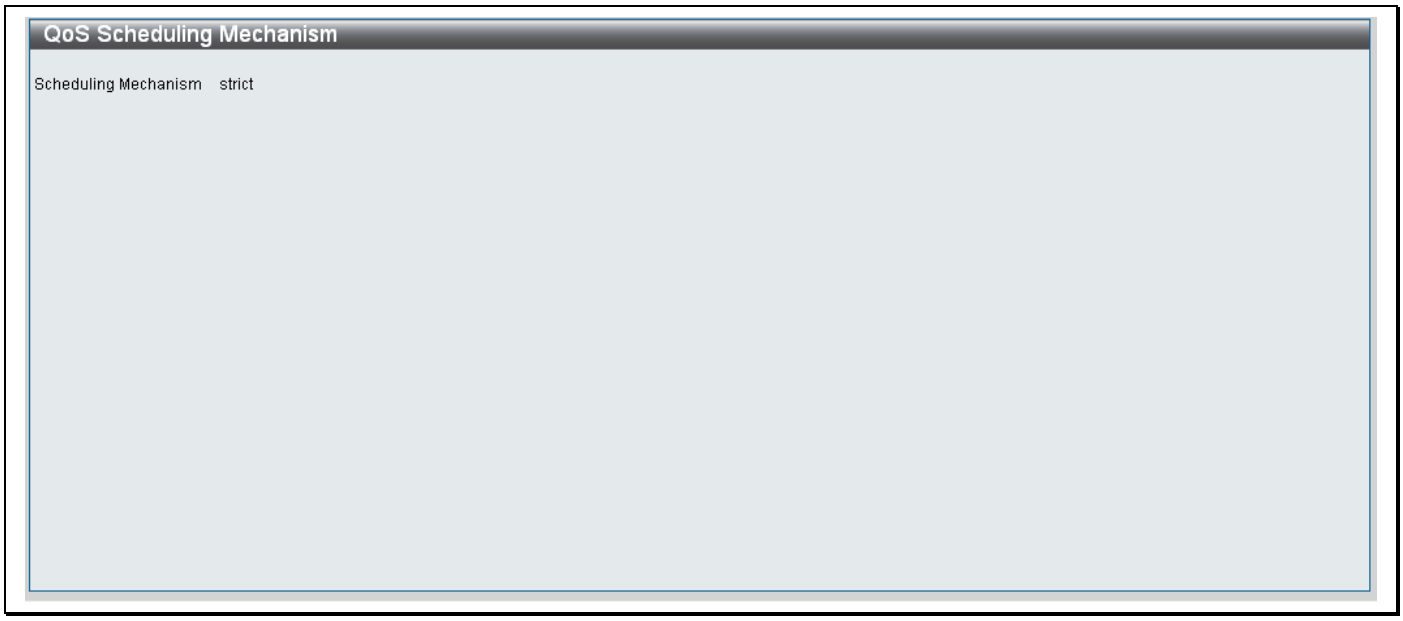


Figure 8- 6. QoS Scheduling Mechanism window

Section 9

ACL

ACL Configuration Wizard

Access Profile List

ACL Finder

Access profiles allow you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header.

ACL Configuration Wizard

Use the ACL Configuration Wizard to create a new ACL. To access the **ACL Configuration Wizard** window, click **ACL> ACL Configuration Wizard**.

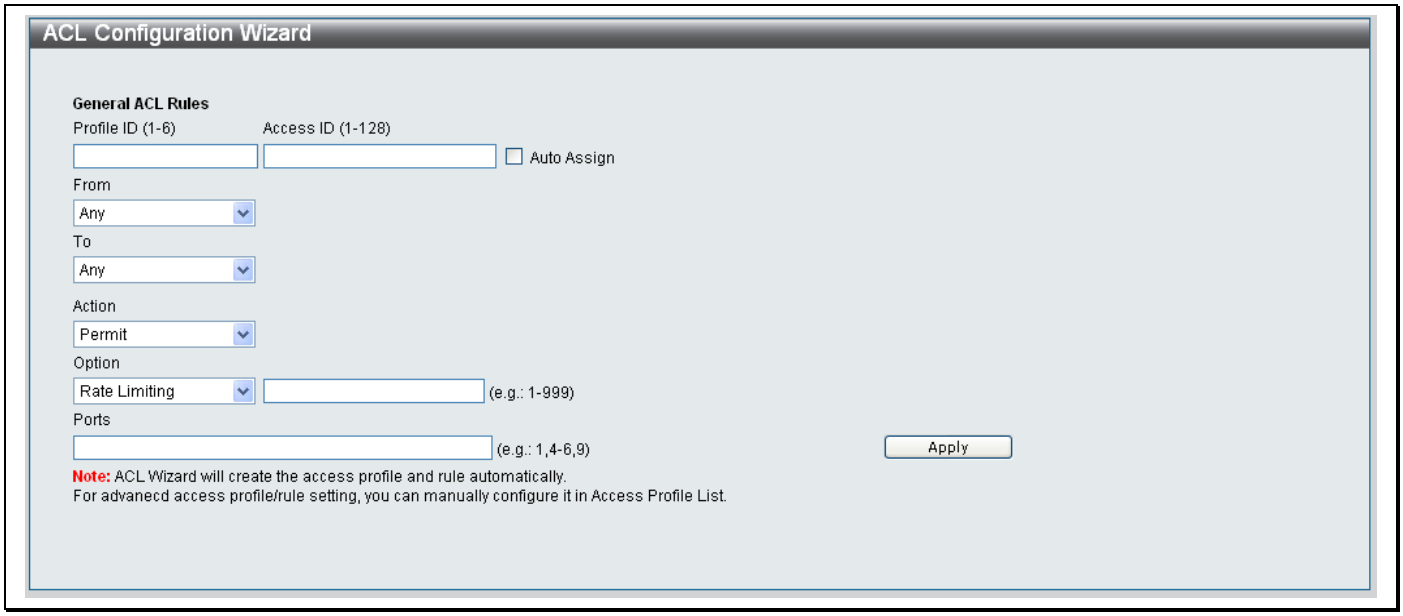


Figure 9- 1. ACL Configuration Wizard window

Configure the parameters as described below:

Parameter	Description
Profile ID (1 - 6)	Type a Profile ID between 1 and 6 to identify the new profile.
Access ID (1 – 128)	Type an ID between 1 and 128 to create a new Access ID. Tick the **Auto Assign** checkbox to have the switch Auto Assign this value.
From / To	Use the drop-down menus to define if the ACL Rule should be based on *MAC Address*, *IPv4 Address* or *IPv6 Address*.

Action	Use the drop-down menu to choose whether to create a *Permit* or *Deny* rule.
Option	Choose the ACL rule option from the drop-down menu. The following options are available: ▪ *Rate Limiting-* ▪ *Change 1P Priority-* ▪ *Replace DSCP-*
Ports	Type the port numbers that the ACL Rule will apply to.

Click **Apply** to add the new ACL Rule.

Access Profile List

The Access Profile List is used to Add ACL Profiles, Delete All profiles and displays all Access Profiles setup on the Switch.

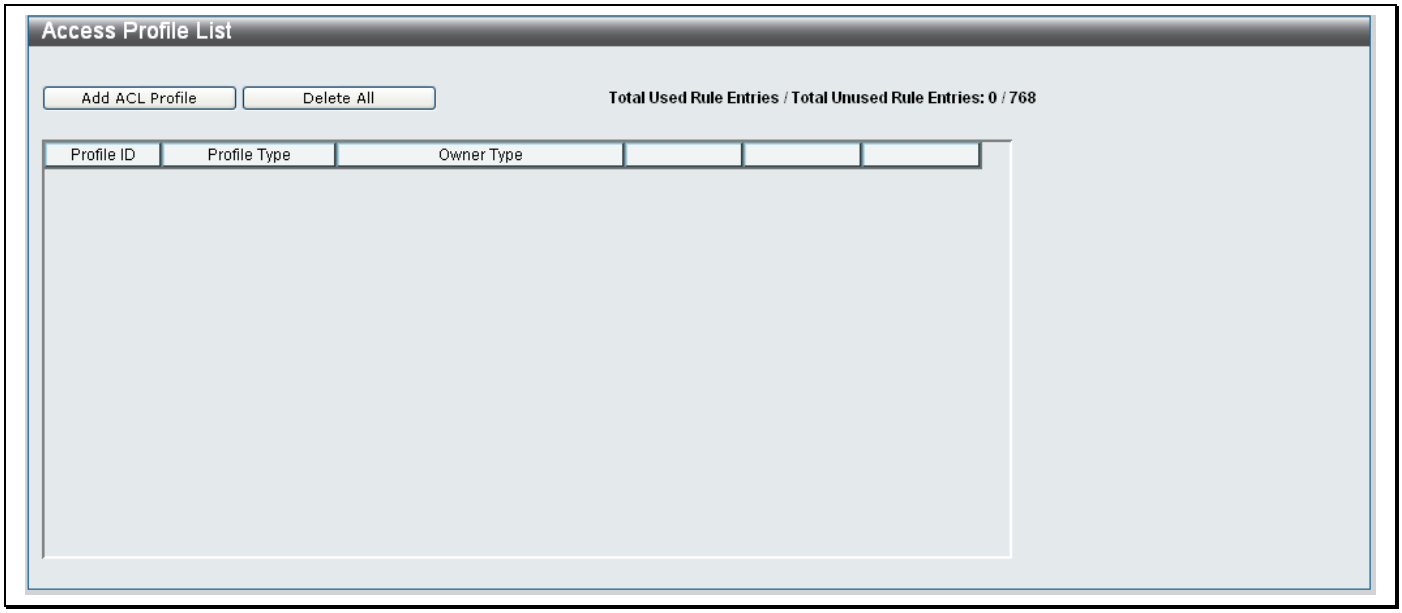


Figure 9- 2. Access Profile List window

Adding a new Access Profile

To add a new Access Profile, click the **Add ACL Profile** button.

The following window appears:

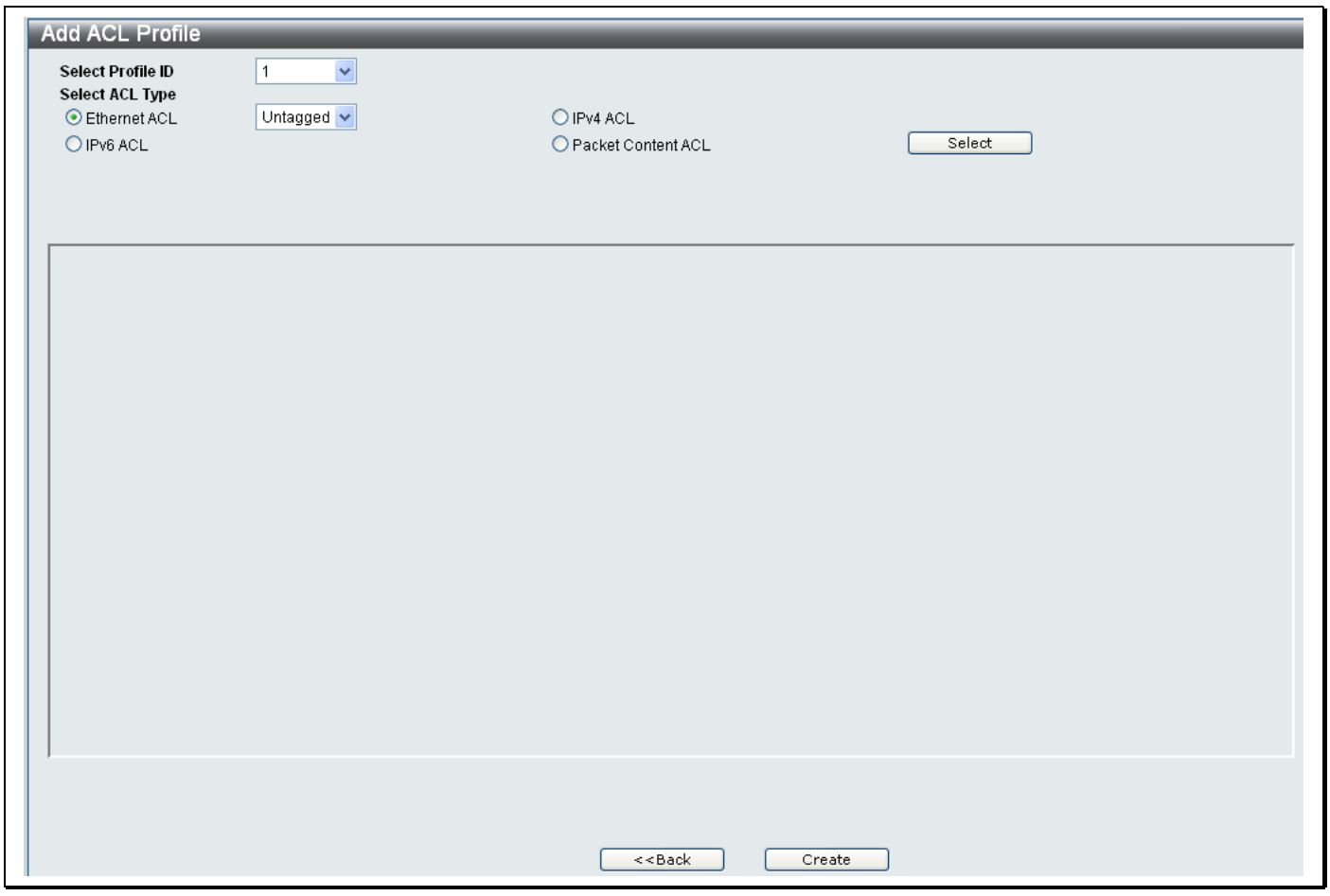


Figure 9- 3. Add ACL Profile window

Use the **Select Profile ID** drop-down menu to choose a Profile ID between *1* and *6*.

Choose a radio button for the type of ACL you want to add.

The types of ACL that are supported by this Switch are:

- Ethernet ACL
- IPv6 ACL
- IPv4 ACL
- Packet Content ACL

Click the **Select** button to add the ACL.

Adding a new Ethernet ACL Access Profile

- Click the **Ethernet ACL** radio button:

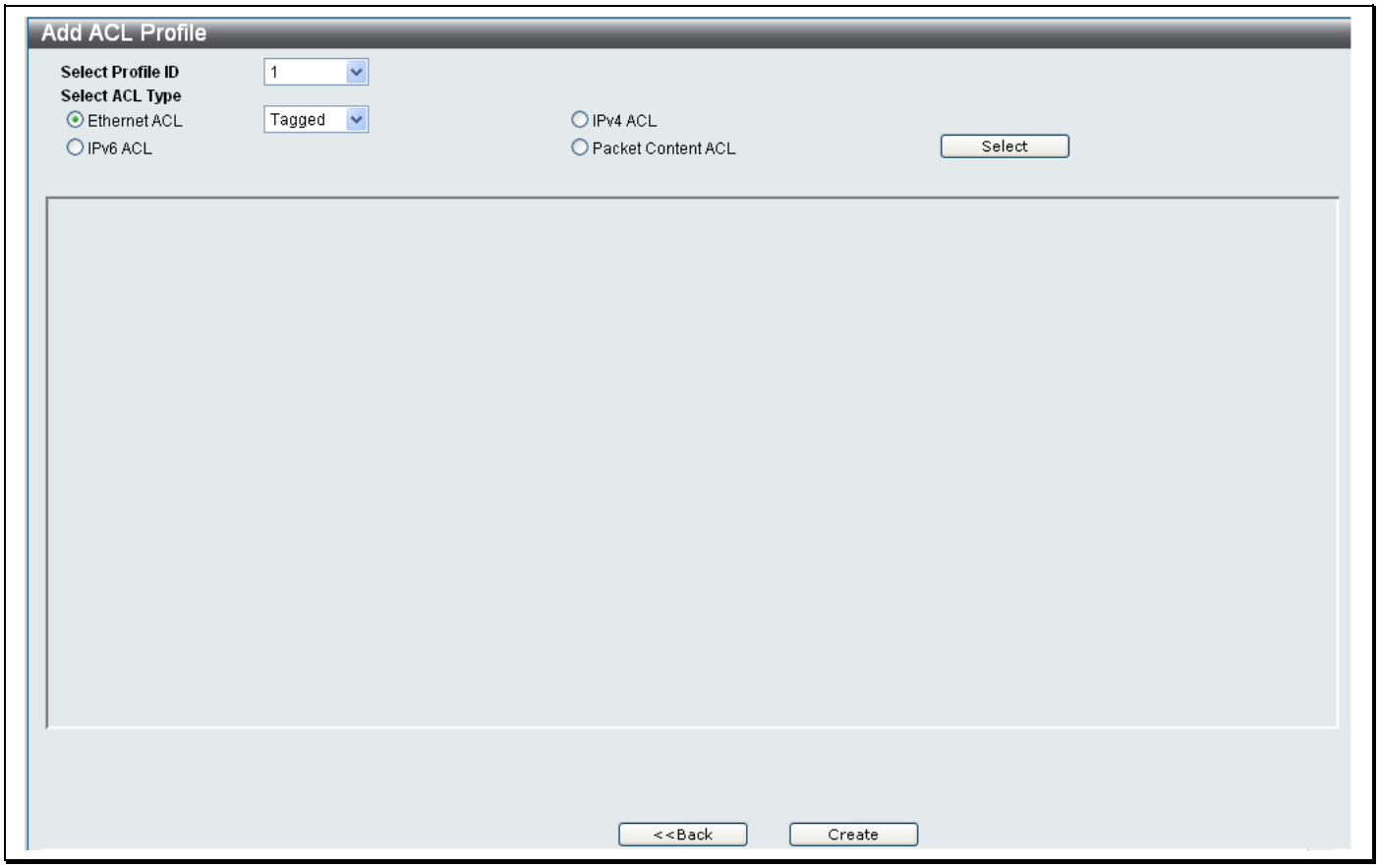


Figure 9- 4. Adding a new Ethernet ACL Access Profile

- Select an option from the **Ethernet ACL** drop-down menu.

  Choose *Tagged* to specify that the Ethernet ACL will apply to Tagged ports.

  Choose *Untagged* to specify that the Ethernet ACL will apply to Untagged ports.

- Click the **Select** button to reveal the following window:

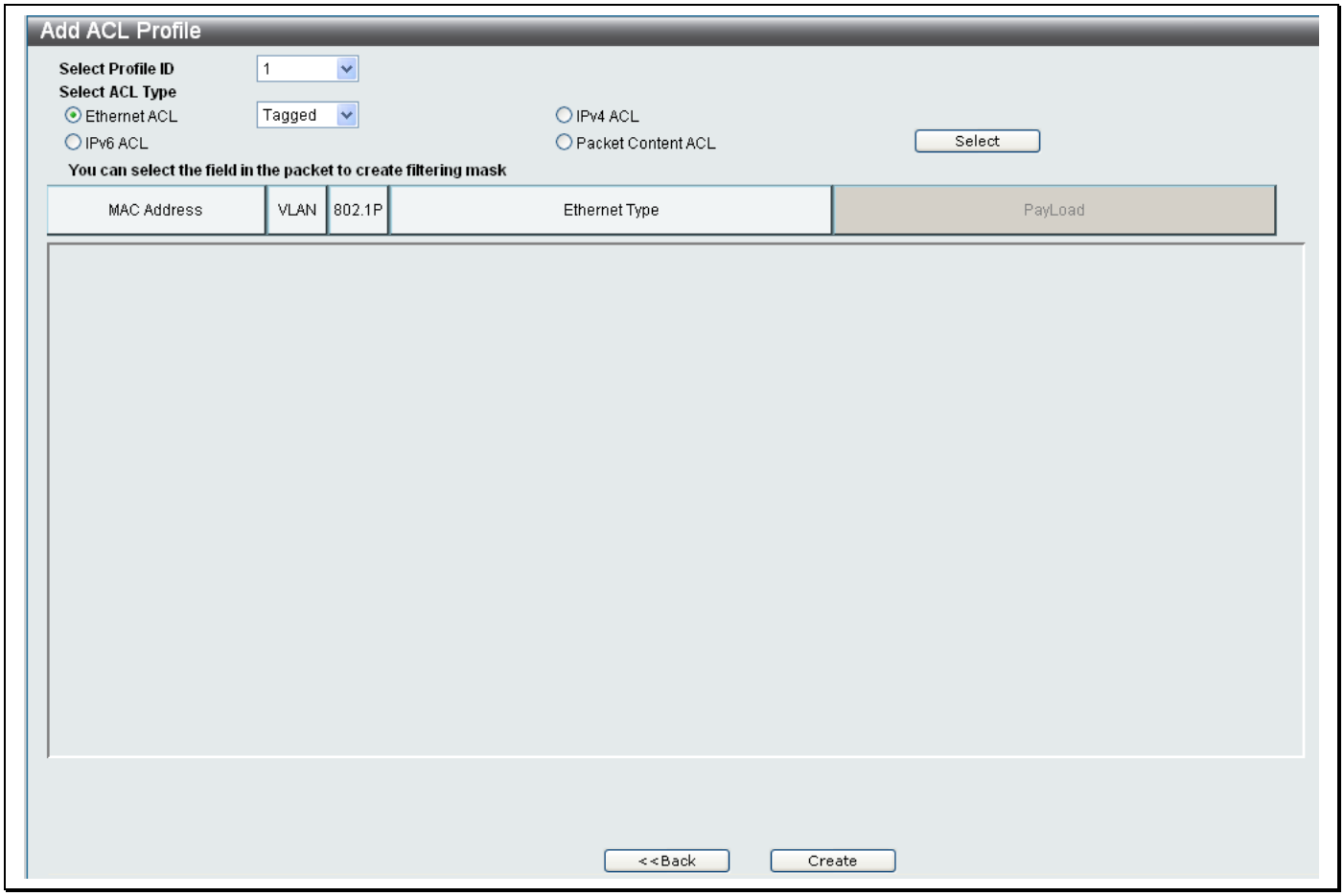


Figure 9- 5. Fields available when adding a new Ethernet ACL Access Profile

- Click the part of the packet that you want to add the filter to, this will highlight red as shown below:

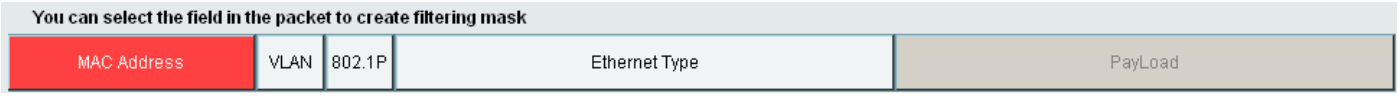


Figure 9- 6. Packet fields available when adding a new Ethernet ACL Access Profile

- This will reveal the different parameters that can be configured for the different parts of the packet:

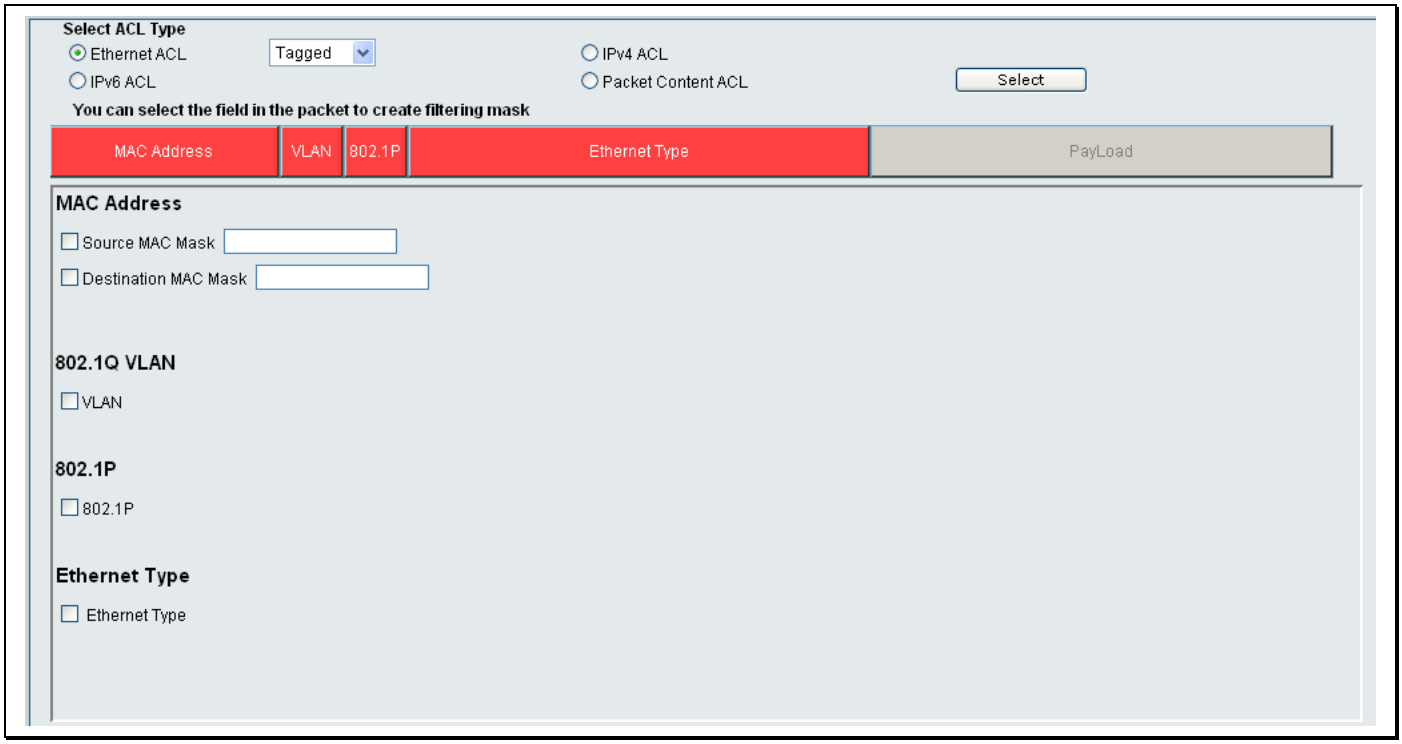


Figure 9- 7. Fields available when adding a new Ethernet ACL Access Profile

Configure the parameters for the different sections as described below:

Parameter	Description
MAC Address	
Source MAC Mask	Tick to add the filter to the Source MAC Mask part of the frame and type in the *Source MAC Mask Address* in the adjacent field.
Destination MAC Mask	Tick to add the filter to the Destination MAC Mask part of the frame and type in the *Destination MAC Mask Address* in the adjacent field.
802.1Q VLAN	
VLAN	If selecting a tagged frame type, tick to add the filter to the 802.1Q VLAN part of the frame. This field is not available for untagged frames.
802.1P	
802.1P	Tick to add the filter to the 802.1P part of the frame.
Ethernet Type	
Ethernet Type	Tick to add the filter to the Ethernet Type part of the frame.

Adding a new IPv6 ACL Profile

- Click the **IPv6 ACL** radio button:

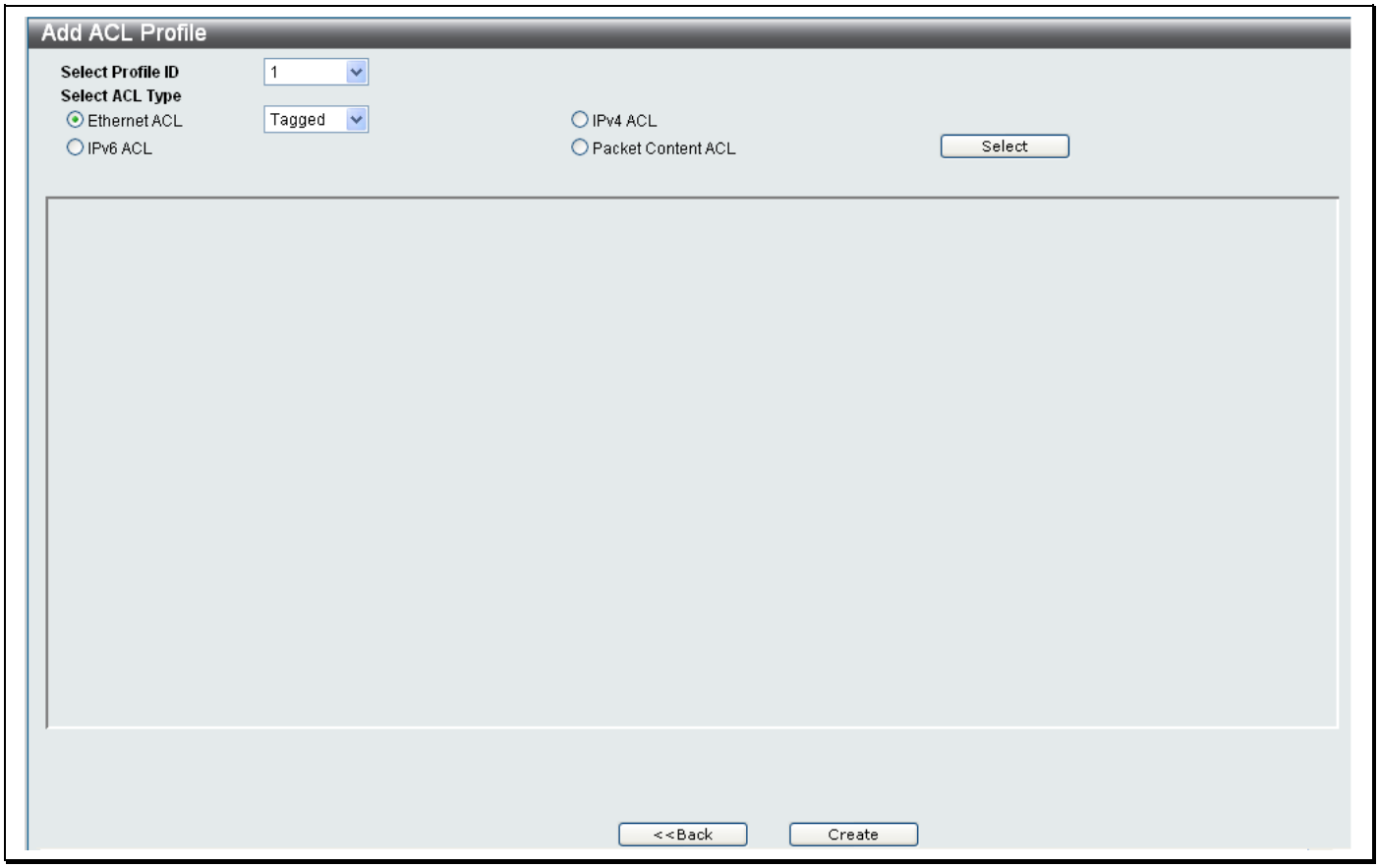


Figure 9- 8. Fields available when adding a new IPv6 ACL Access Profile

- Click the **Select** button to reveal the following window:

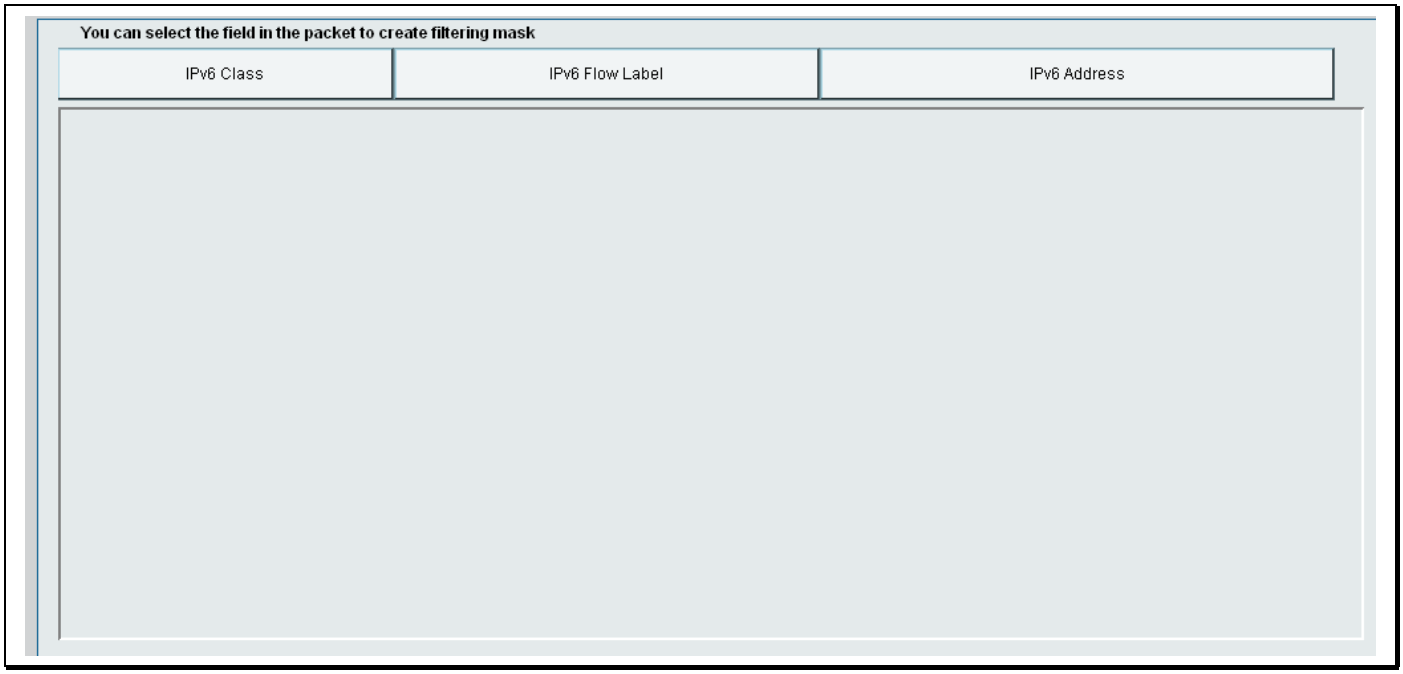


Figure 9- 9. Fields available when adding a new IPv6 ACL Access Profile

- Click the part of the packet that you want to add the filter to, this will highlight red as shown below:

Figure 9- 10. Packet fields available when adding a new Ethernet ACL Access Profile

- This will reveal the different parameters that can be configured for the different parts of the packet:

Configure the parameters for the different sections as described below:

Parameter	Description
IPv6 Class	
IPv6 Class	Tick the checkbox to specify that the filtering mask should apply to the IPv6 Class section of the frame.
IPv6 Flow Label	
IPv6 Flow Label	Tick the checkbox to specify that the filtering mask should apply to the IPv6 Flow Label section of the frame.
IPv6 Address	
IPv6 Source Address	Tick the checkbox and type in the IPv6 Source Address to specify that the filtering mask should apply to this IPv6 address.
IPv6 Destination Address	Tick the checkbox and type in the IPv6 Destination Address to specify that the filtering mask should apply to this IPv6 address.

Adding a new IPv4 ACL Profile

- Click the **IPv4 ACL** radio button:

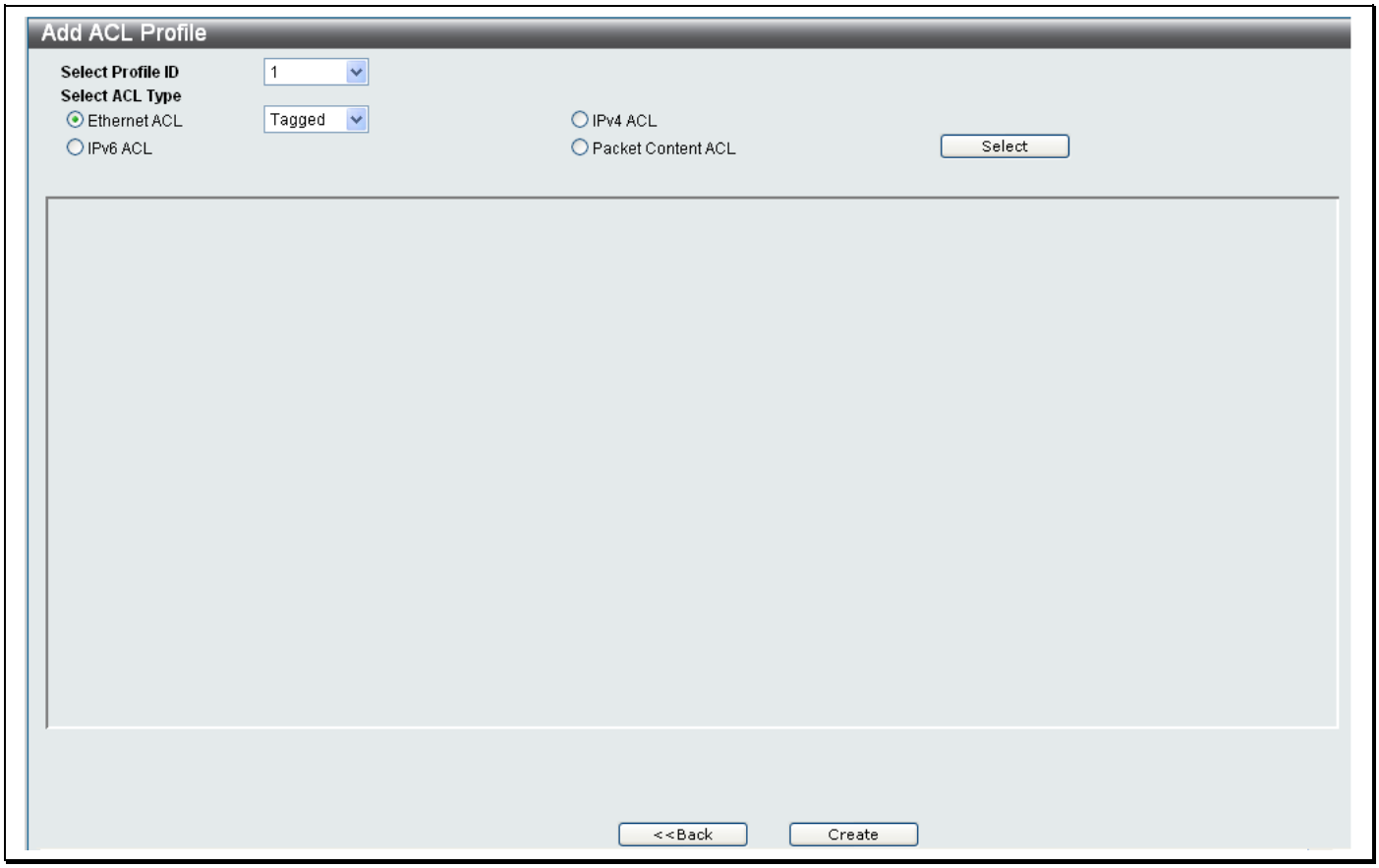


Figure 9- 11. Fields available when adding a new IPv4 ACL Profile

- Select an option from the **IPv4 ACL** drop-down menu.

  Choose *ICMP* to specify that the ACL rule will apply to ICMP traffic.

  Choose *IGMP* to specify that the ACL rule will apply to IGMP traffic.

  Choose *TCP* to specify that the rule applies to the range of TCP ports.

  Choose *UDP* to specify that the rule applies to the range of UDP ports.

  Choose *Protocol ID* to specify that the rule applies to the value of the Protocol ID

- If choosing *ICMP*, click the **Select** button and configure the parameters as described below:

Parameter	Description
IPv4 DSCP	
DSCP	Tick the checkbox to specify that the filtering mask should apply to the DSCP section of the frame.
IPv4 Address	
Source IP Mask	Type in a subnet mask to designate which part of the Source IP Address, set in the *Access Rule List*, should be filtered.
Destination IP Mask	Type in a subnet mask to designate which part of the Destination IP Address, set in the *Access Rule List*, should be filtered.

ICMP	
ICMP	Tick the checkbox to specify that the filtering mask should apply to the ICMP section of the frame.

- Click the **Create** button to add the new ACL Profile.
- A **Success** message indicated the new ACL Profile was added successfully.
- If choosing *IGMP*, click the **Select** button and configure the parameters as described below:

Parameter	Description
IPv4 DSCP	
DSCP	Tick the checkbox to specify that the filtering mask should apply to the DSCP section of the frame.
IPv4 Address	
Source IP Mask	Type in a subnet mask to designate which part of the Source IP Address, set in the *Access Rule List*, should be filtered.
Destination IP Mask	Type in a subnet mask to designate which part of the Destination IP Address, set in the *Access Rule List*, should be filtered.
IGMP	
IGMP	Tick the checkbox to specify that the filtering mask should apply to the IGMP section of the frame.

- Click the **Create** button to add the new ACL Profile.
- A **Success** message indicated the new ACL Profile was added successfully.
- If choosing *TCP*, click the **Select** button and configure the parameters as described below:

Parameter	Description
IPv4 DSCP	
DSCP	Tick the checkbox to specify that the filtering mask should apply to the DSCP section of the frame.
IPv4 Address	
Source IP Mask	Type in a subnet mask to designate which part of the Source IP Address, set in the *Access Rule List*, should be filtered.
Destination IP Mask	Type in a subnet mask to designate which part of the Destination IP Address, set in the *Access Rule List*, should be filtered.
TCP	
TCP	Tick the checkbox to specify that the filtering mask should apply to the TCP section of the frame.
Source Port Mask (0-FFFF)	Input the TCP Source Port Number.
Destination Port Mask (0-FFFF)	Input the TCP Destination Port Number.
TCP Flag Bits	Input the TCP flag fields.

- Click the **Create** button to add the new ACL Profile.
- A **Success** message indicated the new ACL Profile was added successfully.

- If choosing *UDP*, click the **Select** button and configure the parameters as described below:

Parameter	Description
IPv4 DSCP	
DSCP	Tick the checkbox to specify that the filtering mask should apply to the DSCP section of the frame.
IPv4 Address	
Source IP Mask	Type in a subnet mask to designate which part of the Source IP Address, set in the *Access Rule List*, should be filtered.
Destination IP Mask	Type in a subnet mask to designate which part of the Destination IP Address, set in the *Access Rule List*, should be filtered.
UDP	
UDP	Tick the checkbox to specify that the filtering mask should apply to the TCP section of the frame.
Source Port Mask (0-FFFF)	Input the UDP Source Port Mask Number.
Destination Port Mask (0-FFFF)	Input the UDP Destination Port Mask Number.

- Click the **Create** button to add the new ACL Profile.
- A **Success** message indicated the new ACL Profile was added successfully.

- If choosing *ProtocolID*, click the **Select** button and configure the parameters as described below:

Parameter	Description
IPv4 DSCP	
DSCP	Tick the checkbox to specify that the filtering mask should apply to the DSCP section of the frame.
IPv4 Address	
Source IP Mask	Input the Source IP address.
Destination IP Mask	Input the Destination IP address.
Protocol ID	
Protocol ID Mask	Type in a value to specify that the rule will apply to IP protocol ID traffic.
User Define	Type in a value to specify the L4 part of the mask.

- Click the **Create** button to add the new ACL Profile.
- A **Success** message indicated the new ACL Profile was added successfully.

- If choosing *Packet Content ACL*, click the **Select** button and configure the parameters as described below:

Parameter	Description
Packet Content	
Offset 0-15	Tick the checkbox to specify that the frame content mask should have an offset value of 0-15.
Offset 16-31	Tick the checkbox to specify that the frame content mask should have an offset value of 16-31.
Offset 32-47	Tick the checkbox to specify that the frame content mask should have an offset value of 32-47.
Offset 48-63	Tick the checkbox to specify that the frame content mask should have an offset value of 48-63.
Offset 64-79	Tick the checkbox to specify that the frame content mask should have an offset of value of 64-79.

- Click the **Create** button to add the new ACL Profile.
- A **Success** message indicated the new ACL Profile was added successfully.

Viewing the details of an existing Access Profile

- To view the details of an existing Access Profile, click the **Show Details** button, adjacent to the Access Profile you want to view.
- The details are displayed in a new window as shown below:

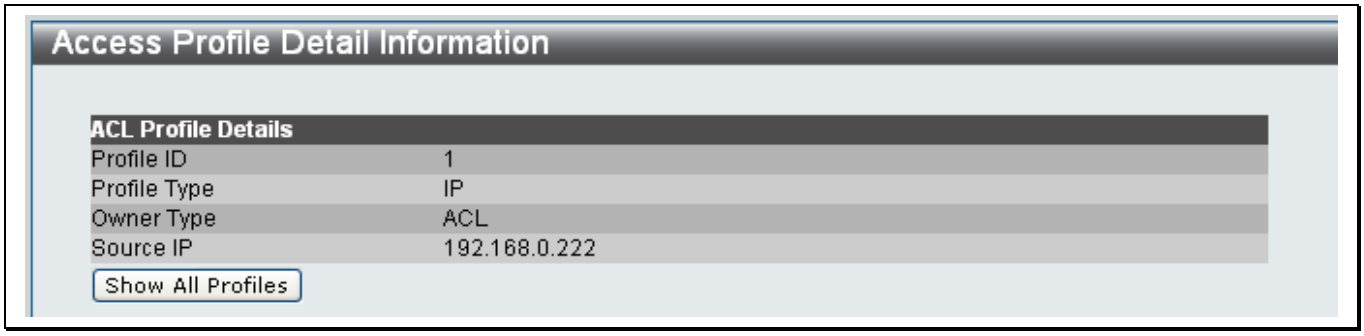


Figure 9- 12. Access Profile Detail Information window

- Click the **Show All Profiles** button to return to the previous screen.

Add/Viewing Rules of an existing Access Profile

- To add or view the rules of an existing Access Profile, click the **Add/View Rules** button, adjacent to the Access Profile you want to add or view the rules for.
- The following window appears, showing all the rules that have been previously configured for the Access Profile:

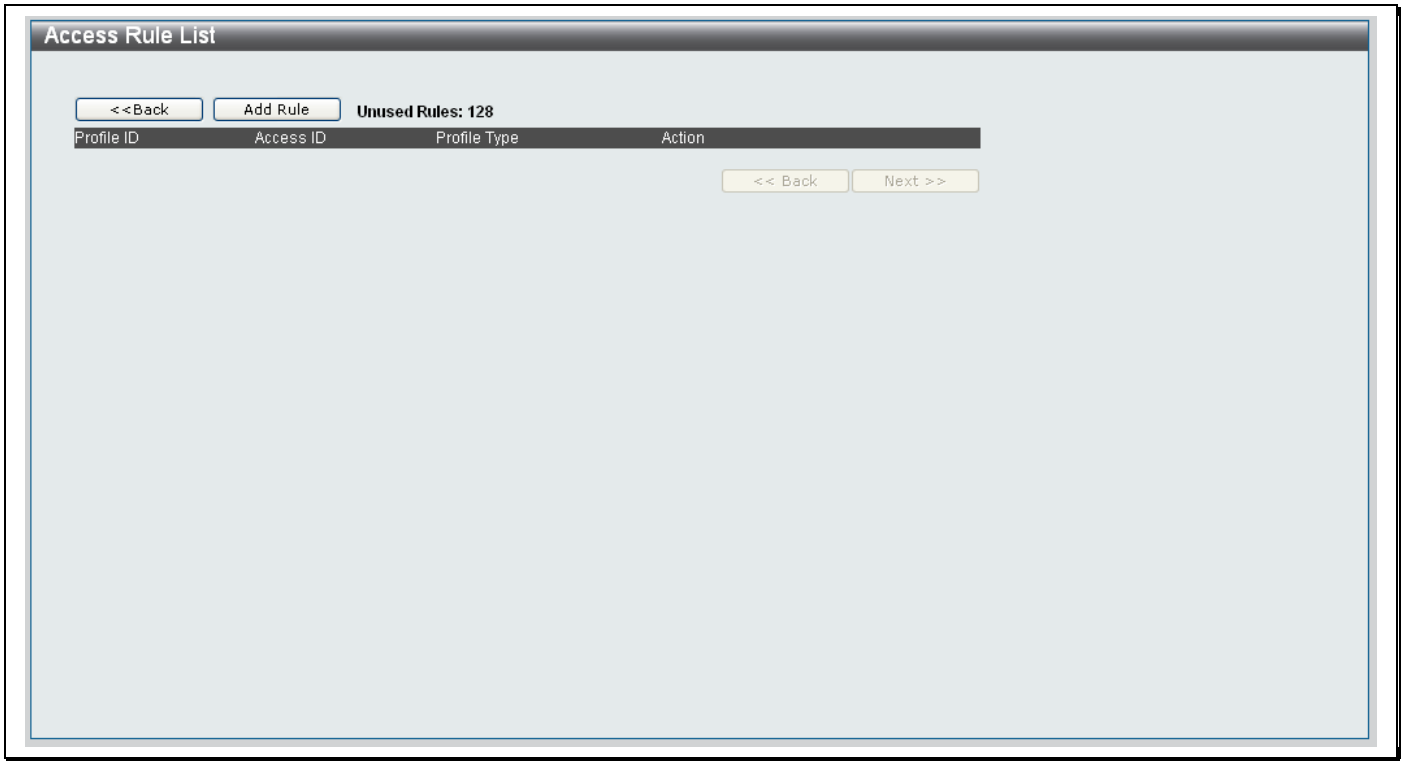


Figure 9- 13. Access Rule List window

Adding a new Access Rule

To add a new Access Rule, carry out the following.

1. Click the **Add Rule** button.
2. The **Add Access Rule** window appears as shown below:

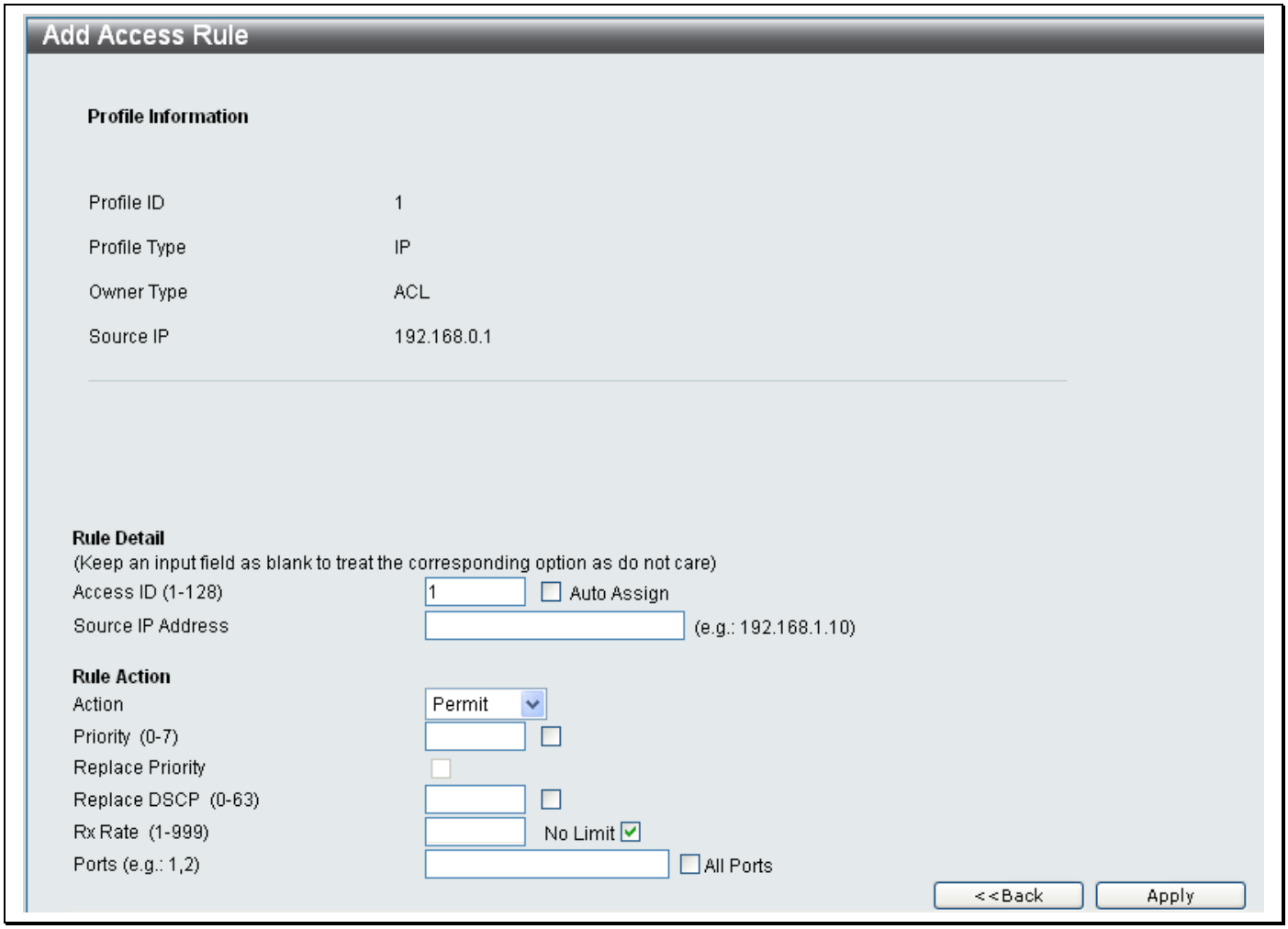


Figure 9- 14. Add Access Rule List window

3. Configure the parameters as explained below:

Parameter	Description
Rule Detail	
Access ID (1-128)	Type an ID for the Access rule between 1 and 128. Tick the **Auto Assign** checkbox have an Access ID automatically assigned.
Source IP Address	Type the *Source IP Address* for the Access rule.
Rule Action	
Action	Choose *Permit* from the drop-down menu to specify that packets matching the Access Profile are permitted by the Switch. Choose *Deny* to specify that packets matching the Access Profile are filtered by the Switch
Priority (0-7)	Type the priority number that the access profile will be remap the 802.1p priority field to on the Switch.
Replace Priority	Tick to enable the priority number to change a packet matching the access profile is received.

Replace DSCP (0-63)	Type a number between 0 and 63 to specify the number that the DSCP's of packets matching this access profile will be modified to
RX Rate (1-999)	Type a value between 1 and 999 to specify the received data rate limit. Tick the **No Limit** checkbox to specify no limit.
Ports (e.g : 1,2)	Type the *port numbers* that you want the Access Rule to apply to.

4. Click the **Apply** button to add the new Access Rule.

Deleting an Access Profile

- To delete an existing Access Profile, click the **Delete** button, adjacent to the Access Profile you want to delete.

Deleting all Access Profiles

- To delete all Access Profiles, click the **Delete All** button at the top of the window.

ACL Finder

Use the **ACL Finder** window to identify any rule that has been assigned to a specific port.

To access the **ACL Finder** window, click **ACL> ACL Configuration Wizard**.

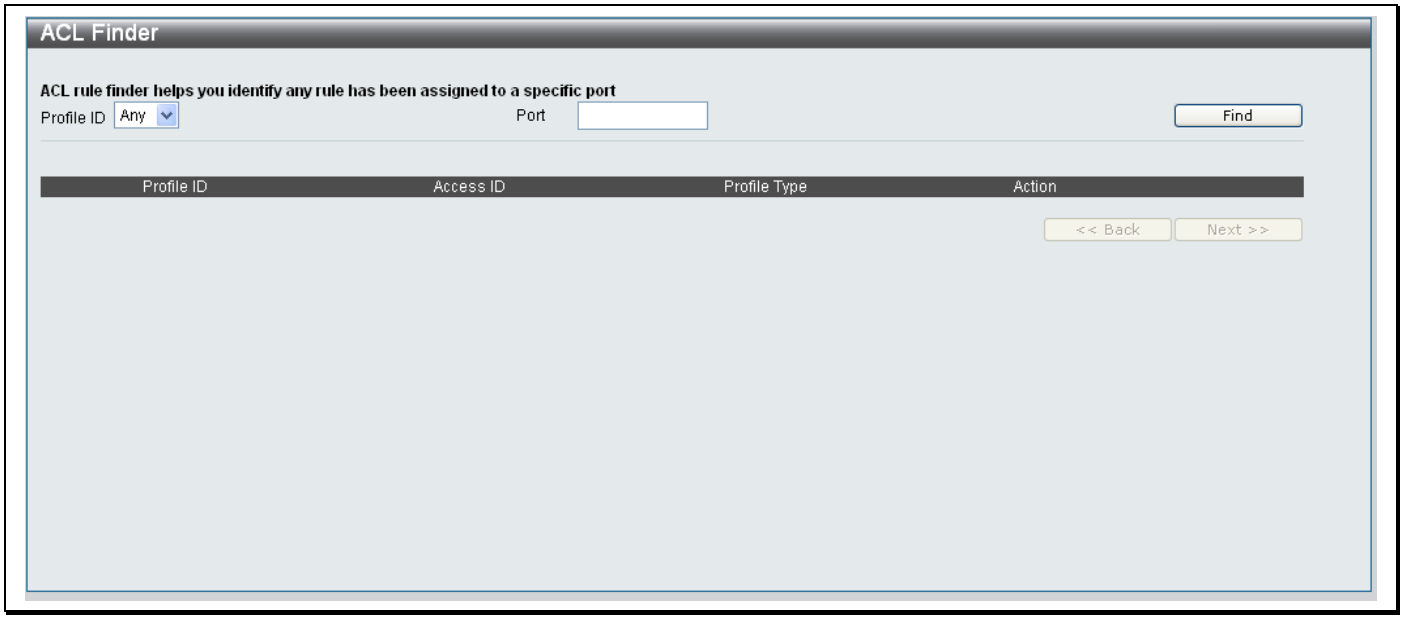


Figure 9- 15. ACL Finder window

Carry out the following steps to find an ACL rule:

- Choose the profile from the **Profile ID** drop-down menu
- Type the Port Number in the **Port** field
- Click **Find** to search for the ACL rule.

Section 10

Monitoring

Device Status

Click **Monitoring> Device Status** to access the **Device Status** window. This window displays the *Thermal Status* of the hardware and the *Fan Status*.

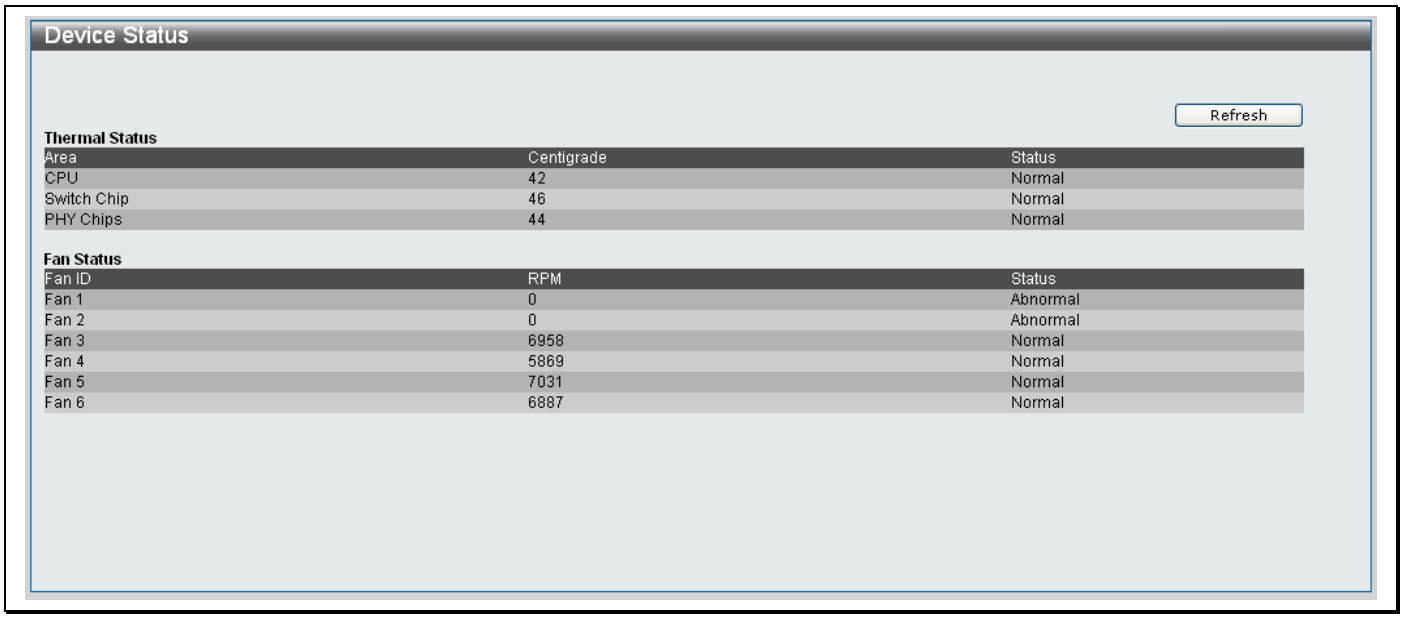


Figure 10- 1. Device Status window

CPU Utilization

This window displays the percentage of CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. To access the **CPU Utilization** window, click **Monitoring > CPU Utilization**.

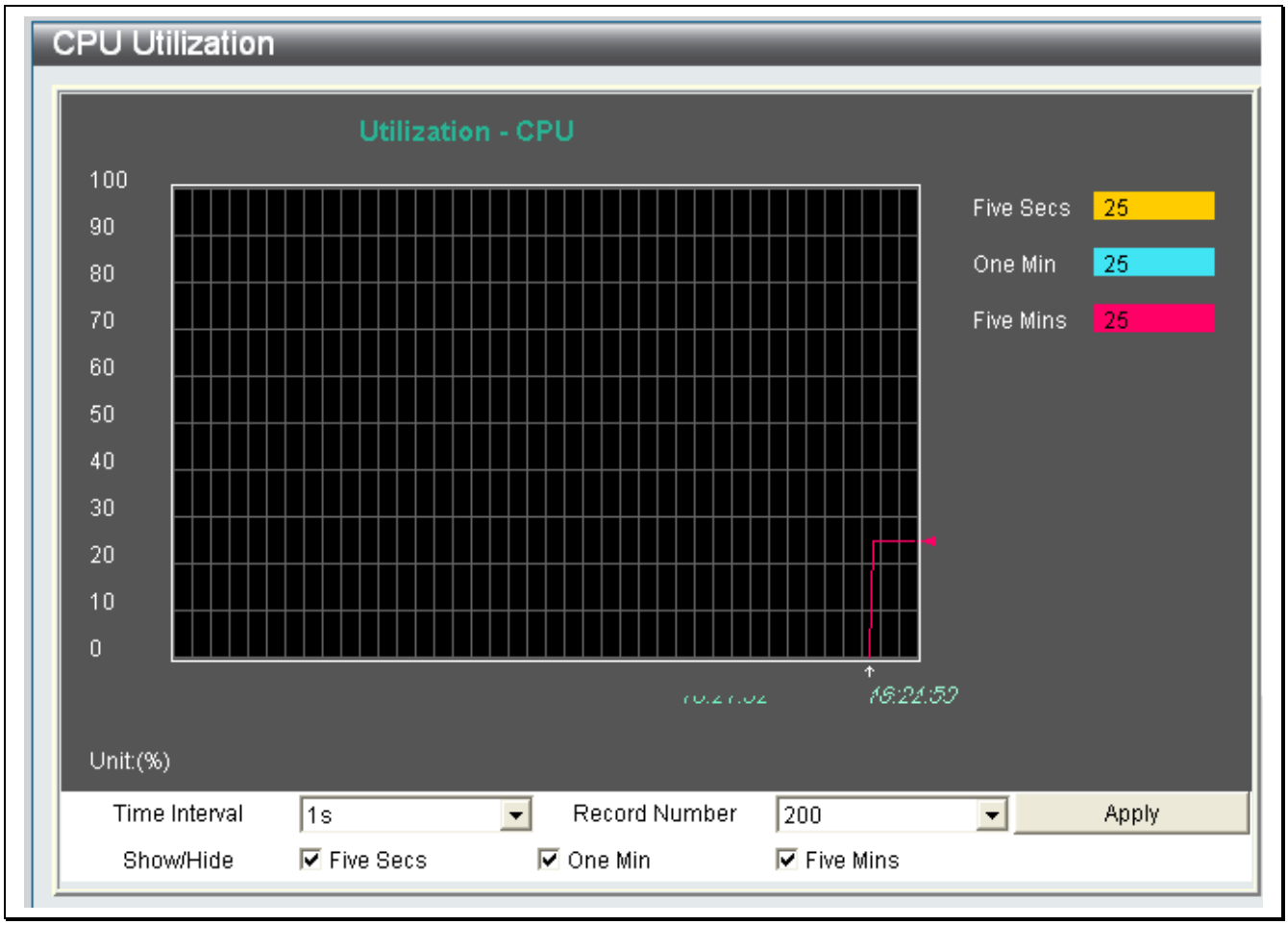


Figure 10- 2. CPU Utilization window

Configure the parameters as described below:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkboxes to Show/Hide the CPU Utilization chart for *Five Seconds, One Minute* and *Five Minutes*.

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

Port Utilization

This window displays the percentage of the total available bandwidth being used on the port. To view the port utilization, click **Monitoring > Port Utilization**.

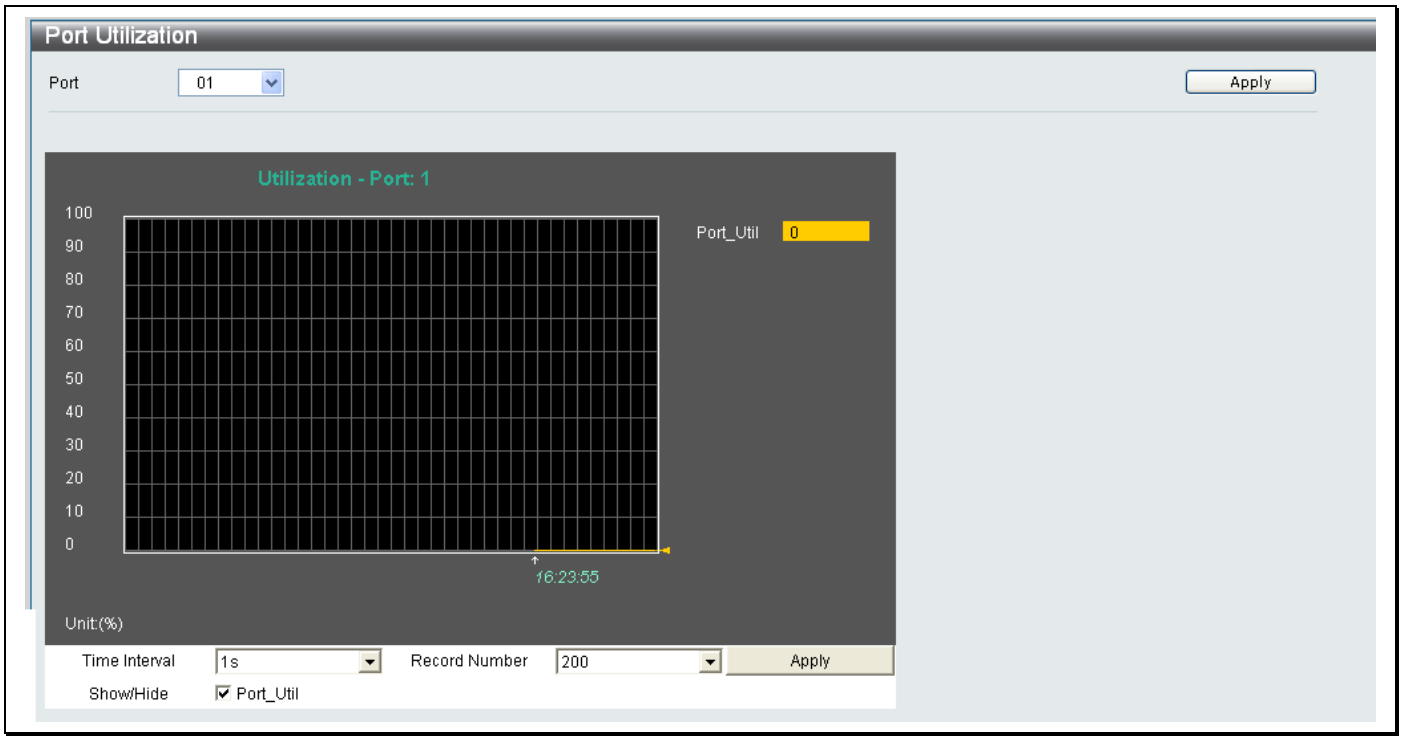


Figure 10- 3. Port Utilization window

Select a port number from the **Port** drop-down menu at the top of the window to view the available bandwidth for that port.

The following fields can be set on the **Port Utilization** window:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkbox to Show/Hide the Port Utilization chart for *Five Seconds, One Minute* and *Five Minutes.*

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

OLT Port Utilization

This window displays the percentage of the total available bandwidth being used on the port. To view the port utilization, click **Monitoring > OLT Port Utilization**.

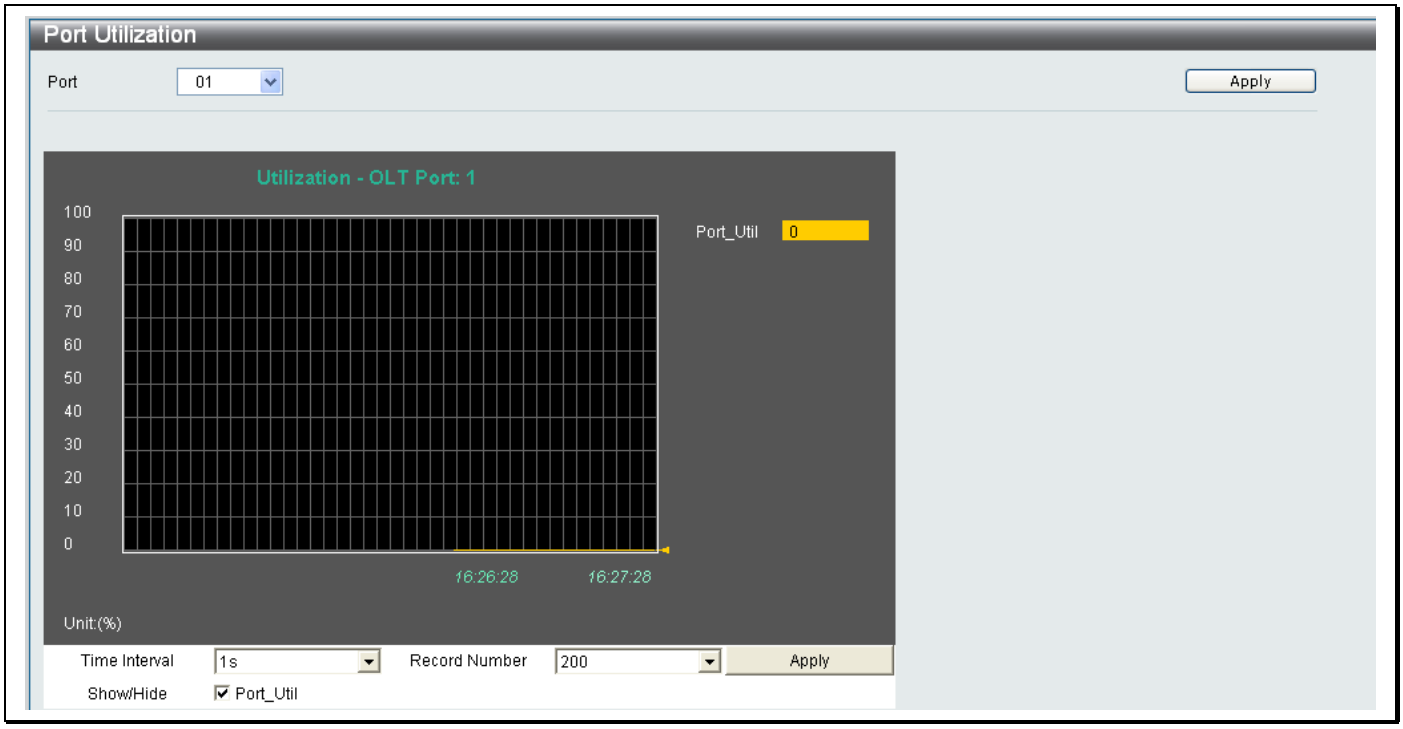


Figure 10- 4. OLT Port Utilization window

Select a port number from the **Port** drop-down menu at the top of the window to view the available bandwidth for that port.

The following fields can be set in the **OLT Port Utilization** window:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkbox to Show/Hide the OLT Port Utilization chart for *Five Seconds, One Minute* and *Five Minutes*.

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

Packet Size

This window displays the size of the packets received by the Switch as a line graph. The graph arranges packets in six groups that are classed in size. To view the Packet Size graph, click **Monitoring > Packet Size**.

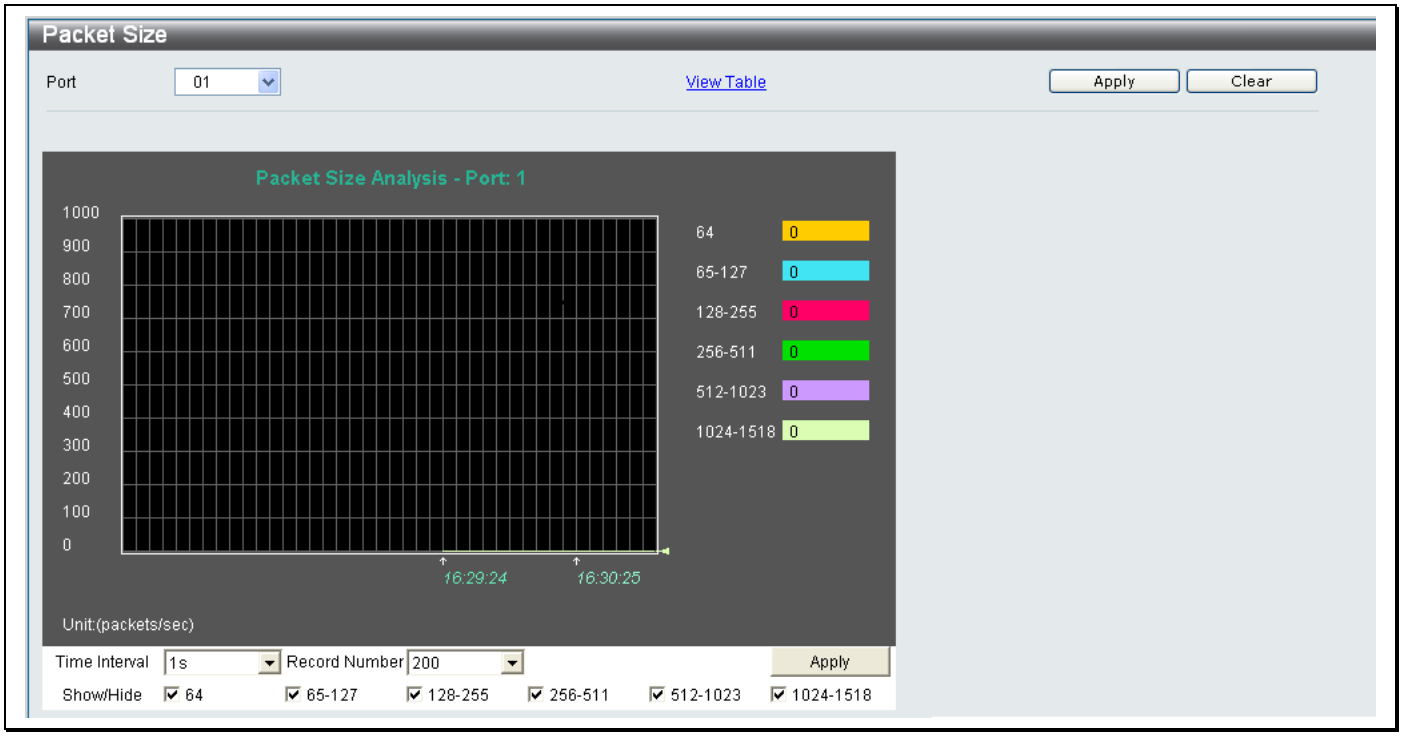


Figure 10- 5. Packet Size window

Select a port number from the **Port** drop-down menu at the top of the window to view the packet size information for that port.

The following fields can be set in the **Packet Size** window:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkboxes to show/hide the different packet size groups.

To view the **Packet Size Table**, click the **View Table** link, which will show the following table:

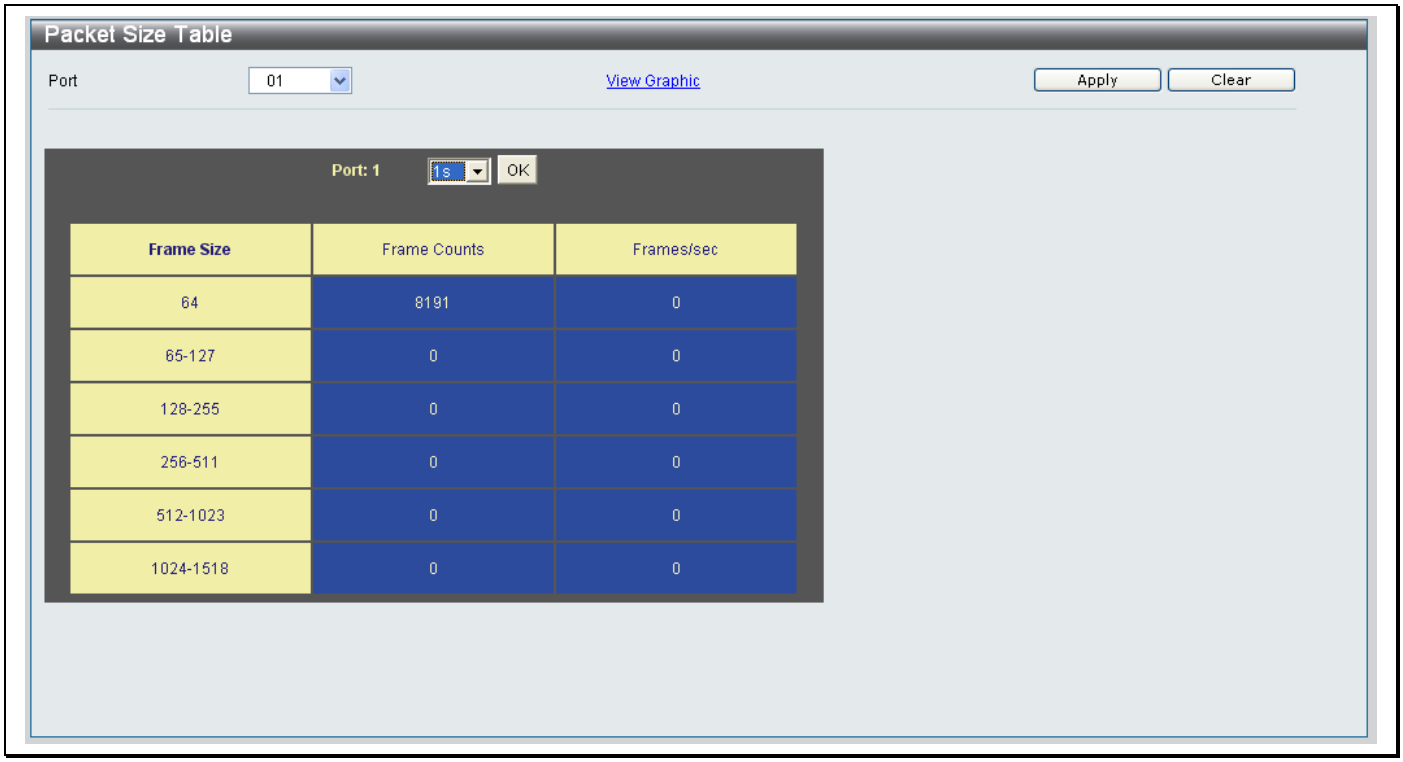


Figure 10- 6. Packet Size Table

Packets

Received (RX)

This window displays the packets received by the Switch as a line graph or a table. To view the Packets Received (RX) graph, click **Monitoring > Packets > Received (RX)**.

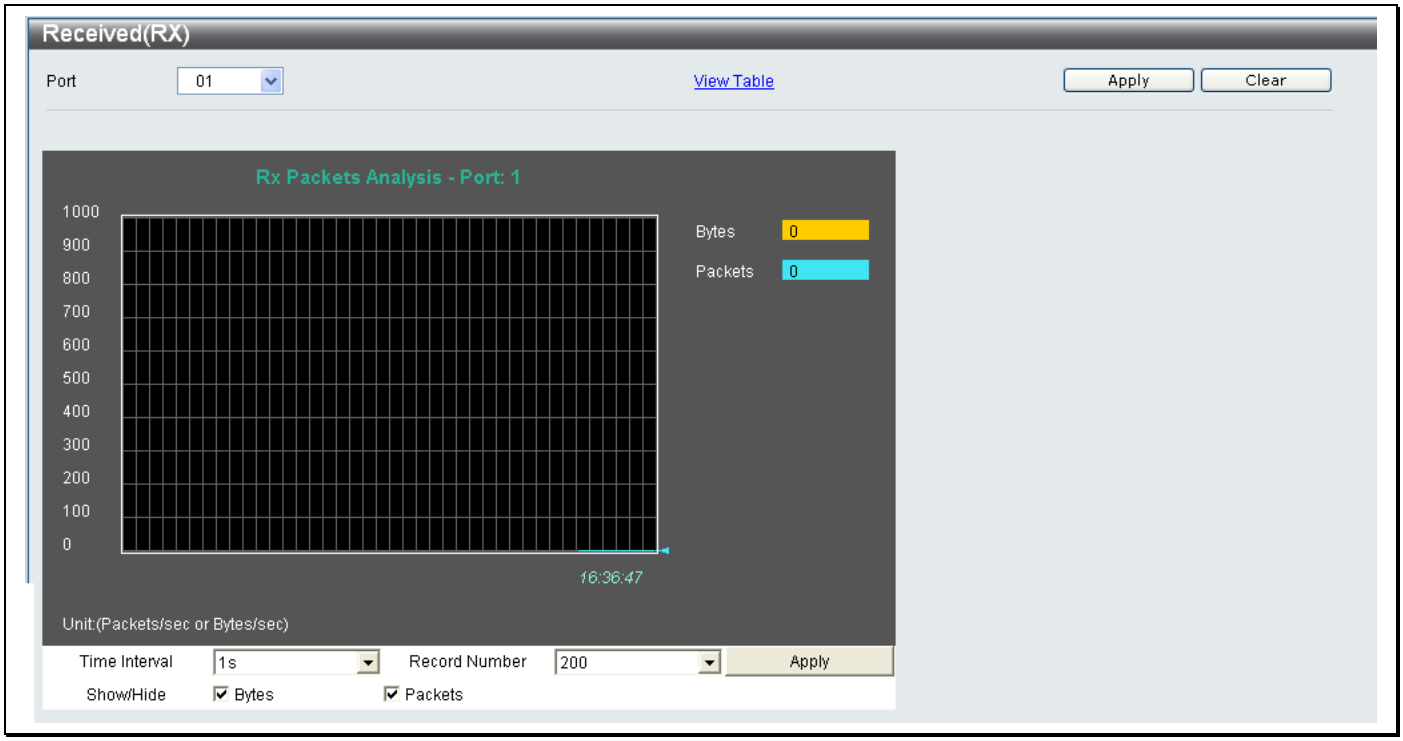


Figure 10- 7. Received (RX) window

Select a port number from the **Port** drop-down menu at the top of the window to view information about the received packets for that port.

The following fields can be set in the **Received** window:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkboxes to show/hide the Bytes and Packets for the port.

To view the Received (RX) Packets Table, click the **View Table** link, which will show the following table:

Figure 10- 8. Received (RX) table

UMB_cast (RX)

This window displays the Unicast, Multicast and Broadcast packets received by the Switch as a line graph or as a Table. To view the UMB_cast (RX) graph, click **Monitoring > Packets > UMB_cast (RX)**.

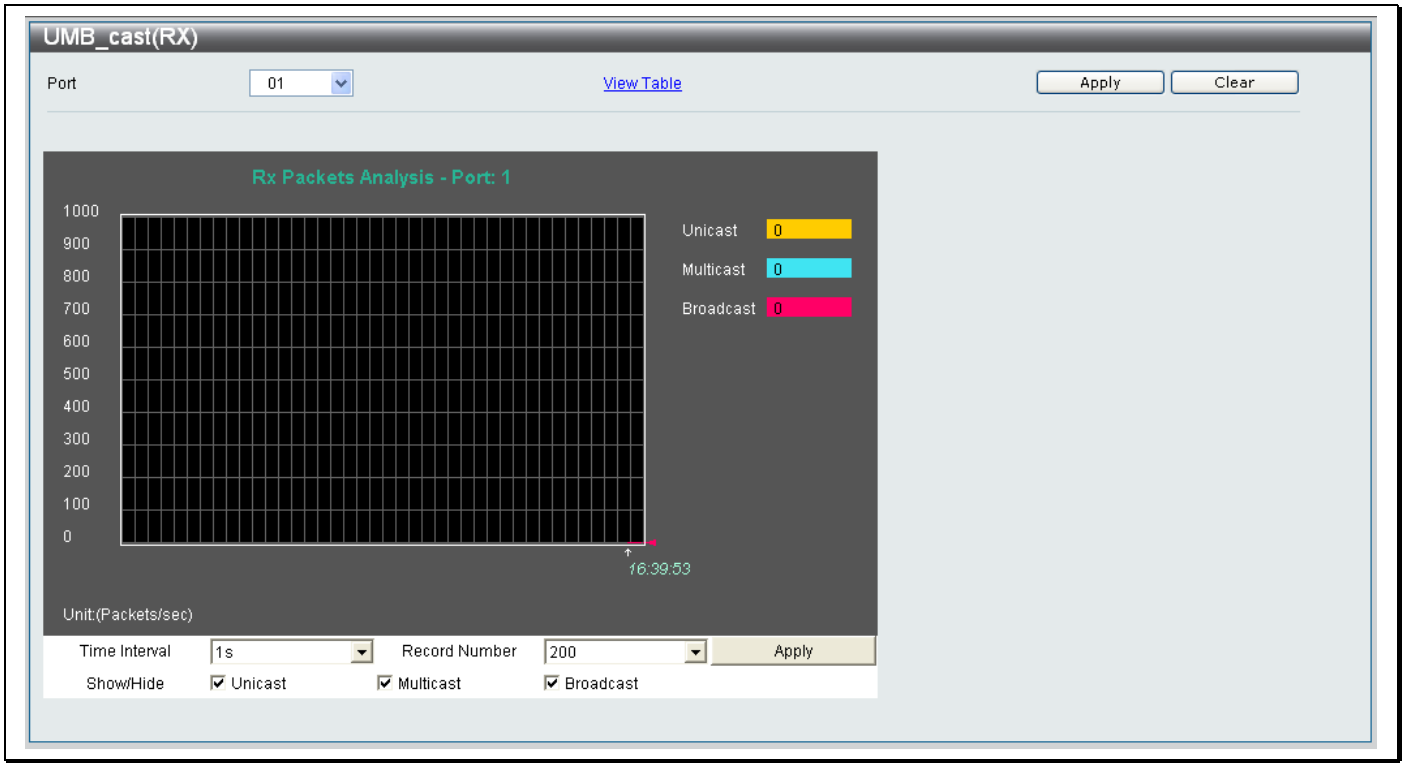


Figure 10- 9. UMB_cast (RX) window

Select a port number from the **Port** drop-down menu at the top of the window to view information about the received packets for that port.

The following fields can be set in the **UMB_cast (RX)** window:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkboxes to show/hide the Unicast, Multicast and Broadcast packets for the port.

To view the UMB_cast (RX) Packets Table, click the **View Table** link, which will show the following table:

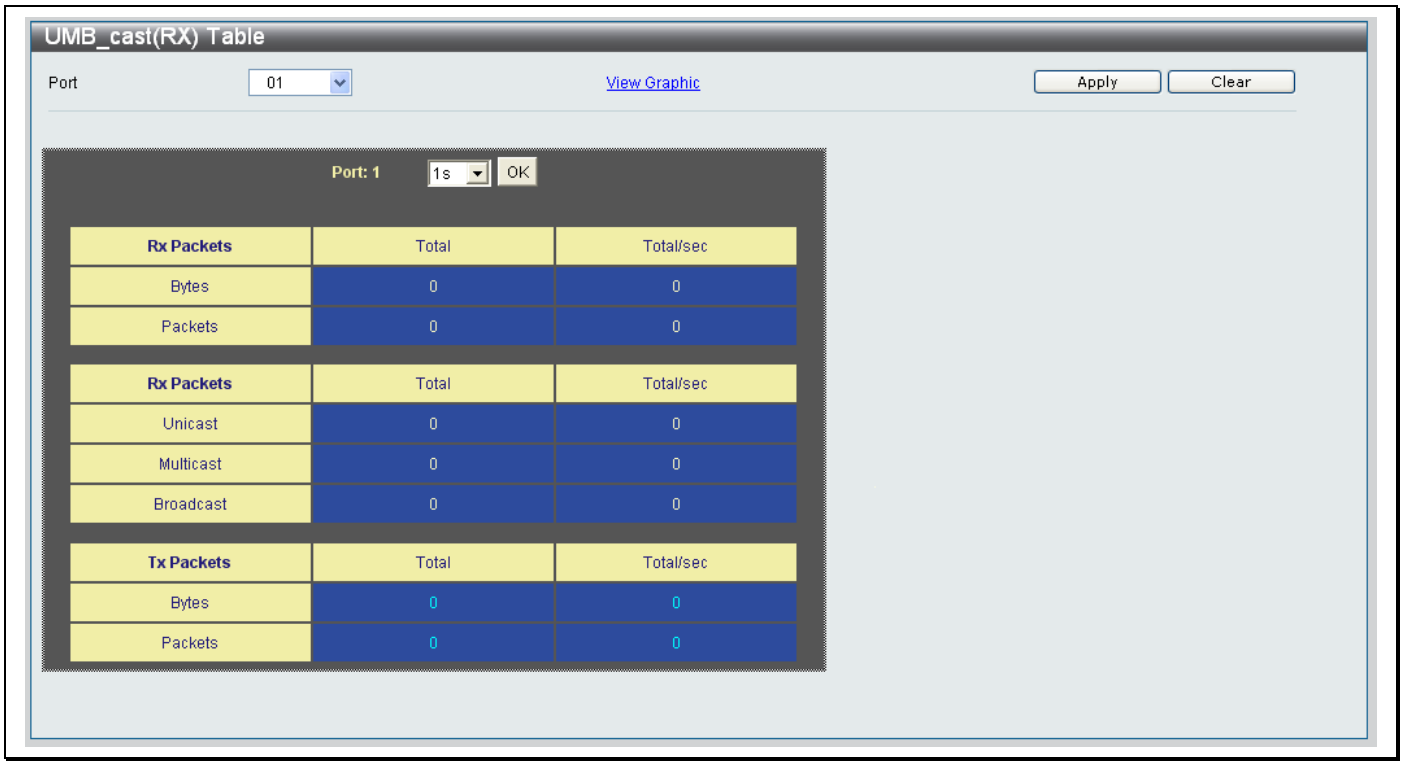


Figure 10- 10. UMB_cast (RX) Table

Transmitted (TX)

This window displays the Transmitted (TX) packets transmitted by the Switch as a line graph or as a Table. To view the Transmitted (TX) graph, click **Monitoring > Packets > Transmitted (TX)**.

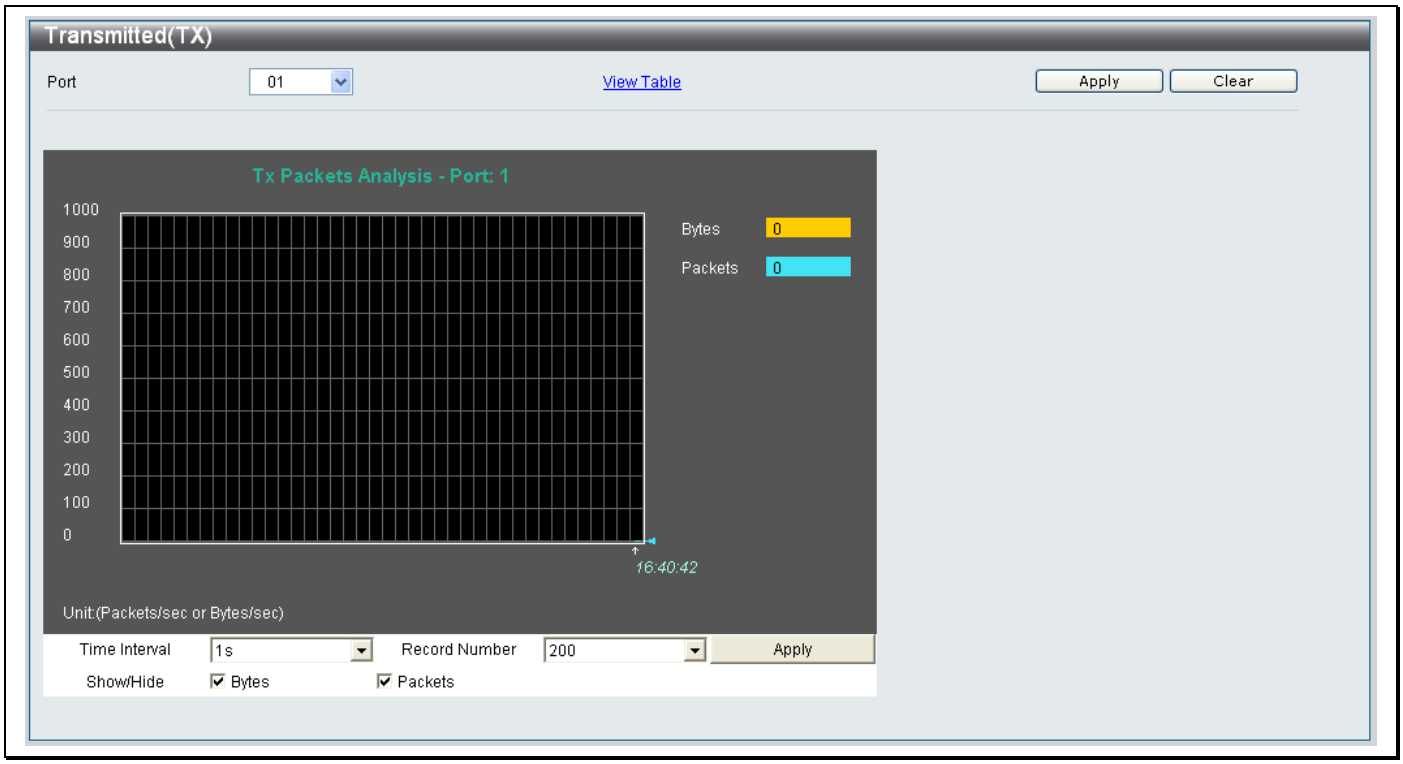


Figure 10- 9. Transmitted (TX) window

Select a port number from the **Port** drop-down menu at the top of the window to view information about the transmitted packets for that port.

The following fields can be set in the **Transmitted** window:

Parameter	Description
Time Interval	Use the drop-down menu to select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is one second.
Record Number	Use the drop-down menu to select the number of times the Switch will be polled between *20* and *200*. The default value is *200*.
Show/Hide	Tick/Un-tick the checkboxes to show/hide the Bytes and Packets for the port.

To view the Transmitted Packets Table, click the **View Table** link, which will show the following table:

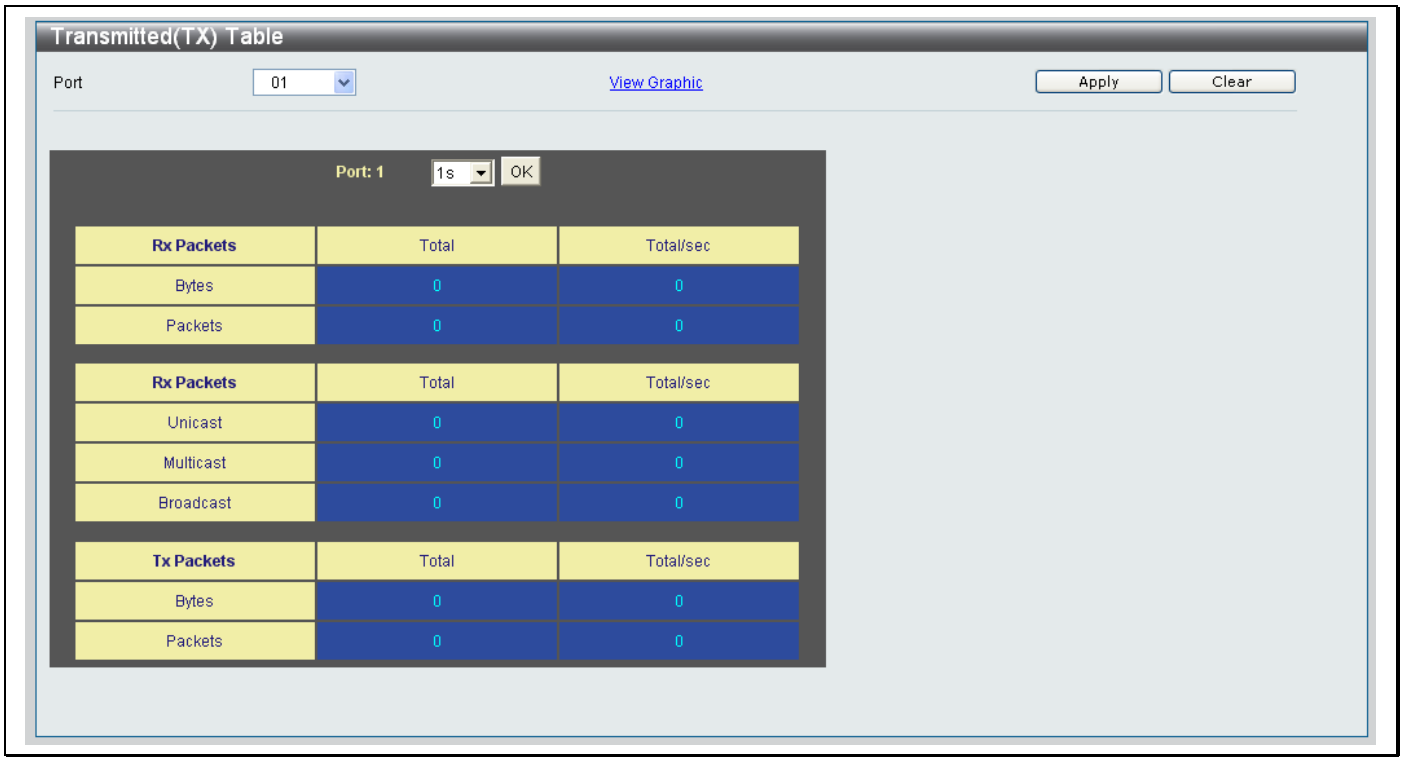


Figure 10- 10. Transmitted (TX) Table

Errors

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. Two windows are available.

Received (RX)

Click **Monitoring> Errors> Received (RX)** to view the following graph showing the error packets received on the Switch:

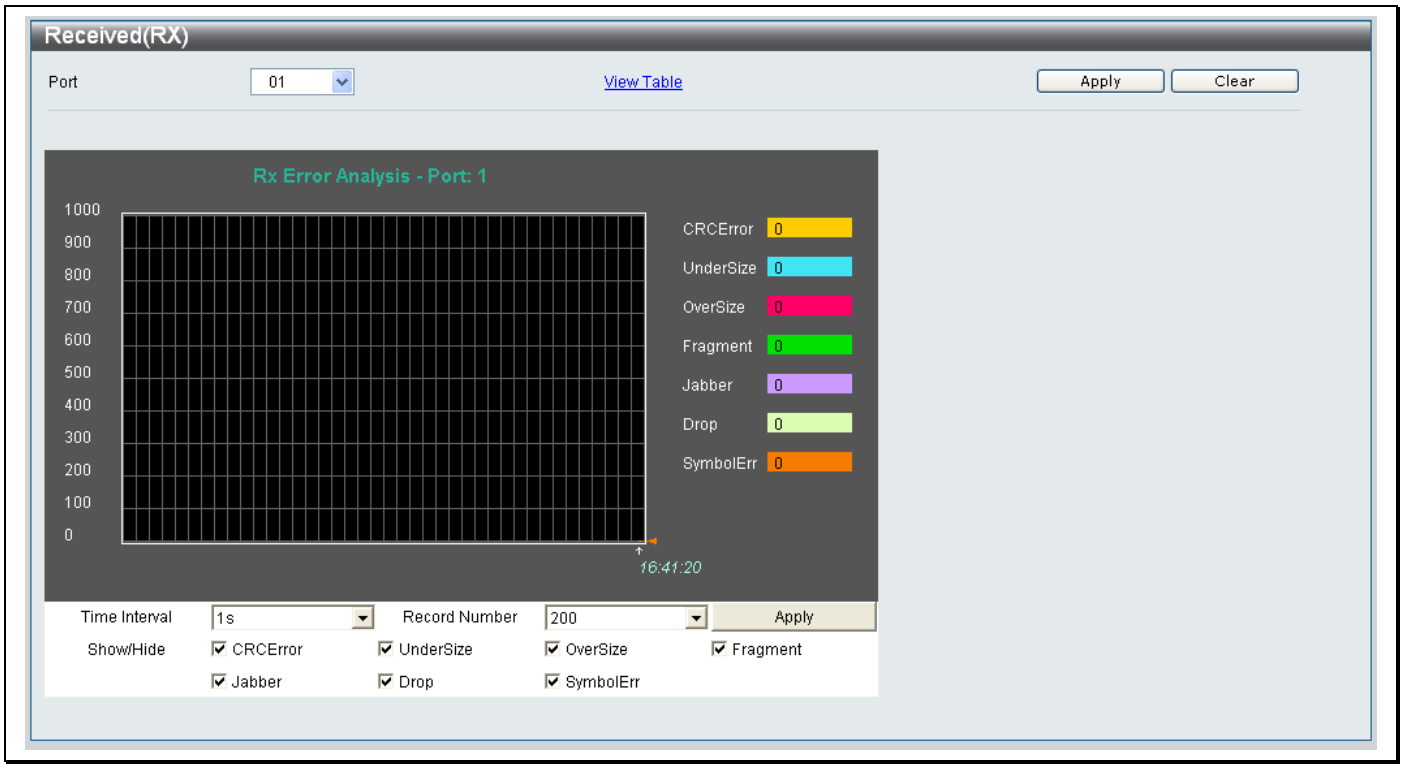


Figure 10- 11. Errors Received (RX) window

To view the Received Error Packets Table, click the **View Table** link, which will show the following table:

Figure 10- 12. Errors Received (RX) Table

Transmitted (TX)

Click **Monitoring> Errors> Transmitted** to view the following graph showing the error packets transmitted by the Switch:

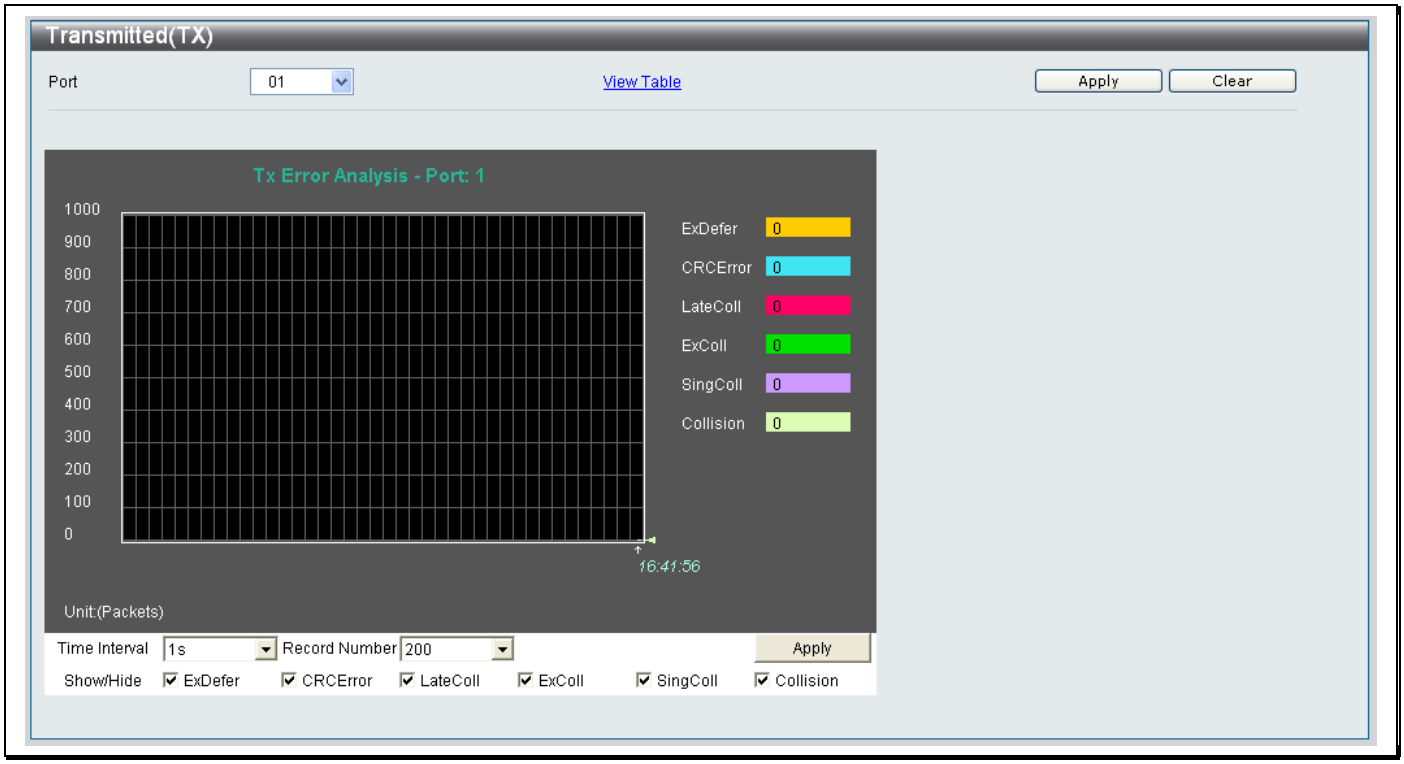


Figure 10- 13. Errors Transmitted (TX) graph

To view the Transmitted Error Packets Table, click the **View Table** link, which will show the following table:

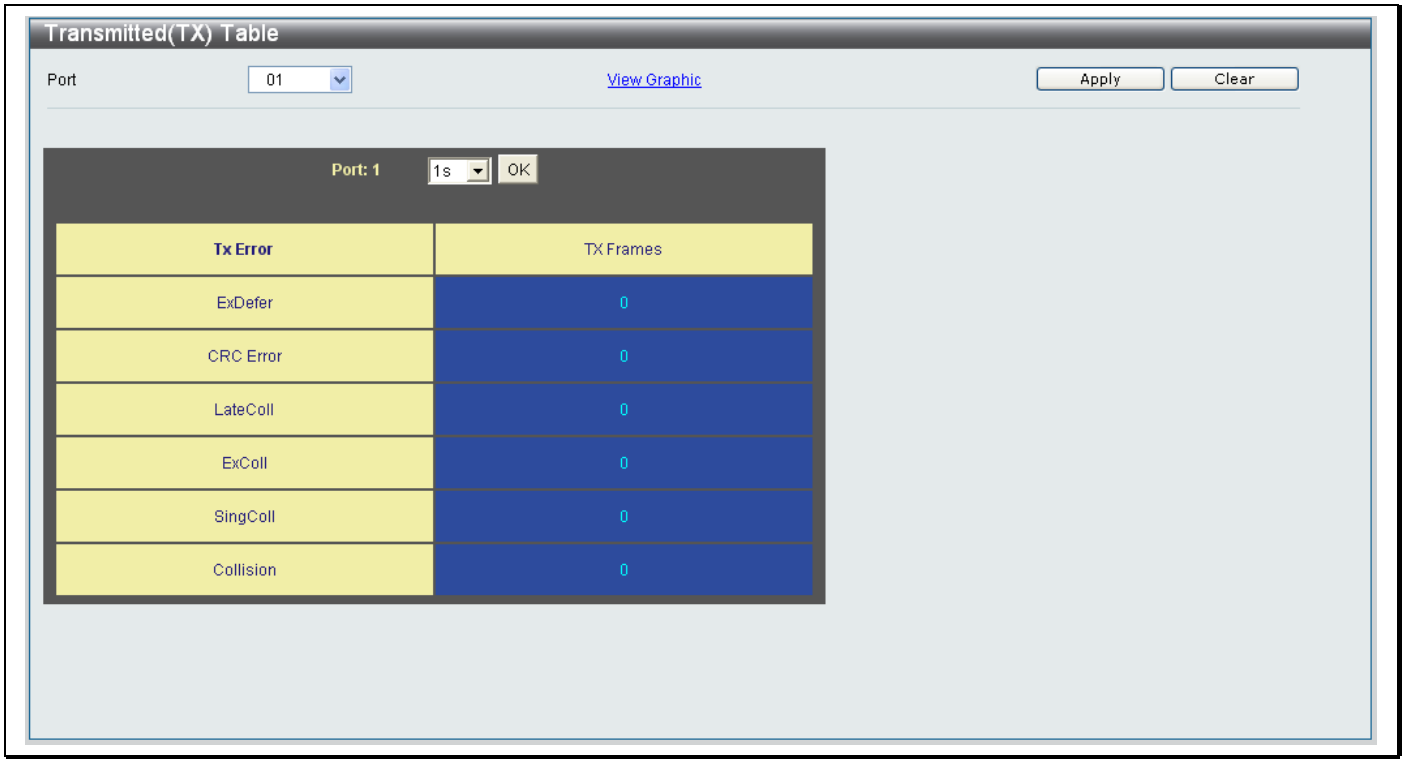


Figure 10- 14. Errors Transmitted (TX) Table

Browse ARP Table

The **Browse ARP Table** window shows current ARP entries on the Switch.

Click **Monitoring> Browse ARP Table** to view the following window:

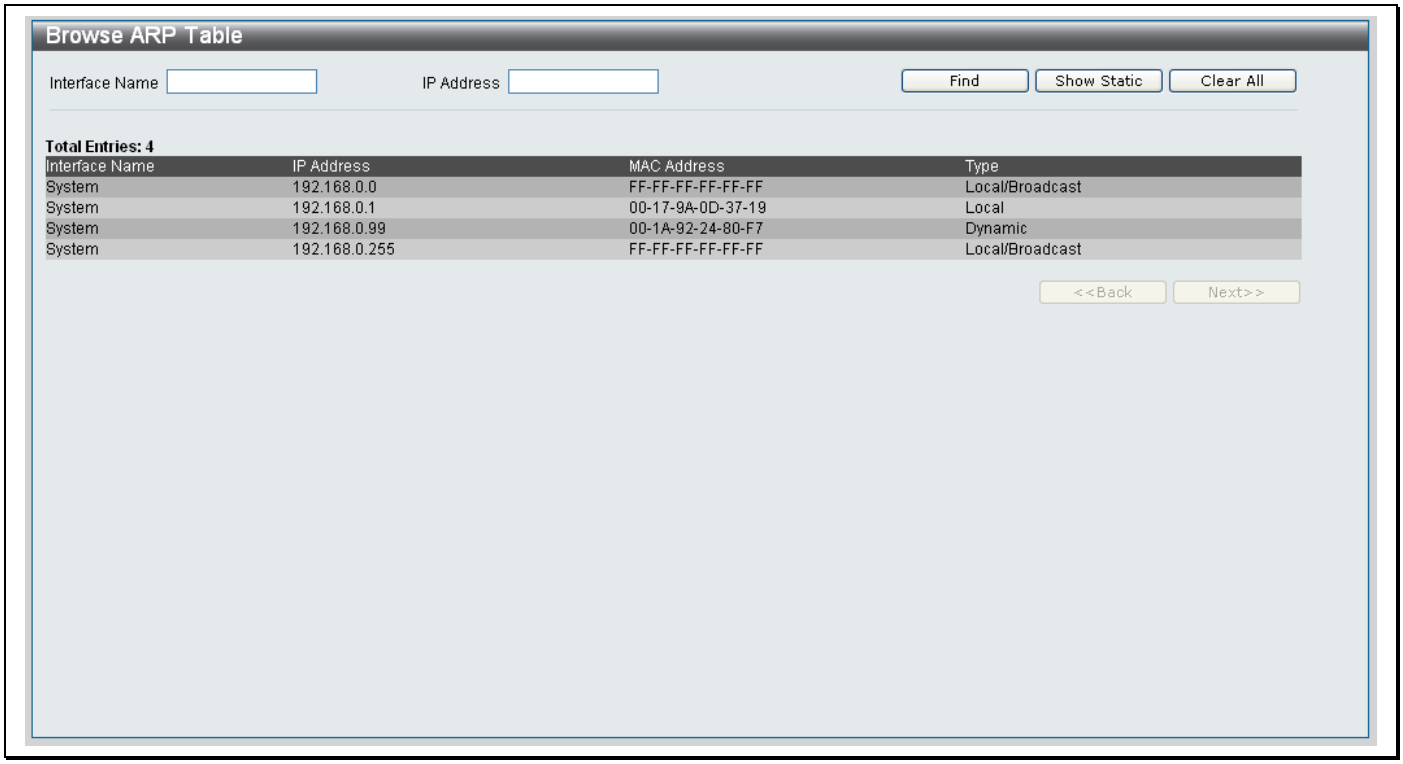


Figure 10- 15. Browse ARP Table window

To search for a specific ARP entry, enter an *Interface Name* into the **Interface Name** field or an *IP Address* in the **IP address** and click **Find.**

Click the **Show Static** button to show statically configured ARP entries made on the Switch.

To clear the **ARP Table**, click **Clear All**.

Browse VLAN

The **Browse VLAN** window shows the current VLAN's configured on the Switch.

Click **Monitoring> Browse VLAN** to view the following window:

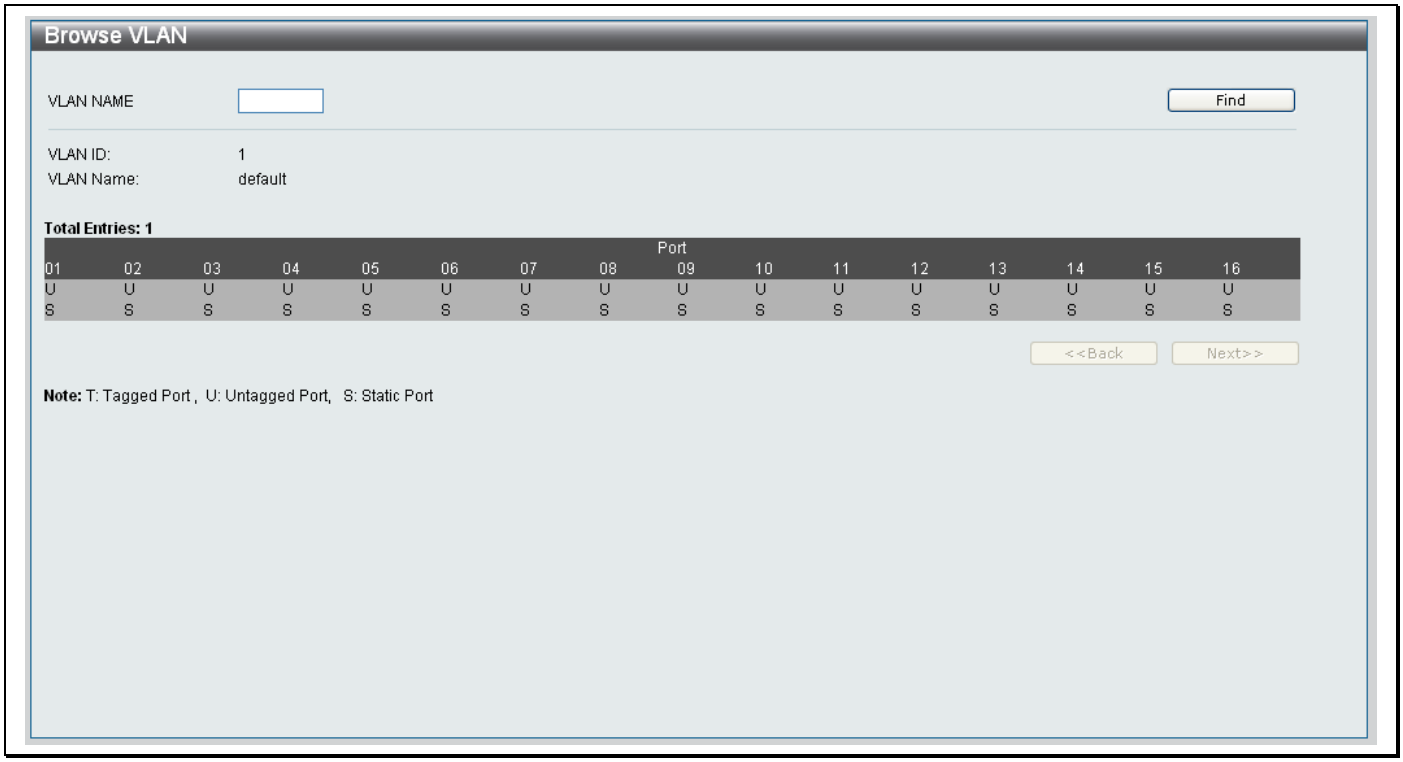


Figure 10- 16. Browse VLAN window

To view information about a VLAN and the port roles within the VLAN, type the *VLAN Name* in the **VLAN Name** textbox and click the **Find** button.

The VLAN will display in the bottom of the window.

Show VLAN Ports

The **Show VLAN Ports** window allows you to view the **VID**, **Ingress Checking** and **Acceptable Frame Type** configured on the Switch.

Click **Monitoring> Show VLAN Ports** to view the following window:

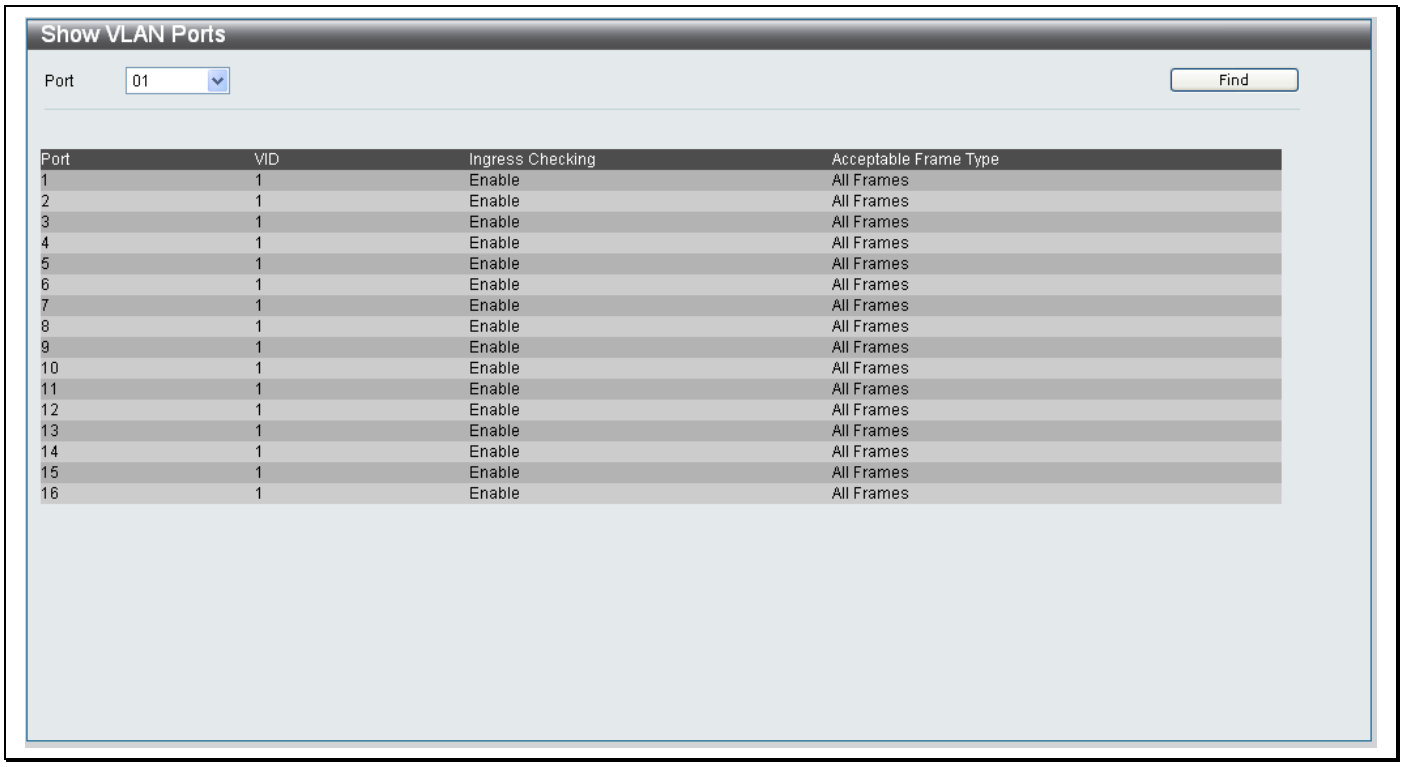


Figure 10- 17. Show VLAN Ports window

To show information about a specific port:

- Choose the port from the **Port** drop-down menu.
- Click the **Find** button.
- Information about the port will display in window.

Browse Session Table

The **Browse Session Table** window allows you to view the **ID**, the length of time connected, the source, **Level** and User Name of sessions connected to the Switch.

Click **Monitoring> Browse Session Table** to view the following window:

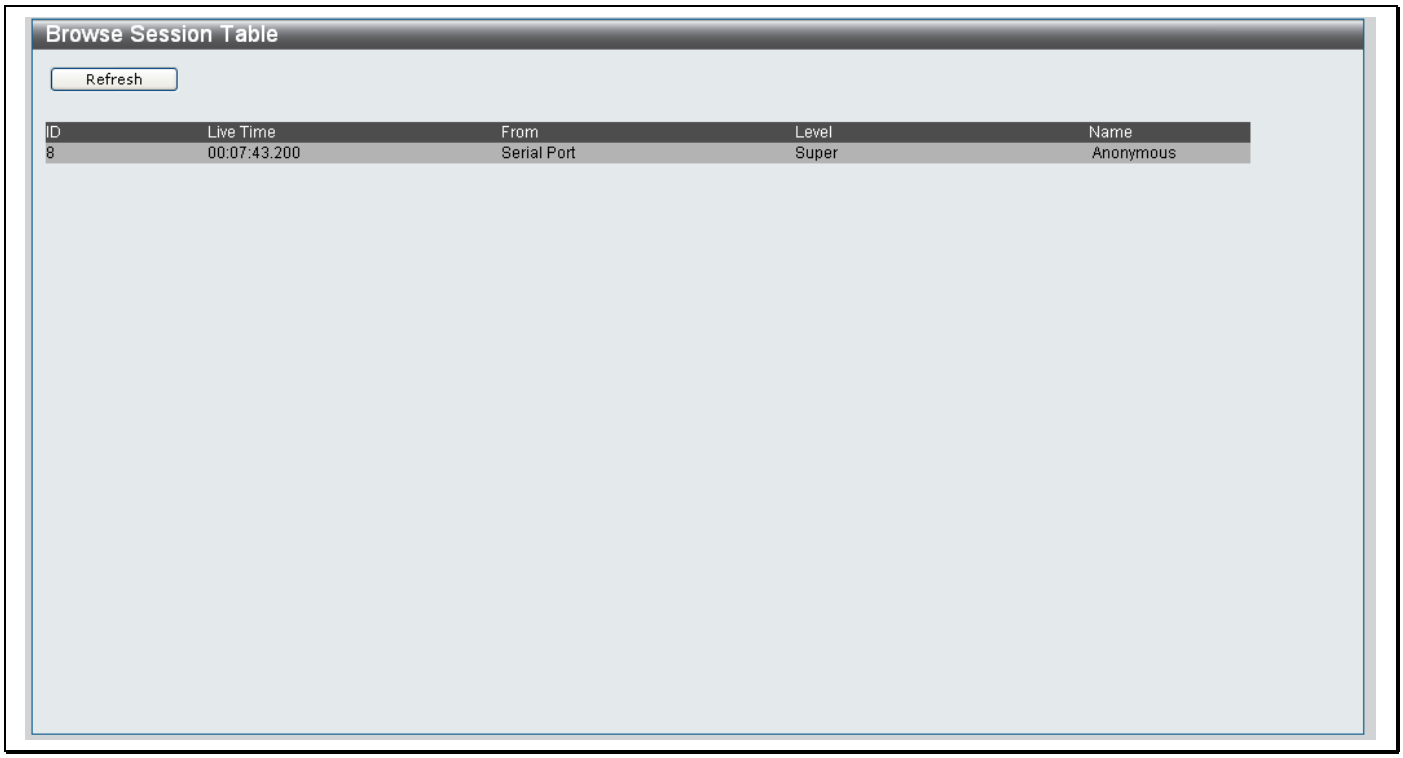


Figure 10- 18. Browse Session Table

Click the **Refresh** button to refresh the window.

IGMP Snooping Group

Use the IGMP Snooping Group window to view IGMP Snooping information about a previously created VLAN configured on the Switch.

Click **Monitoring> IGMP Snooping Group** to view the following window:

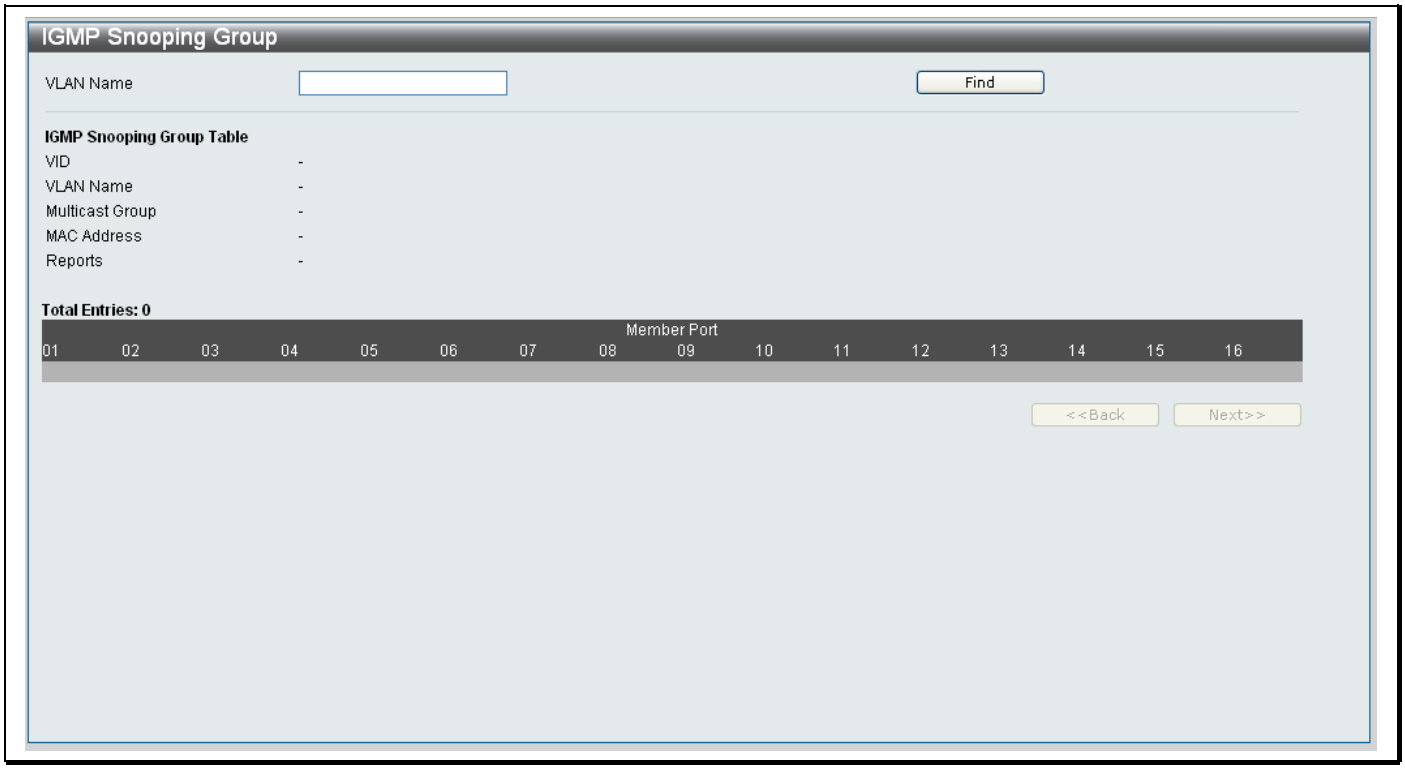


Figure 10- 19. IGMP Snooping Group Table

- Type the name of the VLAN you want to view IGMP Snooping Group information for in the **VLAN Name** field.
- Click the **Find** button.
- The IGMP Snooping Group information will display in the **Member Port** section at the bottom of the window.

MAC Address Table

Use the **MAC Address Table** window to view and clear entries on the Switch's MAC Address Table.

To access the **MAC Address Table** window, click **Monitoring> MAC Address Table:**

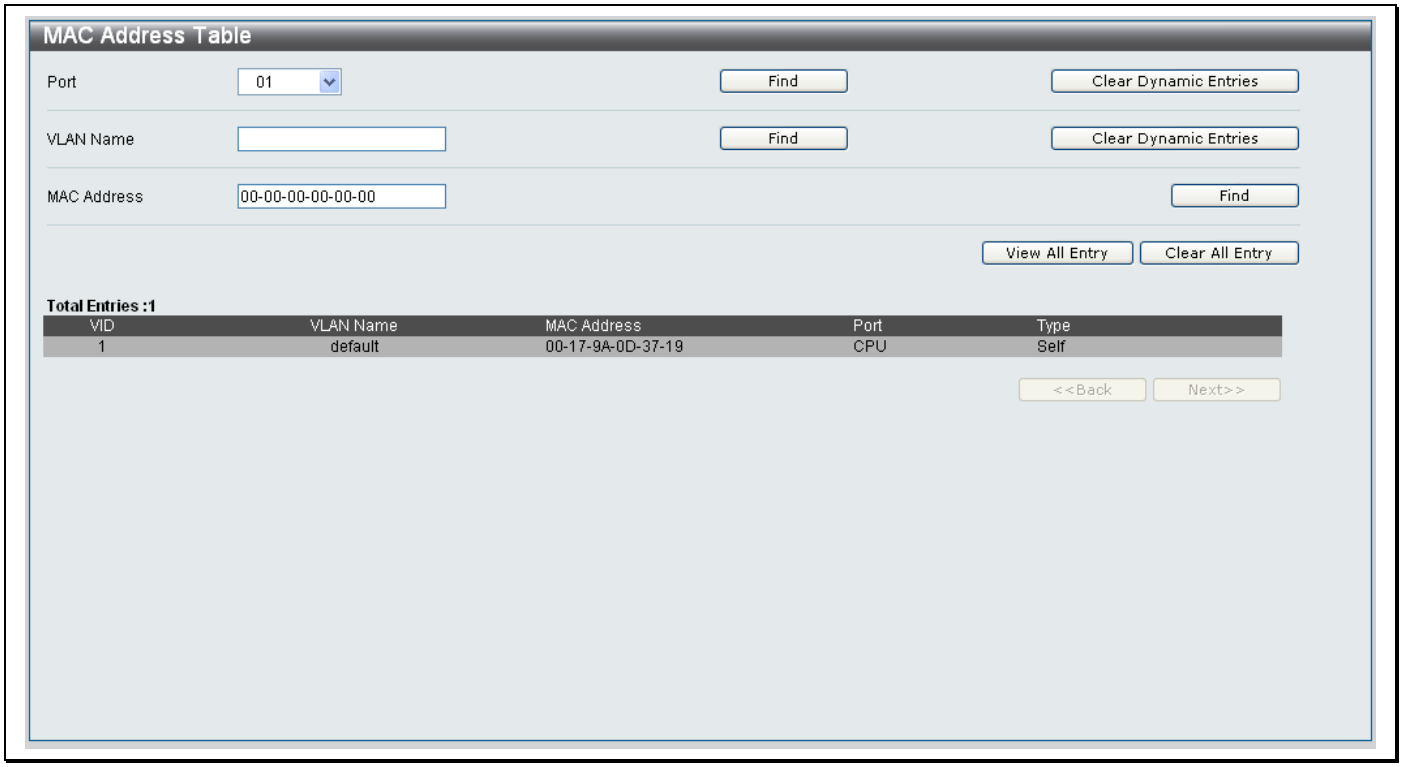


Figure 10- 20. MAC Address Table

The following table show describes the different parameters in the MAC Address table:

Parameter	Description
Port	Use the drop-down menu to select the port you want to view or clear MAC address information for. Click the adjacent **Find** button to view the MAC Addresses associated with that port. Click the adjacent **Clear Dynamic Entries** button to clear all current dynamic MAC Address entries associated with the port.
VLAN Name	Type the name of the VLAN in the **VLAN Name** field to view all the MAC Address entries associated with the port. Click the adjacent **Find** button to view the MAC Addresses associated with the VLAN. Click the adjacent **Clear Dynamic Entries** button to clear all current dynamic MAC Address entries associated with the VLAN.
MAC Address	Use the **MAC Address** field to find out which VLAN and port the MAC Address is connected to. To use this feature type the *MAC Address* in the **MAC Address** field and click the **Find** button. The VLAN Name the MAC Address is connected to, along with the port number will be displayed in the table at the bottom of the window.

Section 11

PON

PON ONU firmware upgrade
ONU Information
Reboot OLT&ONU
OLT Port Settings
MAC Authentication
PON Bandwidth Control
ONU FEC Settings
ONU UNI Port Settings
ONU Encryption Settings
Diagnostic Test
ONU IGMP Snooping Settings
ONU IGMP Snooping Groups
OLT VLAN
ONU 802.1Q VLAN PVID Settings
ONU 802.1Q VLAN Settings
ONU Port Base VLAN Settings
P2P
OLT FDB Address Limitation
ONU MAC Address Table
Policing Queue Bandwidth Settings
Policing Queue Size Settings
ONU Default Filter Settings
ONU Classifier Filter Settings
ONU Default VLAN Rule Settings
ONU VLAN Rule Settings
ONU Priority Rule Settings
ONU Priority Map Settings
PON Profile

The PON section contains the settings that configure the ONU and PON units that connect to the Switch.

PON ONU firmware upgrade

Use the PON ONU firmware upgrade window to upload a new version of firmware onto the ONU.

Click **PON> PON ONU firmware upgrade** to access the window below:

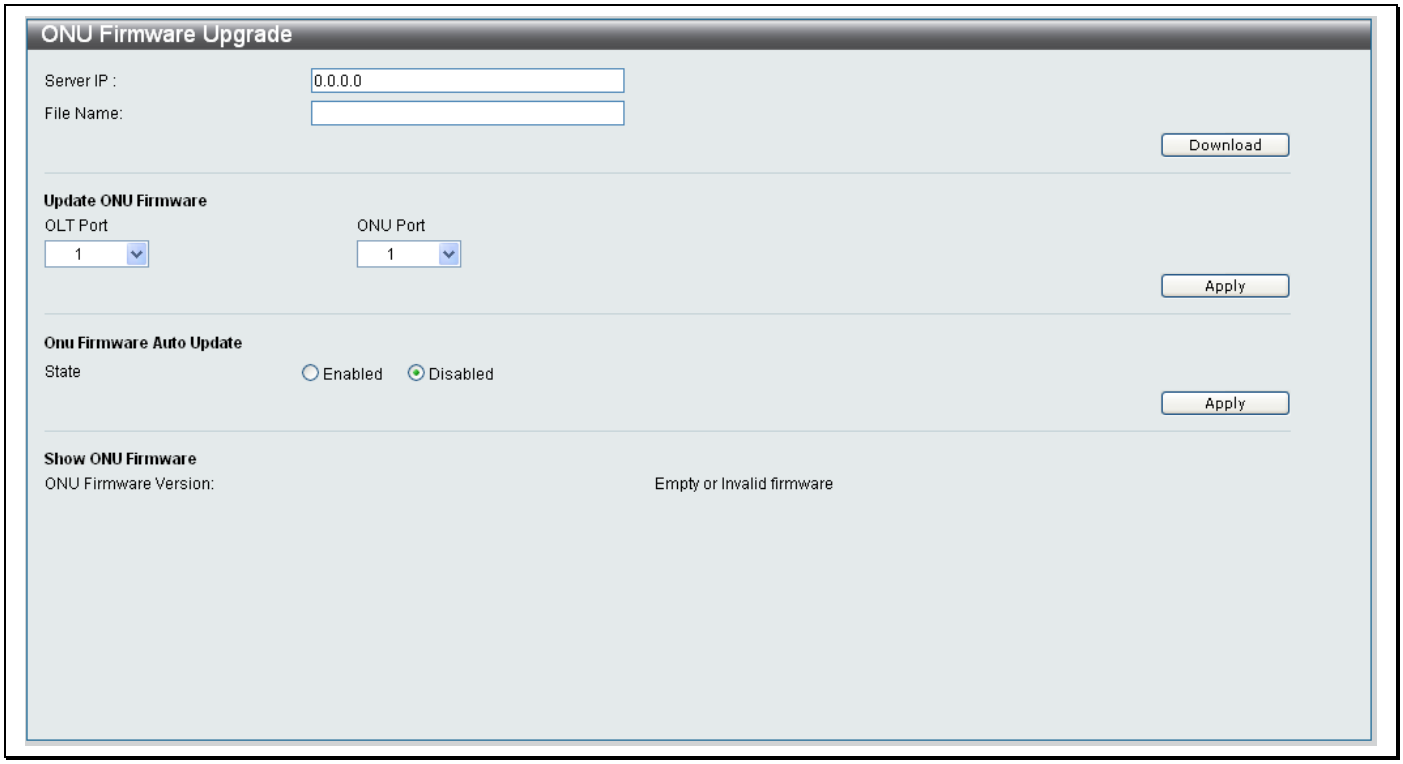


Figure 11- 1. ONU Firmware Upgrade window

To upgrade the firmware manually carry out the following steps:

1. Type the *IP address* of the TFTP Server that contains the latest version of Firmware in the **Server IP** field.
2. Type the filename of the latest version of firmware.
3. Click the **Download** button.
4. When the Firmware has loaded onto the Switch, it will display in the **Show ONU Firmware** section.
5. Use the drop-down ports from the **Update ONU Firmware** section to choose the **OLT Port** and **ONU Port** that you want to carry out the Firmware upgrade on. Click the **Apply** button in the **Update ONU Firmware** section to carry out the Firmware upgrade.

To enable automatic firmware updates of the ONU:

1. Click the **Enabled** radio button in the **Onu Firmware Auto Update** section.
2. Click the **Apply** button.

ONU Information

The **ONU Information** window displays information about the ONU's connected to the Switch and allows you to assign a Description to each of the ONU's to help you identify the ONU.

To access the **ONU Information** window click **PON> ONU Information.**

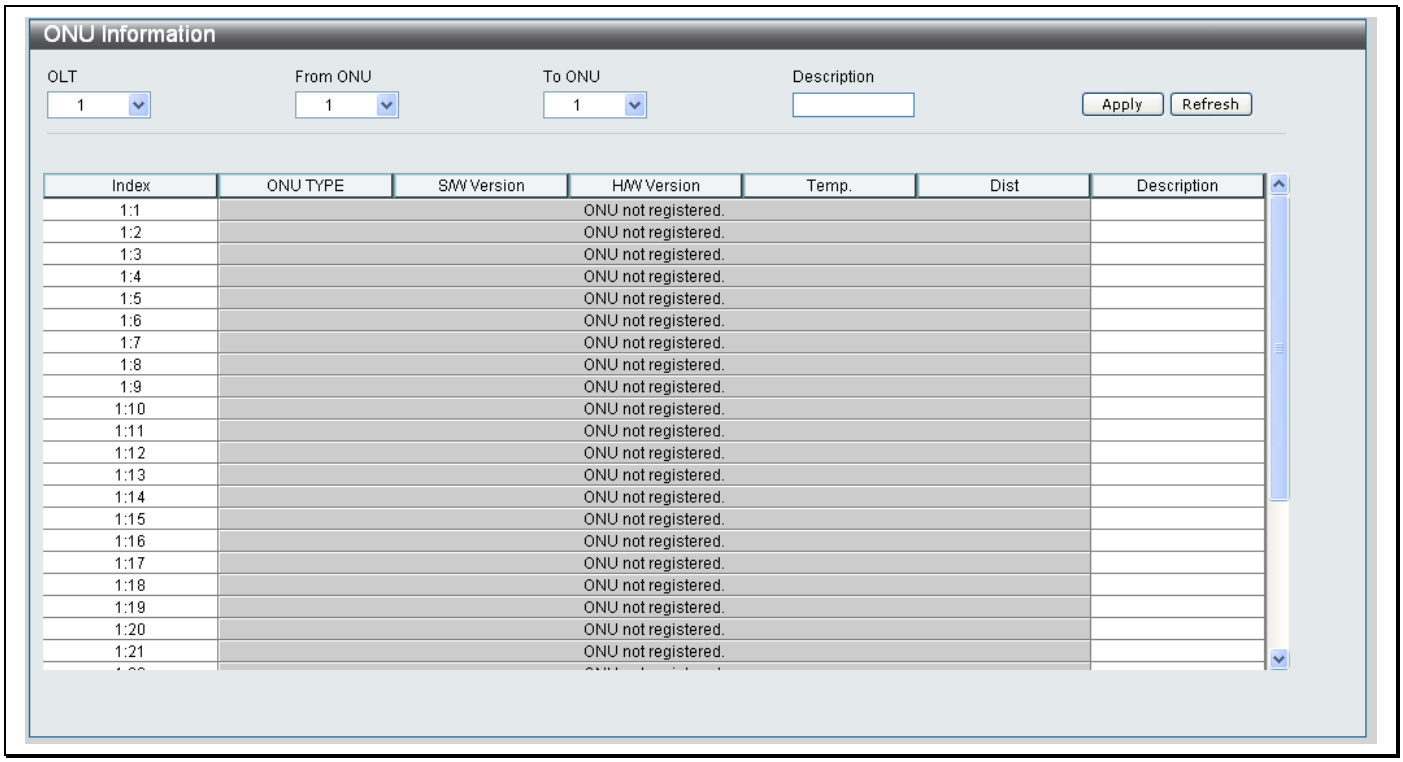


Figure 11- 2. ONU Information window

Adding a Description to ONU's

1. Choose the OLT the ONU is connected to from the **OLT** drop-down menu.
2. Use the **From ONU** and **To ONU** drop-down menus to specify the ONU's that you want to add a **Description** for.
3. Type a description to identify the ONU or range of ONU's in the **Description** field.
4. Click the **Apply** button to add the description.

Reboot OLT&ONU

The **Reboot OLT & ONU** window allows you to carry out a reboot on a specified range of OLT's and ONU's connected to the Switch.

To access the **Reboot OLT & ONU** window click **PON> Reboot OLT & ONU.**

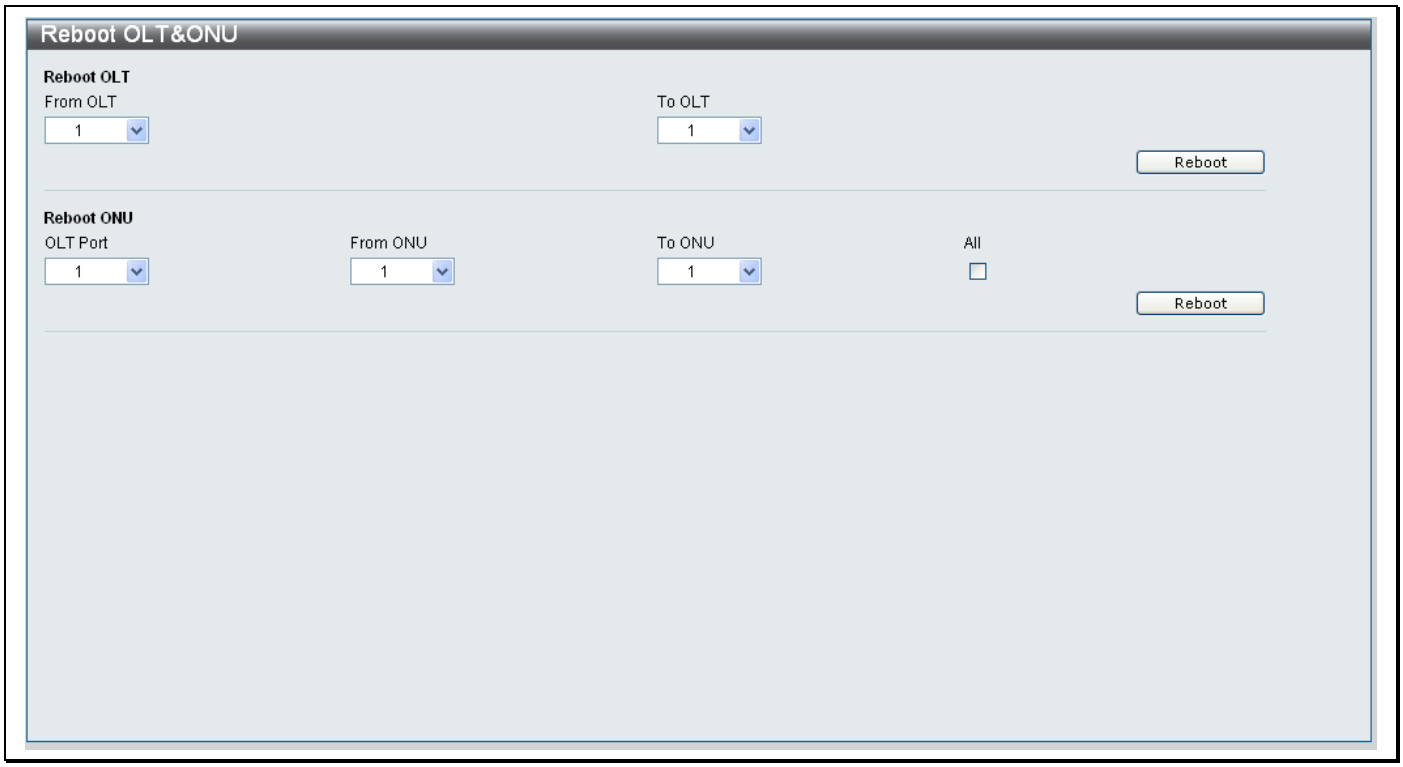


Figure 11- 3. Reboot OLT & ONU window

Reboot OLT

To reboot an OLT or range of OLT's, carry out the following in the **Reboot OLT** section:

1. Use the **From OLT** and **To OLT** drop-down menus to specify the OLT's that you want to reboot.
2. Click the adjacent **Reboot** button.

Reboot ONU

To reboot an ONU or range of ONU's, carry out the following in the **Reboot ONU** section:

1. Use the **OLT Port** drop-down menu to specify the OLT port that the ONU you want to restart is connected to.
2. Use the **From ONU** and **To ONU** drop-down menus to specify the ONU's that you want to reboot, tick the **All** checkbox to specify all ports.
3. Tick the **Reboot** button.

OLT Port Settings

The **OLT Port Settings** window allows you to configure the **MAC Authentication** settings and assign a **Description** to each of OLT's connected to the Switch.

To access the **OLT Port Settings** window click **PON> OLT Port Settings.**

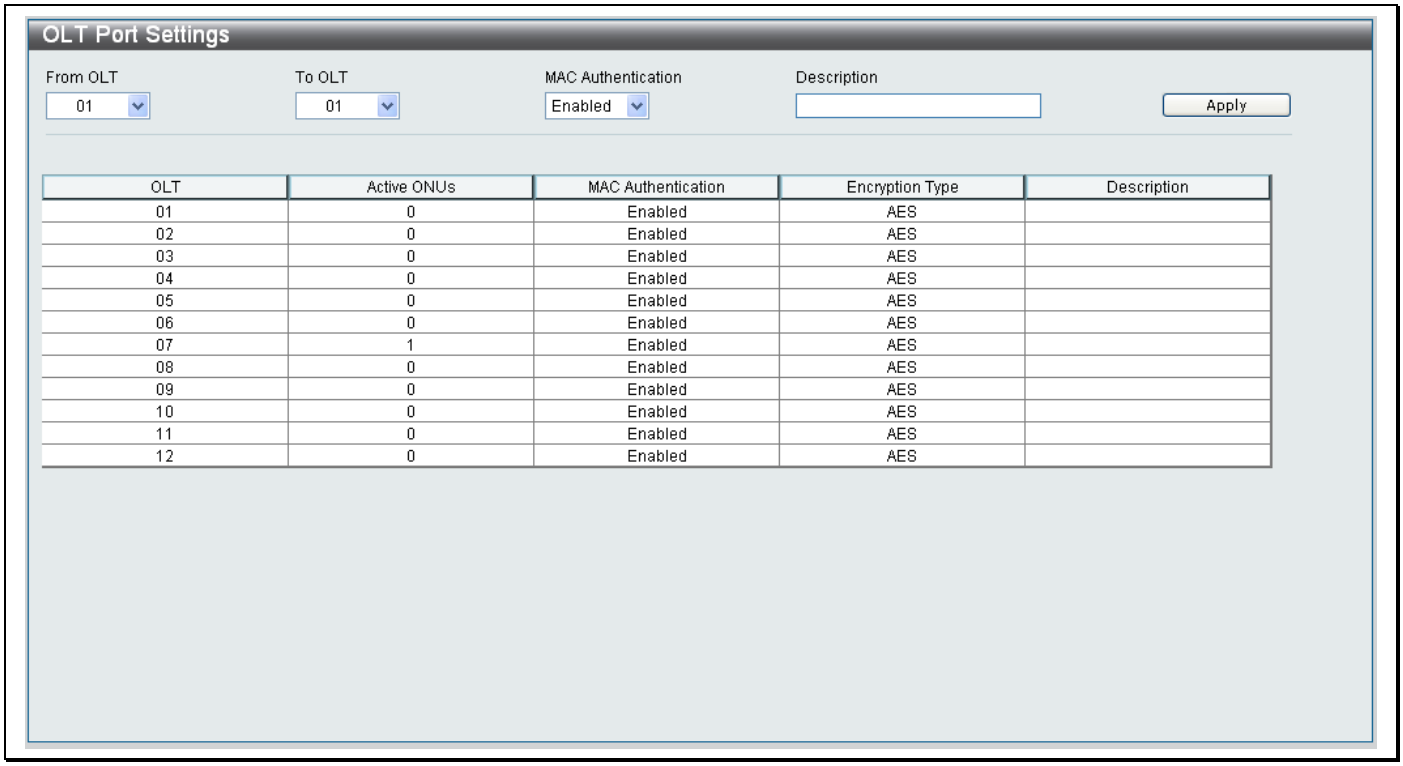


Figure 11- 4. OLT Port Settings window

Configuring OLT Ports

1. Use the **From OLT** and **To OLT** drop-down menus to specify the OLT's that you want to configure.
2. Choose whether to enable or disable **MAC Authentication** on the OLT Ports by choosing *Enabled* or *Disabled* from the drop-down menu.
3. Type a description to identify the OLT or range of OLT's in the **Description** field.
4. Click the **Apply** button to save the changes.

MAC Authentication

MAC Authentication ONU MAC Setting

The **MAC Authentication ONU MAC Setting** window allows you to enable or disable OLT automatic MAC Authentication.

To access the **MAC Authentication ONU MAC Setting** window click **PON> MAC Authentication > MAC Authentication ONU MAC Setting.**

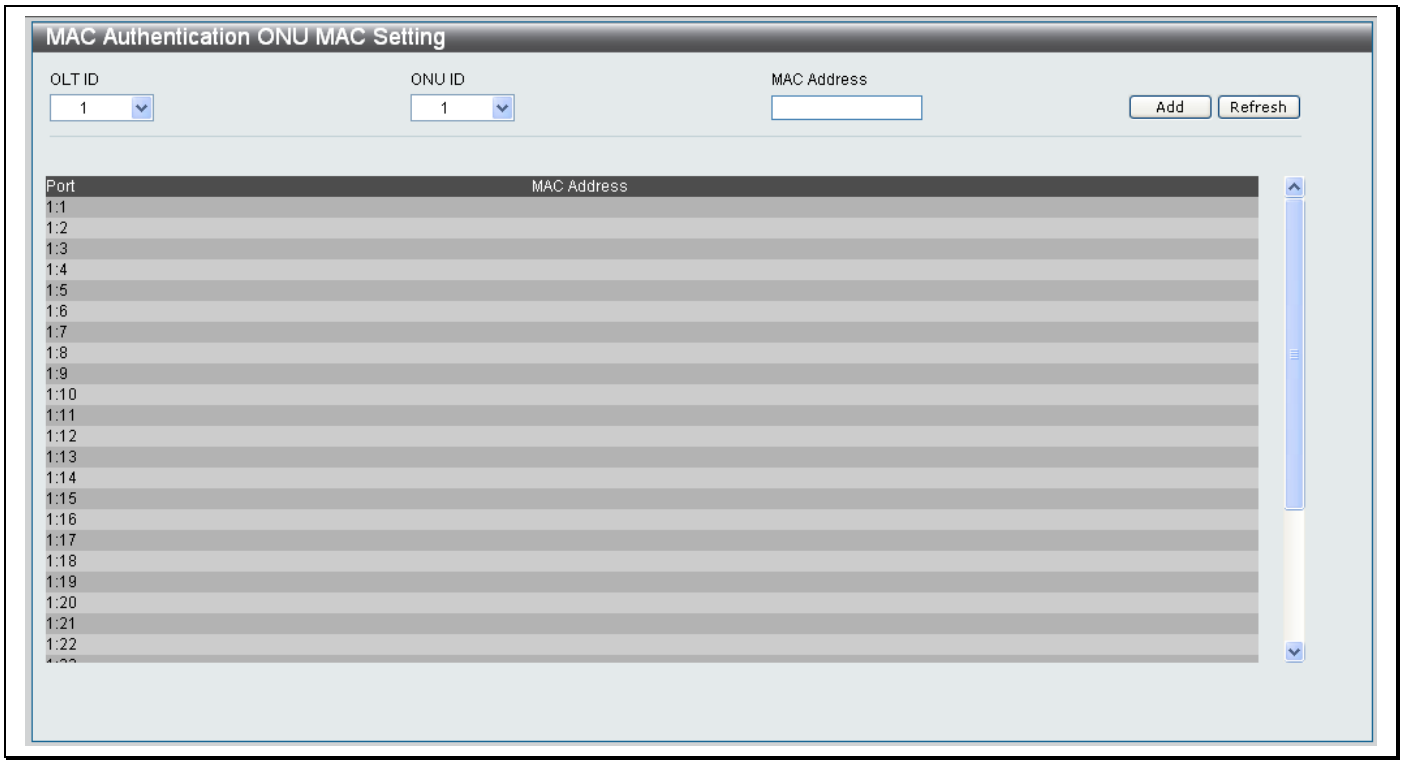


Figure 11- 5. MAC Authentication ONU MAC Setting window

Adding a MAC Address to the MAC Authentication ONU MAC Setting window

1. Use the **OLT ID** and **ONU ID** drop-down menus to specify the OLT's and ONU's that you want to add a MAC Address to.
2. Type the MAC Address you want to add in the **MAC Address** field.
3. Click the **Add** button to add the MAC Address.

Deleting a MAC Address from the MAC Authentication ONU MAC Setting window

1. Click the **Delete** button next to the MAC Address that corresponds with the MAC Address entry that you want to remove from the list.

OLT MAC Authentication Fail Table

The OLT MAC Authentication Fail Table window allows you to view the MAC entries that failed to authenticate. If an ONU has sent a register request, but the OLT has no MAC addresses assigned to this ONU or this MAC address has been assigned to another ONU port, the ONU will fail to authenticate and the MAC address will be recorded into the OLT MAC Authentication Fail Table.

If the table is full, and a new entry arrives, the oldest entry will be removed to accommodate the new entry.

To access the **OLT MAC Authentication Fail Table** window click **PON> MAC Authentication > OLT MAC Authentication Fail Table.**

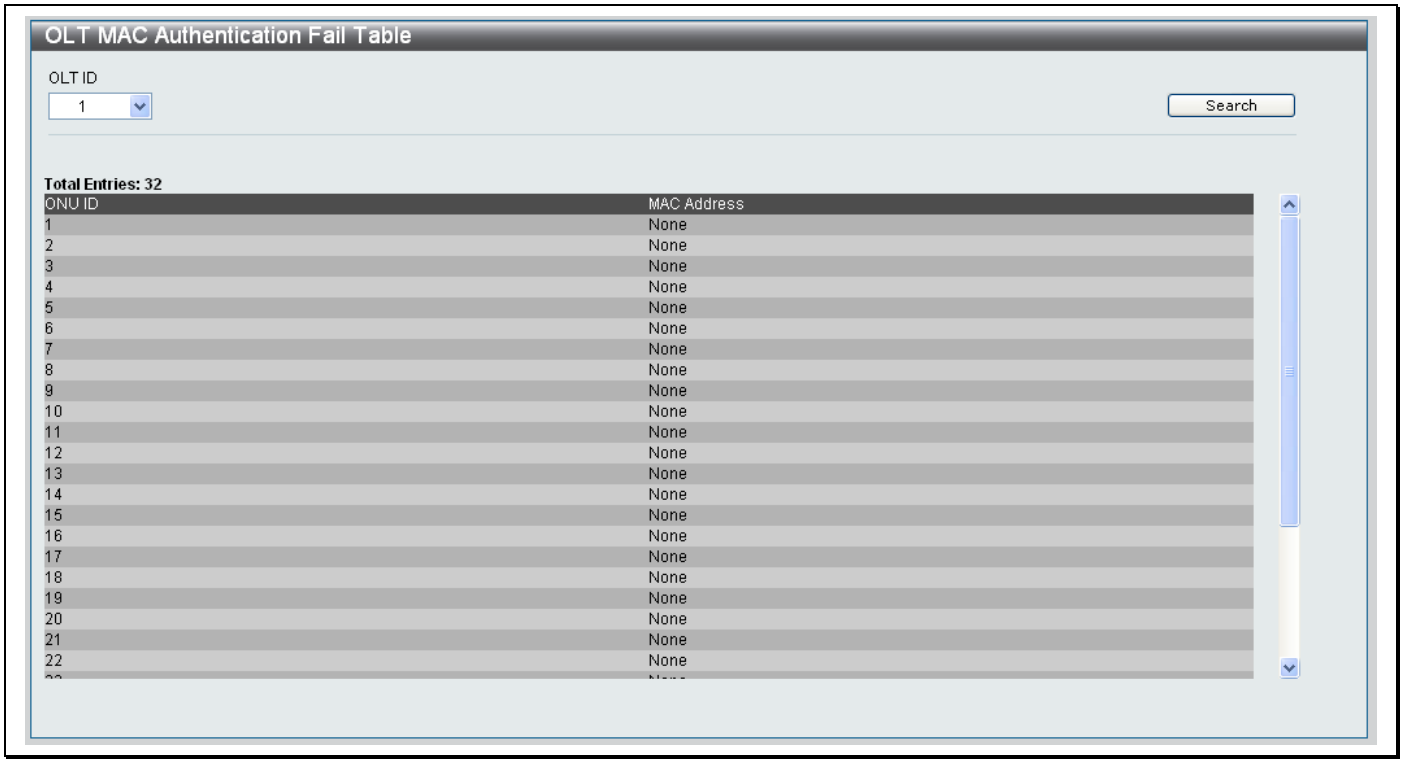


Figure 11- 6. OLT MAC Authentication Fail Table window

Searching for OLT MAC Authentication Failure entries

1. Use the **OLT ID** drop-down menu to select the OLT that you want to view the MAC Authentication failures for.
2. Click the **Search** button.
3. The results will appear in the table at the bottom of the window.

PON Bandwidth Control

Downstream Settings

The **Downstream Settings** window allows you to define the *Maximum Bandwidth* and *Maximum Burst Size* settings for downstream connections on the Switch.

To access the **Downstream Settings** window click **PON> PON Bandwidth Control > Downstream Settings.**

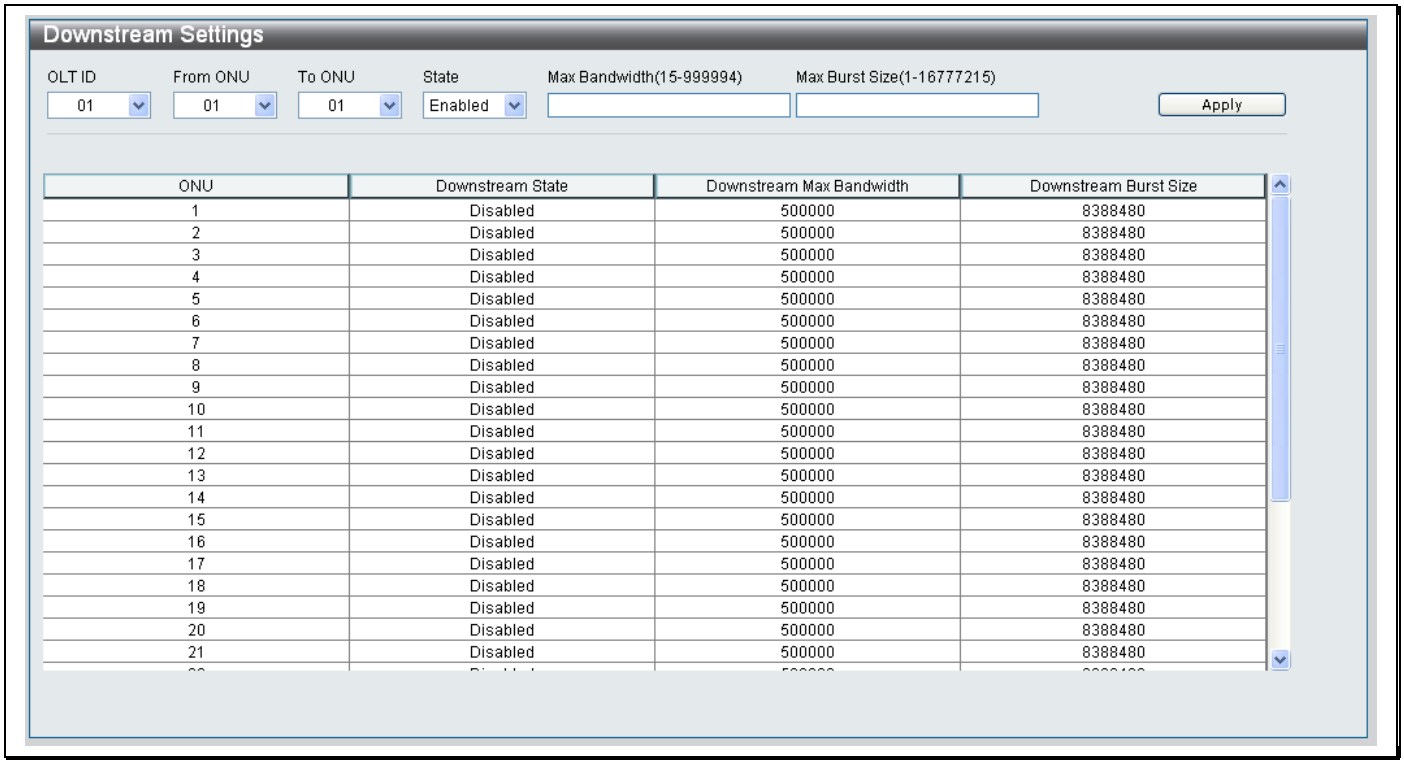


Figure 11- 7. PON Bandwidth Control- Downstream Settings window

Configuring PON Bandwidth Control Downstream Settings

1. Use the **OLT ID** drop-down menu to specify the OLT that you want to configure.
2. Use the **From ONU** and **To ONU** drop-down menus to specify the range of ONU's that you want to configure the Downstream Settings for.
3. Type a *Maximum Bandwidth* value, between 15 and 999994, in the **Max Bandwidth (15-999994)** field.
4. Type a *Maximum Burst Size* value, between 1 and 16777215, in the **Max Bandwidth (1-16777215)** field.
5. Click the **Apply** button to finish configuring the PON Bandwidth Control Downstream Settings.

Upstream Settings

The **Upstream Settings** window allows you to define the ONU's Upstream traffic control rules.

To access the **Upstream Settings** window click **PON> PON Bandwidth Control > Upstream Settings.**

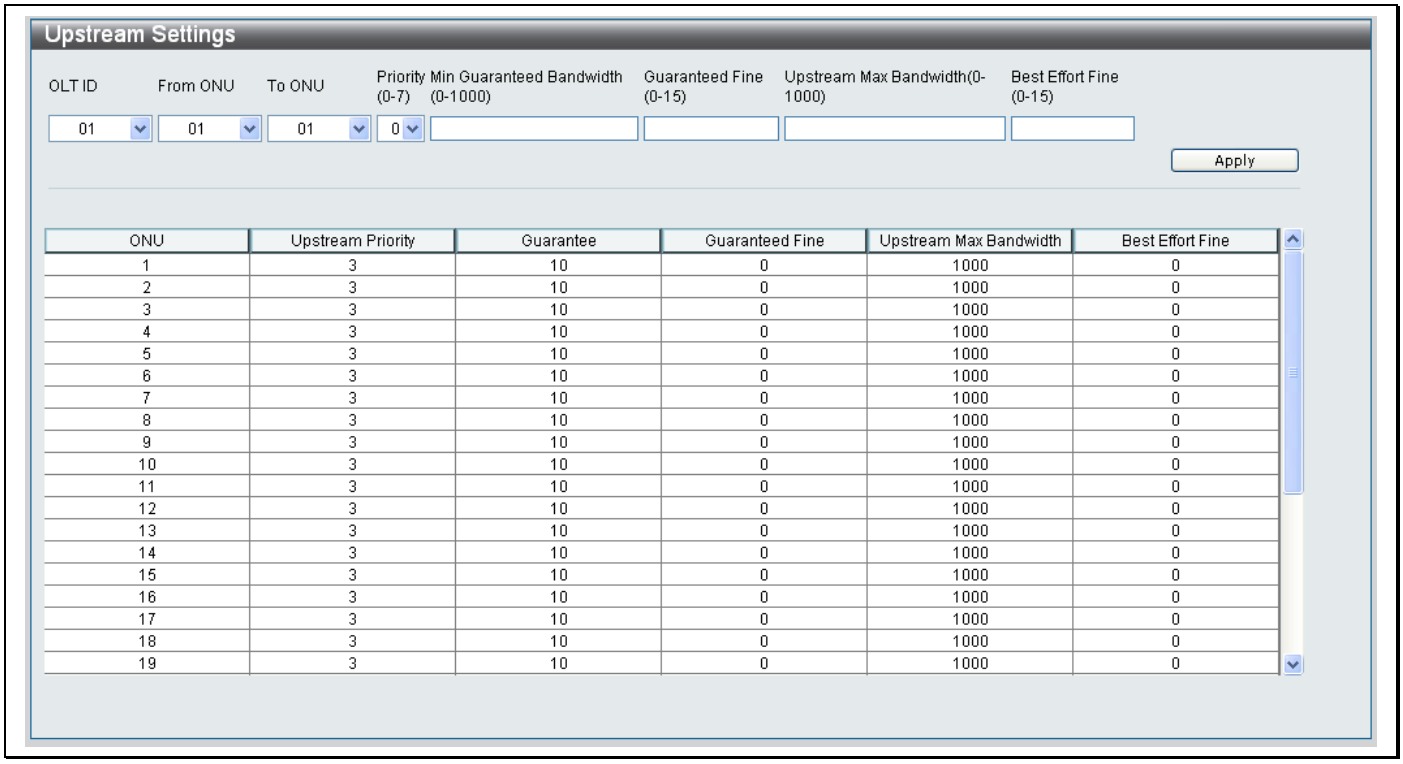


Figure 11- 8. PON Bandwidth Control- Upstream Settings window

Configuring PON Bandwidth Control Upstream Settings

1. Use the **OLT ID** drop-down menu to specify the OLT that you want to configure.
2. Use the **From ONU** and **To ONU** drop-down menus to specify the range of ONU's that you want to configure the Up Settings for.
3. Use the **Priority (0-7)** drop-down menu to choose a priority value between *0* and *7* for the specified ONU ports.
4. Type a *Minimum Guaranteed Bandwidth* value, between 0-1000, in the **Min. Guaranteed Bandwidth (0-1000)** field.
5. Type a *Guaranteed Fine* value, between 0-15, in the **Guaranteed Fine (0-15)** field.
6. Type an *Upstream Max Bandwidth* value, between 0-1000, in the **Upstream Max Bandwidth (0-1000)** field.
7. Type a *Best Effort Fine* value, between 0-15, in the **Best Effort Fine (0-15)** field.
8. Click the **Apply** button to finish configuring the PON Bandwidth Control Downstream Settings.

ONU FEC Settings

The **ONU FEC Settings** window allows you to configure the OLT FEC mode per ONU.

To access the **ONU FEC Settings** window click **PON> ONU FEC Settings.**

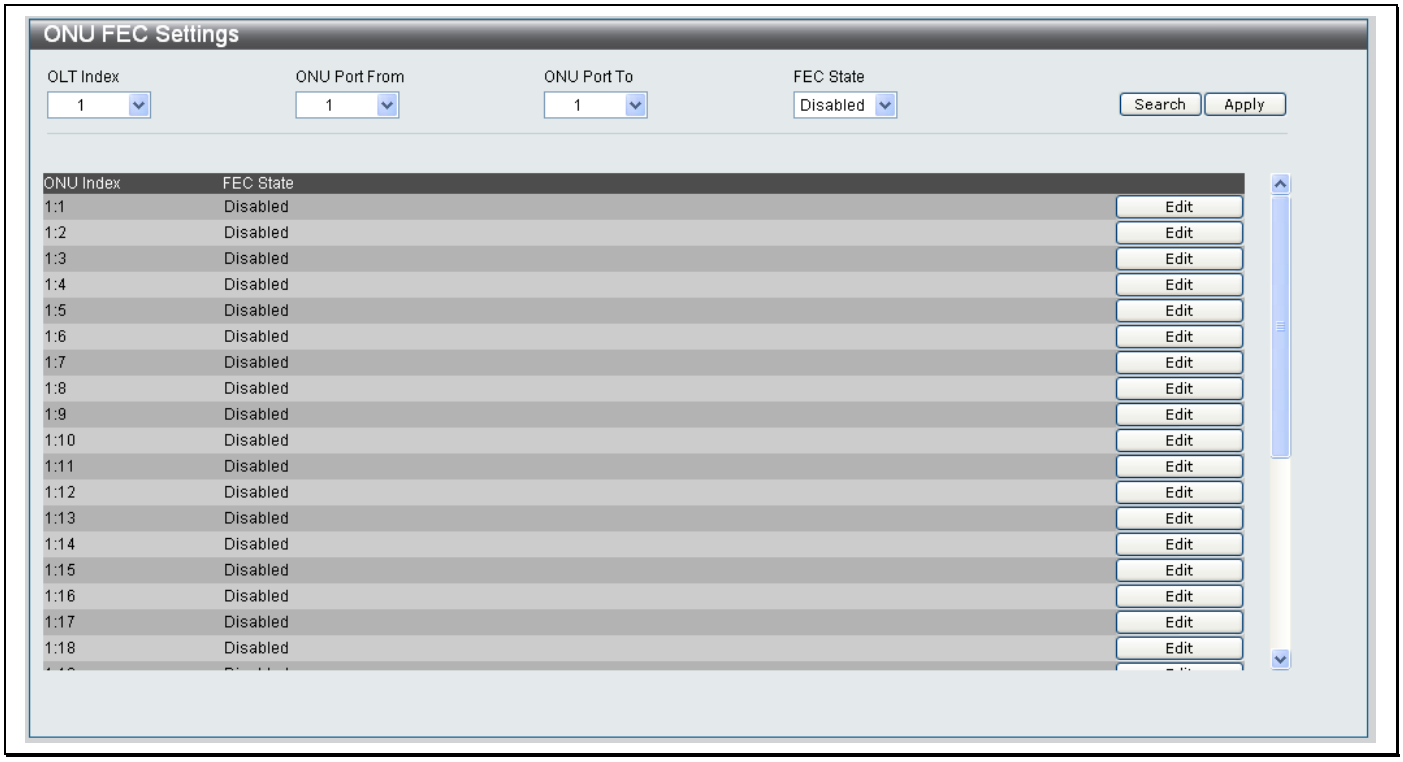


Figure 11- 9. ONU FEC Settings window

Configuring ONU FEC Settings

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to configure.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to configure the FEC Settings for.
3. Use the **FEC State** drop-down menu to specify if the specified ONU ports should be *Enabled* or *Disabled*.
4. Click the **Apply** button to finish configuring the ONU FEC Settings.

Searching for an existing ONU FEC Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to view information about.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to view information about.
3. Use the **FEC State** drop-down menu to specify if the specified ONU port is *Enabled* or *Disabled*.
4. Click the **Search** button to search for the specified ONU FEC Setting.

Editing an existing ONU FEC Setting

1. Click the **Edit** button next to the OLT Index that you want to edit
2. Use the **FEC State** drop-down menus to specify if the FEC State should be *Enabled* or *Disabled*.
3. Click the **Apply** button to apply the change.

ONU UNI Port Settings

The **ONU UNI Port Settings** window allows you to show specific Ethernet port information for specific ONU's.

To access the **ONU UNI Port Settings** window click **PON> ONU UNI Port Settings.**

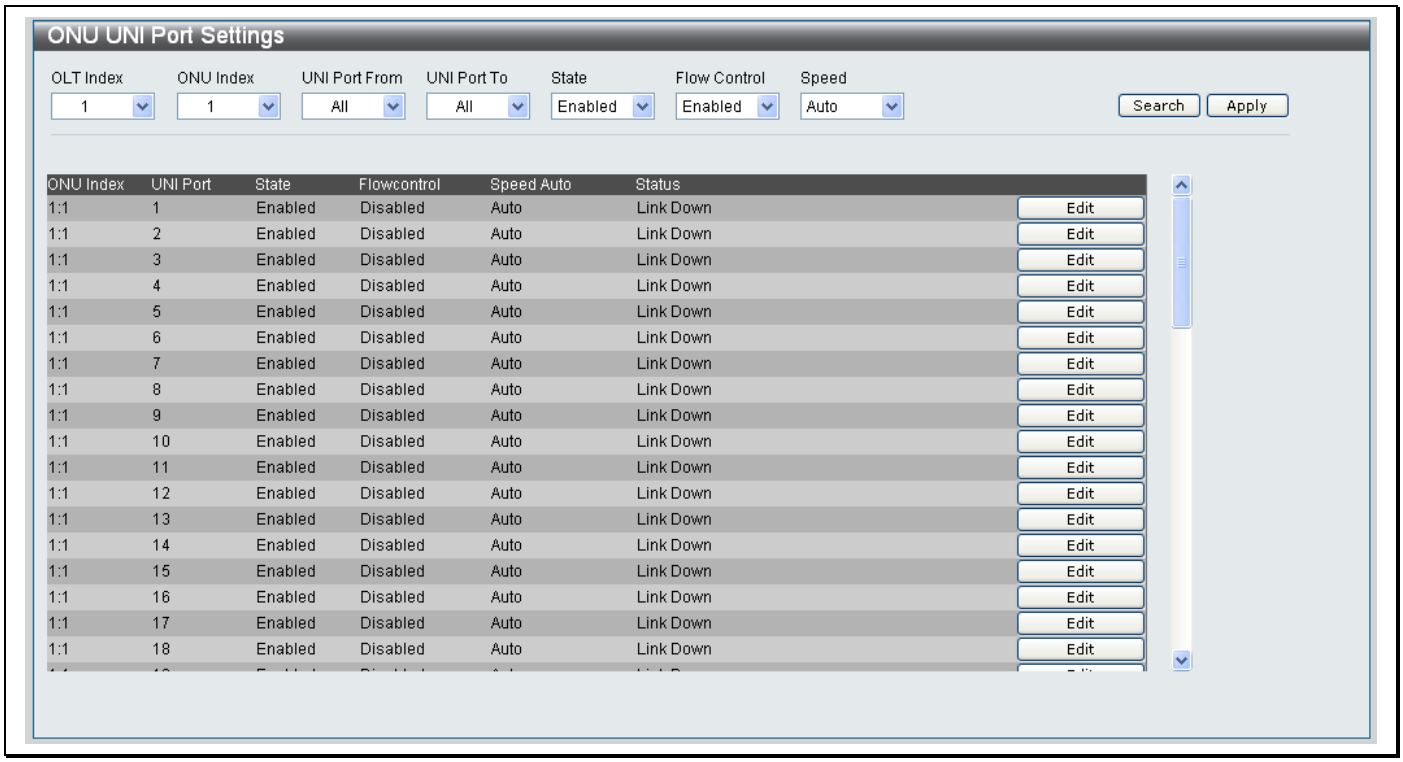


Figure 11- 10. ONU UNI Port Settings window

Configuring ONU UNI Port Settings

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to configure.
2. Use the **ONU Index** drop-down menu to specify the ONU Index that you want to configure.
3. Use the **UNI Port From** and **UNI Port To** drop-down menus to specify the range of UNI ports that you want to configure the ONU UNI Port Settings for.
4. Use the **State** drop-down menu to specify if the State of the specified ONU UNI ports should be *Enabled* or *Disabled*.
5. Use the **Flow Control** drop-down menu to specify if Flow Control on the specified ONU UNI ports should be *Enabled* or *Disabled*.
6. Click the **Apply** button to finish configuring the ONU FEC Settings.

Searching for an existing ONU UNI Port Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to view ONU UNI Port information about.
2. Use the **ONU Index** drop-down menu to specify the ONU Index that you want to view ONU UNI Port information about.
3. Use the **UNI Port From** and **UNI Port To** drop-down menus to specify the range of UNI ports that you want to view information about.
4. Use the **State** drop-down menu to specify if the State of the specified UNI port you are searching for should be *Enabled* or *Disabled*.
5. Use the **Flow Control** drop-down menu to specify if Flow Control on the specified ONU UNI ports you are searching for should be *Enabled* or *Disabled*.
6. Click the **Search** button to search for the ONU UNI Port Setting.

Editing an existing ONU UNI Port Setting

1. Click the **Edit** button next to the ONU UNI Port Setting that you want to edit.
2. Use the **State** drop-down menus to specify if the ONU UNI Port State should be *Enabled* or *Disabled*.
3. Use the **Flowcontrol** drop-down menu to specify if Flowcontrol on the ONU UNI Port should be *Enabled* or *Disabled*.
4. Choose whether the ONU UNI Port should run at *Auto, 10M_Half, 10M_Full, 100M_Half* or *100M_Full* from the **Speed Auto** drop-down menu.
5. Click the **Apply** button to apply the changes.

ONU Encryption Settings

The **ONU Encryption Settings** window allows you to enable or disable encryption on the ONU's/

To access the **ONU Encryption Settings** window click **PON> ONU Encryption Settings.**

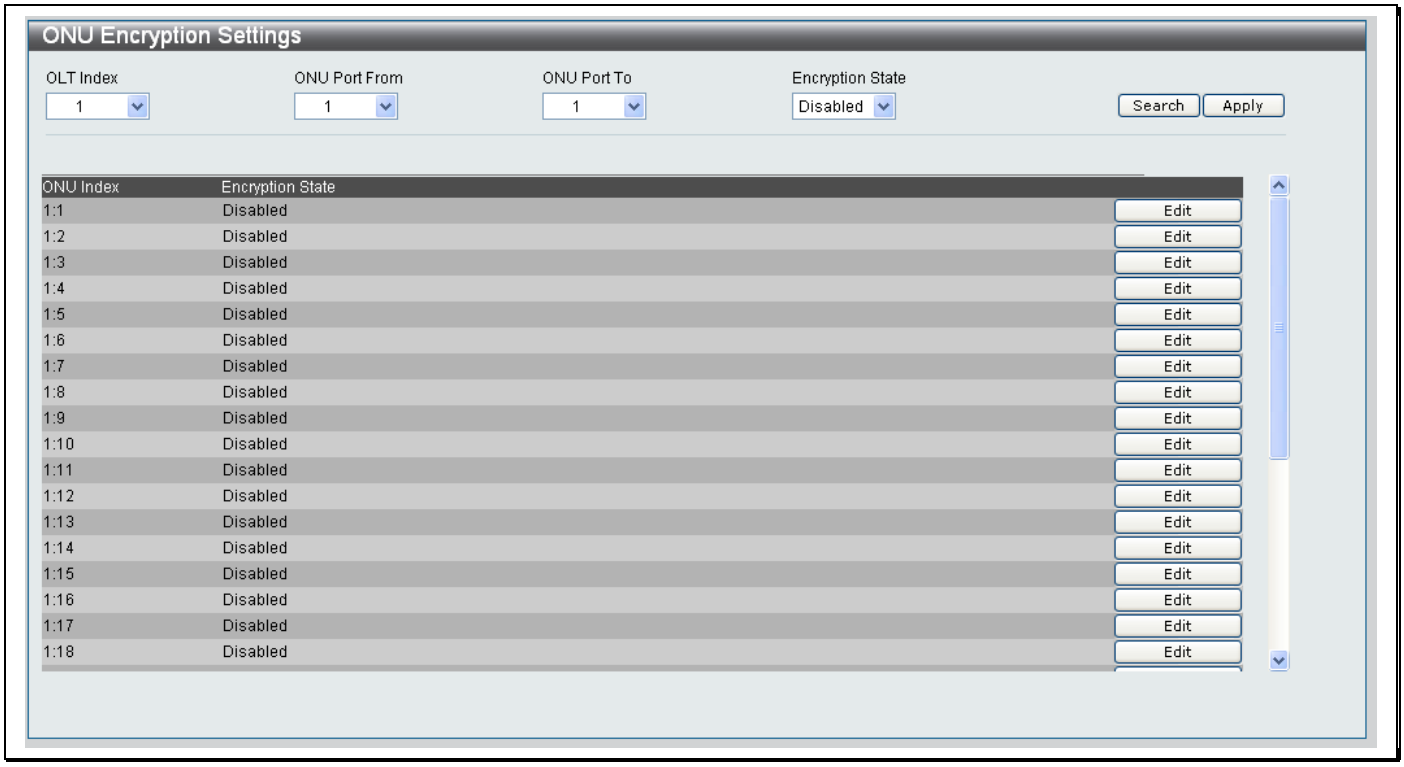


Figure 11- 11. ONU Encryption Settings window

Configuring ONU Encryption Settings

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to configure ONU Encryption on.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to configure ONU Encryption on.
3. Use the **Encryption State** drop-down menu to specify if the specified ONU UNI ports have encryption *Enabled* or *Disabled* on them
4. Click the **Apply** button to finish configuring the ONU Encryption Settings.

Searching for an existing ONU Encryption Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to view the ONU Encryption settings for.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to view the ONU Encryption Settings for.
3. Use the **Encryption State** drop-down menu to specify if the ONU UNI ports you want to search for has encryption *Enabled* or *Disabled* on them
4. Click the **Search** button to search for the ONU UNI Port Setting.

Editing an existing ONU UNI Port Setting

1. Click the **Edit** button next to the ONU UNI Port Setting that you want to edit.
2. Use the **Encryption State** drop-down menu to specify if the ONU UNI port you want to edit has encryption *Enabled* or *Disabled* on them.
3. Click the **Apply** button to apply the changes.

Diagnostic Test

The **Diagnostic Test** window allows you to carry out various diagnostic tests on the Switch.

To access the **Diagnostic Test** window click **PON> Diagnostic Test.**

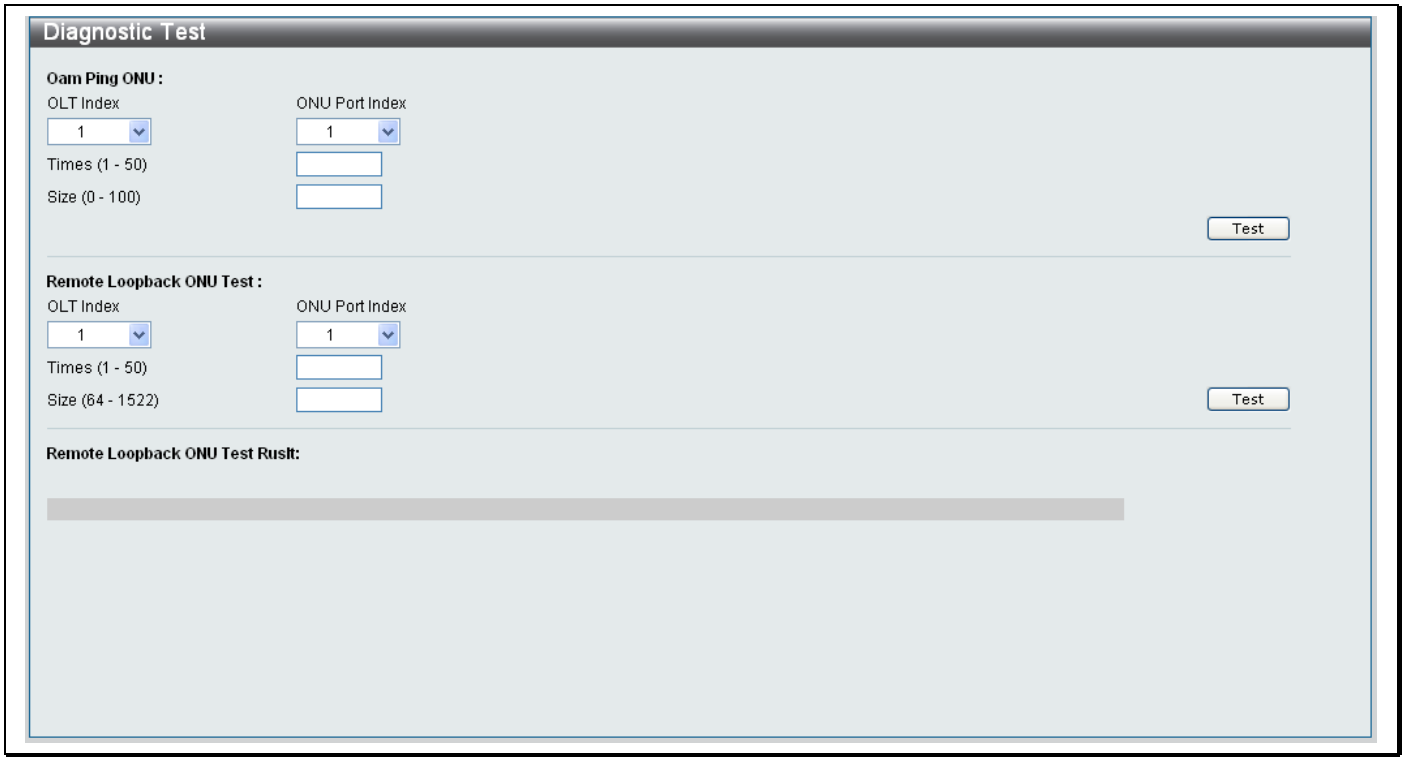


Figure 11- 12. Diagnostic Test window

The **Diagnostic Test** window allows you to carry out an **Oam Ping ONU** and **Remote Loopback ONU Test.**

Oam Ping Test

The Oam ping test is used to ping a registered ONU. This test can't be carried out on ONU's that aren't registered on the Switch.

To carry out an **Oam Ping ONU** configure the parameters in the **Oam Ping ONU** section as described below:

Parameter	Description
OLT Index	Use the drop-down menu to identify the Index number of the OLT the ONU is connected to.
ONU Port Index	Use the drop-down menu to identify the Port Index number of the port the ONU is connected to.
Times (1-50)	Type a number between *1* and *50* to specify the number of packets you want to send in the test.
Size (0-100)	Type a number between *0* and *100* to specify the ping packet size.

Click the **Test** button to start the OAM Ping ONU.

The results will appear in the **Ping Test Result** window as shown below:

- Click the **Stop** button to pause the Test.
- Click the **Resume** button to resume the Test.
- To return to the **Diagnostic Test** window click the *Return to Ping Test Screen* hyperlink.

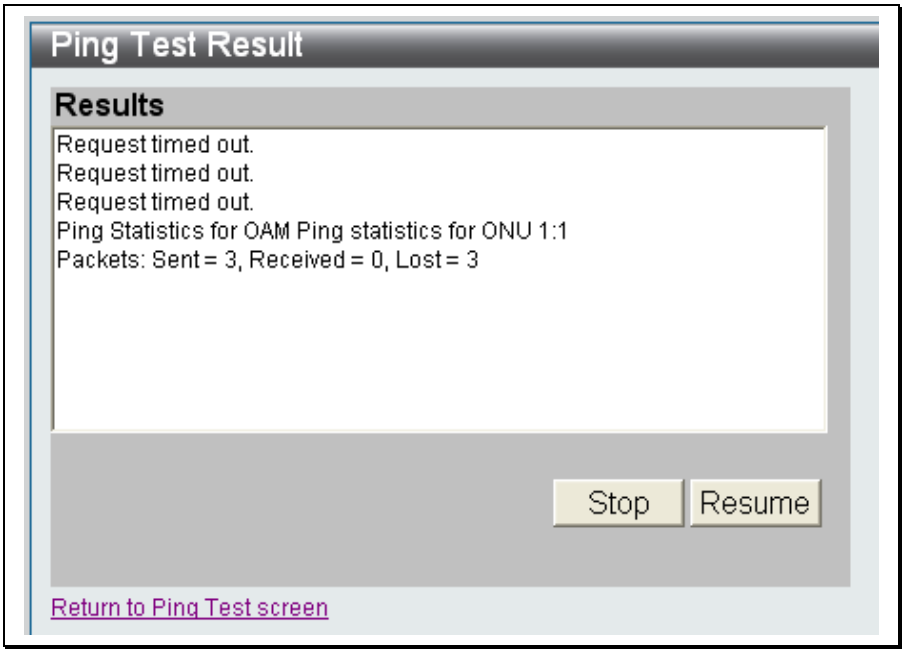


Figure 11- 13. Ping Test Result window

Remote Loopback ONU Test

The **Remote Loopback ONU Test** is used to test the remote loopback between the OLT and ONU. The OLT will send packets to the ONU, which the ONU will loop back. This tests that the packets can transmit correctly between the ONU and OLT.

When the ONU is in loopback mode, the downstream traffic will be echoed back to OLT. After the Remote Loopback ONU Test is completed, the ONU will automatically return back to normal mode.

To carry out a **Remote Loopback ONU Test** configure the parameters in the **Remote Loopback ONU Test** section as described below:

Parameter	Description
OLT Index	Use the drop-down menu to identify the Index number of the OLT the ONU is connected to.
ONU Port Index	Use the drop-down menu to identify the Port Index number of the port the ONU is connected to.
Times (1-50)	Type a number between *1* and *50* to specify the number of packets you want to send in the test.
Size (64-1522)	Type a number between *64* and *1522* to specify the ping packet size.

Click the **Test** button to start the OAM Ping ONU.

The results will appear in the **Remote Loopback ONU Result** section at the bottom of the **Diagnostic Test** window.

ONU IGMP Snooping Settings

The **ONU IGMP Snooping Settings** window allows you to view and configure the ONU IGMP Snooping Settings.

To access the **ONU IGMP Snooping Settings** window click **PON> ONU IGMP Snooping Settings.**

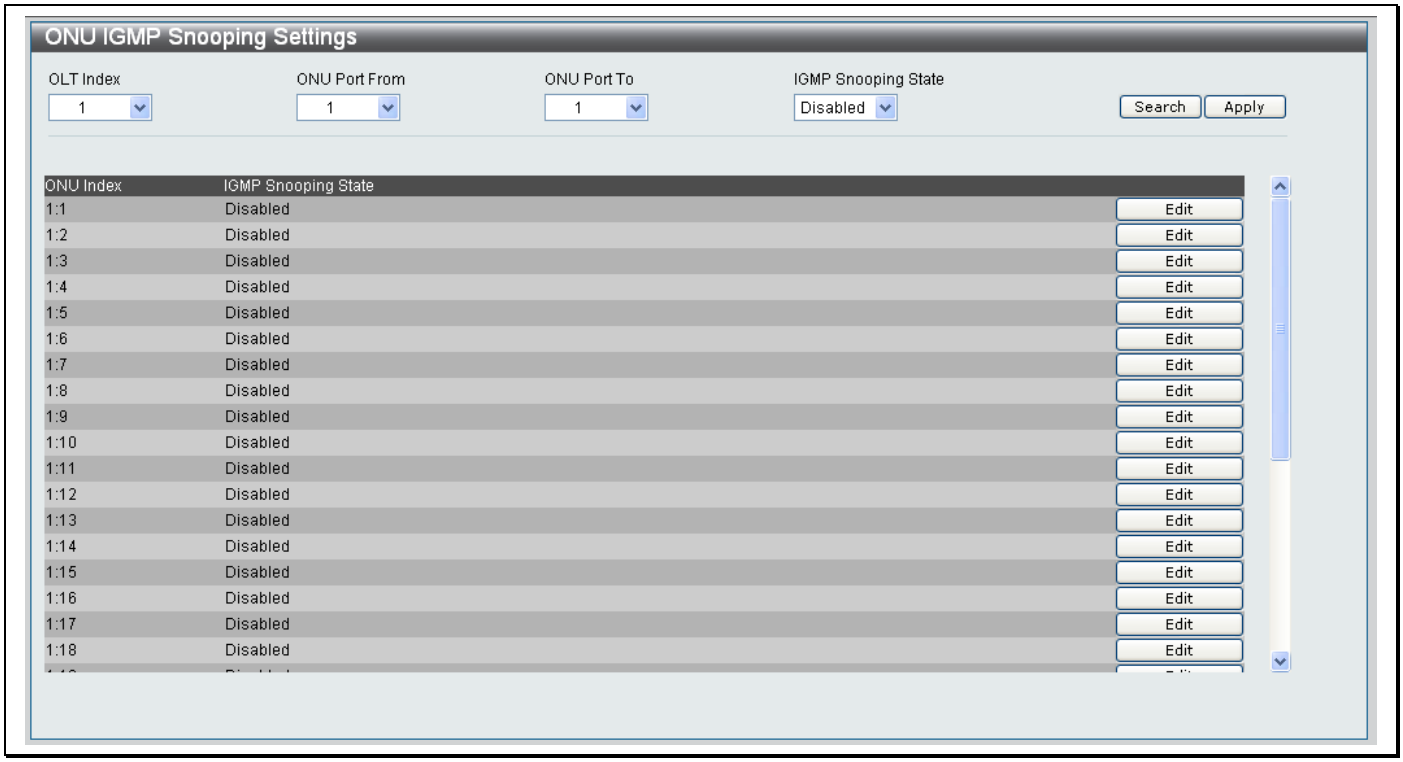


Figure 11- 14. ONU IGMP Snooping Settings window

Configuring ONU IGMP Snooping Settings

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to configure ONU IGMP Snooping on.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to configure IGMP Snooping State settings on.
3. Use the **IGMP Snooping State** drop-down menu to specify if the specified ONU ports have IGMP Snooping *Enabled* or *Disabled* on them
4. Click the **Apply** button to finish configuring the ONU IGMP Snooping Settings.

Searching for an existing ONU IGMP Snooping Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index that you want to view the ONU IGMP Snooping settings for.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to view the ONU IGMP Snooping Settings for.
3. Use the **IGMP Snooping State** drop-down menu to specify if the ONU UNI ports you want to search for has IGMP Snooping *Enabled* or *Disabled* on them
4. Click the **Search** button to search for the IGMP Snooping Setting.

Editing an existing ONU IGMP Snooping Setting

1. Click the **Edit** button next to the IGMP Snooping ONU Index that you want to edit.
2. Use the **IGMP Snooping State** drop-down menu to specify if the ONU Index you want to edit should have its IGMP Snooping State *Enabled* or *Disabled*.
3. Click the **Apply** button to apply the changes.

ONU IGMP Snooping Groups

The **ONU IGMP Snooping Groups** window allows you to search for existing ONU IGMP Snooping Groups configured on the Switch.

To access the **ONU IGMP Snooping Groups** window click **PON> ONU IGMP Snooping Groups.**

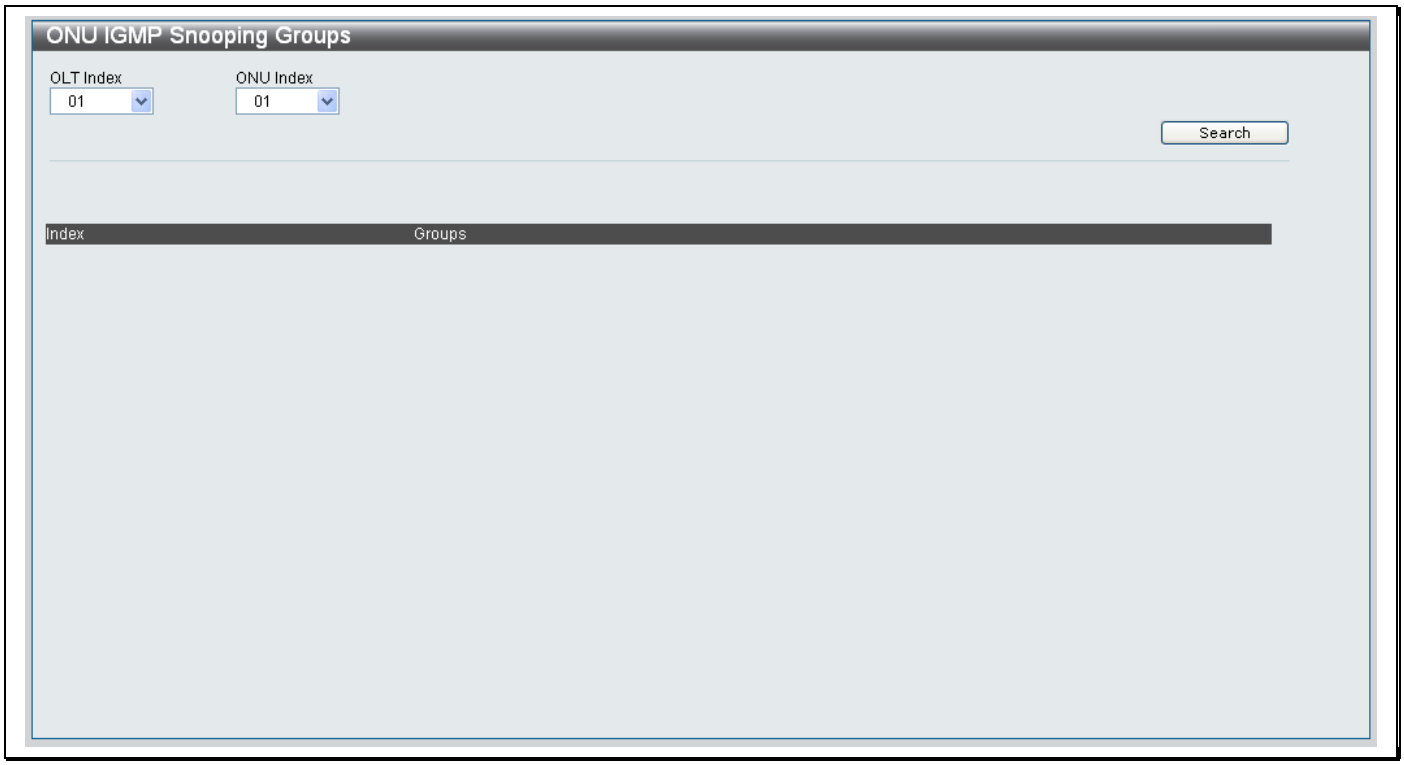


Figure 11- 15. ONU IGMP Snooping Groups window

To search for an ONU IGMP Snooping Group

1. Select the *OLT Index* you want to view ONU IGMP Snooping Group information about from the drop-down menu.
2. Select the *ONU Index* you want to view ONU IGMP Snooping Group information about from the drop-down menu.
3. Click the **Search** button.
4. The result of the search will appear at the bottom of the **IGMP Snooping Group** window.

OLT VLAN

OLT VLAN tpid Settings

The **OLT VLAN tpid** settings window allows you to view and edit the OLT VLAN tpid settings configured on the Switch.

To access the **ONU VLAN tpid** window click **PON> OLT VLAN> OLT VLAN tpid Settings.**

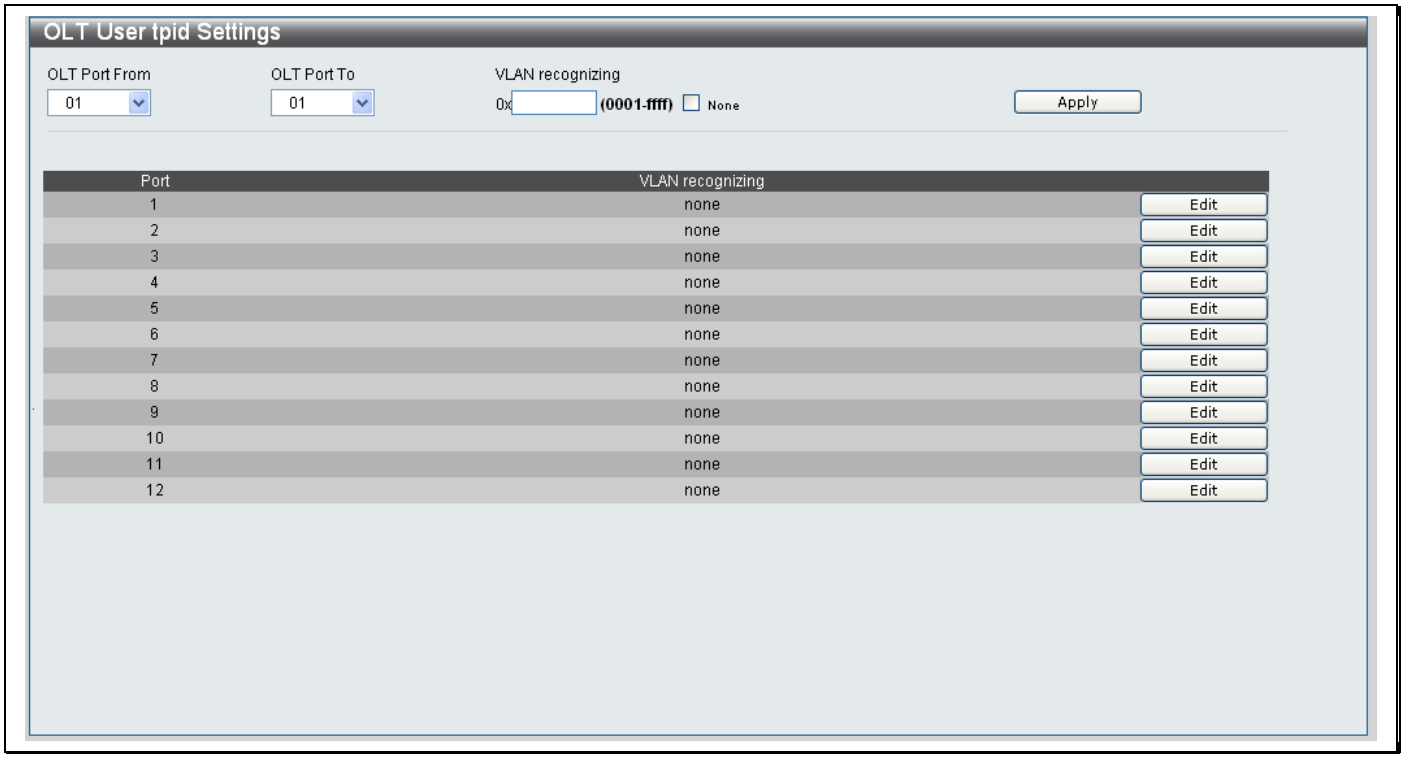


Figure 11- 16. OLT User tpid Settings window

Configuring OLT VLAN tpid Settings

1. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the range of ONU ports that you want to configure VLAN tpid settings on.
2. Type the *hexadecimal* value of the VLAN in the **VLAN recognizing** field. Tick the **None** checkbox to specify that no VLAN's should be specified.
3. Click the **Apply** button to finish configuring the OLT VLAN tpid Settings.

Editing OLT VLAN tpid Settings

1. Click the **Edit** button next to the entry that you want to edit.
2. Type a new *hexadecimal* value for the VLAN in the **VLAN recognizing** field, next to the new entry.
3. Click the **Apply** button next to the entry being edited to apply the change.

ONU Upstream VLAN Mode Settings

The **ONU Upstream VLAN Mode Settings** window allows you to view existing and configure new ONU Upstream VLAN Mode Settings.

To access the **ONU Upstream VLAN Mode Settings** window click **PON> OLT VLAN> ONU Upstream VLAN Mode Upstream Settings.**

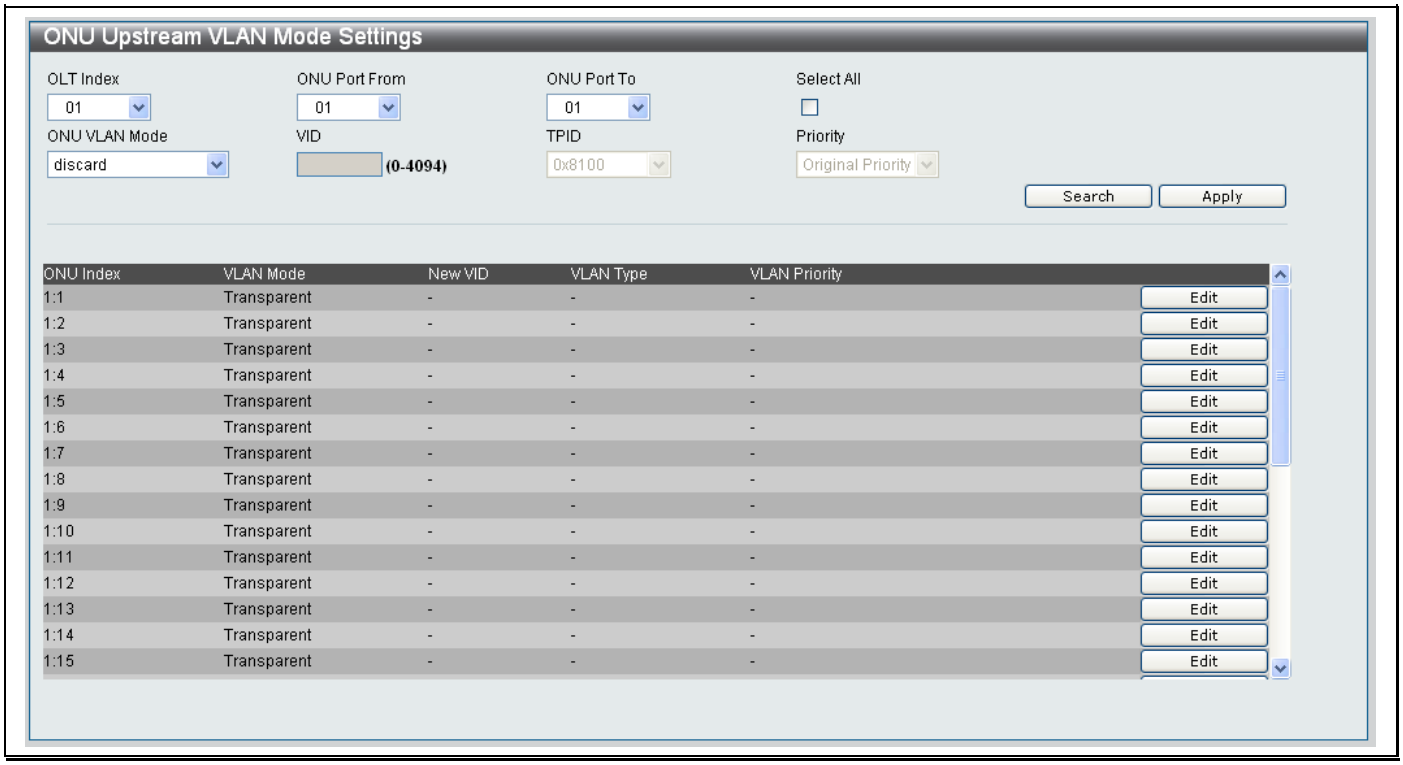


Figure 11- 17. ONU Upstream VLAN Mode Settings window

Adding a new ONU Upstream VLAN Mode Upstream setting

To add a new ONU Upstream VLAN Mode setting, configure the parameters as described below:

Parameter	Description
OLT Index	Use the drop-down menu to select the OLT Index number that the ONU is connected to.
ONU Port From / ONU Port To	Use the drop-down menus to specify the ONU Port range that you want to configure.
ONU VLAN Mode	Choose *discard*, *transparent*, *tag* or *translation* from the drop-down menu.
VID	If selecting the *tag* or *translation* setting from the drop-down menu, type the VLAN ID you want to tag or translate in the textbox.
TPID	Choose a TPID value from the drop-down menu.
Priority	Choose a *Priority* value from the drop-down menu.

Click the **Apply** button to add the ONU Upstream setting.

Searching for an existing ONU Upstream VLAN Mode Upstream setting

To search for an existing ONU Upstream VLAN Mode setting, configure the parameters as described below:

Parameter	Description
OLT Index	Use the drop-down menu to select the OLT Index number that the ONU is connected to.
ONU Port From / ONU Port To	Use the drop-down menus to specify the ONU Port range that you want to configure.
ONU VLAN Mode	Choose *discard*, *transparent*, *tag* or *translation* from the drop-down menu.
VID	If selecting the *tag* or *translation* setting from the drop-down menu, type the VLAN ID you want to tag or translate in the textbox.
TPID	Choose a TPID value from the drop-down menu.
Priority	Choose a *Priority* value from the drop-down menu.

Click the **Search** button to start the search.

Editing an existing ONU Upstream VLAN Mode Upstream setting

To edit an existing ONU Upstream VLAN Mode setting, click the **Edit** button next to the corresponding entry. The following parameters can be edited in the table at the bottom of the screen.

Parameter	Description
VLAN Mode	Choose a new VLAN Mode from the drop-down menu. The choices are *discard*, *transparent*, *tag* and *translation*
New VID	If selecting the *tag* or *translation* setting from the drop-down menu, type the VLAN ID you want to tag or translate in the textbox.
VLAN Type	Choose a *VLAN Type* value from the drop-down menu.
VLAN Priority	Choose a *VLAN Priority* value from the drop-down menu.

Click the **Apply** button to save the changes made.

ONU Upstream VLAN Authentication Settings

The **ONU Upstream VLAN Authentication Settings** window allows you to configure the upstream VLAN authentication for a specific ONU.

To access the **ONU Upstream VLAN Authentication Settings** window click **PON> OLT VLAN> ONU Upstream VLAN Authentication Settings.**

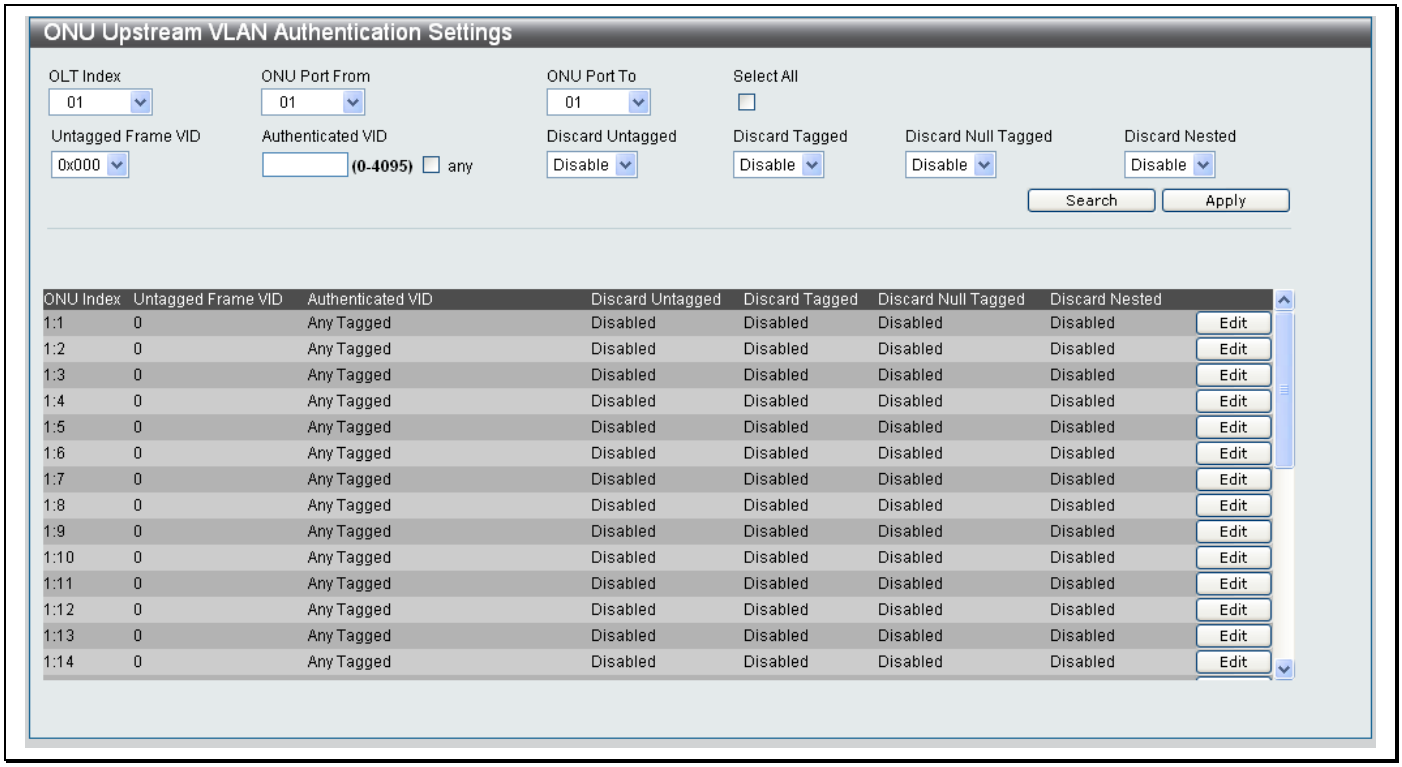


Figure 11- 18. ONU Upstream VLAN Authentication Settings window

Adding a new ONU Upstream VLAN Authentication setting

To add a new ONU Upstream VLAN Authentication setting, configure the parameters as described below:

Parameter	Description
OLT Index	Use the drop-down menu to specify the OLT Index of the ONU's you want to configure.
ONU Port From / ONU Port To	Use the drop-down menus to specify the ONU ports that you want to configure the ONU Upstream VLAN Authentication settings for.
Untagged Frame VID	Choose a *VID* from the drop-down menu that will be assigned to a frame that does not have VLAN tag. This *VID* will be assigned to it during authentication. This setting is only used for authentication.
Authenticated VID	Type the VID is required for authentication. Tick the adjacent **Any** checkbox to allow all VID's to be forwarded.
Discard Untagged	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames without a VLAN tag. Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames without a VLAN tag.
Discard Tagged	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames with a VLAN tag. Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames with a VLAN tag.
Discard Null Tagged	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames with a Null VLAN tag (vid is 0 in tag). Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames with a Null VLAN tag (vid is 0 in tag).
Discard Nested	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames with a Nested VLAN tag (double VLAN tag). Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames with a Nested VLAN tag (double VLAN tag).

Click the **Apply** button to add the ONU Upstream setting.

Searching for an existing ONU Upstream VLAN Authentication setting

To search for an existing ONU Upstream VLAN Authentication setting, configure the parameters as described below:

Parameter	Description
OLT Index	Use the drop-down menu to specify the OLT Index of the ONU's you are searching for.
ONU Port From / ONU Port To	Use the drop-down menus to specify the ONU ports that you want to view the ONU Upstream VLAN Authentication settings for.
Untagged Frame VID	Choose the *Untagged Frame VID* from the drop-down menu that is being used by the *ONU Authentication Setting* you are looking for.
Authenticated VID	Type the *Authenticated VID* required for authentication that is being used by the *ONU Authentication Setting* you are looking for. Tick the adjacent **Any** checkbox to search for an *ONU Authentication Setting* that allows all VID's to be forwarded.
Discard Untagged	Choose *Enable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to drop all frames without a VLAN tag. Choose *Disable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to NOT drop all frames without a VLAN tag.
Discard Tagged	Choose *Enable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to drop all frames with a VLAN tag. Choose *Disable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to NOT drop all frames with a VLAN tag.
Discard Null Tagged	Choose *Enable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to drop all frames with a Null VLAN tag (vid is 0 in tag). Choose *Disable* from the drop-down menu to drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to NOT drop all frames with a Null VLAN tag (vid is 0 in tag).
Discard Nested	Choose *Enable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to drop all frames with a Nested VLAN tag (double VLAN tag). Choose *Disable* from the drop-down menu to specify if the *ONU Authentication Setting* you are looking for instructs the Switch to NOT drop all frames with a Nested VLAN tag (double VLAN tag).

Click the **Search** button to start the search.

Editing an existing ONU Upstream VLAN Mode Upstream setting

To edit an existing ONU Upstream VLAN Mode setting, click the **Edit** button next to the corresponding entry. The following parameters can be edited in the table at the bottom of the screen.

Parameter	Description
Untagged Frame VID	Choose a *VID* from the drop-down menu that will be assigned to a frame that does not have VLAN tag. This *VID* will be assigned to it during authentication. This setting is only used for authentication.
Authenticated VID	Type the VID is required for authentication. Tick the adjacent **Any** checkbox to allow all VID's to be forwarded.
Discard Untagged	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames without a VLAN tag. Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames without a VLAN tag.
Discard Tagged	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames with a VLAN tag. Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames with a VLAN tag.
Discard Null Tagged	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames with a Null VLAN tag (vid is 0 in tag). Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames with a Null VLAN tag (vid is 0 in tag).
Discard Nested	Choose *Enable* from the drop-down menu to specify that the Switch will drop all frames with a Nested VLAN tag (double VLAN tag). Choose *Disable* from the drop-down menu to specify that the Switch will NOT drop all frames with a Nested VLAN tag (double VLAN tag).

Click the **Apply** button to save the changes made.

OLT VLAN Downstream Settings

The **OLT VLAN Downstream Settings** window allows you to view and show VLAN handling settings for downstream connections.

To access the **OLT VLAN Downstream Settings** window click **PON> OLT VLAN> OLT VLAN Downstream Settings.**

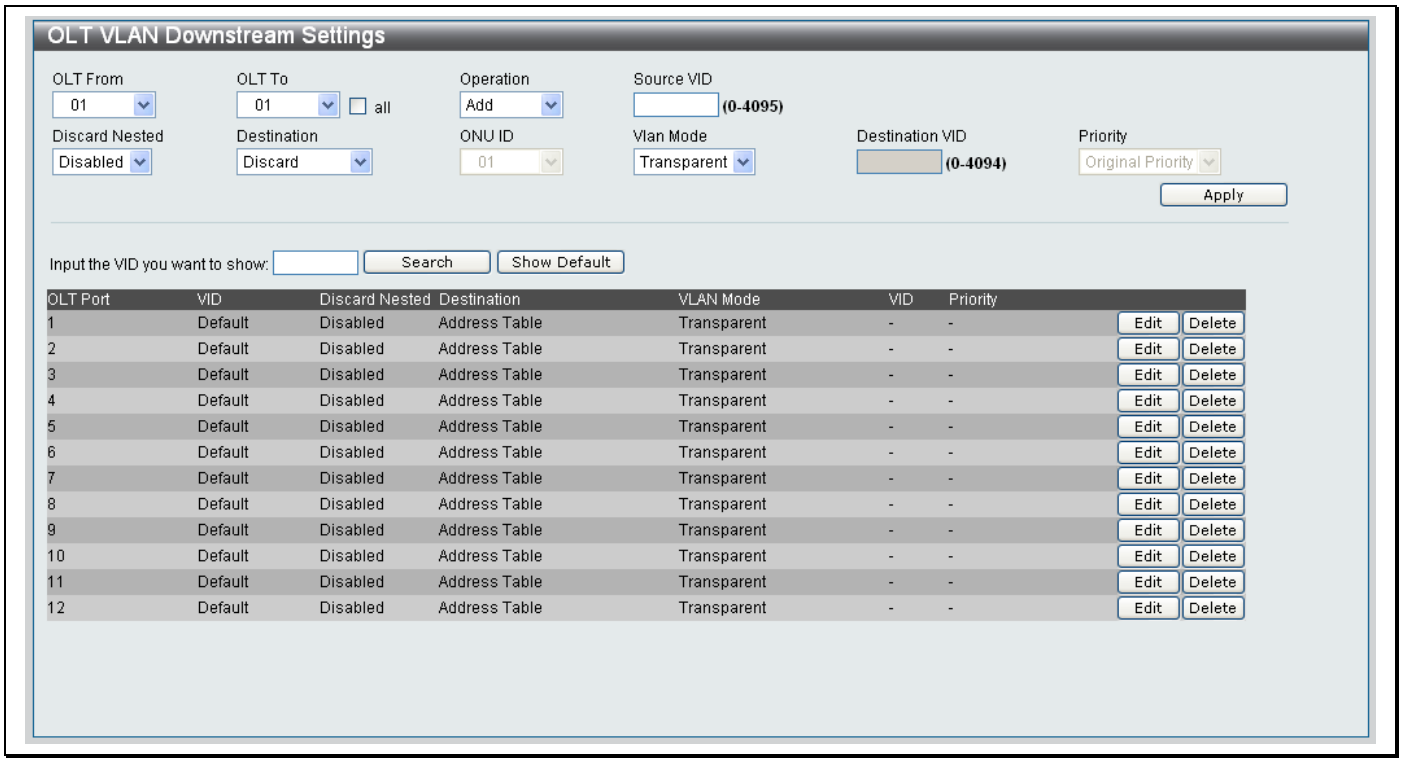


Figure 11- 19. OLT VLAN Downstream Settings window

To add/remove an OLT VLAN Downstream setting, configure the parameters as described below:

Parameter	Description
OLT From / OLT To	Use the drop-down menus to specify the OLT ports that you want to configure the ONU Downstream Settings on. Tick the **all** checkbox to specify all OLT ports.
Operation	Choose the *Add* option from the drop-down menu to add or update a VLAN rule. Choose the *Delete* option to delete a VLAN rule.
Source VID	Type in the Source *VID* that needs to be configured. The range is between *0* and *4095*.
Discard Nested	Choose *Disable* from the drop-down menu to specify that frames with a nested tag should NOT be dropped. Choose *Enable* from the drop-down menu to specify that frames with a nested tag should be dropped.
Destination	Choose *Discard* from the drop-down menu to specify that frames should be dropped with a specific VID tag. Choose *Address Table* from the drop-down menu to specify that frames should be forwarded, according to the Address Table. Choose *Specific ONU* from the drop-down menu to specify that frames should be forwarded to a specific ONU or be broadcasted. Choose *Address And ONU* from the drop-down menu to specify that frames should be forwarded to a specific ONU.

ONU ID	If specifying *Specific ONU* in the Destination field, choose an *ONU ID* to specify where the frames should be forwarded to: Choose *Broadcast* to specify that the frames should be broadcasted. If specifying *Address AND ONU* in the Destination field: Choose an *ONU ID* between *01* and *32* from the drop-down menu.
Vlan Mode	Choose *Transparent* from the drop-down menu to specify that a tag should never be removed or added. Choose *Tag* from the drop-down menu to specify that the tag should be removed in downstream connections. Choose *Translation* from the drop-down menu to exchange the original VID in frames with a new VID and priority.
Destination VID	If selecting *Translation* in the **Vlan mode** field, type the Destination *VID* that needs to be configured. The range is between *0* and *4095*.
Priority	If selecting *Translation* in the **Vlan mode** field, choose a *Priority value* from the drop-down menu. Select *Original Priority* to keep the original priority value of the frame. Select *Specific Priority* to specify that an outer VLAN tag (comprised by the specified VLAN, specified TPID and the specified priority) will be added.

Click the **Apply** button to add the OLT VLAN Downstream Setting.

Searching for an existing OLT VLAN Downstream Setting

1. Type the *VID number* in the **Input the VID you want to show** field.
2. Click the **Search** button to start the search.
3. The VID information will display at the bottom of the window.

Showing the default VID

1. Click the **Show Default** button.
2. The Default VID information will display at the bottom of the window.

Editing an existing OLT VLAN Downstream Setting

To edit an existing OLT VLAN Downstream Setting, click the **Edit** button next to the corresponding entry. The following parameters can be edited in the table at the bottom of the screen.

Parameter	Description
Discard Nested	Choose *Disable* from the drop-down menu to specify that frames with a nested tag should NOT be dropped. Choose *Enable* from the drop-down menu to specify that frames with a nested tag should be dropped.
Destination	Choose *Discard* from the drop-down menu to specify that frames should be dropped with a specific VID tag. Choose *Address Table* from the drop-down menu to specify that frames should be forwarded, according to the Address Table. Choose *Specific ONU* from the drop-down menu to specify that frames should be forwarded to a specific ONU or be broadcasted. Choose *Address And ONU* from the drop-down menu to specify that frames should be forwarded to a specific ONU.
VLAN Mode	Choose *Transparent* from the drop-down menu to specify that a tag should never be removed or added. Choose *Tag* from the drop-down menu to specify that the tag should be removed in downstream connections. Choose *Translation* from the drop-down menu to exchange the original VID in frames with a new VID and priority.
VID	If selecting *Translation* in the **Vlan mode** field, type the Destination *VID* that needs to be configured. The range is between *0* and *4095*.
Priority	If selecting *Translation* in the **Vlan mode** field, choose a *Priority value* from the drop-down menu. Select *Original Priority* to keep the original priority value of the frame. Select *Specific Priority* to specify that an outer VLAN tag (comprised by the specified VLAN, specified TPID and the specified priority) will be added.

Click the corresponding **Apply** button to save the changes made.

Deleting an existing OLT VLAN Downstream Setting

Click the corresponding **Delete** button to delete the OLT VLAN Downstream Setting entry.

OLT Tagged Broadcast Forwarding Settings

To access the **OLT Tagged Broadcast Forwarding Settings** window click **PON> OLT VLAN> OLT Tagged Broadcast Forwarding Settings.**

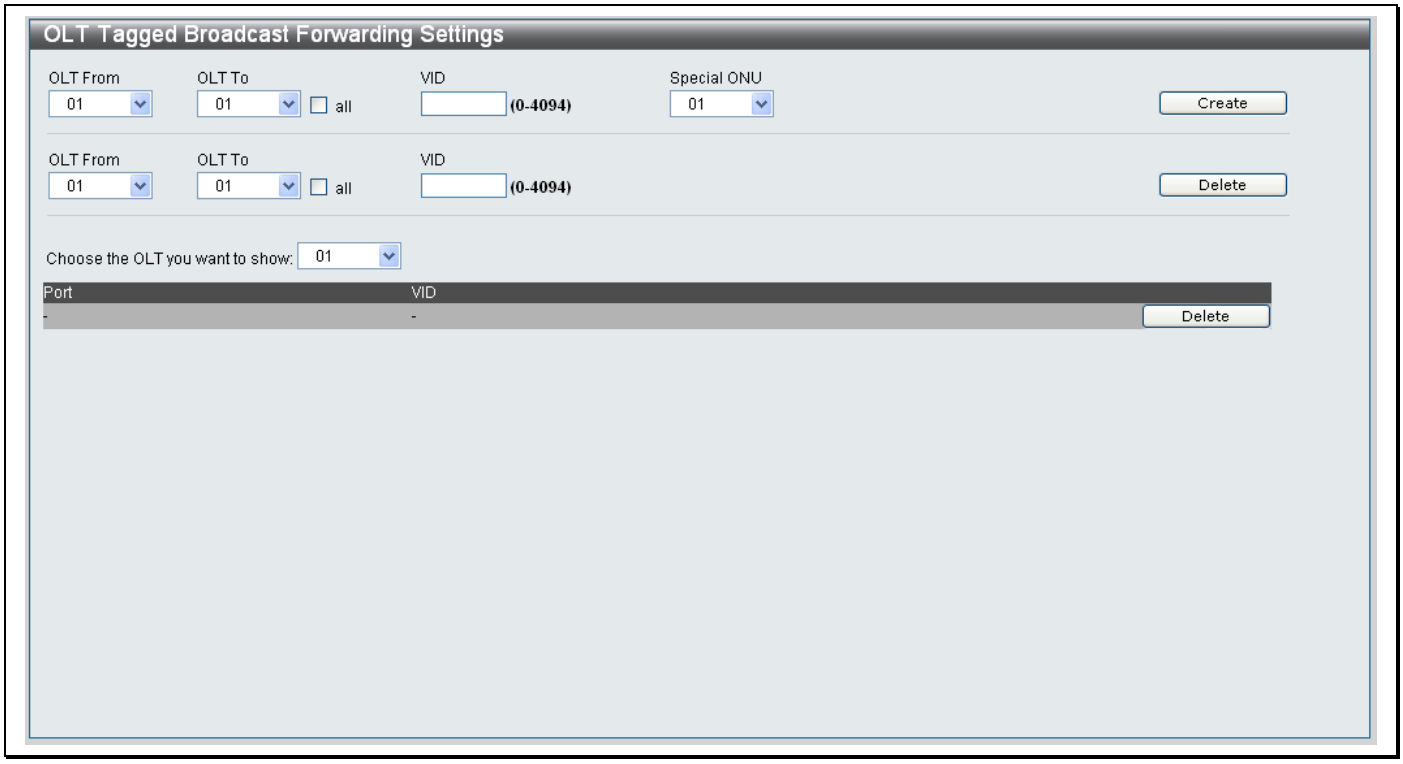


Figure 11- 20. OLT Tagged Broadcast Forwarding Settings window

The OLT Tagged Broadcast Forwarding Settings window is divided into three sections:

- The top part of the window is used to **Create** a new OLT Tagged Broadcast Setting.
- The center section is used to **Delete** a OLT Tagged Broadcast Setting.
- The bottom section is used to show OLT information and can be used to delete the OLT entry.

Creating a new OLT Tagged Broadcast Setting

1. Use the **OLT From** and **OLT To** drop-down menus in the top section of the window to specify the range of OLT ports that require a new OLT Tagged Broadcast Setting. Tick the **all** checkbox to specify that the setting should apply to all ports.
2. Type in a *VID number* between 0 and 4094 to specify the VID the broadcast frame will carry in the **VID** field.
3. Choose a *Special ONU* number from the drop-down menu to specify the ONU that the broadcast frame with the specified VID will be forwarded to.
4. Click the **Create** button.

Deleting an existing OLT Tagged Broadcast Setting

1. Use the **OLT From** and **OLT To** drop-down menus in the center section of the window to specify the range of OLT ports that require an OLT Tagged Broadcast Setting to be deleted. Tick the **all** checkbox to specify that the setting should apply to all ports.
2. Type in a *VID number* between 0 and 4094 to specify the VID the broadcast frame will carry in the **VID** field.
3. Click the **Delete** button to delete the entry.

Viewing an existing OLT Tagged Broadcast Setting

1. Select an OLT from the **Choose the OLT you want to show** drop-down menu at the bottom of the window to display the existing OLT Tagged Broadcast setting.
2. Click the corresponding **Delete** button at the bottom of the window to delete the entry.

ONU 802.1Q VLAN PVID Settings

The **ONU 802.1Q VLAN PVID Settings** window allows you to configure the PVID for a specific ONU.

To access the **ONU 802.1Q VLAN PVID Settings** window click **PON> ONU 802.1Q VLAN PVID Settings.**

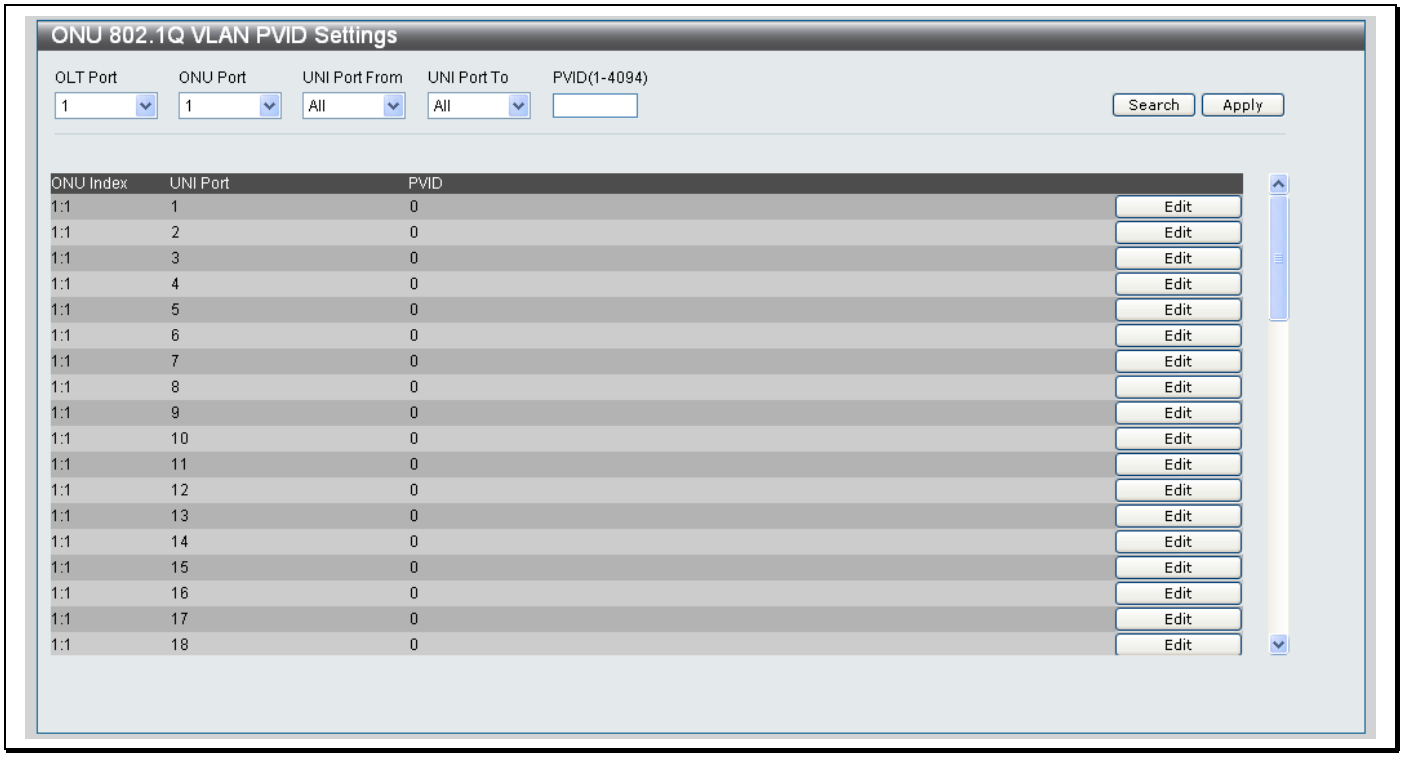


Figure 11- 21. ONU 802.1Q VLAN PVID Settings window

Creating a new ONU 802.1Q VLAN PVID Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want the ONU 802.1Q VLAN PVID Setting applied to.
2. Use the **ONU Port** drop-down menu to specify the ONU Port you want the ONU 802.1Q VLAN PVID Setting applied to.
3. Use the **UNI Port From** and **UNI Port To** drop-down menus to specify the UNI Port range you want the ONU 802.1Q VLAN PVID Setting applied to.
4. Type a PVID number between 1 and 4094 in the **PVID (1-4094)**.
5. Click the **Apply** button to add the new ONU 802.1Q VLAN PVID Setting.

Searching for an existing ONU 802.1Q VLAN PVID Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want to search for the ONU 802.1Q VLAN PVID Setting on.
2. Use the **ONU Port** drop-down menu to specify the ONU Port you want to search for the ONU 802.1Q VLAN PVID Setting on.
3. Use the **UNI Port From** and **UNI Port To** drop-down menus to specify the UNI Port range you want to search for the ONU 802.1Q VLAN PVID Setting on.
4. Use the **PVID (1-4094)** drop-down menu to specify the PVID in the ONU 802.1Q VLAN PVID that you want to search for.
5. Click the **Search** button to search for the ONU 802.1Q VLAN PVID Setting.

Editing an existing ONU 802.1Q VLAN PVID Setting

1. Click the **Edit** button next to the entry that you want to edit.
2. Type a new *PVID* value in the **PVID** field, next to the new entry.
3. Click the corresponding **Apply** button to save the changes made.

ONU 802.1Q VLAN Settings

The **ONU 802.1Q VLAN Settings** window allows you to configure the ONU 802.1Q VLAN Settings on the ONU. The DPN-3012-E RU supports two types of ONU, one type of ONU has a single UNI port (named DPN301), the other type of ONU has four UNI ports, (named DPN304); DPN304 supports 802.1Q VLAN function.

To access the **ONU 802.1Q VLAN Settings** window click **PON> ONU 802.1Q VLAN Settings.**

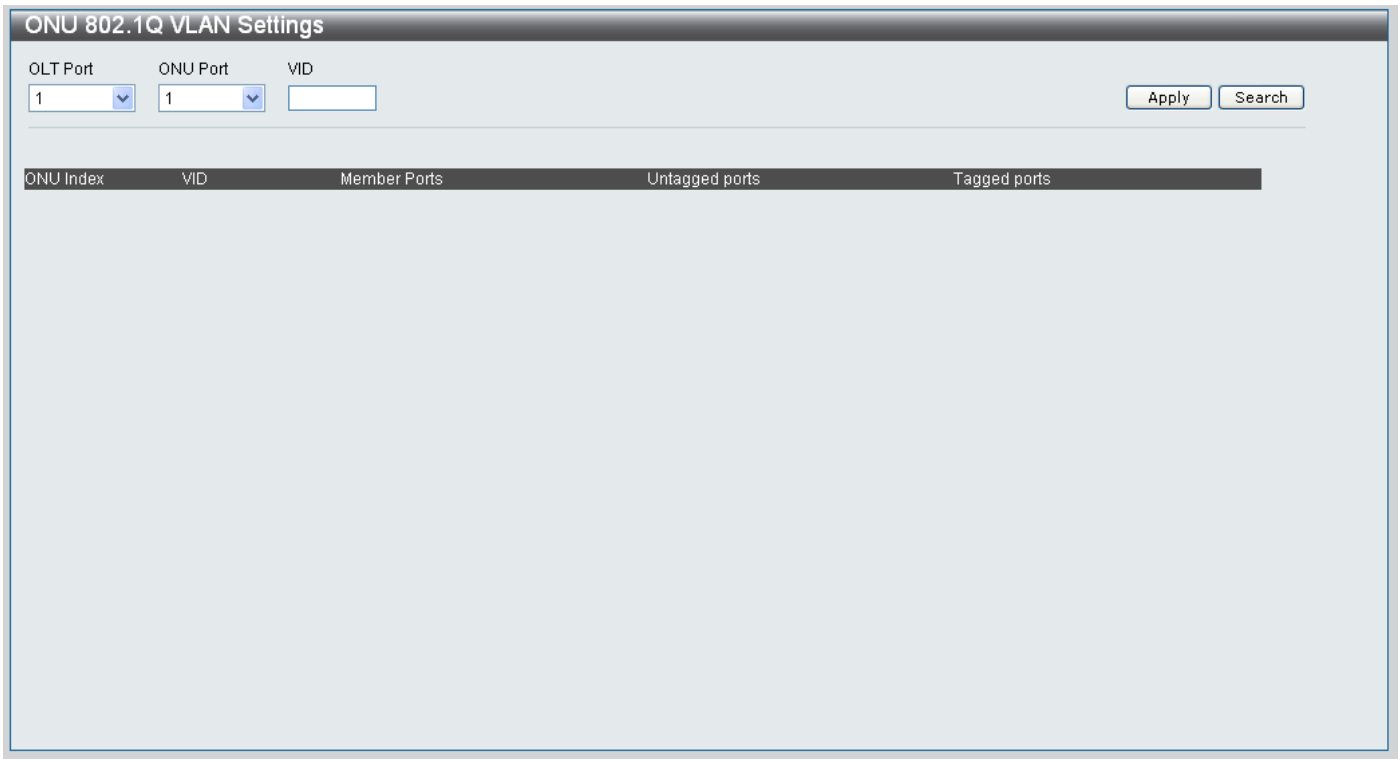


Figure 11- 22. ONU 802.1Q VLAN Settings window

Creating a new ONU 802.1Q VLAN Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want the ONU 802.1Q VLAN Setting applied to.
2. Use the **ONU Port** drop-down menu to specify the ONU Port you want the ONU 802.1Q VLAN Setting applied to.
3. Type a VID number in the **VID** textbox.
4. Click the **Apply** button to add the new ONU 802.1Q VLAN Setting.

Searching for an existing ONU 802.1Q VLAN Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want to search for the ONU 802.1Q VLAN Setting on.
2. Use the **ONU Port** drop-down menu to specify the ONU Port you want to search for the ONU 802.1Q VLAN Setting on.
3. Type the *VID number* of the ONU 802.1Q VLAN that you want to search for in the **VID** textbox.
4. Click the **Search** button to search for the ONU 802.1Q VLAN Setting.

Editing an existing ONU 802.1Q VLAN Setting

1. Click the **Edit** button next to the entry that you want to edit.
2. On the following screen click the radio buttons to define if a port should be *Tagged*, *Untagged* or if it should be a *Non Member* port. Tick the corresponding **All** button to define the role of all adjacent ports.

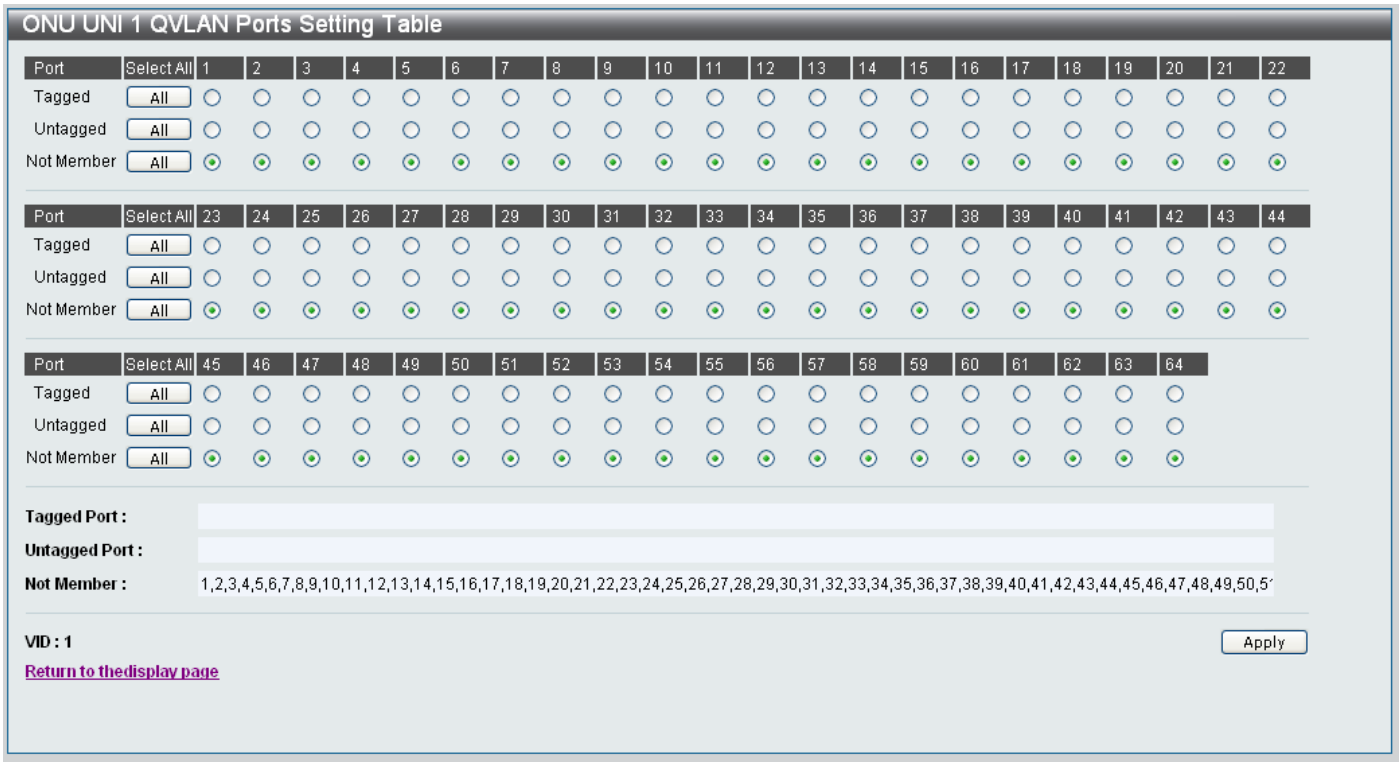


Figure 11- 23. ONU UNI 1 QVLAN Ports Setting Table window

3. The table at the bottom of the window summarizes the existing configuration of the ports.
4. Click the **Apply** button to save the changes.
5. A **Success** message indicates that the changes were successful.
6. Click the **Return to the display page** hyperlink to return to the main **802.1Q VLAN Settings** window.

Deleting an existing ONU 802.1Q VLAN Setting

1. Click the **Delete** button next to the entry that you want to edit.
2. A **Success** message indicates that the ONU 802.1Q VLAN Setting was deleted successfully.

ONU Port Base VLAN Settings

The **ONU Port Base VLAN Settings** window allows you to configure Port based VLAN's on the Switch.

To access the **ONU Port Base VLAN Settings** window click **PON> ONU Port Base VLAN Settings.**

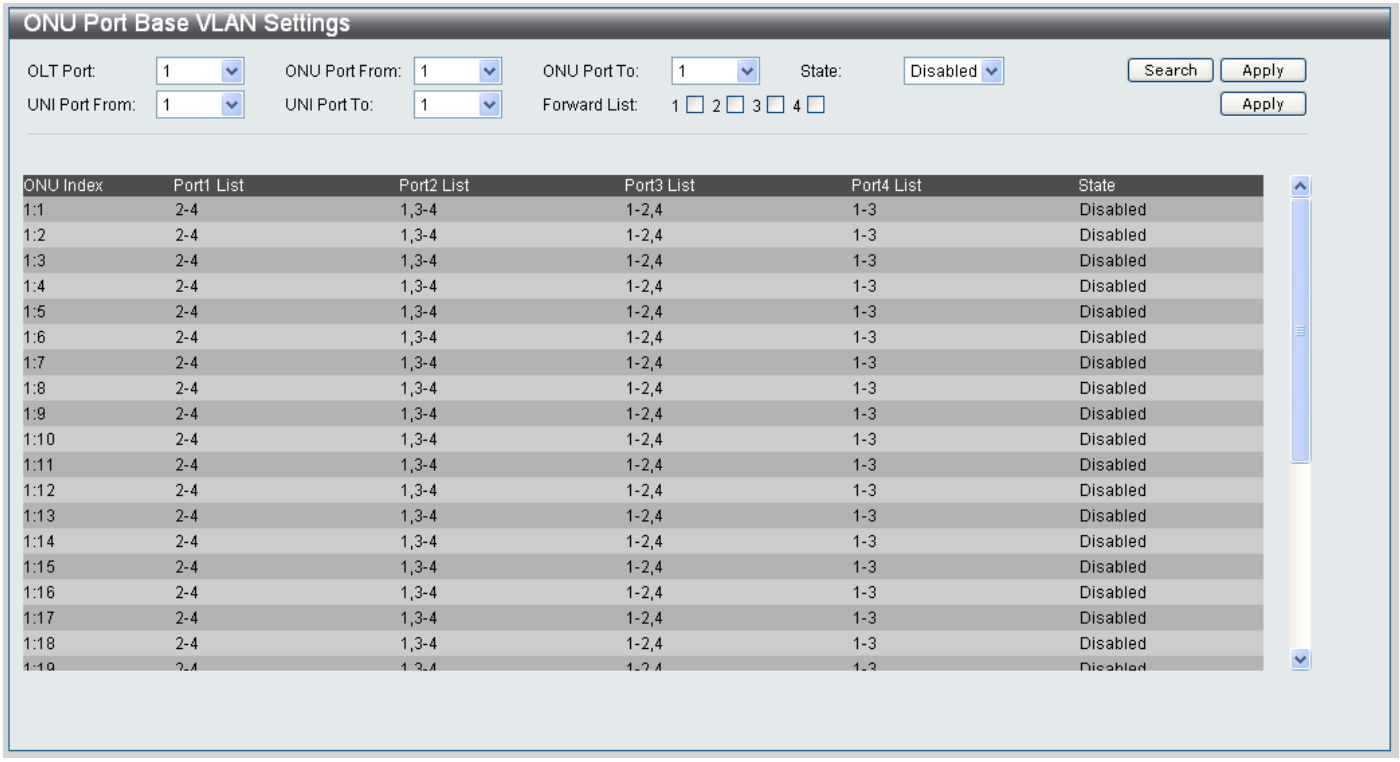


Figure 11- 24. ONU Port Base VLAN Settings window

The ONU Port Base VLAN Settings window configures the ONU ports and UNI Ports.

To configure the **ONU Ports** configure the parameters as described below:

Parameter	Description
OLT Port	Choose the *OLT Port* you want to configure the ONU Port Base VLAN Settings on from the drop-down menu.
ONU Port From/ ONU Port To	Choose the *ONU Ports* you want to configure from the drop-down menu.
State	Choose *Enabled* from the drop-down menu to enable the ONU Port Base VLAN Setting. Choose *Disabled* from the drop-down menu to disable.

Click the **Apply** button next to the **State** drop-down menu to save the changes.

Click the **Search** button to search for a previously added entry, using the parameters mentioned above.

To configure the **UNI Ports** configure the parameters as described below:

Parameter	Description
UNI Port From/ UNI Port To	Use the drop-down menus to choose the range of UNI Ports that need to be configured.
Forward List	Tick the checkboxes to specify the forwarding ONU UNI Port list of the port base VLAN.

Click the **Apply** button next to the **Forward List** boxes to save the changes.

P2P

P2P Traffic Control Settings

The **P2P Traffic Control Settings** window allows you to configure the P2P access policy for the traffic from a specific ONU to other ONU's, which are registered in the same OLT.

To access the **P2P Traffic Control Settings** window click **PON> P2P> P2P Traffic Control Settings.**

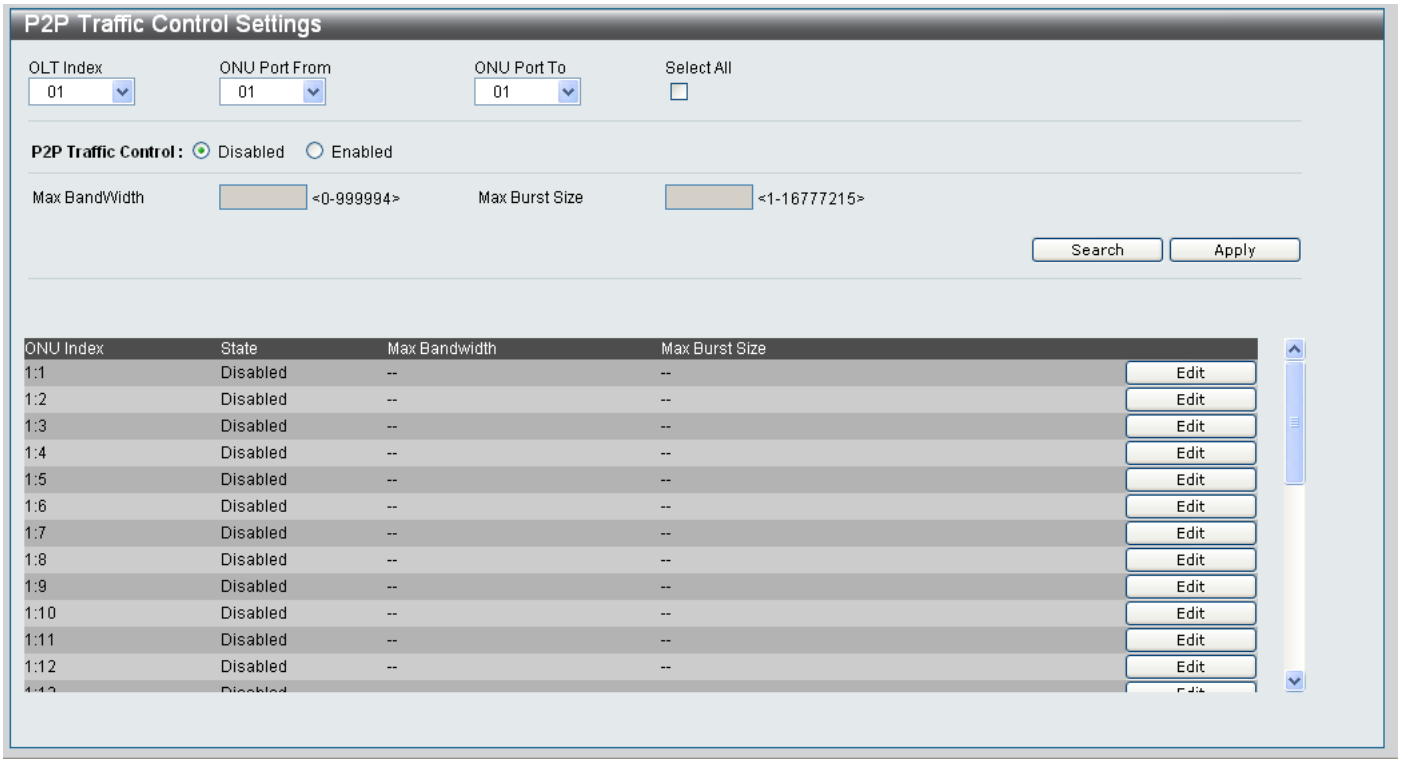


Figure 11- 25. P2P Traffic Control Settings window

Creating a new P2P Traffic Control Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want the P2P Traffic Control Setting applied to.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want the P2P Traffic Control Setting applied to. Tick the **Select All** checkbox to select all ONU Ports.
3. Click the **Enabled** radio button to enable P2P Traffic Control on the specified ports.
4. Type a Maximum Bandwidth value between 0 and 999994 in the **Max Bandwidth** field.
5. Type a Maximum Burst Size value between 1 and 16777215 in the **Max Burst Size** textbox.
6. Click the **Apply** button to add the new P2P Traffic Control Setting.

Searching for an existing P2P Traffic Control Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want to search for the P2P Traffic Control Setting on.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want to search for the P2P Traffic Control Setting on.
3. Click the **Enabled** radio button to search for a P2P Traffic Control setting that is set to Enabled.
4. Type the *Maximum Bandwidth* value of the P2P Traffic Control setting that you want to search for in the **Max Bandwidth** textbox.
5. Type the *Maximum Burst Size* value of the P2P Traffic Control setting that you want to search for in the **Max Burst Size** textbox.
6. Click the **Search** button to search for the ONU 802.1Q VLAN Setting.

Editing an existing P2P Traffic Control Setting

1. Click the **Edit** button next to the P2P Traffic Control Settings you want to edit.
2. The following fields can be edited **State**, **Max Bandwidth** and **Max Burst Size**.
3. Use the **State** drop-down menu to specify if the ONU Index should be *Enabled* or *Disabled*.
4. If you want to set a new *Maximum Bandwidth* value for the P2P Traffic Control, type this value into the **Max Bandwidth** textbox.
5. If you want to set a new *Maximum Burst Size* value for the P2P Traffic Control, type this value into the **Max Burst Size** textbox.
6. Click the **Apply** button to save the changes.

P2P Access Control Settings

The **P2P Access Control Settings** window allows you to configure the P2P access policy for traffic from a specific ONU to other ONU's which are registered in the same OLT.

To access the **P2P Access Control Settings** window click **PON> P2P> P2P Access Control Settings.**

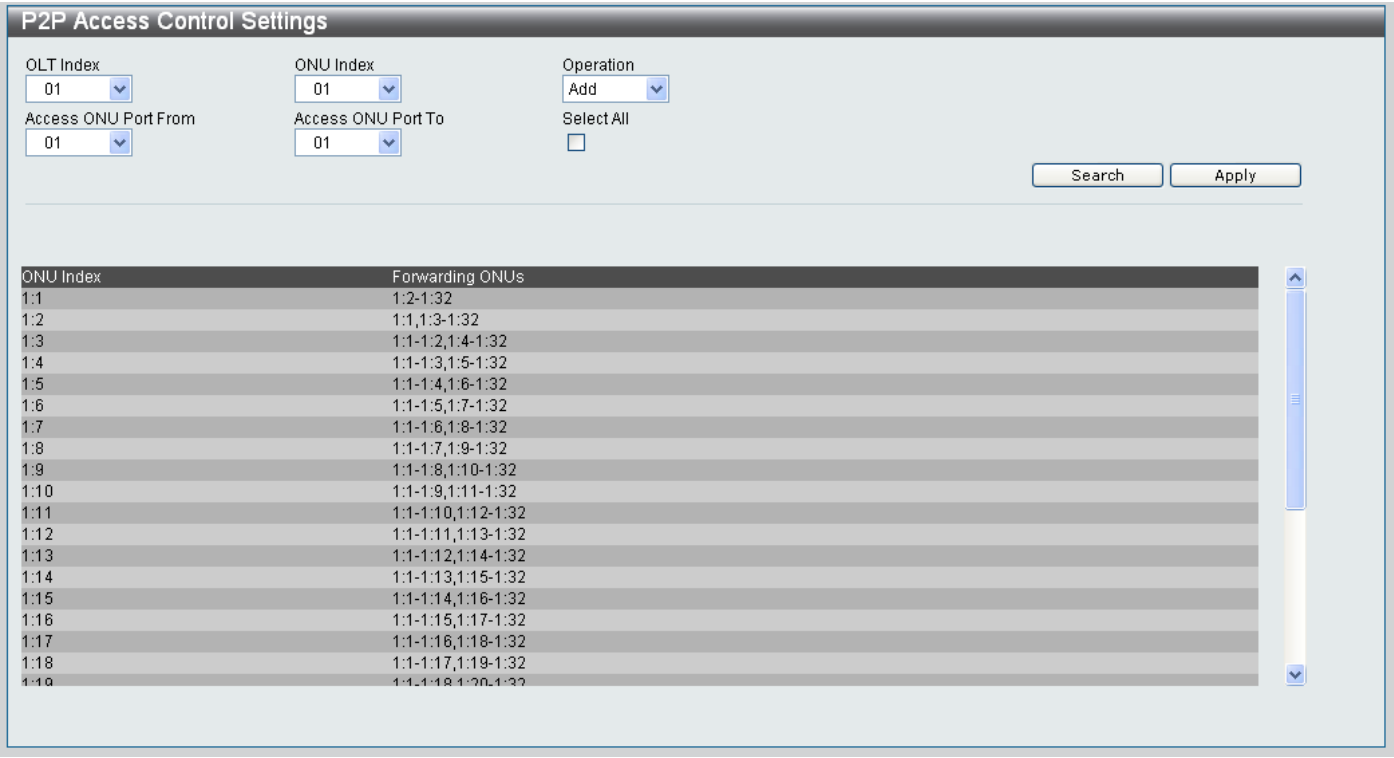


Figure 11- 26. P2P Access Control Settings window

Adding or Searching for a P2P Access Control Setting

To add a new P2P Access Control setting, configure the parameters as described below:

Parameter	Description
OLT Index	Choose the OLT index number of the OLT that is connected to the ONU you want to configure, from the drop-down menu.
ONU Index	Choose the ONU index number of the ONU you want to configure, from the drop-down menu.
Operation	Choose *Add* from the drop-down menu to add a new P2P Access Control Setting. Choose *Delete* to remove.
Access ONU Port From/ Access ONU Port To	Use the drop-down menus to specify the ONU port range you want to configure the P2P Access Control Settings on.

Searching for an existing P2P Access Control Setting

1. Populate the parameters in the P2P Access Control Settings window as described earlier.
2. Click the **Search** button to start the search.
3. The results of the search will appear at the bottom of the **P2P Access Control Settings** window.

OLT FDB Address Limitation

OLT FDB Address Limitation State

The **OLT FDB Address Limitation State** window is used to configure the FDB Address Limitation State of the OLT units installed in the Switch.

To access the **OLT FDB Address Limitation State** window click **PON> OLT FDB Address Limitation> OLT FDB Address Limitation State.**

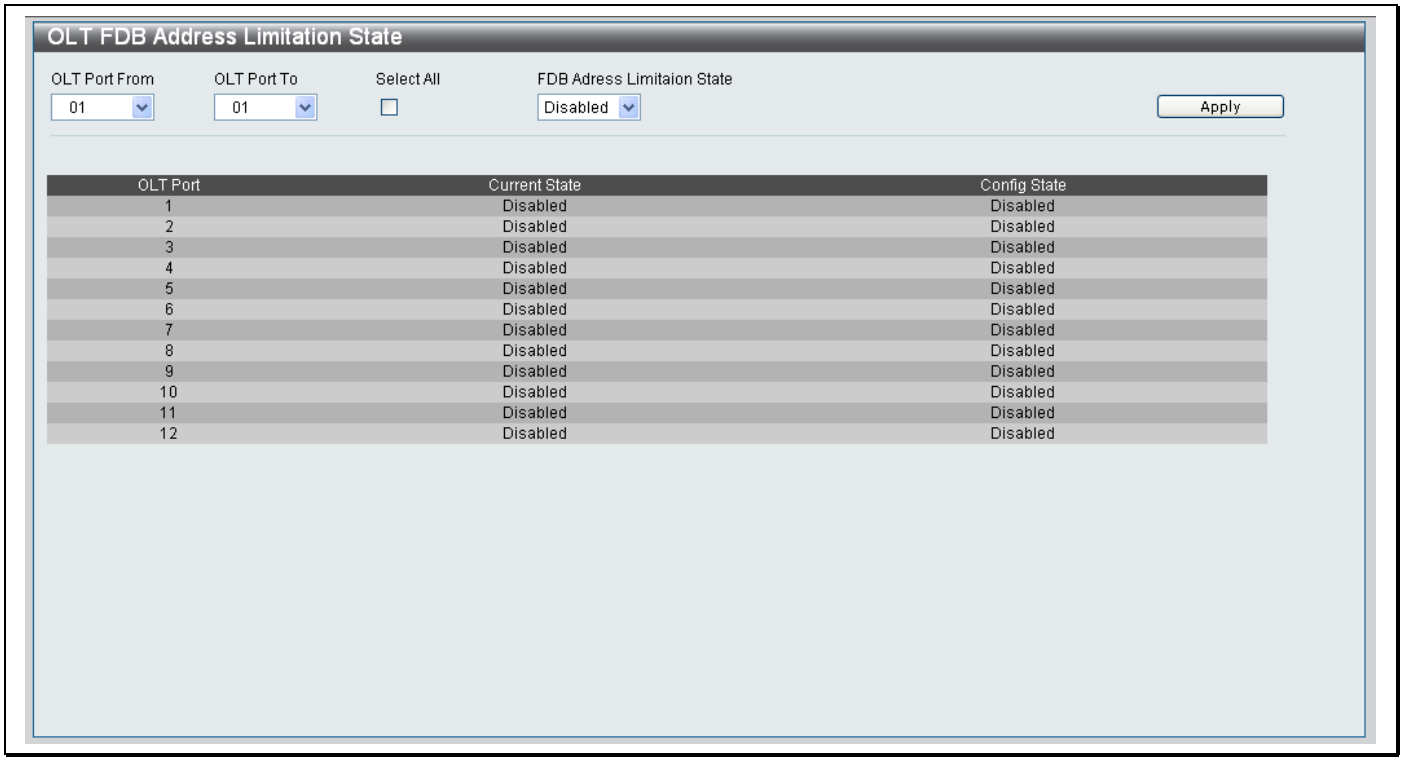


Figure 11- 27. OLT FDB Address Limitation State window

Configure the parameters as described below:

Parameter	Description
OLT Port From / OLT Port To	Use the drop-down menus to specify the OLT Ports you want to configure. Click the **Select All** checkbox to specify all OLT Ports.
FDB Address Limitation State	Click *Enabled* from the drop-down menu to enabled OLT FDB Address Limitation on the specified ports. Choose *Disabled* to disable.

Click **Apply** save the changes made.

ONU FDB Address Limitation Max Entries

The **ONU FDB Address Limitation Max Entries** window to configure the FDB Address Limitation Max entries for the ONU units installed in the Switch.

To access the **ONU FDB Address Limitation Max Entries** window click **PON> OLT FDB Address Limitation> ONU FDB Address Limitation Max Entries.**

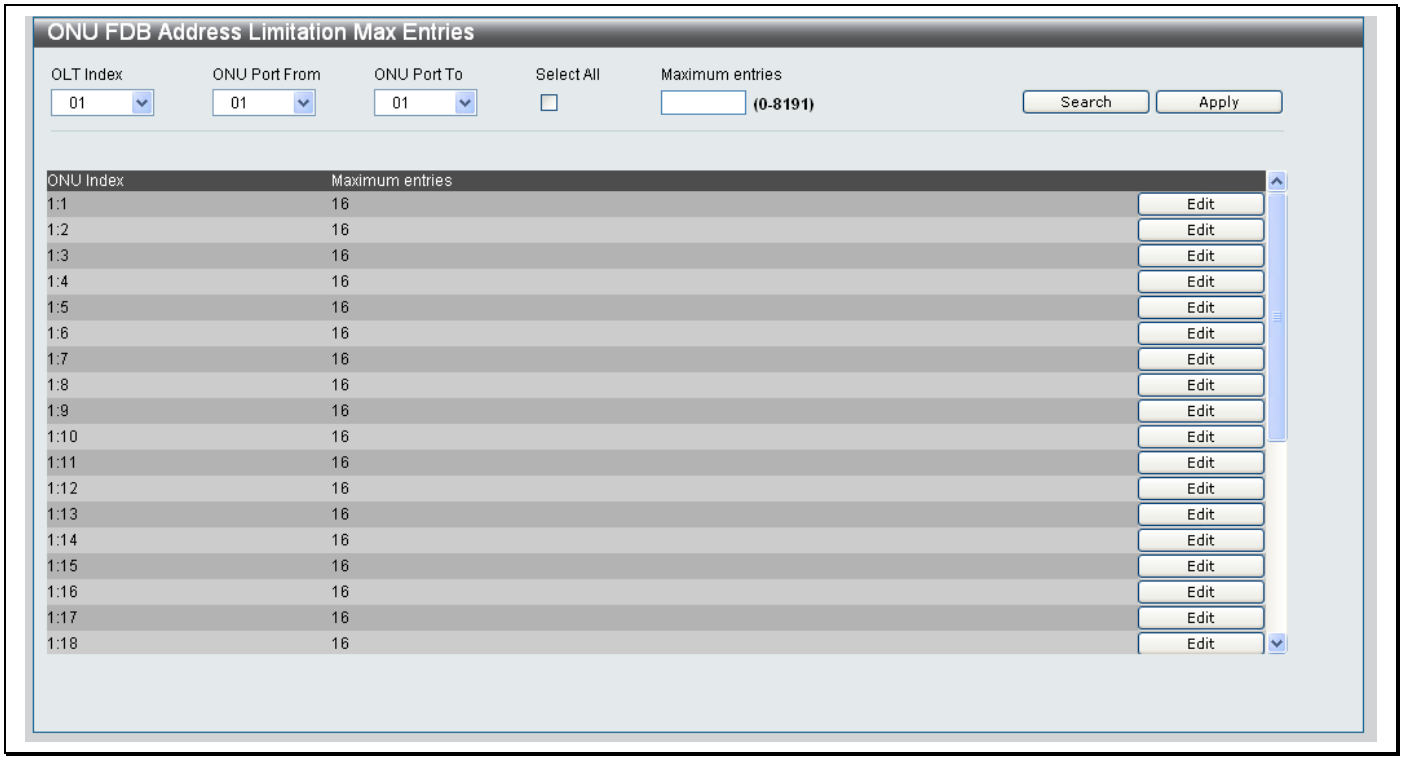


Figure 11- 28. OLT FDB Address Limitation Max Entries window

Creating a new ONU FDB Address Limitation Max Entry

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want the ONU FDB Address Limitation Max Entry applied to.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want the ONU FDB Address Limitation Max Entry applied to. Tick the **Select All** checkbox to select all ONU Ports.
3. Type a *Maximum entries* value between 0 and 8191 in the **Maximum Entries** textbox.
4. Click the **Apply** button to add the new Maximum Entry Setting.

Searching for an existing ONU FDB Address Limitation Max Entry

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want to search for the ONU FDB Address Limitation Max Entry on.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want to search for the ONU FDB Address Limitation Max Entry on.
3. Type the *Maximum entries* value between 0 and 8191 of the ONU FDB Address Limitation Max Entry setting that you want to search for in the **Maximum Entries** textbox.
4. Click the **Search** button to search for the ONU FDB Address Limitation Max Entry setting.

Editing an existing ONU FDB Address Limitation Setting

1. Click the **Edit** button next to the ONU FDB Address Limitation Max Entry setting you want to edit.
2. The **Maximum entries** field can be edited. Type a number between *0* and *16* to specify the new **Maximum entry** number.
3. Click the **Apply** button next to the ONU FDB Address Limitation Max Entry you just modified.
4. A **Success** message indicates the change was carried out successfully.

ONU UNI Port FDB Address Limitation Max Entries

The **ONU UNI Port FDB Address Limitation Max Entries** window is used to configure the UNI Port FDB Address Limitation Max entries for the ONU units installed in the Switch.

To access the **ONU UNI Port FDB Address Limitation Max Entries** window click **PON> OLT FDB Address Limitation> ONU UNI Port FDB Address Limitation Max Entries.**

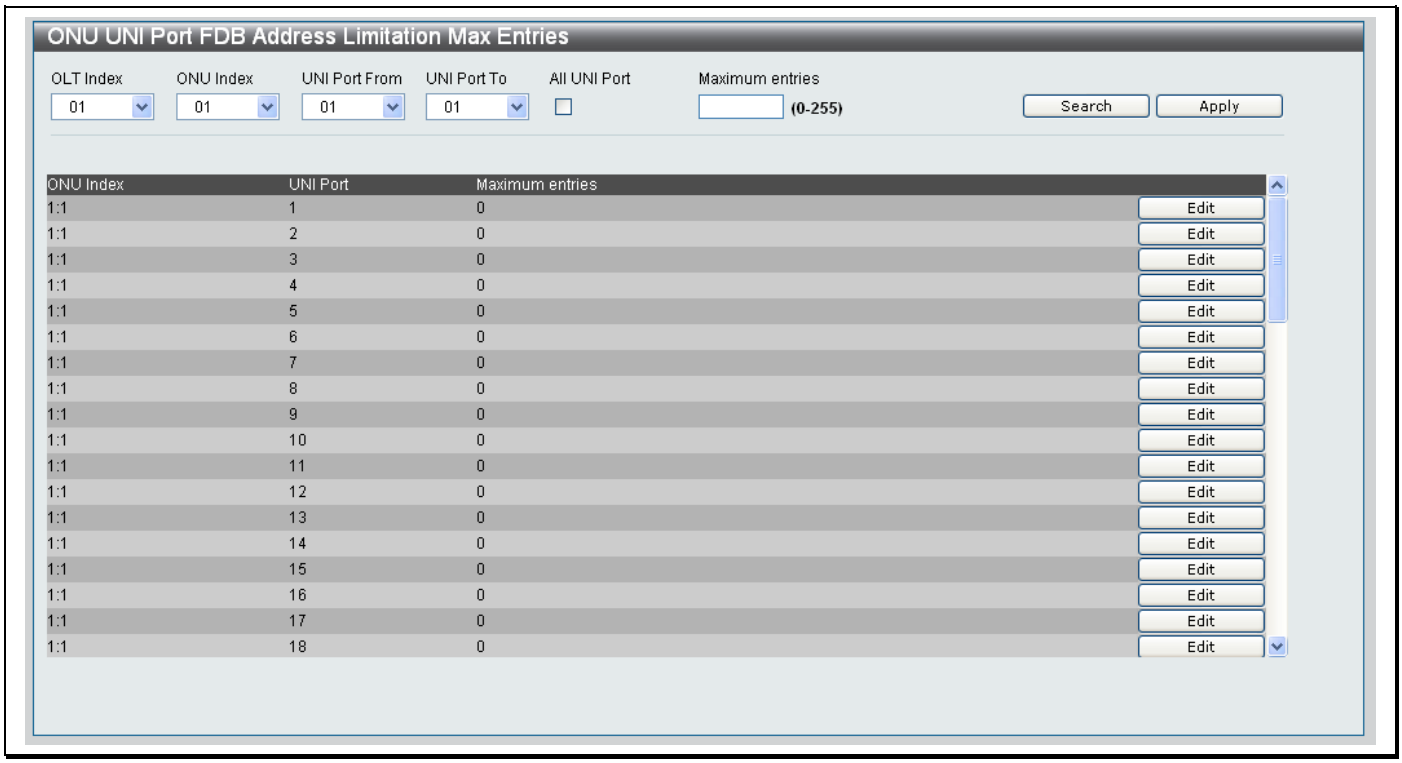


Figure 11- 29. OLT UNI Port FDB Address Limitation Max Entries window

Creating a new ONU UNI Port FDB Address Limitation Max Entry

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want the ONU UNI Port FDB Address Limitation Max Entry applied to.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want the ONU UNI Port FDB Address Limitation Max Entry applied to. Tick the **Select All** checkbox to select all ONU Ports.
3. Type a *Maximum entries* value between *0* and *255* in the **Maximum Entries** textbox.
4. Click the **Apply** button to add the new ONU UNI Port FDB Address Limitation Maximum Entry Setting.

Searching for an existing ONU UNI Port FDB Address Limitation Max Entry

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want to search for the ONU UNI Port FDB Address Limitation Max Entry on.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want to search for the ONU UNI Port FDB Address Limitation Max Entry on.
3. Type the *Maximum entries* value between 0 and 255 of the ONU UNI Port FDB Address Limitation Max Entry setting that you want to search for in the **Maximum Entries** textbox.
4. Click the **Search** button to search for the ONU UNI Port FDB Address Limitation Max Entry setting.

Editing an existing ONU UNI Port FDB Address Limitation Setting

1. Click the **Edit** button next to the ONU UNI Port FDB Address Limitation Max Entry setting you want to edit.
2. The **Maximum entries** field can be edited. Type a number between *0* and *255* to specify the new **Maximum entry** number.
3. Click the **Apply** button next to the ONU UNI Port FDB Address Limitation Max Entry you just modified.
4. A **Success** message indicates the change was carried out successfully.

ONU MAC Address Table

The **ONU MAC Address Table** window is used to display the information in the OLT's FDB. Each entry shown is associated with an ONU number.

To access the **ONU MAC Address Table** window click **PON> ONU MAC Address Table.**

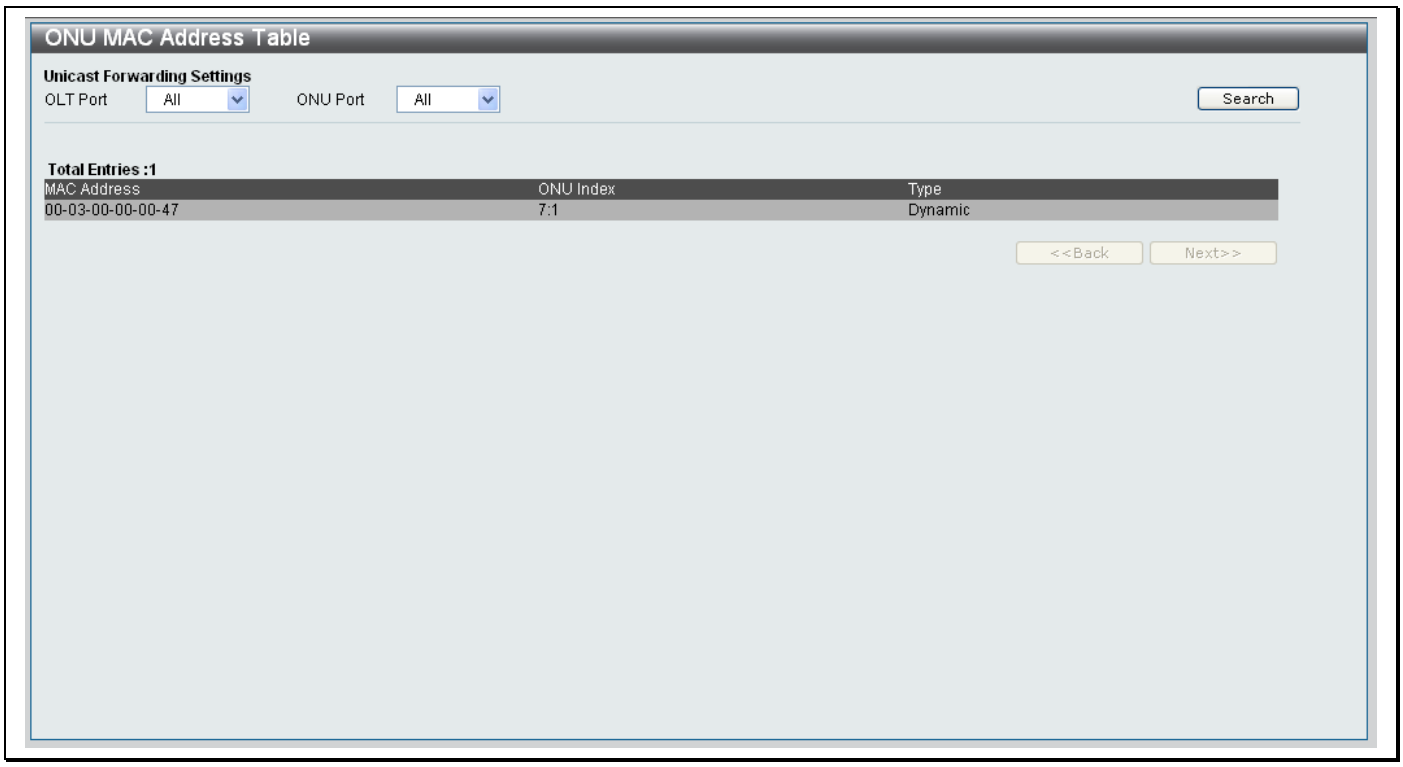


Figure 11- 30. ONU MAC Address Table window

To view the MAC Address entries for a specific port

1. Choose the OLT Port you want to view the MAC Address information for from the **OLT Port** drop-down menu.
2. Choose the ONU Port you want to view the MAC Address information for from the **ONU Port** drop-down menu.
3. Click the **Search** button to start the search.
4. If there is a MAC Address entry for the ONU port specified this will show in the table below the parameters.

Policing Queue Bandwidth Settings

The **Policing Queue Bandwidth Settings** window is used to police the bandwidth of upstream or downstream queues for the PON port of the ONU.

To access the **Policing Queue Bandwidth Settings** window click **PON> Policing Queue Bandwidth Settings.**

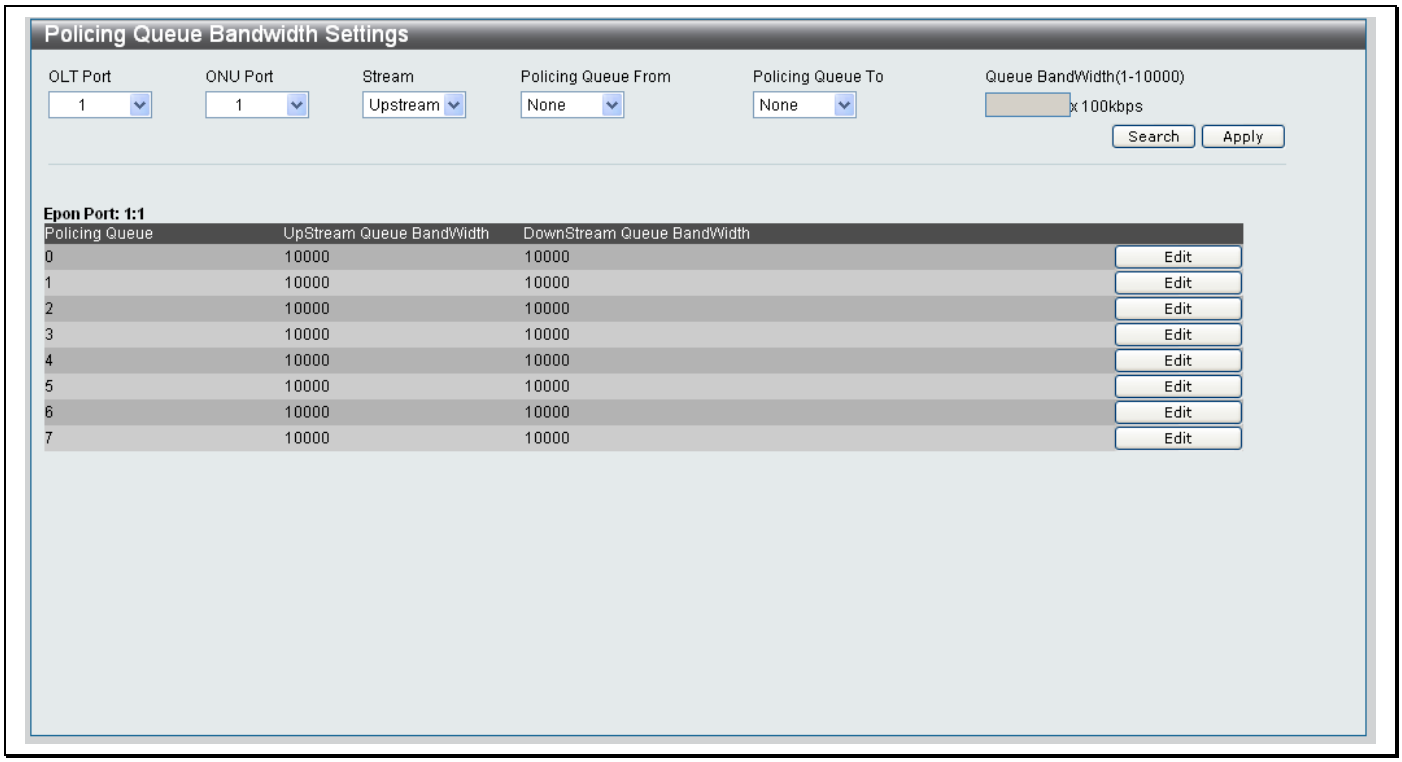


Figure 11- 31. Policing Queue Bandwidth Settings window

Creating a new Policing Queue Bandwidth Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want the Policing Queue Bandwidth Setting applied to.
2. Use the **ONU Port** drop-down menu to specify the ONU Port you want the Policing Queue Bandwidth Setting applied to.
3. Select whether you want the Policing Queue Bandwidth Setting to apply to *Upstream* or *Downstream* traffic from the **Stream** drop-down menu.
4. Select a Policing Queue number between *0* and *7* from the **Policing Queue From** drop-down menu.
5. Select a Policing Queue number between *0* and *7* from the **Policing Queue To** drop-down menu.
6. Type a value between *1-10000* for the Queue bandwidth in the **QueueBandWidth** field
7. Click the **Apply** button to add the new Policing Queue Bandwidth Setting.

Searching for an existing Policing Queue Bandwidth Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want to search for the Policing Queue Bandwidth Setting on.
2. Use the **ONU Port From** drop-down menu to specify the ONU Port you want to search for the Policing Queue Bandwidth Setting on.
3. Select whether the Policing Queue Bandwidth Setting you are searching for applies to *Upstream* or *Downstream* traffic from the **Stream** drop-down menu.
4. Select the Policing Queue number the Policing Queue Bandwidth Setting you are searching for is using from the **Policing Queue From** drop-down menu.

5. Select the Policing Queue number the Policing Queue Bandwidth Setting you are searching for is using from the **Policing Queue To** drop-down menu.
6. Click the **Search** button to search for the Policing Queue Bandwidth Setting.

Editing an existing Policing Queue Bandwidth Setting

1. Click the **Edit** button next to the Policing Queue Bandwidth setting you want to edit.
2. The **UpStream Queue Bandwidth** and **DownStream Queue Bandwidth** settings can be edited.
3. Type the desired values in the **UpStream Queue Bandwidth** and **DownStream Queue Bandwidth** fields.
4. Click the **Apply** button next to the Policing Queue Bandwidth Setting y you just modified.
5. A **Success** message indicates the change was carried out successfully.

Policing Queue Size Settings

The **Policing Queue Size Settings** window is used to configure the queue size for upstream, or downstream queues for the PON port of the ONU.

To access the **Policing Queue Size Settings** window click **PON> Policing Queue Size Settings.**

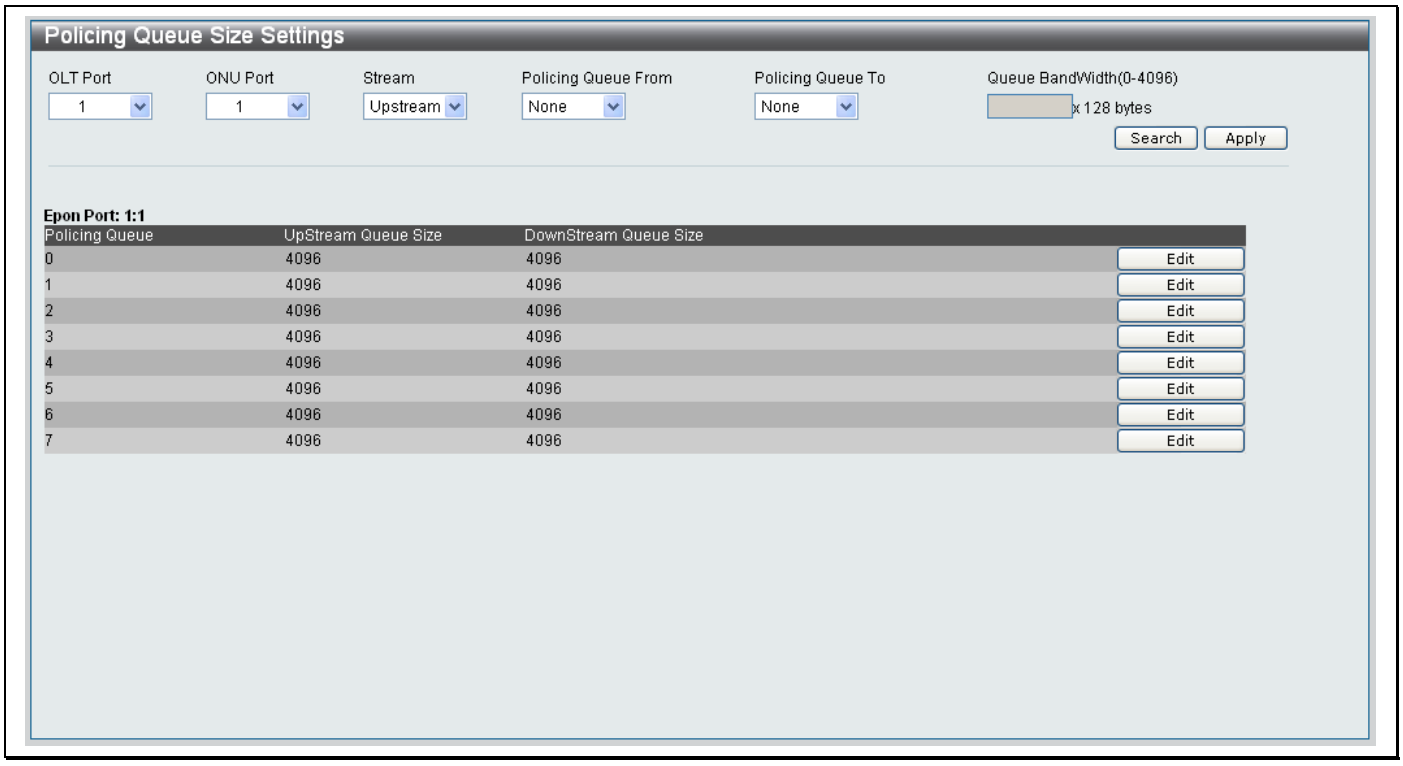


Figure 11- 32. Policing Queue Size Settings window

Creating a new Policing Queue Size Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want the Policing Queue Size Setting applied to.
2. Use the **ONU Port** drop-down menu to specify the ONU Port you want the Policing Queue Size Setting applied to.
3. Select whether you want the Policing Queue Size Setting to apply to *Upstream* or *Downstream* traffic from the **Stream** drop-down menu.
4. Select a Policing Queue number between *0* and *7* from the **Policing Queue From** drop-down menu.
5. Select a Policing Queue number between *0* and *7* from the **Policing Queue To** drop-down menu.
6. Type a value between *1-10000* for the Queue bandwidth in the **QueueBandWidth** field
7. Click the **Apply** button to add the new Policing Queue Size Setting.

Searching for an existing Policing Queue Size Setting

1. Use the **OLT Index** drop-down menu to specify the OLT Index you want to search for the Policing Queue Size Setting on.
2. Use the **ONU Port From** drop-down menu to specify the ONU Port you want to search for the Policing Queue Size Setting on.
3. Select whether the Policing Queue Size Setting you are searching for applies to *Upstream* or *Downstream* traffic from the **Stream** drop-down menu.
4. Select the Policing Queue number the Policing Queue Size Setting you are searching for is using from the **Policing Queue From** drop-down menu.
5. Select the Policing Queue number the Policing Queue Size Setting you are searching for is using from the **Policing Queue To** drop-down menu.
6. Click the **Search** button to search for the Policing Queue Size Setting.

Editing an existing Policing Queue Size Setting

1. Click the **Edit** button next to the Policing Queue Size setting you want to edit.
2. The **UpStream Queue Size** and **DownStream Queue Size** settings can be edited.
3. Type the desired values in the **UpStream Queue Size** and **DownStream Queue Size** fields.
4. Click the **Apply** button next to the Policing Queue Size Setting you just modified.
5. A **Success** message indicates the change was carried out successfully.

ONU Default Filter Settings

The **ONU Default Filter Settings** window is used to show and edit the default filter for upstream and downstream traffic passing through the PON port of the ONU. There are two types of filters, default filter and classifier filter. For packets that match the classifier filter, the rule in the matched classifier filter is applied.

There is one exception. If the default rule specifies to discard both tagged and untagged packets, then only the classifier rules that match against the VID field will take effect.

To access the **ONU Default Filter Settings** window click **PON> ONU Default Filter Settings.**

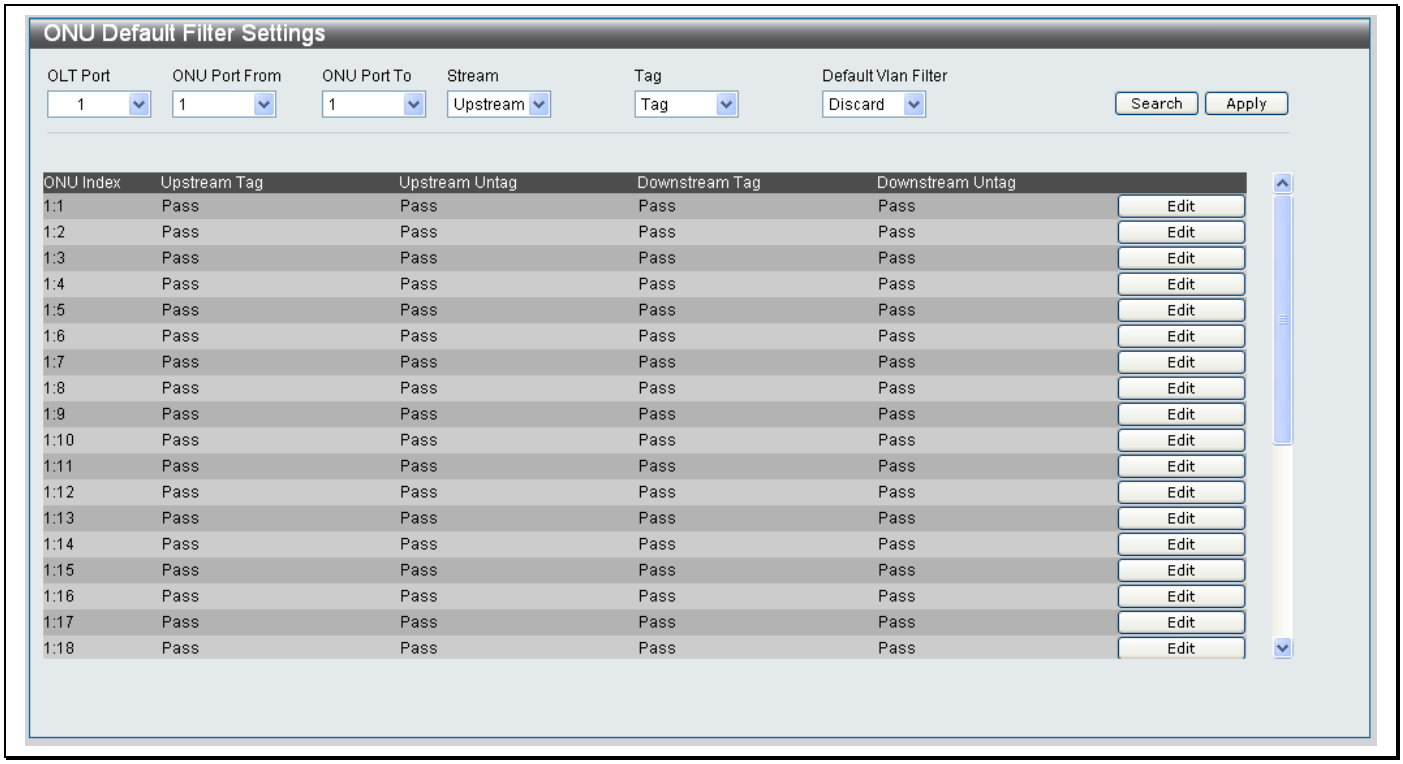


Figure 11- 33. ONU Default Filter Settings window

Creating a new ONU Default Filter Size Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want the ONU Default Filter Setting applied to.
2. Use the **ONU Port From** and **ONU Port To** drop-down menus to specify the ONU Ports you want the ONU Default Filter Setting applied to
3. Select whether you want the ONU Default Filter Size Setting to apply to *Upstream* or *Downstream* traffic from the **Stream** drop-down menu.
4. Select whether to filter *Tag* or *Untag* ports from the **Tag** drop-down menu.
5. Select whether to *Discard* or *Pass* the Default Vlan Filter from the **Default Vlan Filter** drop-down menu.
6. Click the **Apply** button to add the new ONU Default Filter Setting.

Searching for an existing ONU Default Filter Size Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want to search for the ONU Default Filter Size Setting on.
2. Use the **ONU Port From** drop-down menu to specify the ONU Port you want to search for the ONU Default Filter Size Setting on.
3. Select whether the ONU Default Filter Size Setting you are searching for applies to *Upstream* or *Downstream* traffic from the **Stream** drop-down menu.
4. Select whether the ONU Default Filter Setting filters *Tag* or *Untag* ports from the **Tag** drop-down menu.
5. Select whether the ONU Default Filter Setting you are searching for has its Default VLAN Filter setting set to *Discard* or *Pass* from the **Default Vlan Filter** drop-down menu.
6. Click the **Search** button to search for the ONU Default Filter Setting.

Editing an existing ONU Default Filter Size Setting

1. Click the **Edit** button next to the ONU Default Size setting you want to edit.
2. The **UpStream Tag**, **Upstream Untag**, **DownStream Tag** and **Downstream Untag** settings can be edited.
3. Type the desired values in the **UpStream Tag**, **Upstream Untag**, **DownStream Tag** and **Downstream Untag** fields.
4. Click the **Apply** button next to the ONU Default Filter Size Setting you just modified.
5. A **Success** message indicates the change was carried out successfully.

ONU Classifier Filter Settings

The **ONU Classifier Filter Settings** windows are used to configure the classifier filter for upstream and downstream traffic passing through the PON port of the ONU. For each direction of each ONU , up to 56 rules can be specified . For each field type (also named filter type), up to 8 rules can be configured.

a. At the same time the packet matches VID, Ethertype and IPv4, in one or more of the rules.

b. At the same time the packet matches SIP and DIP, in one or more of the rules..

c. At the same time the packet matches STCP or SUDP rules.

If the data packets meet condition “a” and the set up of the forwarding of data packets are discarded, then that data packet will be discarded.

If the data packets meet condition “b”, the first set of rules will be applied.

If the data packets meet the "a" and "b" conditions at the same time the following occurs; If set of rules “a” is set to discard packets the packets will be discarded. If only set of rules "b" is set to discard packets the packets will be discarded according to the first set of rules transmitted data packets.

If the data packets meet both the "a" and "c" conditions, if the operation is set to discard packets, discard the packets.

If the data packets meet both the "b" and "c" conditions, "b" will have a higher priority then "c".

By default, there are two upstream rules. A rule through the match Ethertype type, capture the ARP packet to the CPU, another through the match DIP and one for the local IP packet capture to the CPU.

Note that if the packet matches an upstream filter rule, the upstream filter rule will be applied. If the packet does not match any upstream filter rule, then default upstream filter rule will be applied except with the following exception. If the default upstream filter is specified to discard tag and untag packet, then only those classifier rule that match against VID field rule will take effect.

The same situation also applies to the downstream default filter and downstream classifier filter.

Common Ethernet Type Numbers	
Ethernet Type	**Number**
IP ETH	0800
X.75 internet	0801
NBS internet	0802
ECMA internet	0803
chaosnet	0804
X.25 Level 3	0805
XNS Comat	0807
BanYan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
Apple Talk AARP	80F3

Figure 11- 34. Common Ethernet Type Numbers

Common Protocol Types	
Protocol Name	**Number**
ICMP	1
IGMP	2
TCP	6
UDP	17
IPV6	41

Figure 11- 35. Common Protocol Types

ONU Classifier Filter Upstream Settings

To access the **ONU Classifier Filter Upstream Settings** window click **PON> ONU Classifier Filter Settings> ONU Classifier Filter Upstream Settings.**

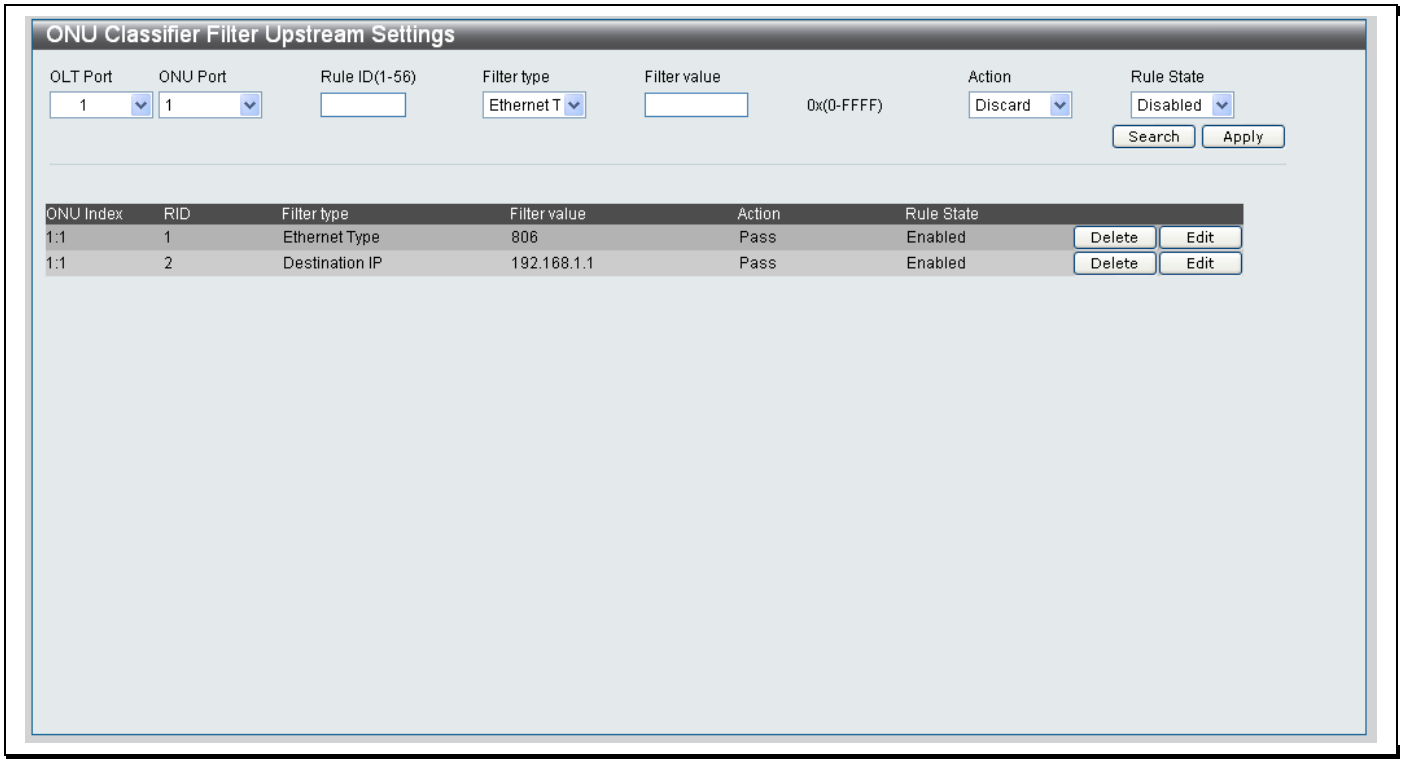


Figure 11- 36. ONU Classifier Filter Upstream Settings window

Creating a new ONU Classifier Filter Upstream Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want the ONU Classifier Filter Upstream Setting applied to.
2. Use the **ONU Port** drop-down menu to specify the ONU Ports you want the ONU Classifier Filter Upstream Setting applied to.
3. Type an identity number for the rule in the **Rule ID(1-56)** field.
4. Choose whether to create an *Ethernet Type, VID, IPV4 Protocol, Source TCP, Source UDP, Source IP* or *Destination IP* filter from the **Filter type** drop-down menu.
5. The **Filter Value** field accepts different value types depending on the type of filter:
    - If choosing an *Ethernet Type* filter, type in a *Filter Value* in the following hexadecimal format *0x(0-FFFF)*
    - If choosing a *VID* filter, type in a *Filter Value* of between *0* and *4094,* which matches the VID of the VLAN you want to apply the Filter to.
    - If choosing an *IPV4 Protocol* filter, type in a *Filter Value* between *1* and *255*.
    - If choosing a *Source TCP* filter, type in a *Filter Value* between *1* and *65535* that represents the Source TCP Port number the Source TCP Filter will use.
    - If choosing a *Source UDP* filter, type in a *Filter Value* between *1* and *65535* that represents the Source UDP Port number the Source UDP Filter will use.
    - If choosing a *Source IP* filter, type in the IP address of the Source IP address that will be filtered.
    - If choosing a *Destination IP* filter, type in the IP address of the Destination IP address that will be filtered.
6. Choose whether the Filter should *Pass* or *Discard* an item that matches the filter.
7. Choose whether the rule should be *Enabled* or *Disabled* from the **Rule State** drop-down menu.
8. Click the **Apply** button to add the new ONU Classifier Upstream Filter Setting.

Searching for an existing ONU Classifier Filter Upstream Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want to search for the ONU Classifier Filter Upstream Setting on.
2. Use the **ONU Port From** drop-down menu to specify the ONU Port you want to search for the ONU Classifier Filter Upstream Setting on.
3. Type the identity number of the rule you are searching for in the **Rule ID(1-56)** field.
4. Choose whether the ONU Classifier Filter Upstream you are searching for has an *Ethernet Type, VID, IPV4 Protocol, Source TCP, Source UDP, Source IP* or *Destination IP* filter from the **Filter type** drop-down menu.
5. Type in the *Filter value* that is used by the ONU Classifier Filter Upstream Setting you are searching for in the **Filter Type** field.
6. Select whether the ONU Classifier Filter Upstream Setting you are searching for has its **Action** setting set to *Discard* or *Pass* from the **Action** drop-down menu.
7. Click the **Search** button to search for the ONU Classifier Upstream Settings.

Editing an existing ONU Classifier Upstream Setting

1. Click the **Edit** button next to the ONU Classifier Upstream setting you want to edit.
2. The **Filter type**, **Filter value**, **Action** and **Rule State** settings can be edited.
3. Edit the desired values in the **Filter type**, **Filter value**, **Action** and **Rule State** fields.
4. Click the **Apply** button next to the ONU Default Filter Size Setting you just modified.
5. A **Success** message indicates the change was carried out successfully.

Deleting an existing ONU Classifier Upstream Setting

1. Click the **Delete** button next to the ONU Classifier Upstream setting you want to delete.
2. A **Success** message indicates the ONU Classifier Upstream setting was deleted successfully.

ONU Classifier Filter Downstream Settings

To access the **ONU Classifier Filter Downstream Settings** window click **PON> ONU Classifier Filter Settings> ONU Classifier Filter Downstream Settings.**

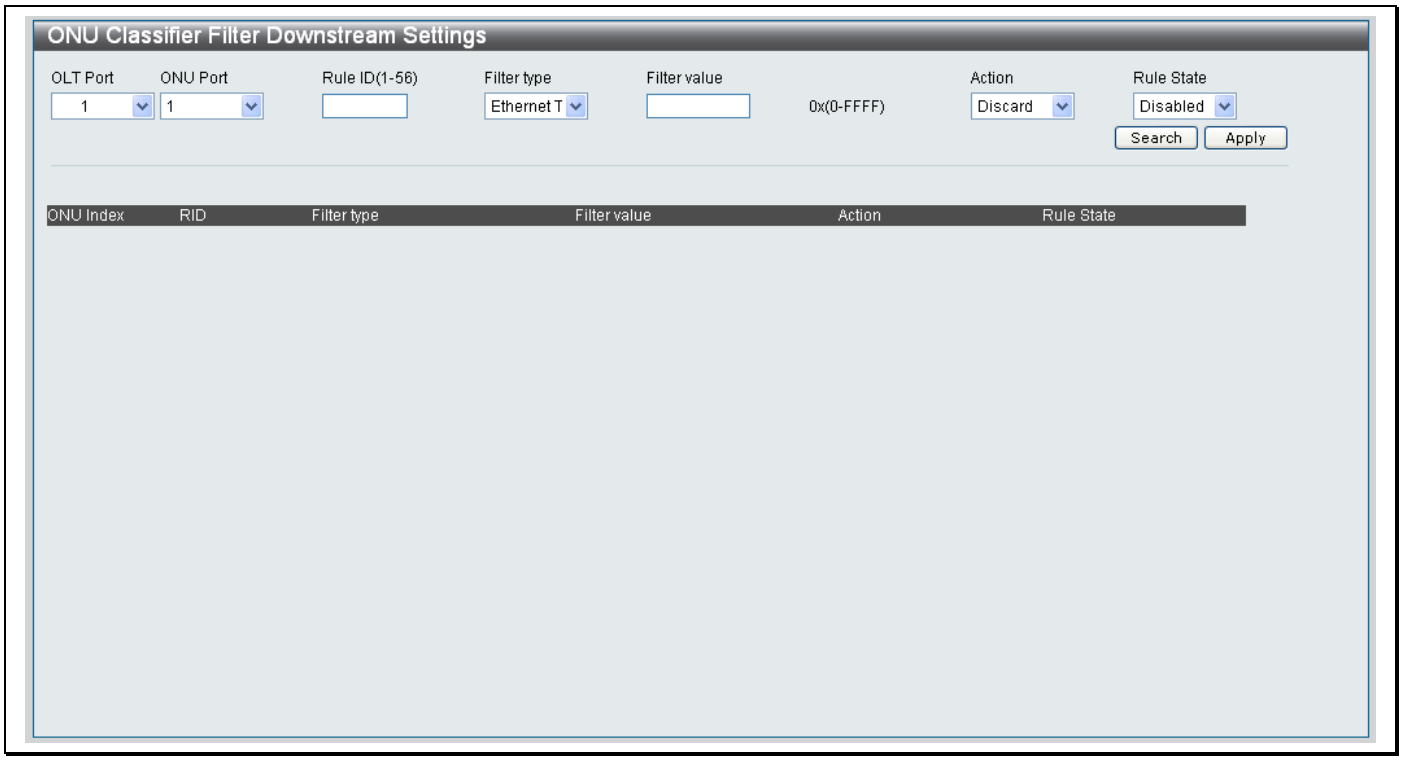


Figure 11- 37. ONU Classifier Filter Downstream Settings window

Creating a new ONU Classifier Filter Downstream Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want the ONU Classifier Filter Downstream Setting applied to.
2. Use the **ONU Port** drop-down menu to specify the ONU Ports you want the ONU Classifier Filter Downstream Setting applied to.
3. Type an identity number for the rule in the **Rule ID(1-56)** field.
4. Choose whether to create an *Ethernet Type, VID, IPV4 Protocol, Source TCP, Source UDP, Source IP* or *Destination IP* filter from the **Filter type** drop-down menu.
5. The **Filter Value** field accepts different value types depending on the type of filter:
    - If choosing an *Ethernet Type* filter, type in a *Filter Value* in the following hexadecimal format *0x(0-FFFF)*
    - If choosing a *VID* filter, type in a *Filter Value* of between *0* and *4094,* which matches the VID of the VLAN you want to apply the Filter to.
    - If choosing an *IPV4 Protocol* filter, type in a *Filter Value* between *1* and *255*.
    - If choosing a *Source TCP* filter, type in a *Filter Value* between *1* and *65535* that represents the Source TCP Port number the Source TCP Filter will use.
    - If choosing a *Source UDP* filter, type in a *Filter Value* between *1* and *65535* that represents the Source UDP Port number the Source UDP Filter will use.
    - If choosing a *Source IP* filter, type in the IP address of the Source IP address that will be filtered.
    - If choosing a *Destination IP* filter, type in the IP address of the Destination IP address that will be filtered.
6. Choose whether the Filter should *Pass* or *Discard* an item that matches the filter.
7. Choose whether the rule should be *Enabled* or *Disabled* from the **Rule State** drop-down menu.
8. Click the **Apply** button to add the new ONU Classifier Downstream Filter Setting.

Searching for an existing ONU Classifier Filter Downstream Setting

1. Use the **OLT Port** drop-down menu to specify the OLT Port you want to search for the ONU Classifier Filter Downstream Setting on.
2. Use the **ONU Port From** drop-down menu to specify the ONU Port you want to search for the ONU Classifier Filter Downstream Setting on.
3. Type the identity number of the rule you are searching for in the **Rule ID(1-56)** field.
4. Choose whether the ONU Classifier Filter Downstream you are searching for has an *Ethernet Type, VID, IPV4 Protocol, Source TCP, Source UDP, Source IP* or *Destination IP* filter from the **Filter type** drop-down menu.
5. Type in the *Filter value* that is used by the ONU Classifier Filter Downstream Setting you are searching for in the **Filter Type** field.
6. Select whether the ONU Classifier Filter Downstream Setting you are searching for has its **Action** setting set to *Discard* or *Pass* from the **Action** drop-down menu.
7. Click the **Search** button to search for the ONU Classifier Downstream Settings.

Editing an existing ONU Classifier Downstream Setting

6. Click the **Edit** button next to the ONU Classifier Downstream setting you want to edit.
7. The **Filter type**, **Filter value**, **Action** and **Rule State** settings can be edited.
8. Edit the desired values in the **Filter type**, **Filter value**, **Action** and **Rule State** fields.
9. Click the **Apply** button next to the ONU Default Filter Size Setting you just modified.
10. A **Success** message indicates the change was carried out successfully.

Deleting an existing ONU Classifier Downstream Setting

3. Click the **Delete** button next to the ONU Classifier Downstream setting you want to delete.
4. A **Success** message indicates the ONU Classifier Downstream setting was deleted successfully

ONU Default VLAN Rule Settings

ONU Default VLAN Rule Upstream Settings

To access the **ONU Default VLAN Rule Upstream Settings** window click **PON> ONU Default VLAN Rule Settings > ONU Default VLAN Rule Upstream Settings.**

The ONU Default VLAN Rule Upstream Settings window is divided into two main sections. The top half is used to create new ONU Default VLAN Rule Upstream Settings. The bottom half is used to **Search** and **Edit** existing ONU Default VLAN Rule Upstream Settings.

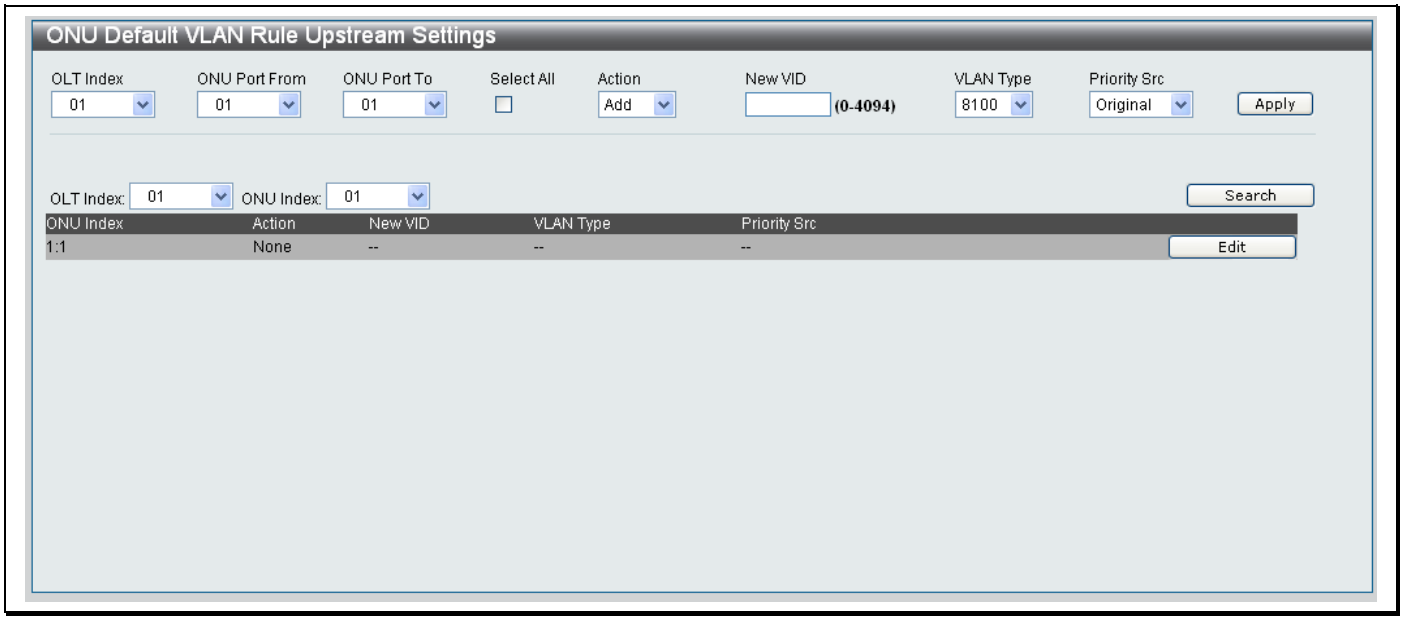


Figure 11- 38. ONU Default VLAN Rule Upstream Settings window

Adding a new ONU Default VLAN Rule Upstream Setting

Configure the parameters in the top half of the window, as described below, to add a new ONU Default VLAN Rule Upstream Setting:

Parameter	Description
OLT Index	Choose the OLT Index from the drop-down menu.
ONU Port From / ONU Port To	Use the drop-down menus to specify the range of ONU ports to be configured. Click the **Select All** checkbox to select all ONU ports.
Action	Choose *Add* from the drop-down menu to add the VLAN tag of the packet. Choose *Replace* from the drop-down menu to replace the VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	Type a new VID number for the *ONU Default VLAN Rule Upstream Setting*.
VLAN Type	Choose either an *8100*, 9100 or *88A8 VLAN Type* from the *Delete* or *Replace* option from the **Action** drop-down menu.
Priority Src	Choose *Original* from the drop-down menu to not change the priority of the packet. Choose *Priority* from the drop-down menu to change the packet priority based on the settings in the "ONU Priority Rule Settings" for the ONU. If no priority rule setting is matched, the priority will be “0”.

Click **Apply** to add the new ONU Default VLAN Upstream setting.

Searching and Editing an existing ONU Default VLAN Rule Upstream Setting

1. Choose the OLT Index you want to view or edit from the **OLT Index** drop-down menu on the bottom half of the screen.
2. Choose the ONU Index you want to view or edit from the **ONU Index** drop-down menu.
3. Click the **Search** button.
4. The result will appear underneath the **Search** button at the bottom of the window.
5. The following parameters can be edited if required:

Parameter	Description
Action	Choose *Add* from the drop-down menu to add the VLAN tag of the packet. Choose *Replace* from the drop-down menu to replace the VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	Type a new VID number for the *ONU Default VLAN Rule Upstream Setting*.
VLAN Type	Choose either an *8100*, 9100 or *88A8 VLAN Type* from the *Delete* or *Replace* option from the **Action** drop-down menu.
Priority Src	Choose *Original* from the drop-down menu to not change the priority of the packet. Choose *Priority* from the drop-down menu to change the packet priority based on the settings in the "ONU Priority Rule Settings" for the ONU. If no priority rule setting is matched, the priority will be "0".

Click **Apply** to save the changes to the ONU Default VLAN Rule Upstream setting.

ONU Default VLAN Rule Downstream Settings

The **ONU Default VLAN Rule Downstream Settings** window is used to configure the default VLAN rule of the ONU.

To access the **ONU Default VLAN Rule Downstream Settings** window click **PON> ONU Default VLAN Rule Settings > ONU Default VLAN Rule Downstream Settings.**

The ONU Default VLAN Rule Downstream Settings window is divided into two main sections. The top half is used to create new ONU Default VLAN Rule Downstream Settings. The bottom half is used to **Search** and **Edit** existing ONU Default VLAN Rule Downstream Settings.

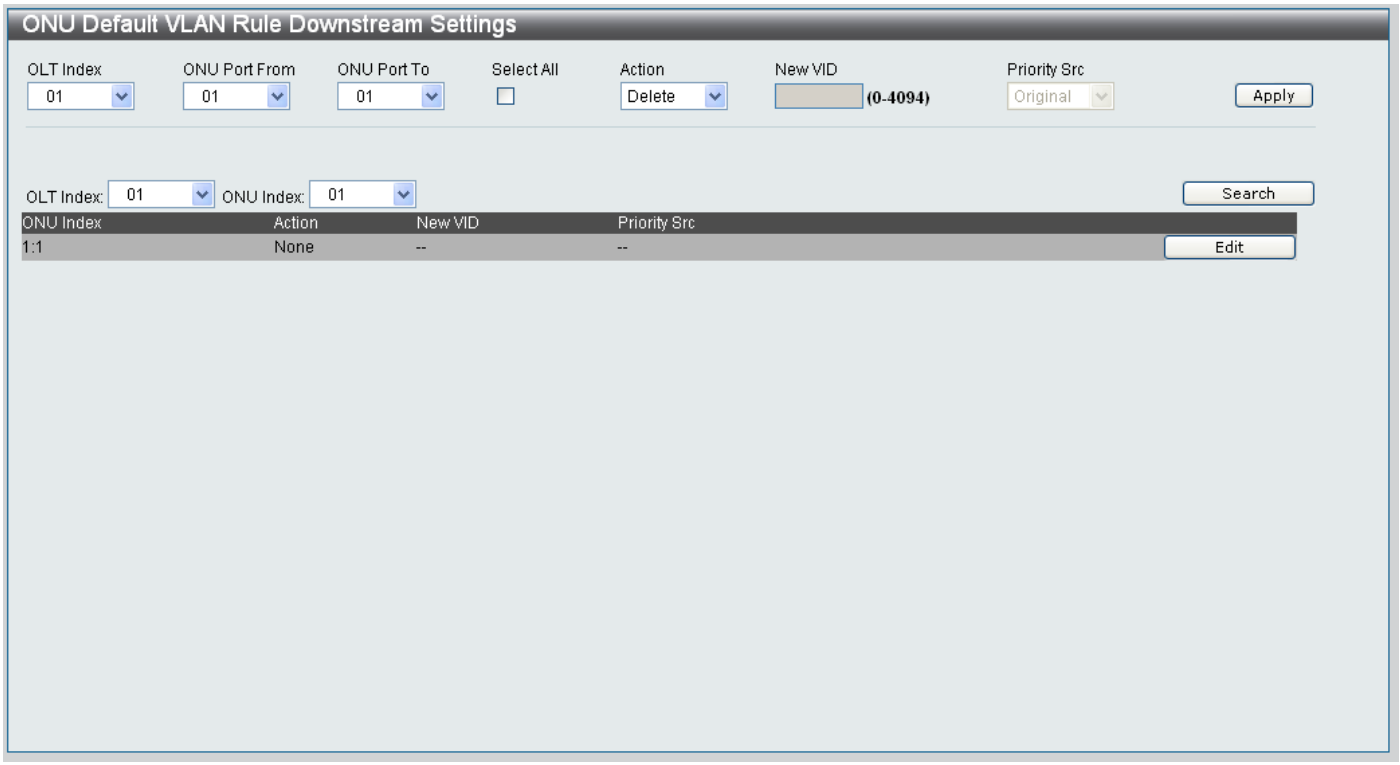


Figure 11- 39. ONU Default VLAN Rule Downstream Settings window

Adding a new ONU Default VLAN Rule Downstream Setting

Configure the parameters in the top half of the window, as described below, to add a new ONU Default VLAN Rule Downstream Setting:

Parameter	Description
OLT Index	Choose the OLT Index from the drop-down menu.
ONU Port From / ONU Port To	Use the drop-down menus to specify the range of ONU ports to be configured. Click the **Select All** checkbox to select all ONU ports.
Action	Choose *Delete* from the drop-down menu to remove the VLAN tag of the packet. Choose *Replace* from the drop-down menu to replace the VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	If choosing the *Replace* option from the **Action** drop-down menu type the new VID number that you want the VLAN tag to have.
Priority Src	If choosing the *Delete* or *Replace* option from the **Action** drop-down menu, choose *Original* from the drop-down menu to keep the same priority number. Choose *Priority Profile* to set the priority number if the profile.

Click **Apply** the new ONU Default VLAN Rule Downstream Setting.

Searching and Editing an existing ONU Default VLAN Rule Downstream Setting

1. Choose the OLT Index you want to view or edit from the **OLT Index** drop-down menu on the bottom half of the screen.
2. Choose the ONU Index you want to view or edit from the **ONU Index** drop-down menu.
3. Click the **Search** button.
4. The result will appear underneath the **Search** button at the bottom of the window.
5. The following parameters can be edited if required:

Parameter	Description
Action	Choose *Delete* from the drop-down menu to remove the VLAN tag of the packet. Choose *Replace* from the drop-down menu to replace the VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	If choosing the *Replace* option from the **Action** drop-down menu type the new VID number that you want the VLAN tag to have.
Priority Src	If choosing the *Replace* option from the **Action** drop-down menu, choose *Original* from the drop-down menu to keep the same priority number. Choose *Priority Profile* to set the priority number if the profile.

Click **Apply** to save the changes.

ONU VLAN Rule Settings

ONU VLAN Rule Upstream Settings

The **ONU VLAN Rule Upstream Settings** window is used to configure the upstream VLAN rule of the ONU.

To access the **ONU VLAN Rule Upstream Settings** window click **PON> ONU VLAN Rule Settings > ONU VLAN Rule Upstream Settings.**

The ONU VLAN Rule Upstream Settings window is divided into two main sections. The top half is used to create new ONU VLAN Rule Upstream Settings. The bottom half is used to **Search** and **Edit** existing ONU VLAN Rule Upstream Settings.

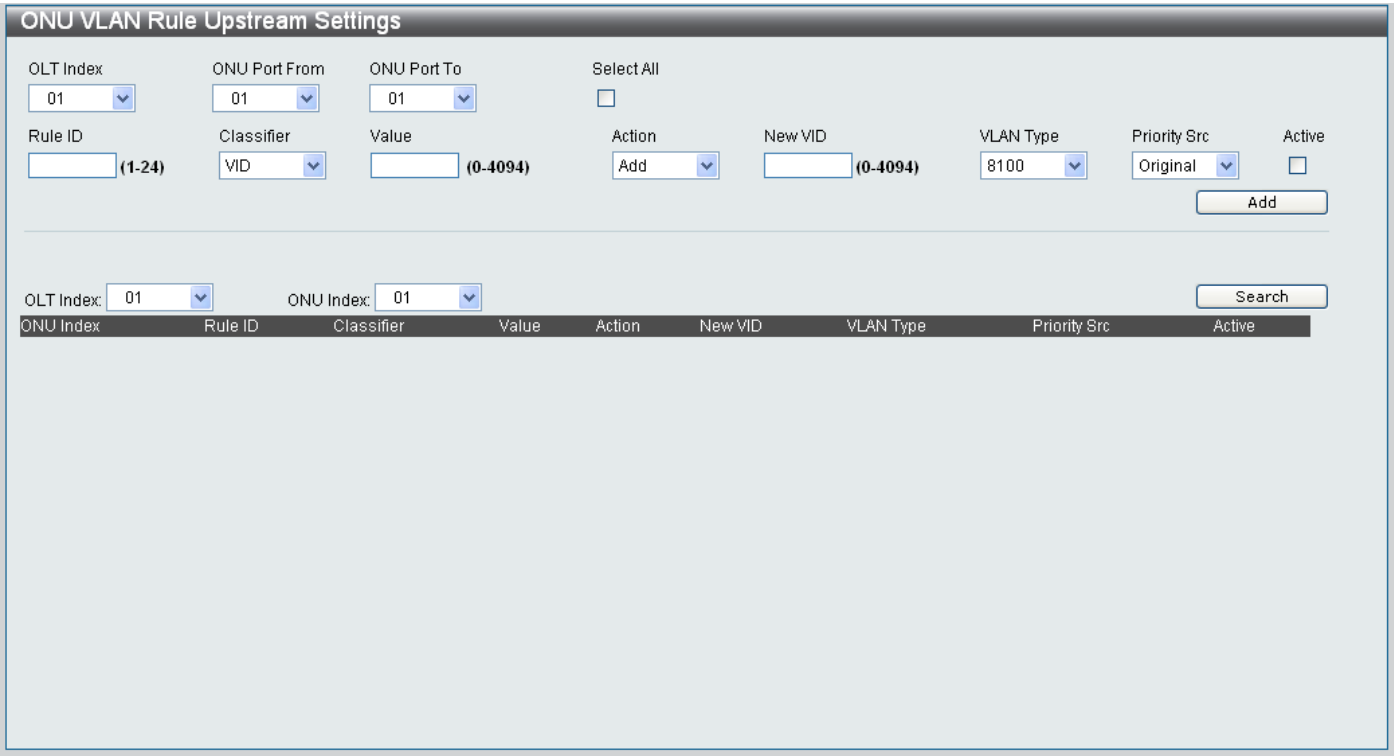


Figure 11- 40. ONU VLAN Rule Upstream Settings window

Adding a new ONU VLAN Rule Upstream Setting

Configure the parameters in the top half of the window, as described below, to add a new ONU VLAN Rule Upstream Setting:

Parameter	Description
OLT Index	Use the drop-down menus to choose the OLT Index you want to configure the ONU VLAN Rule Upstream Settings on.
ONU Port From / ONU Port To	Use the drop-down menus to choose the range of ONU Ports you want to configure the ONU VLAN Rule Upstream Settings on. Tick the **Select All** checkbox to select all ports.
Rule ID	Type a rule index value between 1 and 24.
Classifier	Choose whether to create the setting based on a *VID*, *IPv4* or *Ethernet Type* from the drop-down menu.
Value	If choosing *VID* from the **Classifier** drop-down menu, type the VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type the value in the textbox. If choosing *Ethernet Type* from the drop-down menu, type the hexadecimal address in the textbox.

Action	Choose *Add* from the drop-down menu to add a new VLAN tag to the packet. Choose *Replace* from the drop-down menu to replace the original VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	If choosing *Add* or *Replace* from the **Action** drop-down menu type the VID that you want to add or replace on the packet.
VLAN Type	If choosing *Add* from the drop-down menu choose whether you want to add an *8100*, *9100* or 88A8 VLAN type from the drop-down menu.
Priority Src	Choose *Original* from the drop-down menu to keep the same priority number. Choose *Priority Profile* to set the priority number if the profile.
Active	Tick the **Active** checkbox to make the ONU VLAN Rule Upstream Setting active.

Click **Add** the new ONU VLAN Rule Upstream Setting.

Searching and Editing an existing ONU VLAN Rule Upstream Setting

1. Choose the OLT Index you want to view or edit from the **OLT Index** drop-down menu on the bottom half of the screen.
2. Choose the ONU Index you want to view or edit from the **ONU Index** drop-down menu.
3. Click the **Search** button.
4. The result will appear underneath the **Search** button at the bottom of the window.
5. The following parameters can be edited if required:

Parameter	Description
Classifier	Use the drop-down menu to edit the Classifier setting if required
Value	Type a new value in the textbox. If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type a new value in the textbox. If choosing *Ethernet Type* from the drop-down menu, type a new hexadecimal address in the textbox.
Action	Choose *Add* from the drop-down menu to add a new VLAN tag to the packet. Choose *Replace* from the drop-down menu to replace the original VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	If choosing *Add* or *Replace* from the **Action** drop-down menu type a new VID that you want to add or replace on the packet.
VLAN Type	If choosing *Add* from the drop-down menu choose whether you want to add an *8100*, *9100* or 88A8 VLAN type from the drop-down menu.
Priority Src	Choose *Original* from the drop-down menu to keep the same priority number. Choose *Priority Profile* to set the priority number if the profile.
Active	Tick the **Active** checkbox to make the ONU VLAN Rule Upstream Setting active.

Click **Apply** to save the changes to the Switch.

ONU VLAN Rule Downstream Settings

The **ONU VLAN Rule Downstream Settings** window is used to configure the downstream VLAN rule of the ONU.

To access the **ONU VLAN Rule Downstream Settings** window click **PON> ONU VLAN Rule Settings > ONU VLAN Rule Downstream Settings.**

The ONU VLAN Rule Downstream Settings window is divided into two main sections. The top half is used to create new ONU VLAN Rule Downstream Settings. The bottom half is used to **Search** and **Edit** existing ONU VLAN Rule Downstream Settings.

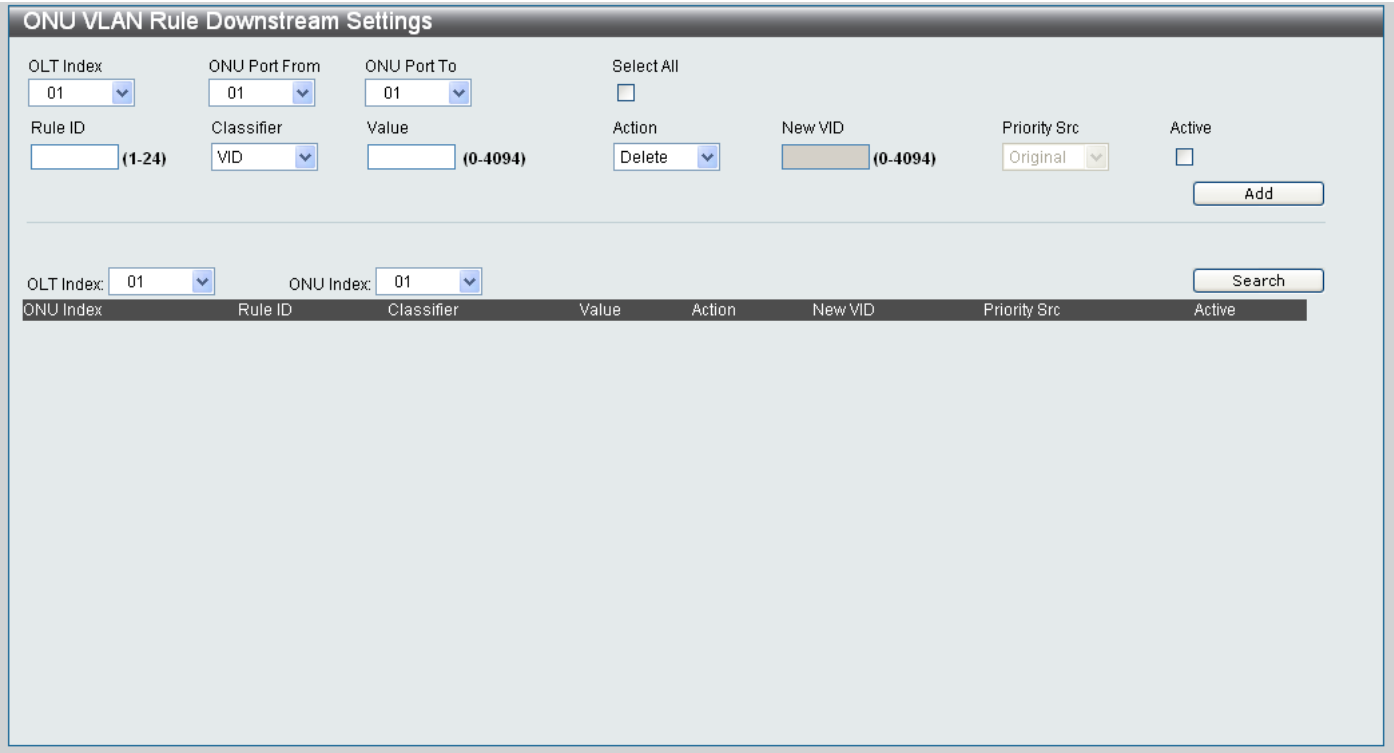


Figure 11- 41. ONU VLAN Rule Downstream Settings window

Adding a new ONU VLAN Rule Downstream Setting

Configure the parameters in the top half of the window, as described below, to add a new ONU Default VLAN Rule Downstream Setting:

Parameter	Description
OLT Index	Use the drop-down menus to choose the OLT Index you want to configure the ONU VLAN Rule Downstream Settings on.
ONU Port From / ONU Port To	Use the drop-down menus to choose the range of ONU Ports you want to configure the ONU VLAN Rule Downstream Settings on. Tick the **Select All** checkbox to select all ports.
Rule ID	Type a rule index value between 1 and 24.
Classifier	Choose whether to create the setting based on a *VID*, *IPv4* or *Ethernet Type* from the drop-down menu.
Value	If choosing *VID* from the **Classifier** drop-down menu, type the VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type the value in the textbox. If choosing *Ethernet Type* from the drop-down menu, type the hexadecimal address in the textbox.
Action	Choose *Add* from the drop-down menu to add a new VLAN tag to the packet.

	Choose *Replace* from the drop-down menu to replace the original VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	If choosing *Add* or *Replace* from the **Action** drop-down menu type the VID that you want to add or replace on the packet.
VLAN Type	If choosing *Add* from the drop-down menu choose whether you want to add an *8100*, *9100* or 88A8 VLAN type from the drop-down menu.
Priority Src	If choosing *Replace* in the Action drop-down menu, choose to use an *Original* or the *Priority Profile* source from the drop-down menu
Active	Tick the **Active** checkbox to make the ONU VLAN Rule Downstream Setting active.

Click **Add** the new ONU VLAN Rule Downstream Setting.

Searching and Editing an existing ONU VLAN Rule Downstream Setting

1. Choose the OLT Index you want to view or edit from the **OLT Index** drop-down menu on the bottom half of the screen.
2. Choose the ONU Index you want to view or edit from the **ONU Index** drop-down menu.
3. Click the **Search** button.
4. The result will appear underneath the **Search** button at the bottom of the window.
5. The following parameters can be edited if required:

Parameter	Description
Classifier	Use the drop-down menu to edit the Classifier setting if required
Value	Type a new value in the textbox. If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type a new value in the textbox. If choosing *Ethernet Type* from the drop-down menu, type a new hexadecimal address in the textbox.
Action	Choose *Delete* from the drop-down menu to delete the VLAN tag of the packet. Choose *Replace* from the drop-down menu to replace the original VLAN tag of the packet. Choose *None* from the drop-down menu to not take any action.
New VID	If choosing *Add* or *Replace* from the **Action** drop-down menu type a new VID that you want to add or replace on the packet.
VLAN Type	If choosing *Add* from the drop-down menu choose whether you want to add an *8100*, *9100* or 88A8 VLAN type from the drop-down menu.
Priority Src	If choosing *Replace* in the Action drop-down menu, choose to use an *Original* or the *Priority Profile* source from the drop-down menu.
Active	Tick the **Active** checkbox to make the ONU VLAN Rule Downstream Setting active.

Click **Apply** to save the changes to the Switch.

ONU Priority Rule Settings

The **ONU Priority Rule Settings** windows are used to configure the priority rules. The purpose of the priority rule is two fold. One of the purposes is to determine the priority that will be used in the VLAN tag of the packet, and the other is to determine the priority queue for holding the packet.

For the rule to determine the priority to be used in the VLAN tag, the rule will be used when the VLAN rules or the default VLAN rule are configured to use the priority rule. The priority defined in the matched priority rule will be used by the VLAN rule. If no priority rule matches the packet, then the default priority, 0, will be used.

In order for the rule to determine the priority queue for holding the packet, one of the following must happen. If the packet matches a priority rule, the priority rule will determine the priority queue. Otherwise, the priority queue will be determined based on the priority mapping rule.

Up to 40 rules can be specified for both inbound and outbound connections to and from the ONU. For each field type (also named filter type), up to 8 rules can be configured.

ONU Priority Rule Upstream Settings

To access the **ONU Priority Rule Upstream Settings** window click **PON> ONU Priority Rule Settings > ONU Priority Rule Upstream Settings.**

The ONU Priority Rule Upstream Settings window is divided into two main sections. The top half of the window is used to Search existing and add new ONU Priority Rule Upstream Settings. The bottom half is used to display the ONU Priority Rule Upstream Settings that are configured on the Switch.

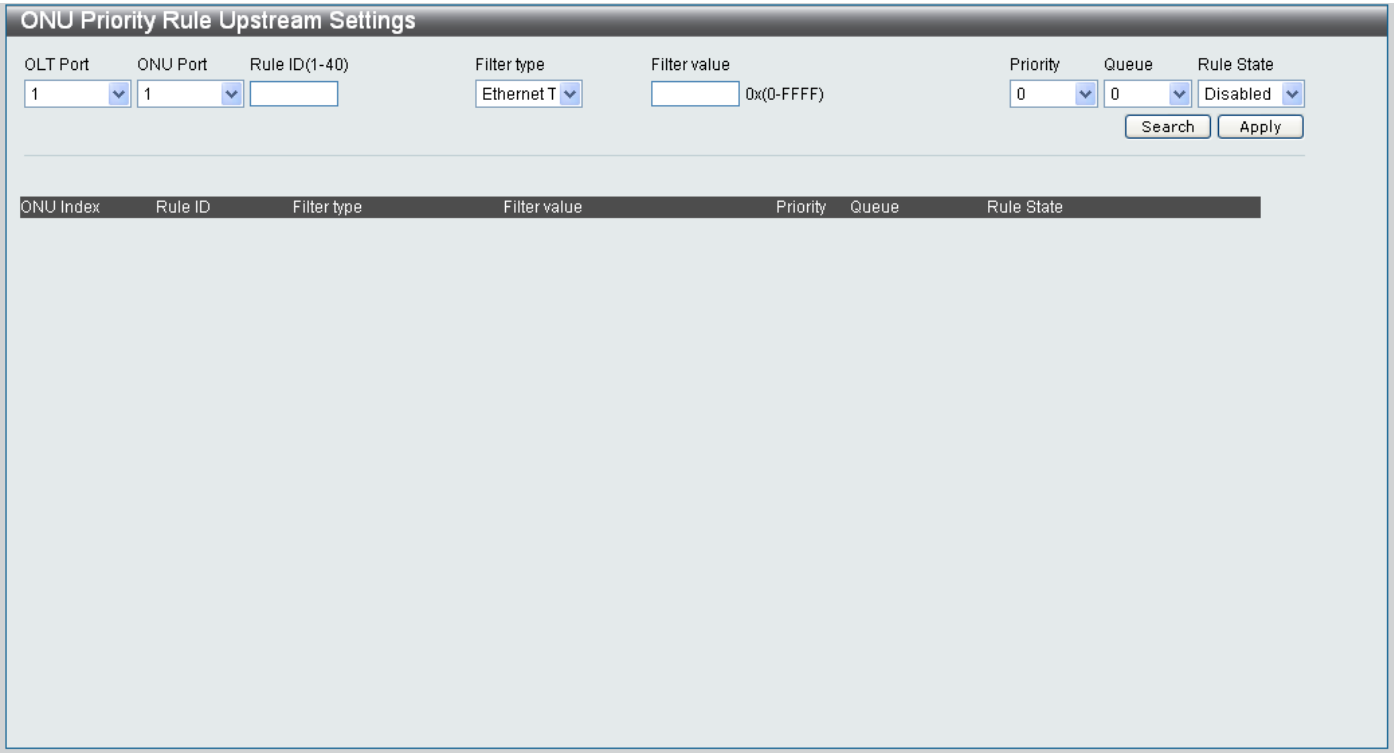


Figure 11- 42. ONU Priority Rule Upstream Settings window

The parameters used to Find or Add an ONU Priority Rule Upstream Setting are described below:

Parameter	Description
OLT Port	Use the drop-down menu to choose the OLT Port you want to view/add the ONU Priority Rule Upstream Settings to.
ONU Port	Use the drop-down menu to choose the ONU Port you want to view/add the ONU Priority Rule Upstream Settings to.
Rule ID (1-40)	Type the rule index rule of the ONU Priority Rule Upstream Setting that you want to view.
Filter type	Use the drop-down menu to choose the type of filter you want to view/add the ONU Priority Rule Upstream Setting to.
Filter value	If choosing *Ethernet Type* from the **Filter Type** drop-down menu, type a new hexadecimal address in the textbox. If choosing *VID* from the **Filter Type** drop-down menu, type a new VID value in the textbox. If choosing *IPv4 Protocol* from the **Filter Type** drop-down menu, type a new value in the textbox. If choosing *Source IP* from the **Filter Type** drop-down menu, type the *Source IP Address* in the textbox. If choosing *Destination IP* from the **Filter Type** drop-down menu, type the *Destination IP Address* in the textbox.
Priority	If choosing *Ethernet Type*, *VID* or *IPv4 Protocol* from the **Filter Type** drop-down

	menu, use the drop-down menu to choose a *Priority number* between *0* and *7*.
Queue	If choosing *Ethernet Type*, *VID* or *IPv4 Protocol* from the **Filter Type** drop-down menu, use the drop-down menu to choose a *Queue number* between *0* and *7*.
Rule State	Click *Enabled* from the drop-down menu to enable the *ONU Priority Upstream Setting.* Click *Disabled* to disable.

Finding an existing ONU Priority Rule Upstream Setting

To find an existing ONU Priority Rule for upstream connections configure the parameters as mentioned above and click the **Search** button.

Adding a new ONU Priority Rule Upstream Setting

To add a new ONU Priority Rule for upstream connections configure the parameters as mentioned above and click the **Apply** button.

ONU Priority Rule Downstream Settings

To access the **ONU Priority Rule Downstream Settings** window click **PON> ONU Priority Rule Settings > ONU Priority Rule Downstream Settings.**

The ONU Priority Rule Downstream Settings window is divided into two main sections. The top half of the window is used to Search existing and add new ONU Priority Rule Downstream Settings. The bottom half is used to display the ONU Priority Rule Downstream Settings that are configured on the Switch.

Figure 11- 43. ONU Priority Rule Downstream Settings window

The parameters used to Find or Add an ONU Priority Rule Downstream Setting are described below:

Parameter	Description
OLT Port	Use the drop-down menu to choose the OLT Port you want to view/add the ONU Priority Rule Downstream Settings to.
ONU Port	Use the drop-down menu to choose the ONU Port you want to view/add the ONU Priority Rule Downstream Settings to.
Rule ID (1-40)	Type the rule index of the ONU Priority Rule Downstream Setting that you want to view.

Filter type	Use the drop-down menu to choose the type of filter you want to view/add the ONU Priority Rule Downstream Setting to.
Filter value	If choosing *Ethernet Type* from the **Filter Type** drop-down menu, type a new hexadecimal address in the textbox. If choosing *VID* from the **Filter Type** drop-down menu, type a new VID value in the textbox. If choosing *IPv4 Protocol* from the **Filter Type** drop-down menu, type a new value in the textbox. If choosing *Source IP* from the **Filter Type** drop-down menu, type the *Source IP Address* in the textbox. If choosing *Destination IP* from the **Filter Type** drop-down menu, type the *Destination IP Address* in the textbox.
Priority	If choosing *Ethernet Type*, *VID* or *IPv4 Protocol* from the **Filter Type** drop-down menu, use the drop-down menu to choose a *Priority number* between *0* and *7*.
Queue	If choosing *Ethernet Type*, *VID* or *IPv4 Protocol* from the **Filter Type** drop-down menu, use the drop-down menu to choose a *Queue number* between *0* and *7*.
Rule State	Click *Enabled* from the drop-down menu to enable the *ONU Priority Downstream Setting.* Click *Disabled* to disable.

Finding an existing ONU Priority Rule Downstream Setting

To find an existing ONU Priority Rule for downstream connections configure the parameters as mentioned above and click the **Search** button.

Adding a new ONU Priority Rule Downstream Setting

To add a new ONU Priority Rule for downstream connections configure the parameters as mentioned above and click the **Apply** button.

ONU Priority Map Settings

The **ONU Priority Map Settings** window maps the priority queue for the upstream and downstream traffic passing through the PON port.

The mapping to a priority queue can be either based on IP TOS or based on 1p priority in the VLAN tag. For the tagged packet, the mapping will be based on the 1p priority. For the untagged IP packet, the mapping will be based on IP TOS value. Other untagged packets will be mapped to queue 0.

For default tag_priority mapping, priority 0 is mapped to class 0, priority 1 is mapped to class 1, priority 2 is mapped to class 2, priority 3 is mapped to class 3, priority 4 is mapped to class 4, priority 5 is mapped to class 5, priority 6 is mapped to class 6, priority 7 is mapped to class 7.

For default IP TOS mapping, priority 0 is mapped to class 0, priority 1 is mapped to class 1, priority 2 is mapped to class 2, priority 3 is mapped to class 3, priority 4 is mapped to class 4, priority 5 is mapped to class 5, priority 6 is mapped to class 6, priority 7 is mapped to class 7.

To access the **ONU Priority Map Settings** window click **PON> ONU Map Settings.**

The ONU Priority Map Settings window is divided into three main sections. The top section is used to add new ONU Priority Map Settings, the center section is used to edit IP ToS Priority Queue Mappings and the bottom section is used to configure Tag Priority Queue Mapping settings.

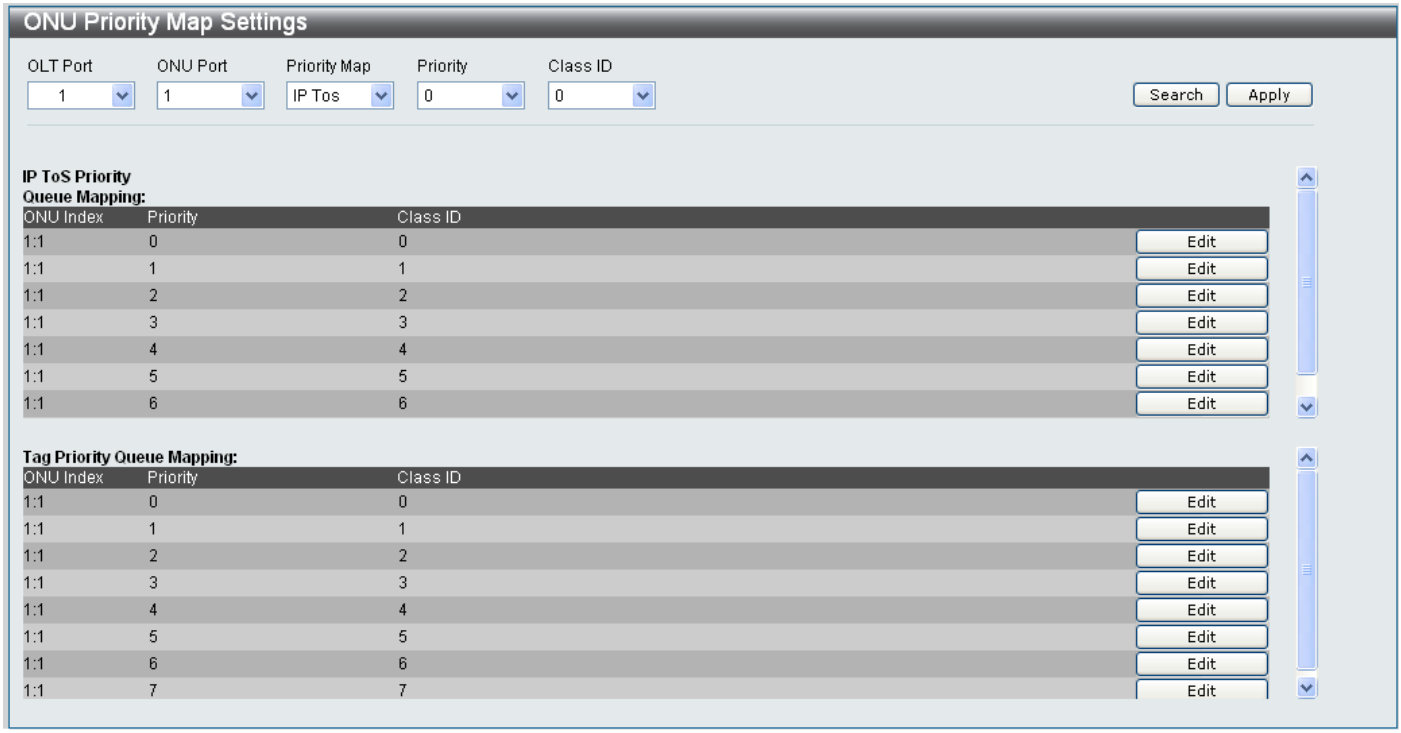


Figure 11- 44. ONU Priority Map Settings window

The parameters used to Find or Add the ONU Priority Map Settings are described below:

Parameter	Description
OLT Port	Use the OLT Port drop-down menu to choose the OLT Port you want to view/edit the ONU Priority Map Settings for.
ONU Port	Use the ONU Port drop-down menu to choose the ONU Port you want to view/edit the ONU Priority Map Settings for.
Priority Map	Choose to configure an *IP ToS* or *Tag Priority Map* from the drop-down menu.
Priority	Choose a *Priority value* between *0* and *7* from the drop-down menu.
Class ID	Choose a *Class ID value* between *0* and *7* from the drop-down menu.

Click the **Add** button to add the new Priority Map Setting.

Click the **Search** button to search for the specified Priority Map Setting.

Editing an IP ToS Priority Queue Mapping

1. Click the **Edit** button next to the IP ToS Priority Queue Mapping entry you want to edit.
2. Choose a new *Class ID* from the drop-down menu.
3. Click the **Apply** button next to the IP ToS Priority Queue Mapping to save the change.

Editing a Tag Priority Queue Mapping

1. Click the **Edit** button next to the Tag Priority Queue Mapping entry you want to edit.
2. Choose a new *Class ID* from the drop-down menu.
3. Click the **Apply** button next to the Tag Priority Queue Mapping to save the change.

PON Profile

ONU Profile Setup

The **ONU Profile Setup** window is used to setup new ONU Profiles and configure existing ones.

To access the **ONU Profile Setup** window click **PON> PON Profile> ONU Profile Setup.**

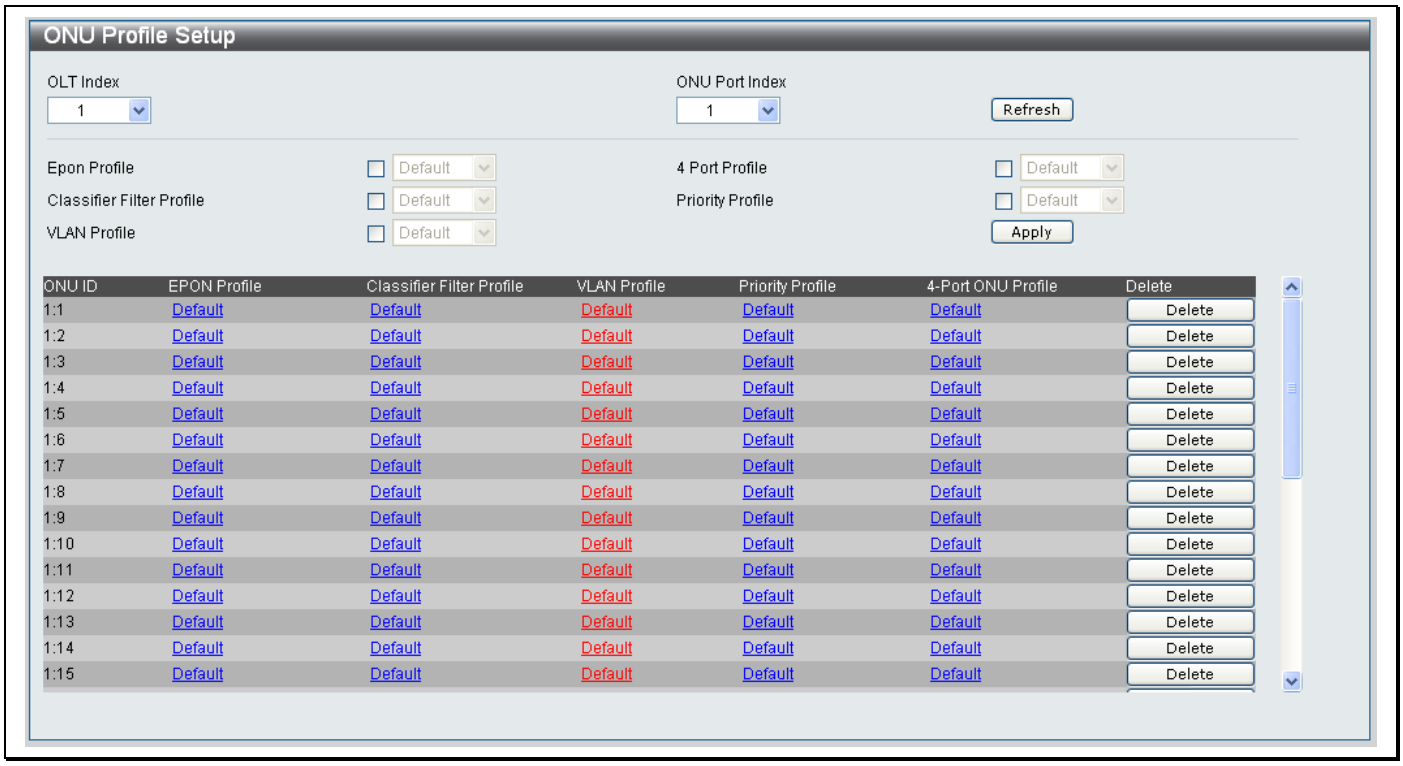


Figure 11- 45. ONU Profile Setup window

The ONU Profile Setup window is divided into three main sections.

The top section of the window is used to select the OLT Index and ONU Port Index numbers that you want to configure the ONU Profile for.

The center section is used to configure the different parameters available for an ONU Profile.

The bottom section is used to view existing ONU Profiles.

Creating a new ONU Profile

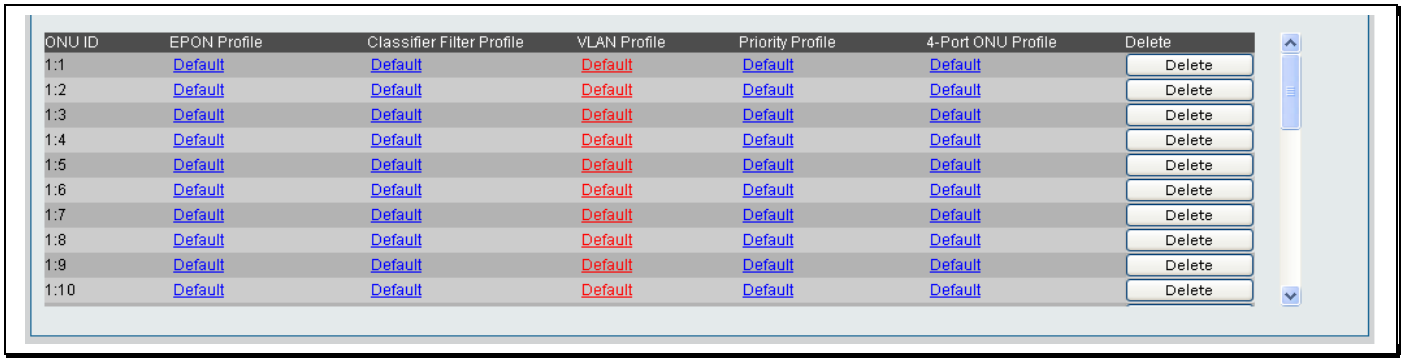
1. Choose the *OLT Index* number and *ONU Port Index* numbers from the drop-down menus.
2. Configure the parameters in the center section as described below:

Parameter	Description
Epon Profile	Tick to change the Epon Profile Setting. Choose a new Epon Profile from the adjacent drop-down menu.
4 Port Profile	Tick to change the 4 Port Profile Setting. Choose a new 4 Port Profile from the adjacent drop-down menu.
Classifier Filter Profile	Tick to change the Classifier Filter Profile Setting. Choose a new Classifier Port Profile from the adjacent drop-down menu.
Priority Profile	Tick to change the Priority Profile Setting. Choose a new Priority Profile from the adjacent drop-down menu.
VLAN Profile	Tick to change the VLAN Profile Setting. Choose a new VLAN Profile from the adjacent drop-down menu.

3. Tick the **Apply** button to save the changes.

Viewing an ONU Profile

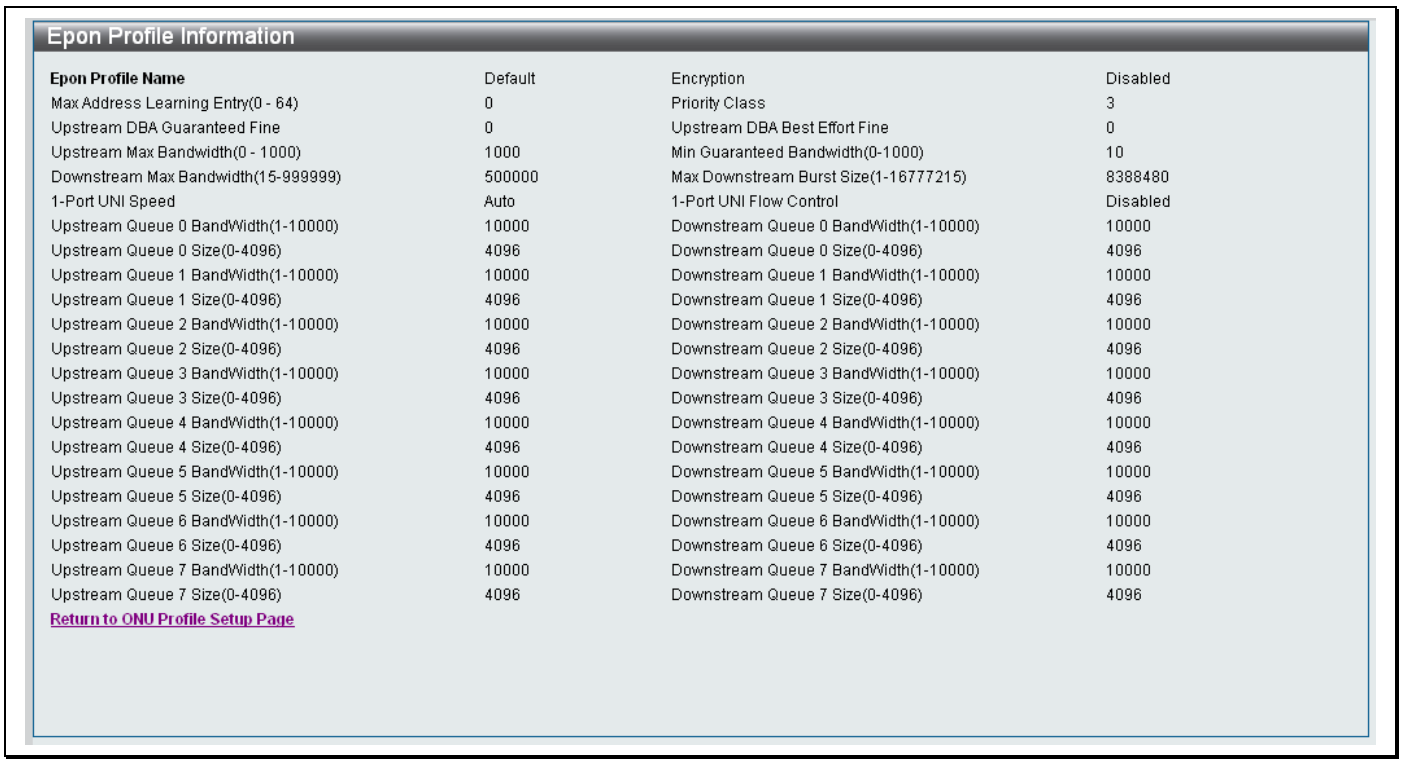
1. To view an existing ONU Profile click the attribute link you want to view at the bottom section of the window, as shown below:



ONU ID	EPON Profile	Classifier Filter Profile	VLAN Profile	Priority Profile	4-Port ONU Profile	Delete
1:1	Default	Default	Default	Default	Default	Delete
1:2	Default	Default	Default	Default	Default	Delete
1:3	Default	Default	Default	Default	Default	Delete
1:4	Default	Default	Default	Default	Default	Delete
1:5	Default	Default	Default	Default	Default	Delete
1:6	Default	Default	Default	Default	Default	Delete
1:7	Default	Default	Default	Default	Default	Delete
1:8	Default	Default	Default	Default	Default	Delete
1:9	Default	Default	Default	Default	Default	Delete
1:10	Default	Default	Default	Default	Default	Delete

Figure 11- 46. Edit section in ONU Profile Setup window

2. Click the *hyperlink* of the setting you want to view
3. The details of the ONU Profile will appear in a new window as shown below:



Epon Profile Information

Epon Profile Name	Default	Encryption	Disabled
Max Address Learning Entry(0 - 64)	0	Priority Class	3
Upstream DBA Guaranteed Fine	0	Upstream DBA Best Effort Fine	0
Upstream Max Bandwidth(0 - 1000)	1000	Min Guaranteed Bandwidth(0-1000)	10
Downstream Max Bandwidth(15-999999)	500000	Max Downstream Burst Size(1-16777215)	8388480
1-Port UNI Speed	Auto	1-Port UNI Flow Control	Disabled
Upstream Queue 0 BandWidth(1-10000)	10000	Downstream Queue 0 BandWidth(1-10000)	10000
Upstream Queue 0 Size(0-4096)	4096	Downstream Queue 0 Size(0-4096)	4096
Upstream Queue 1 BandWidth(1-10000)	10000	Downstream Queue 1 BandWidth(1-10000)	10000
Upstream Queue 1 Size(0-4096)	4096	Downstream Queue 1 Size(0-4096)	4096
Upstream Queue 2 BandWidth(1-10000)	10000	Downstream Queue 2 BandWidth(1-10000)	10000
Upstream Queue 2 Size(0-4096)	4096	Downstream Queue 2 Size(0-4096)	4096
Upstream Queue 3 BandWidth(1-10000)	10000	Downstream Queue 3 BandWidth(1-10000)	10000
Upstream Queue 3 Size(0-4096)	4096	Downstream Queue 3 Size(0-4096)	4096
Upstream Queue 4 BandWidth(1-10000)	10000	Downstream Queue 4 BandWidth(1-10000)	10000
Upstream Queue 4 Size(0-4096)	4096	Downstream Queue 4 Size(0-4096)	4096
Upstream Queue 5 BandWidth(1-10000)	10000	Downstream Queue 5 BandWidth(1-10000)	10000
Upstream Queue 5 Size(0-4096)	4096	Downstream Queue 5 Size(0-4096)	4096
Upstream Queue 6 BandWidth(1-10000)	10000	Downstream Queue 6 BandWidth(1-10000)	10000
Upstream Queue 6 Size(0-4096)	4096	Downstream Queue 6 Size(0-4096)	4096
Upstream Queue 7 BandWidth(1-10000)	10000	Downstream Queue 7 BandWidth(1-10000)	10000
Upstream Queue 7 Size(0-4096)	4096	Downstream Queue 7 Size(0-4096)	4096

Return to ONU Profile Setup Page

Figure 11- 47. EPON Profile Information window

4. Click the *Return to ONU Profile Setup Page* hyperlink to return to the previous page.

EPON Profile Settings

The **EPON Profile Settings** window is used to create and edit EPON Profiles.

To access the **Epon Profile Settings** window click **PON> PON Profile> EPON Profile Settings.**

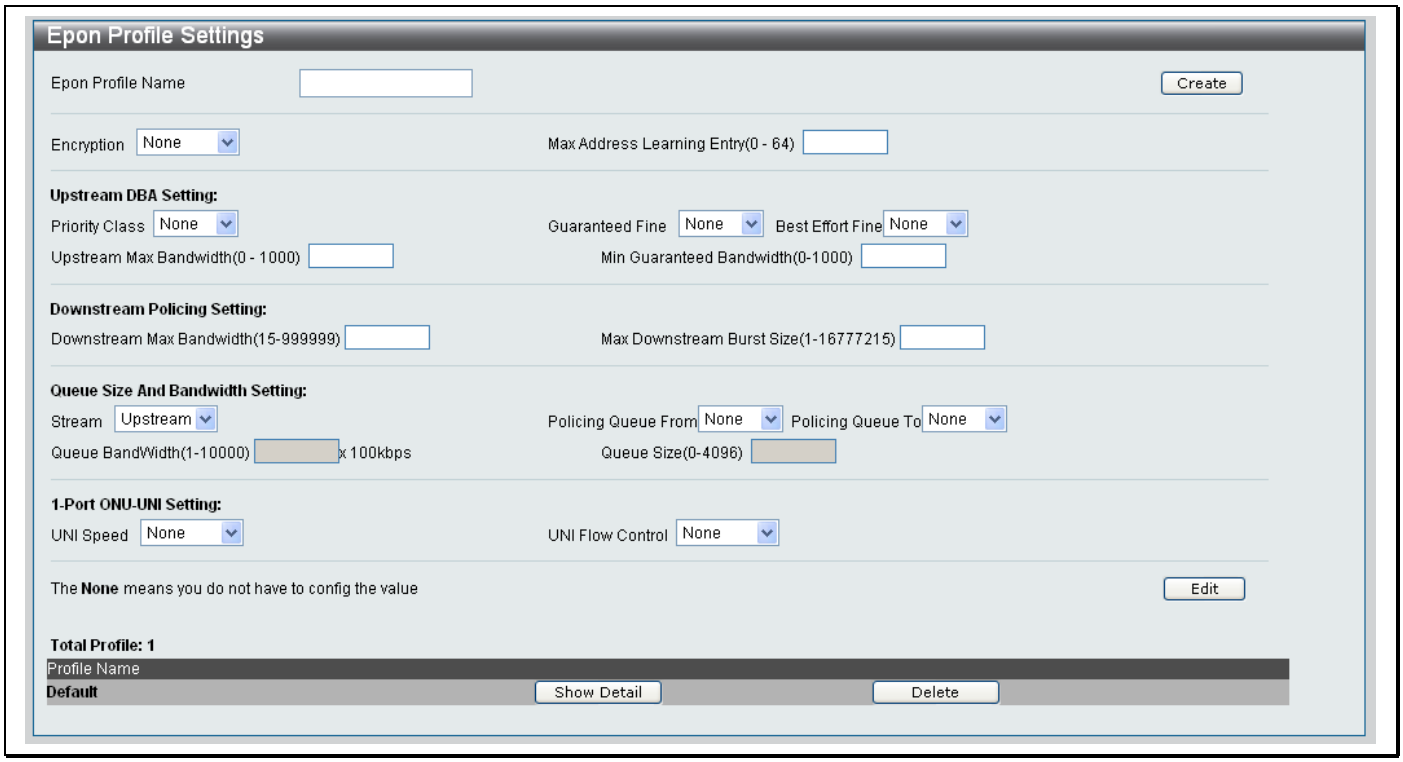


Figure 11- 48. EPON Profile Settings window

Use the following parameters to Add/Edit an Epon Profile Setting:

Parameter	Description
Epon Profile Name	Type a name to identify the new Epon Profile.
Encryption	Choose whether Encryption on the Epon Profile should be *Enabled/Disabled.*
Max Address Learning Entry (0-64)	Type a maximum address learning entry between *0* and *64*.
Priority Class	Choose a Priority Class between *0* and *7*. Choose *None* to specify that no Priority Class should be used.
Guaranteed Fine	Choose a *Fine Guarantee* value from the drop-down menu
Best Effort Fine	Choose a *Best Effort Fine* value from the drop-down menu
Upstream Max Bandwidth (0-1000)	Type an Upstream Maximum Bandwidth value between *0* and *1000*.
Min Guaranteed Bandwidth (0-1000)	Type a Minimum Bandwidth value between *0* and *1000*.
Downstream Max Bandwidth (15-999999)	Type a Downstream Maximum Bandwidth value between *15* and *999999*.
Max Downstream Burst Size (1-16777215)	Type a Maximum Downstream Burst Size between *1* and *16777215.*

Stream	Choose *Upstream* or *Downstream* from the drop-down menu.
Policing Queue From / Policing Queue To	Use the drop-down menus to specify the *Policing Queue* range.
Queue BandWidth (1-10000)	Type a Queue BandWidth value between *1* and *10000* in the textbox.
Queue Size (0-4096)	Type a Queue Size between *0* and *4096* in the textbox.
UNI Speed	Choose whether the 1 Port ONU-UNI should operate at *Auto*, *10m_full*, *10m_half*, *100m_full*, *100m_half* or *1000m_full* from the drop-down menu to specify the UNI Speed.
UNI Flow Control	Choose whether UNI Flow Control should be *Enabled* or *Disabled* from the drop-down menu.

Viewing Details of an Existing Epon Profile Setting

1. Click the **Show Detail** button next to the *Profile Name* that you want to edit at the bottom of the window.
2. The following window appears

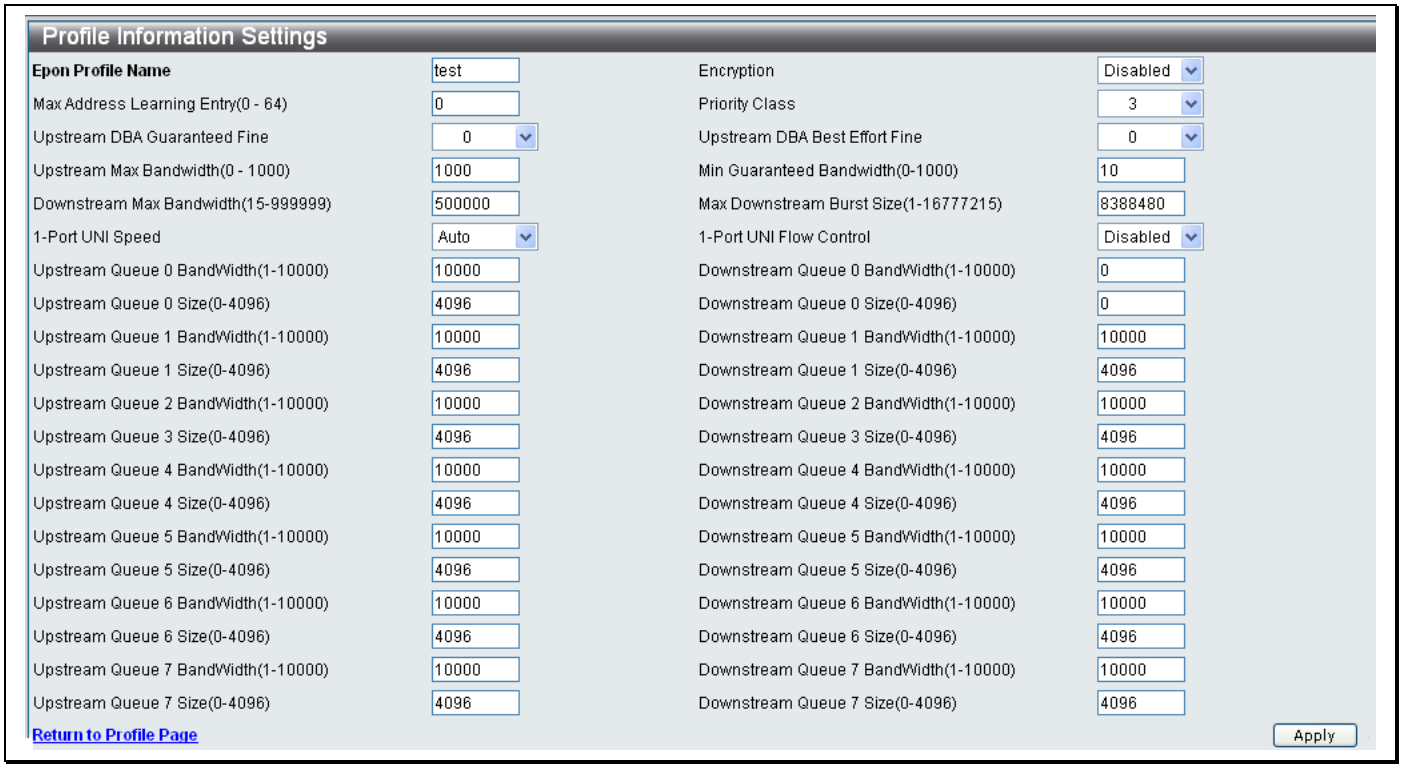


Figure 11- 49. EPON Profile Information Settings window

3. Edit the parameters as described in the table above.
4. Click the **Apply** button to save the changes or click the *Return to Profile Page* link to return to the Profile Page.

Deleting an Existing Epon Profile Setting

1. Click the **Delete** button next to the *Profile Name* that you want to delete.
2. A **Success** message indicates the Epon Profile was deleted successfully.

4 Port ONU Profile Settings

The **4 Port ONU Profile Settings** window is used to configure the ONU UNI Port settings.

To access the **4 Port ONU Profile Settings** window click **PON> PON Profile> 4 Port ONU Profile Settings.**

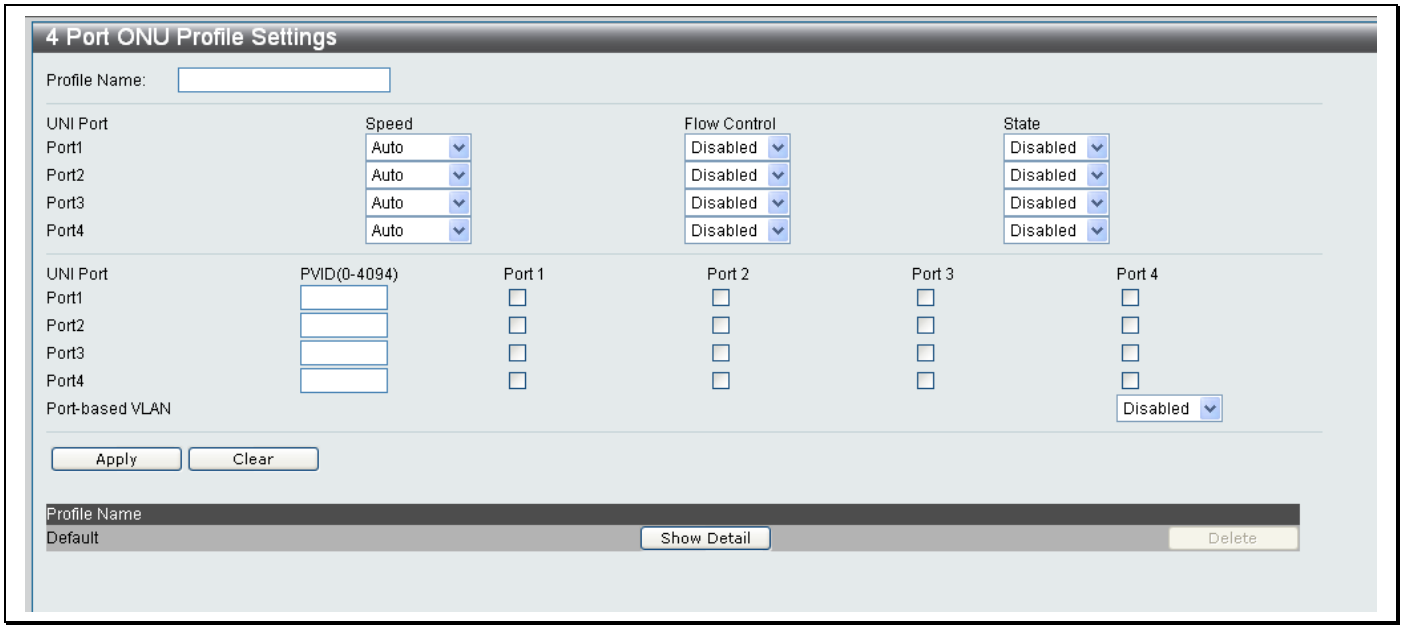


Figure 11- 47. 4 Port ONU Profile Settings window

Use the following parameters to Add/Edit a 4 Port ONU Profile Setting:

Parameter	Description
Profile Name	Type a Profile Name to identify the 4 Port ONU Profile.
Speed	Use the drop-down menus to specify if the Ports should operate at *10M/Half*, *10M/Full*, *100M/Half* or *100M/Full* speed.
Flow Control	Choose whether the ports *Flow Control* setting should be *Enabled* or *Disabled* from the drop-down menu.
State	Choose whether the ports *State* setting should be *Enabled* or *Disabled* from the drop-down menu.
PVID (0-4094)	Type a *PVID* number between *0* and *4094*.
Port-based VLAN	Choose whether the **Port-based VLAN** setting should be *Enabled* or *Disabled*.

Click **Apply** to Add/Delete the 4 Port ONU Profile Setting.

Deleting an Existing 4 Port ONU Profile Setting

1. Click the **Delete** button next to the *Profile Name* that you want to delete.
2. A **Success** message indicates the Epon Profile was deleted successfully.

VLAN Profile Settings

To access the **VLAN Profile Settings** window click **PON> PON Profile> VLAN Profile Settings.**

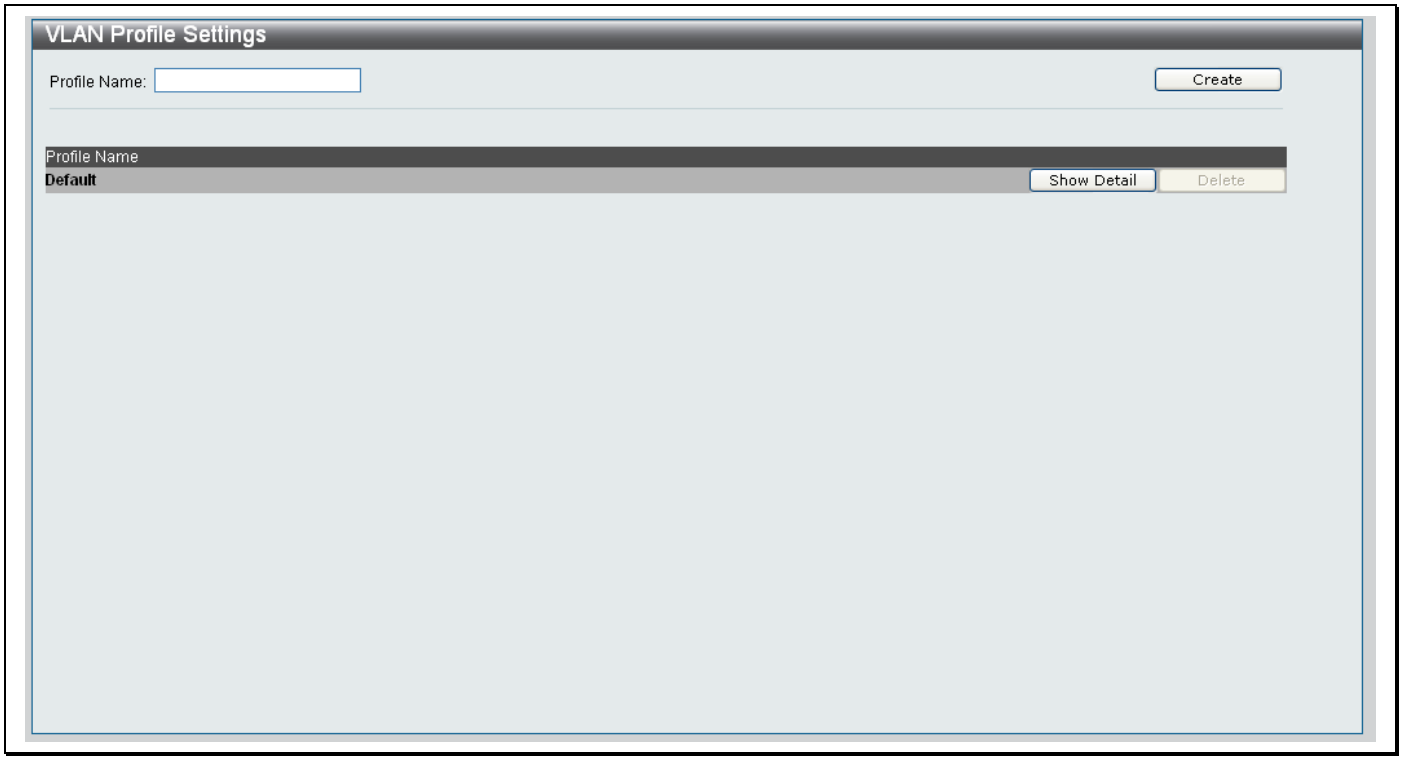


Figure 11- 48. VLAN Profile Settings window

Creating a new VLAN Profile

1. Type a name for the VLAN Profile in the **Profile Name** textbox.
2. Click the **Create** button.
3. The new profile will appear under the **Profile Name** heading.

Editing an existing VLAN Profile

1. Click the **Show Detail** button next to the VLAN you want to modify.
2. The following screen will appear:

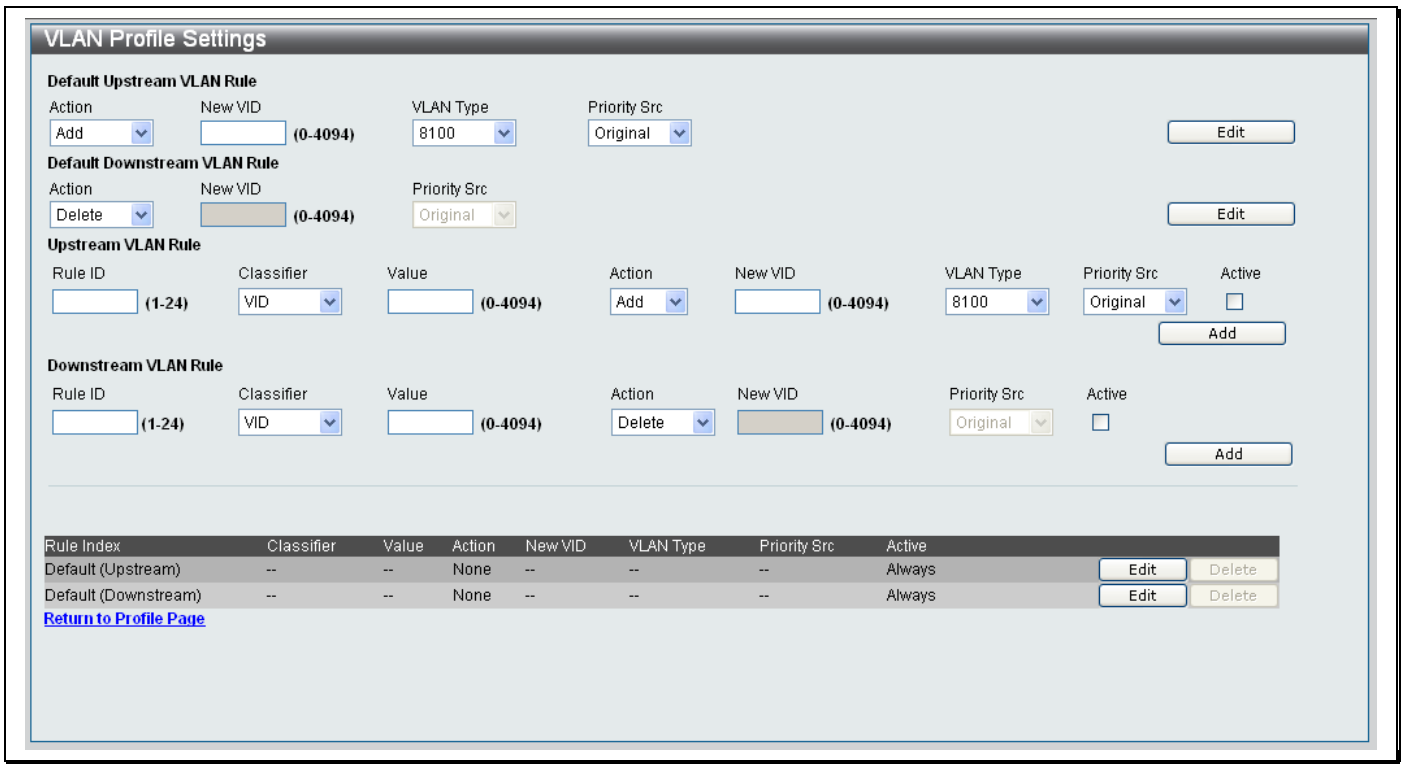


Figure 11- 49. Editing VLAN Profile Setting

3. The window is divided into four main sections, *Default Upstream VLAN Rule*, *Default Downstream VLAN Rule, Upstream VLAN Rule, Downstream VLAN Rule* and a table at the bottom of the screen, which shows the existing rules setup on the system.
4. Configure the *Default Upstream VLAN Rule* parameters as described below:

Parameter	Description
Action	Choose whether to *Add* or *Replace* the Default Upstream Rule from the drop-down menu.
New VID	If choosing to *Add* or *Replace* from the Action menu, type in a new VID value in this field.
VLAN Type	Choose whether to specify an *8100, 9100* or *88A8* type from the drop-down menu.
Priority Src	If choosing *Replace* in the Action drop-down menu, choose to use an *Original* or the *Priority Profile* source from the drop-down menu.

5. Configure the *Default Downstream VLAN Rule* parameters as described below:

Parameter	Description
Action	Choose whether to *Add* or *Replace* the Default Downstream Rule from the drop-down menu.
New VID	If choosing to *Add* or *Replace* from the Action menu, type in a new VID value in this field.
Priority Src	If choosing *Replace* in the Action drop-down menu, choose to use an *Original* or the *Priority Profile* source from the drop-down menu.

6. Configure the *Upstream VLAN Rule* parameters as described below:

Parameter	Description
Rule ID	Type an identity number to identify the Upstream VLAN Rule setting.
Classifier	Use the drop-down menu to choose *VID*, *IPv4* or *Ethertype* as the classifier.
Value	If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4 Protocol* from the **Classifier** drop-down menu, type a new value in the textbox. If choosing *Ethertype* from the **Classifier** drop -down menu, type a new hexadecimal address in the textbox.
Action	Choose whether to *Add* or *Replace* the Default Downstream Rule from the drop-down menu. Click the *None* option to specify that no action should be taken.
New VID	If choosing to *Add* or *Replace* from the **Action** drop-down menu, type in a new VID value in this field.
VLAN Type	Choose whether to specify an *8100, 9100* or *88A8* type from the drop-down menu.
Priority Src	If choosing *Replace* in the **Action** drop-down menu, choose to use an *Original* or the *Priority Profile* source from the drop-down menu.
Active	Tick the checkbox to specify that the Upstream VLAN rule should be *Active*.

7. Configure the *Downstream VLAN Rule* parameters as described below:

Parameter	Description
Rule ID	Type an identity number to identify the Downstream VLAN Rule setting.
Classifier	Use the drop-down menu to choose *VID*, *IPv4* or *Ethertype* as the classifier.
Value	If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4 Protocol* from the **Classifier** drop-down menu, type a new value in the textbox. If choosing *Ethertype* from the **Classifier** drop -down menu, type a new hexadecimal address in the textbox.
Action	Choose whether to *Add* or *Replace* the Downstream VLAN Rule from the drop-down menu. Click the *None* option to specify that no action should be taken.
New VID	If choosing to *Add* or *Replace* from the **Action** drop-down menu, type in a new VID value in this field.
Priority Src	If choosing *Replace* in the **Action** drop-down menu, choose to use an *Original* or the *Priority Profile* source from the drop-down menu.
Active	Tick the checkbox to specify that the Downstream VLAN rule should be *Active*.

Viewing Details of a VLAN Profile

1. Click the **Show Detail** button next to the *Profile Name* that you want to edit at the bottom of the window.
2. The following window appears
3. Edit the parameters as described in the table above.
4. Click the **Apply** button to save the changes or click the *Return to Profile Page* link to return to the Profile Page.

Deleting an Existing VLAN Profile

1. Click the **Delete** button next to the *Profile Name* that you want to delete.
2. A **Success** message indicates the Epon Profile was deleted successfully.

Classifier Profile Settings

To access the **Classifier Profile Settings** window click **PON> PON Profile> Classifier Profile Settings.**

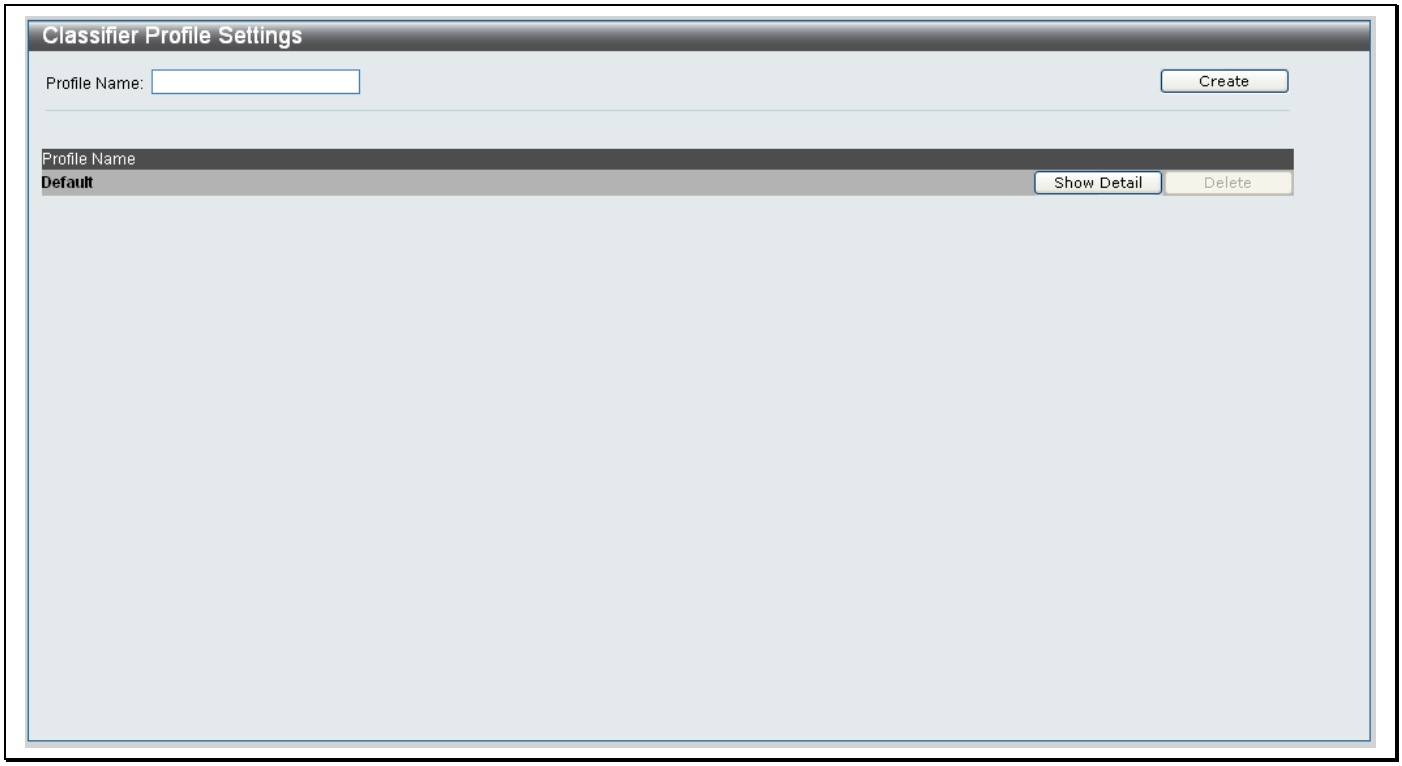


Figure 11- 50. Classifier Profile Settings window

Creating a new Classifier Profile

1. Type a name for the Classifier Profile in the **Profile Name** textbox.
2. Click the **Create** button.
3. The new profile will appear under the **Profile Name** heading.

Editing an existing Classifier Profile

1. Click the **Show Detail** button next to the Classifier you want to modify.
2. The following screen will appear:

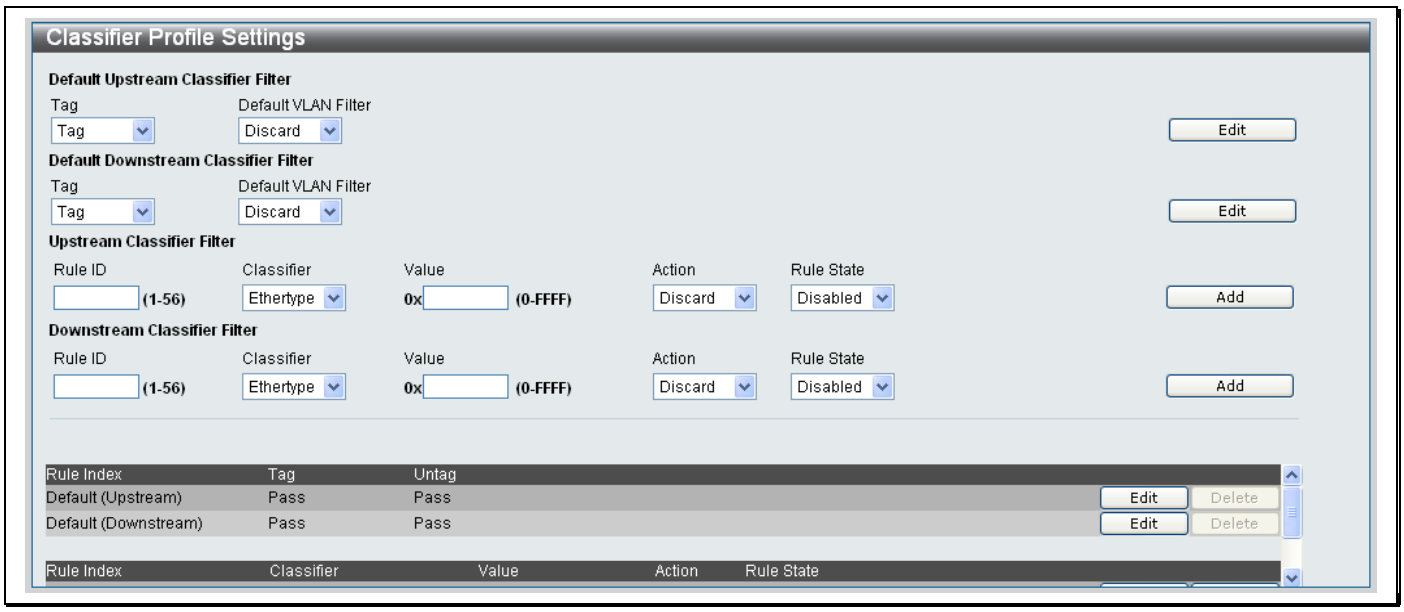


Figure 11- 51. Editing an existing Classifier Profile Setting

3. The window is divided into four main sections, *Default Upstream Classifier Filter*, *Default Downstream Classifier Filter, Upstream Classifier Filter, Downstream Classifier Filter* and a table at the bottom of the screen, which shows the existing rules setup on the system.
4. Configure the *Default Upstream Classifier Filter* parameters as described below:

Parameter	Description
Tag	Choose *Tag* or *Untag* from the drop-down for the Default Upstream Classifier Filter.
Default VLAN Filter	Choose to *Discard* or *Pass* the Default VLAN Filter from the drop-down menu for the Default Upstream Classifier Filter.

5. Configure the *Default Downstream Classifier Filter* parameters as described below:

Parameter	Description
Tag	Choose *Tag* or *Untag* from the drop-down for the Default Downstream Classifier Filter.
Default VLAN Filter	Choose to *Discard* or *Pass* the Default VLAN Filter from the drop-down menu for the Default Downstream Classifier Filter.

6. Configure the *Upstream Classifier Filter* parameters as described below:

Parameter	Description
Rule ID	Type an identity number to identify the Upstream Classifier Filter setting.
Classifier	Use the drop-down menu to choose *VID*, *IPv4* or *Ethertype* as the classifier.
Value	If choosing *Ethertype* from the **Classifier** drop-down menu, type in the hexadecimal of the frame, in the textbox. If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type the IPv4 protocol number you want to use between *1* and *255*. If choosing *Source TCP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source TCP Port number. If choosing *Source UDP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source UDP Port number. If choosing *Source IP* from the **Classifier** drop-down menu, type in the *IP address* of the Source host. If choosing *Destination IP* from the **Classifier** drop-down menu, type in the *IP address* of the Destination host.
Action	Choose whether to *Pass* or *Discard* the Upstream Classifier Filter from the drop-down menu. Click the *None* option to specify that no action should be taken.
Rule State	Choose *Enabled* from the drop-down menu to enable the Upstream Classifier Filter. Choose *Disabled* to disable.

7. Configure the *Downstream Classifier Filter* parameters as described below:

Parameter	Description
Rule ID	Type an identity number to identify the Downstream Classifier Filter setting.
Classifier	Use the drop-down menu to choose *VID*, *IPv4* or *Ethertype* as the classifier.
Value	If choosing *Ethertype* from the **Classifier** drop-down menu, type in the hexadecimal of the frame, in the textbox. If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type the IPv4 protocol number you want to use between *1* and *255*. If choosing *Source TCP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source TCP Port number. If choosing *Source UDP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source UDP Port number. If choosing *Source IP* from the **Classifier** drop-down menu, type in the *IP address* of the Source host. If choosing *Destination IP* from the **Classifier** drop-down menu, type in the *IP address* of the Destination host.
Action	Choose whether to *Pass* or *Discard* the Downstream Classifier Filter from the drop-down menu. Click the *None* option to specify that no action should be taken.
Rule State	Choose *Enabled* from the drop-down menu to enable the Downstream Classifier Filter. Choose *Disabled* to disable.

Deleting an Existing Classifier Profile

1. Click the **Delete** button next to the *Classifier Profile* that you want to delete.

2. A **Success** message indicates the Classifier Profile was deleted successfully.

Priority Profile Settings

To access the **Priority Profile Settings** window click **PON> PON Profile> Priority Profile Settings.**

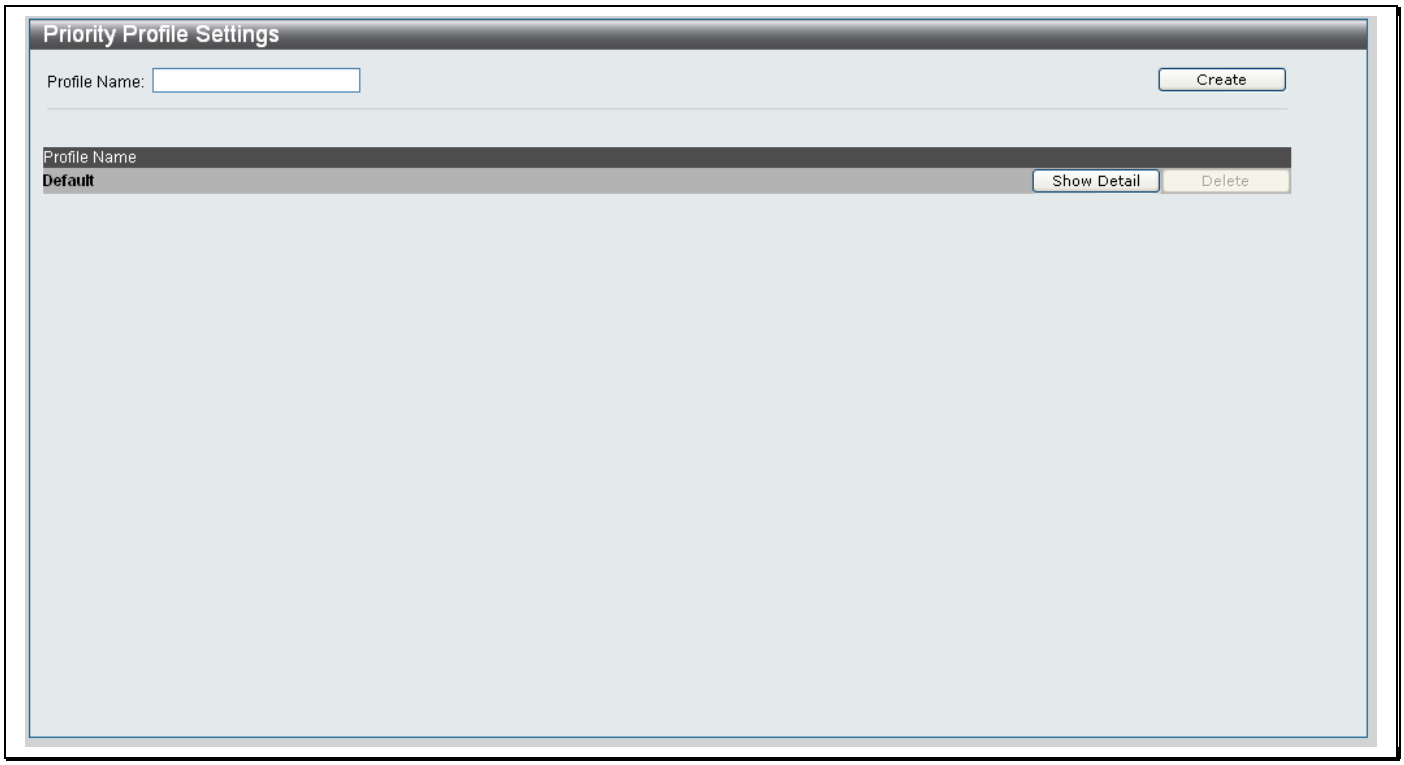


Figure 11- 52. Priority Profile Settings window

Creating a new Priority Profile

1. Type a name for the Priority Profile in the **Profile Name** textbox.
2. Click the **Create** button.
3. The new profile will appear under the **Profile Name** heading.

Editing an existing Priority Profile

1. Click the **Show Detail** button next to the Priority Profile you want to modify.
2. The following screen will appear:

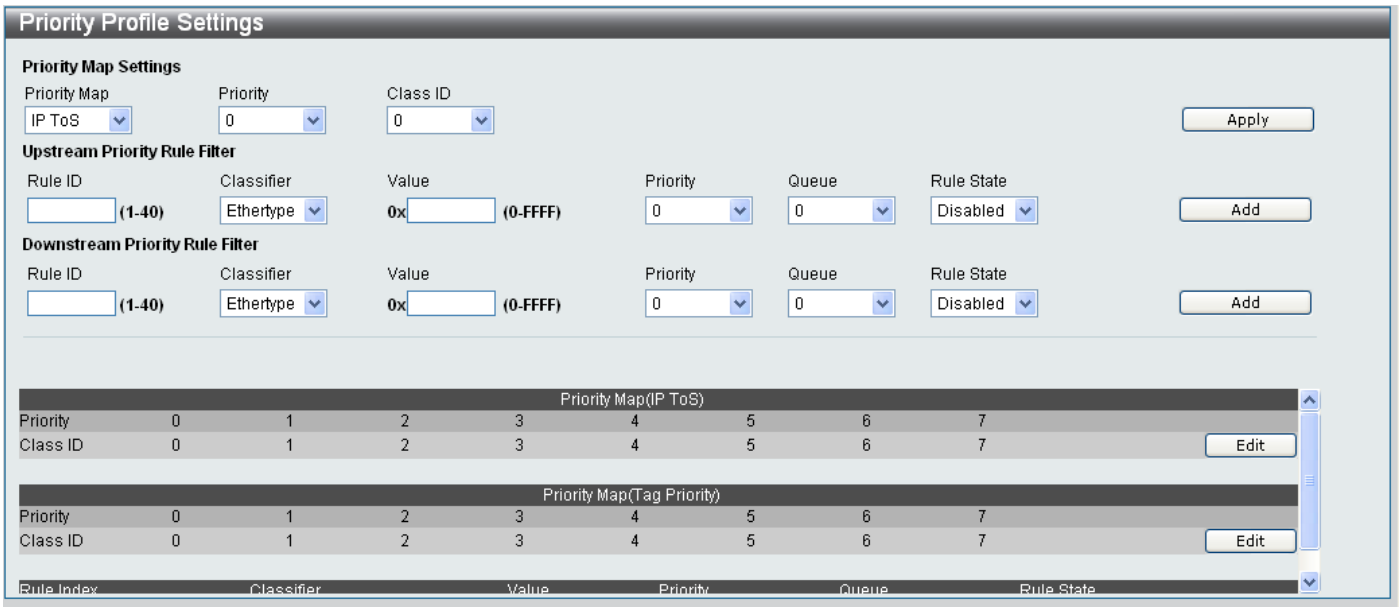


Figure 11- 53. Editing an existing Priority Profile

3. The window is divided into four main sections, *Priority Map Settings, Upstream Priority Rule Filter, Downstream Priority Rule Filter* and a table at the bottom of the screen, which shows the existing rules setup on the system.
4. Configure the *Priority Map Settings* parameters as described below:

Parameter	Description
Priority Map	Use the drop-down menu to create an *IP ToS* or *Tag Priority* mapping rule.
Priority	Use the drop-down menu to choose a *Priority* value for the *IP ToS* or *Tag Priority*.
Class ID	Use the drop-down menu to select the priority queue number for holding the packet.

5. Configure the *Upstream Priority Rule Filter* parameters as described below:

Parameter	Description
Rule ID	Type an identity number to identify the Upstream Priority Rule Filter setting.
Classifier	Use the drop-down menu to choose *VID*, *IPv4* or *Ethertype* as the classifier.
Value	If choosing *Ethertype* from the **Classifier** drop-down menu, type in the hexadecimal of the frame, in the textbox. If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type the IPv4 protocol number you want to use between *1* and *255*. If choosing *Source TCP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source TCP Port number. If choosing *Source UDP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source UDP Port number. If choosing *Source IP* from the **Classifier** drop-down menu, type in the *IP address* of the Source host. If choosing *Destination IP* from the **Classifier** drop-down menu, type in the *IP address* of the Destination host.
Priority	Use the drop-down menu to select the priority used in the VLAN tag of the packet.

Queue	Use the drop-down menu to specify the priority queue used for holding the packet.
Rule State	Choose *Enabled* from the drop-down menu to enable the Upstream Priority Rule Filter setting. Choose *Disabled* to disable.

6. Configure the *Downstream Priority Rule Filter* parameters as described below:

Parameter	Description
Rule ID	Type an identity number to identify the Downstream Priority Rule Filter setting.
Classifier	Use the drop-down menu to choose *VID*, *IPv4* or *Ethertype* as the classifier.
Value	If choosing *Ethertype* from the **Classifier** drop-down menu, type in the hexadecimal of the frame, in the textbox. If choosing *VID* from the **Classifier** drop-down menu, type a new VID value in the textbox. If choosing *IPv4* from the **Classifier** drop-down menu, type the IPv4 protocol number you want to use between *1* and *255*. If choosing *Source TCP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source TCP Port number. If choosing *Source UDP* from the **Classifier** drop-down menu, type a value between *1* and *65535* that represents the Source UDP Port number. If choosing *Source IP* from the **Classifier** drop-down menu, type in the *IP address* of the Source host. If choosing *Destination IP* from the **Classifier** drop-down menu, type in the *IP address* of the Destination host.
Priority	Use the drop-down menu to select the priority used in the VLAN tag of the packet.
Queue	Use the drop-down menu to specify the priority queue used for holding the packet.
Rule State	Choose *Enabled* from the drop-down menu to enable the Downstream Priority Rule Filter setting. Choose *Disabled* to disable.

Deleting an Existing Priority Profile

1. Click the **Delete** button next to the *Priority Profile* that you want to delete.
2. A **Success** message indicates the Priority Profile was deleted successfully.

Appendix A

Technical Specifications

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z 1000BASE-T (SFP "Mini GBIC") IEEE 802.1D Spanning Tree IEEE 802.1W Rapid Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation
Protocols	CSMA/CD
Data Transfer Rates:	Half-duplex Full-duplex
Ethernet	10 Mbps 20Mbps
Fast Ethernet	100Mbps 200Mbps
Gigabit Ethernet	n/a 2000Mbps
Fiber Optic	SFP (Mini GBIC) Support IEEE 802.3z 1000BASE-LX (DEM-310GT transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT transceiver) IEEE 802.3u 100BASE-FX (DEM-211 transceiver (100FX_LC MM 2Km)) IEEE 802.3u 100BASE-FX (DEM-210 transceiver (100 FX_LC SM 15Km))
Topology	Star
Network Cables	Cat.5 Enhanced for 1000BASE-T UTP Cat.5, Cat. 5 Enhanced for 100BASE-TX UTP Cat.3, 4, 5 for 10BASE-T EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)
Number of Ports	24 10/100 Mbps ports 2 combo 1000Base-T/SFP ports (DHS-3628/DHS-3628DC) 2 100BASE-FX SFP ports (DHS-3628F) 2 1000Base-T copper ports

Physical and Environmental

Internal Power Supply	AC Input: 100 – 240 VAC, 50/60 Hz
Power Consumption	24 watts maximum
DC Fan	60 x 60 x 18 mm fan
Operating Temperature	0 - 40°C
Storage Temperature	-40 - 70°C
Humidity	5 - 95% non-condensing
Dimensions	441 mm x 310 mm x 44 mm
Weight	5614 g

Performance

Transmission Method	Store-and-forward
Packet Buffer	32 MB per device
Packet Filtering/Forwarding Rate	14,881 pps (10M port) 148.810 pps (100M port) 1,488,100 pps (1Gbps port)
MAC Address Learning	Automatic update. Supports 16K MAC address.
Priority Queues	8 Priority Queues per port.
Forwarding Table Age Time	Max age: 10-1000000 seconds. Default = 300.

Appendix B

Cables and Connectors

When connecting the Switch to the control port, a straight through cable is necessary. Please review these products for matching cable pin assignment.

The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments for a gigabit Internet Connection.

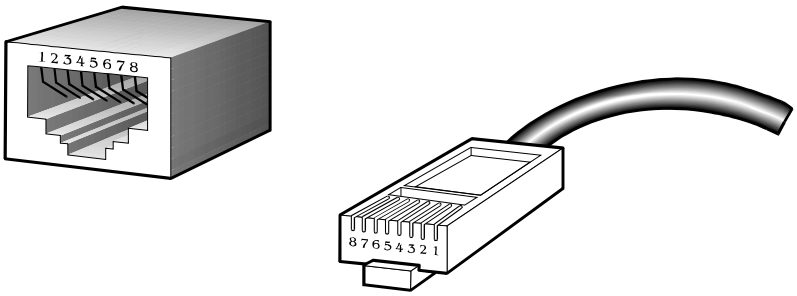


Figure B- . The standard RJ-45 port and connector

Gigabit Ethernet RJ-45 Pin Assignments		
Contact	MDI-X Port	MDI-II Port
1	BI_DB+	BI_DA +
2	BI_DB-	BI_DA -
3	BI_DA +	BI_DB+
4	BI_DD+	BI_DC+
5	BI_DD-	BI_DC-
6	BI_DA -	BI_DB-
7	BI_DC+	BI_DD+
8	BI_DC-	BI_DD-

Table B- . The standard RJ-45 pin assignments

Appendix C

Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

Standard	Media Type	Maximum Distance
Mini-GBIC	100BASE-FX, Multi-mode fiber module 100BASE-FX, Single-mode fiber module 1000BASE-LX, Single-mode fiber module 1000BASE-SX, Multi-mode fiber module 1000BASE-LHX, Single-mode fiber module 1000BASE-ZX, Single-mode fiber module	2km 15km 10km 550m 40km 80km
1000BASE-T	Category 5e UTP Cable Category 5 UTP Cable (1000 Mbps)	100m
100BASE-FX	Multi-mode 2KM Single-mode cable for Max.	2km 15Km
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

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 manual, 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.

Warnung!

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

Precaución!

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

Attention!

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

Attenzione!

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

BSMI Warning

警告使用者
這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,
在這種情況下使用者會被要求採取某些適當的對策

Warranties/Registration

LIMITED WARRANTY

D-Link provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor. D-Link would fulfill the warranty obligation according to the local warranty policy in which you purchased our products.

Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period") if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

Product Type	***Warranty Period***
Product (including Power Supplies and Fans)	One (1) Year
Spare parts and spare kits	Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion may replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:

Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same. The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided. 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 packaged product shall be insured and shipped to Authorized D-Link Service Office with all shipping costs prepaid. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

This limited warranty provided by D-Link does not cover:

Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed;

Initial installation, installation and removal of the product for repair, and shipping costs;

Operational adjustments covered in the operating manual for the product, and normal maintenance;

Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; and

Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE,

COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks

Copyright Statement

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/ TV technician for help.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum 20cm between the radiator and your body.

Tech Support

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the service period, and warranty confirmation service, during the warranty period on this product. U.S. and Canadian customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 354-6555

Monday to Friday 8:00am to 5:00pm PST

D-Link Technical Support over the Internet:

http://support.dlink.com

email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

1-800-361-5265

Monday to Friday 7:30am to 9:00pm EST

D-Link Technical Support over the Internet:

http://support.dlink.com

email: support@dlink.ca

D-Link®

Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link websites.

If you require product support, we encourage you to browse our FAQ section on the Web Site before contacting the Support line. We have many FAQ's which we hope will provide you a speedy resolution for your problem.

D-Link UK & Ireland Technical Support over the Telephone:

United Kingdom

08456 12 0003

BT 3ppm peak, 1.5ppm off peak, 0.5ppm weekends. (UK Pence per mintue). Other carriers could be lower.

Times Mon-Fri 9.00am - 6.00pm Sat 10.00am - 2.00pm

Ireland

+1890 886 899

€0.05ppm peak, €0.045ppm off peak

Times Mon-Fri 9.00am - 6.00pm Sat 10.00am - 2.00pm

D-Link UK & Ireland Technical Support over the Internet:

Web: http://www.dlink.co.uk

E-mail: ftp://ftp.dlink.co.uk

D-Link®

Building Networks for People

Technische Unterstützung

Aktualisierte Versionen von Software und Benutzerhandbuch finden Sie auf der Website von D-Link.

D-Link bietet kostenfreie technische Unterstützung für Kunden innerhalb Deutschlands, Österreichs, der Schweiz und Osteuropas.

Unsere Kunden können technische Unterstützung über unsere Website, per E-Mail oder telefonisch anfordern.

Telefon: +49 (1805)2787

0,14€ pro Minute

Web: http://www.dlink.de

E-Mail: support@dlink.de

D-Link®

Building Networks for People

Assistance technique

Vous trouverez la documentation et les logiciels les plus récents sur le site web D-Link.

Vous pouvez contacter le service technique de

D-Link par notre site internet ou par téléphone.

Assistance technique D-Link par téléphone:

0 820 0803 03

0,12 €/min

Hours : Monday - Friday 9h to 13h and 14h to 19h

Saturday 9h to 13h and from 14h to 16h

Assistance technique D-Link sur internet :

Web: http://www.dlink.fr

E-mail: support@dlink.fr

D-Link®

Building Networks for People

Asistencia Técnica

Puede encontrar las últimas versiones de software así como documentación técnica en el sitio web de D-Link.

D-Link ofrece asistencia técnica gratuita para clientes residentes en España durante el periodo de garantía del producto.

Asistencia Técnica de D-Link por teléfono:

+34 902 30 45 45

0,067 €/min

Lunes a Viernes de 9:00 a 14:00 y de 15:00 a 18:00

Web: http://www.dlink.es

E-mail: soporte@dlink.es

D-Link®

Building Networks for People

Supporto tecnico

Gli ultimi aggiornamenti e la documentazione sono disponibili sul sito D-Link.

Supporto Tecnico dal lunedì al venerdì dalle ore 9.00 alle ore 19.00 con orario continuato

Telefono: 199400057

Web: http://www.dlink.it/support

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within Benelux for the duration of the warranty period on this product.

Benelux customers can contact D-Link technical support through our website, or by phone.

Netherlands

0900 501 2007

€0.15ppm anytime

Web: www.dlink.nl

Belgium

070 66 06 40

€0.175ppm peak, €0.0875ppm off peak

Web: www.dlink.be

Luxemburg

+32 70 66 06 40

Web: www.dlink.be

D-Link®

Building Networks for People

Pomoc techniczna

Najnowsze wersje oprogramowania i dokumentacji użytkownika można znaleźć w serwisie internetowym firmy D-Link.

D-Link zapewnia bezpłatną pomoc techniczną klientom w Polsce w okresie gwarancyjnym produktu.

Klienci z Polski mogą się kontaktować z działem pomocy technicznej firmy D-Link za pośrednictwem Internetu lub telefonicznie.

Telefoniczna pomoc techniczna firmy D-Link:

0 801 022 021

Pomoc techniczna firmy D-Link świadczona przez Internet:

Web: http://www.dlink.pl

E-mail: dlink@fixit.pl

D-Link®

Building Networks for People

Technická podpora

Aktualizované verze software a uživatelských příruček najdete na webové stránce firmy D-Link.

D-Link poskytuje svým zákazníkům bezplatnou technickou podporu

Zákazníci mohou kontaktovat oddělení technické podpory přes webové stránky, mailem nebo telefonicky

Telefon: 225 281 553

Land Line 1,78 CZK/min - Mobile 5.40 CZK/min

Telefonická podpora je v provozu: PO- PÁ od 09.00 do 17.00

Web: http://www.dlink.cz/suppport/

E-mail: support@dlink.cz

D-Link®

Building Networks for People

Technikai Támogatás

Meghajtó programokat és frissítéseket a D-Link Magyarország weblapjáról tölthet le.

Tel: 06 1 461-3001

Fax: 06 1 461-3004

Land Line 14,99 HUG/min - Mobile 49.99,HUF/min

Web: http://www.dlink.hu

E-mail: support@dlink.hu

D-Link®

Building Networks for People

Teknisk Support

Du kan finne programvare oppdateringer og bruker dokumentasjon på D-Links web sider.
D-Link tilbyr sine kunder gratis teknisk support under produktets garantitid.
Kunder kan kontakte D-Links teknisk support via våre hjemmesider, eller på tlf.

D-Link Teknisk telefon Support:
800 10 610
(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett:
Web: http://www.dlink.no

D-Link®
Building Networks for People

Teknisk Support

Du finder software opdateringer og bruger-
dokumentation på D-Link's hjemmeside.

D-Link tilbyder gratis teknisk support til kunder
i Danmark i hele produktets garantiperiode.

Danske kunder kan kontakte D-Link's tekniske
support via vores hjemmeside eller telefonisk.

D-Link teknisk support over telefonen:
Tlf. 7026 9040
Åbningstider: kl. 08:00 – 20:00

D-Link teknisk support på Internettet:
Web: http://www.dlink.dk

D-Link®
Building Networks for People

Teknistä tukea asiakkaille Suomessa

D-Link tarjoaa teknistä tukea asiakkailleen.

Tuotteen takuun voimassaoloajan.

Tekninen tuki palvelee seuraavasti:

numerosta : 0800-114 677

Arkisin klo. 9 - 21

Internetin kautta:

Web: http://www.dlink.fi

D-Link®

Building Networks for People

Teknisk Support

På vår hemsida kan du hitta mer information om mjukvaru uppdateringar och annan användarinformation.

D-Link tillhandahåller teknisk support till kunder i Sverige under hela garantitiden för denna produkt.

D-Link Teknisk Support via telefon:

0770-33 00 35

Vardagar 08.00-20.00

D-Link Teknisk Support via Internet:

Web: http://www.dlink.se

Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de utilizador no site de D-Link Portugal http://www.dlink.pt.

A D-Link fornece suporte técnico gratuito para clientes no Portugal durante o período de vigência de garantia deste produto.

Assistência Técnica da D-Link na Internet:

Web: http://www.dlink.pt

E-mail: soporte@dlink.es

D-Link®

Building Networks for People

Τεχνική Υποστήριξη

Μπορείτε να βρείτε software updates και πληροφορίες για τη χρήση των προϊόντων στις ιστοσελίδες της D-Link

Η D-Link προσφέρει στους πελάτες της δωρεάν υποστήριξη

στον Ελλαδικό χώρο

Μπορείτε να επικοινωνείτε με το τμήμα τεχνικής υποστήριξης μέσω της ιστοσελίδας ή μέσω τηλεφώνου

D-Link Hellas Support Center

Κεφαλληνίας 64, 11251 Αθήνα,

Τηλ: 210 86 11 114 (Δευτέρα- Παρασκευή 09:00-17:00)

Φαξ: 210 8611114

Web: http://www.dlink.gr/support

D-Link®

Building Networks for People

Tehnička podrška

Hvala vam na odabiru D-Link proizvoda. Za dodatne informacije, podršku i upute za korištenje uređaja, molimo vas da posjetite D-Link internetsku stranicu na www.dlink.eu

Web: www.dlink.biz/hr

D-Link®
Building Networks for People

Tehnična podpora

Zahvaljujemo se vam, ker ste izbrali D-Link proizvod. Za vse nadaljnje informacije, podporo ter navodila za uporabo prosimo obiščite D-Link - ovo spletno stran www.dlink.eu

Web: www.dlink.biz/sl

D-Link®
Building Networks for People

Suport tehnica

Vă mulțumim pentru alegerea produselor D-Link. Pentru mai multe informații, suport şi manuale ale produselor vă rugăm să vizitați site-ul D-Link www.dlink.eu

Web: www.dlink.ro


D-Link
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Australia:

Tel: 1300-766-868

Monday to Friday 8:00am to 8:00pm EST

Saturday 9:00am to 1:00pm EST

http://www.dlink.com.au

e-mail: support@dlink.com.au

India:

Tel: 1800-222-002

Monday to Friday 9:30AM to 7:00PM

http://www.dlink.co.in/support/productsupport.aspx

Indonesia, Malaysia, Singapore and Thailand:

Tel: +62-21-5731610 (Indonesia)

Tel: 1800-882-880 (Malaysia)

Tel: +65 66229355 (Singapore)

Tel: +66-2-719-8978/9 (Thailand)

Monday to Friday 9:00am to 6:00pm

http://www.dlink.com.sg/support/

e-mail: support@dlink.com.sg

Korea:

Tel: +82-2-890-5496

Monday to Friday 9:00am to 6:00pm

http://www.d-link.co.kr

e-mail: lee@d-link.co.kr

New Zealand:

Tel: 0800-900-900

Monday to Friday 8:30am to 8:30pm

Saturday 9:00am to 5:00pm

http://www.dlink.co.nz

e-mail: support@dlink.co.nz

D-Link®

Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Egypt:

Tel: +202-2919035 or +202-2919047

Sunday to Thursday 9:00am to 5:00pm

http://support.dlink-me.com

e-mail: amostafa@dlink-me.com

Iran:

Tel: +98-21-88822613

Sunday to Thursday 9:00am to 6:00pm

http://support.dlink-me.com

e-mail: support.ir@dlink-me.com

Israel:

Tel: +972-9-9715701

Sunday to Thursday 9:00am to 5:00pm

http://www.dlink.co.il/support/

e-mail: support@dlink.co.il

Pakistan:

Tel: +92-21-4548158 or +92-21-4548310

Sunday to Thursday 9:00am to 6:00pm

http://support.dlink-me.com

e-mail: support.pk@dlink-me.com

South Africa and Sub Sahara Region:

Tel: +27-12-665-2165

08600 DLINK (for South Africa only)

Monday to Friday 8:30am to 9:00pm South Africa Time

http://www.d-link.co.za

Turkey:

Tel: +90-212-2895659

Monday to Friday 9:00am to 6:00pm

http://www.dlink.com.tr

e-mail: turkiye@dlink-me.com

e-mail: support@d-link.co.za

U.A.E and North Africa:

Tel: +971-4-391-6480 (U.A.E)

Sunday to Wednesday 9:00am to 6:00pm GMT+4

Thursday 9:00am to 1:00pm GMT+4

http://support.dlink-me.com

e-mail: support@dlink-me.com

D-Link®

Building Networks for People

Техническая поддержка

Обновления программного обеспечения и документация доступны на Интернет-сайте D-Link.

D-Link предоставляет бесплатную поддержку для клиентов в течение гарантийного срока.

Клиенты могут обратиться в группу технической поддержки D-Link по телефону или через Интернет.

Техническая поддержка D-Link:

+495-744-00-99

Техническая поддержка через Интернет

http://www.dlink.ru

e-mail: support@dlink.ru

D-Link®

Building Networks for People

Asistencia Técnica

D-Link Latin América pone a disposición de sus clientes, especificaciones, documentación y software mas reciente a través de nuestro Sitio Web

www.dlinkla.com

El servicio de soporte técnico tiene presencia en numerosos países de la Región Latino América, y presta asistencia gratuita a todos los clientes de D-Link, en forma telefónica e internet, a través de la casilla

soporte@dlinkla.com

Soporte Técnico Help Desk Argentina:

TTeléfono: 0800-12235465 Lunes a Viernes 09:00 am a 22:00 pm

Soporte Técnico Help Desk Chile:

Teléfono: 800 8 35465 Lunes a Viernes 08:00 am a 21:00 pm

Soporte Técnico Help Desk Colombia:

Teléfono: 01800-9525465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Ecuador:

Teléfono: 1800-035465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk El Salvador:

Teléfono: 800-6335 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Guatemala:

Teléfono: 1800-8350255 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Panamá:

Teléfono: 00800 0525465 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk Costa Rica:

Teléfono: 0800 0521478 Lunes a Viernes 06:00 am a 19:00 pm

Soporte Técnico Help Desk Perú:

Teléfono: 0800-00968 Lunes a Viernes 07:00 am a 20:00 pm

Soporte Técnico Help Desk México:

Teléfono: 001 800 123-3201 Lunes a Viernes 06:00 am a 19:00

Soporte Técnico Help Desk Venezuela:

Teléfono: 0800-1005767 Lunes a Viernes 08:00 am a 21:00 pm

D-Link®

Building Networks for People

Suporte Técnico

Você pode encontrar atualizações de software e documentação de usuário no site da D-Link Brasil www.dlinkbrasil.com.br.

A D-Link fornece suporte técnico gratuito para clientes no Brasil durante o período de vigência da garantia deste produto.

Suporte Técnico para clientes no Brasil:

Telefone

São Paulo +11-2185-9301

Segunda à sexta

Das 8h30 às 18h30

Demais Regiões do Brasil 0800 70 24 104

E-mail:

e-mail: suporte@dlinkbrasil.com.br

D-Link®
Building Networks for People

D-Link 友訊科技 台灣分公司

技術支援資訊

如果您還有任何本使用手冊無法協助您解決的產品相關問題，台灣地區用戶可以透過我們的網站、電子郵件或電話等方式與 D-Link台灣地區技術支援工程師聯絡。

D-Link 免付費技術諮詢專線
0800-002-615
服務時間：週一至週五，早上8:30 到 晚上9:00
(不含周六、日及國定假日)

網 站：http://www.dlink.com.tw
電子郵件：dssqa_service@dlink.com.tw

如果您是台灣地區以外的用戶，請參考D-Link網站 全球各地分公司的聯絡資訊以取得相關支援服務。

產品保固期限、台灣區維修據點查詢，請參考以下網頁說明：
http://www.dlink.com.tw

D-Link®
Building Networks for People

Dukungan Teknis

Update perangkat lunak dan dokumentasi pengguna dapat diperoleh pada situs web D-Link.

Dukungan Teknis untuk pelanggan:

Dukungan Teknis D-Link melalui telepon:

Tel: +62-21-5731610

Dukungan Teknis D-Link melalui Internet:

Email : support@dlink.co.id

Website : http://support.dlink.co.id

D-Link®

Building Networks for People

技术支持

您可以在 D-Link 的官方網站找到產品的軟件升級和使用手冊

办公地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座 26F 02-05 室 邮编: 100013

技术支持中心电话：8008296688/ (028)66052968

技术支持中心传真：(028)85176948

维修中心地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座 26F 02-05 室 邮编: 100013

维修中心电话：(010) 58257789

维修中心传真：(010) 58257790

网址：http://www.dlink.com.cn

办公时间：周一到周五，早09:00到晚18:00

D-Link®

Building Networks for People

D-Link International Offices

U.S.A

17595 Mt. Herrmann Street
Fountain Valley, CA 92708, USA
TEL: 1-800-326-1688
URL: www.dlink.com

Canada

2180 Winston Park Drive
Oakville, Ontario, L6H 5W1, Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)

D-Link House,
1 Abbey Road, Park Royal,
London NW10 7BX, U.K.
TEL: 44-20-8955-9000
FAX: 44-20-8955-9002
URL: www.dlink.co.uk

Germany

Schwalbacher Strasse 74
D-65760 Eschborn, Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France

41 boulevard Vauban
78280 Guyancourt
France
TEL: 00 33 1 30 23 86 88
FAX: 00 33 1 30 23 86 89
URL: www.dlink.fr

Netherlands

Weena 290
3012 NJ Rotterdam, Netherlands
Tel: +31-10-282-1445
FAX: +31-10-282-1331
URL: www.dlink.nl

Belgium

Rue des Colonies 11
B-1000 Brussels, Belgium
Tel: +32(0)2 517 7111
FAX: +32(0)2 517 6500
URL: www.dlink.be

Italy

Via Nino Bonnet n. 6/b
20154 – Milano, Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden

P.O. Box 15036, S-167 15 Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark

Naverland 2, DK-2600
Glostrup, Copenhagen,
TEL: 45-43-969040
FAX: 45-43-424347
URL:www.dlink.dk

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

Finland

Latokartanontie 7A
FIN-00700 Helsinki, Finland
TEL : +358-10-309 8840
FAX: + 358-10-309 8841
URL: www.dlink.fi

Spain

Avenida Diagonal, 593-95, 9th floor
08014 Barcelona, Spain
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlink.es

Portugal

Rua Fernando Pahla
50 Edificio Simol
1900 Lisbon, Portugal
TEL: 351 21 8688493
URL: www.dlink.es

Czech Republic

Vaclavske namesti 36, Praha 1
Czech Republic
TEL: +420 (603) 276 589
URL: www.dlink.cz

Switzerland

Glatt Tower, 2.OG CH-8301
Glattzentrum Postfach 2.OG
Switzerland
TEL: +41 (0) 1 832 11 00
FAX:+41 (0) 1 832 11 01
URL: www.dlink.ch

Greece

101, Panagoulis Str. 163-43
Heliopolis, Athens, Greece
TEL: +30 210 9914512
FAX:+30 210 9916902
URL: www.dlink.gr

Luxembourg

Rue des Colonies 11
B-1000 Brussels, Belgium
TEL: +32 (0)2 517 7111
FAX:+32 (0)2 517 6500
URL: www.dlink.be

Poland

Budynek Aurum ul. Walic-w11
PL-00-851
Warszawa, Poland
TEL: +48 (0) 22 583 92 75
FAX:+48 (0) 22 583 92 76
URL: www.dlink.pl

Hungary

R-k-czi-t 70-72
HU-1074
Budapest, Hungary
TEL: +36 (0) 1 461 30 00
FAX:+36 (0) 1 461 30 09
URL: www.dlink.hu

Singapore

1 International Business Park
#03-12 The Synergy, Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia

1 Giffnock Avenue,
North Ryde, NSW 2113, Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India

D-Link House, Kurla Bandra Complex Road,
Off CST Road, Santacruz (East), Mumbai – 400098, India
TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)

P.O.Box: 500376, Office No.:103, Building:3
Dubai Internet City, Dubai, United Arab Emirates
TEL:+971-4-3916480
FAX:+971-4-3908881
URL: www.dlink-me.com

Turkey

Ayazaga Maslak Yolu, Erdebil Cevahir Is Merkezi
5/A Ayazaga, Istanbul, Turkiye
TEL: +90 212 289 56 59
FAX: +90 212 289 76 06
URL: www.dlink.com.tr

Egypt

19 El-Shahed Helmy, El Masri, Al-Maza, Heliopolis
Cairo, Egypt
TEL:+202 414 4295
FAX:+202 415 6704
URL: www.dlink-me.com

Israel

11 Hamanofim Street, Ackerstein Towers,
Regus Business Center, P.O.Box 2148,
Hertzelia-Pituach 46120, Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

Latin America

Isidora Goyeechea 2934, Ofcina 702,
Las Condes, Santiago, Chile
TEL: 56-2-583-8950
FAX: 56-2-232-0923
URL: www.dlink.cl

Brasil

Av das Nacoes Unidas, 11857 - 14 - andar - cj 141/142
Brooklin Novo, Sao Paulo - SP – Brazil, CEP 04578-000
TEL: (55 11) 21859300
FAX: (55 11) 21859322
URL: www.dlinkbrasil.com.br

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

Russia

Grafsky per., 14, floor 6, Moscow, 129626 Russia
TEL: 7-495-744-0099
FAX: 7-495-744-0099 #350
URL: www.dlink.ru

China

No.202, C1 Building, Huitong Office Park,
No.71, Jianguo Road, Chaoyang District, Beijing,
100025, China
TEL +86-10-58635800
FAX: +86-10-58635799
URL: www.dlink.com.cn

Taiwan

No. 289, Sinhu 3rd Rd., Neihu District,
Taipei City 114, Taiwan
TEL: 886-2-6600-0123
FAX: 886-2-6600-1188
URL: www.dlinktw.com.tw

Registration Card

(All Countries and Regions excluding USA)

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	* 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?

☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?

☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?

☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?

☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open

☐Banyan Vines ☐Windows NT ☐Windows ME ☐Windows 2000 ☐Windows XP

☐Others_____

5. What network management program does your organization use ?

☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS

☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?

☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP

☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM

☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing

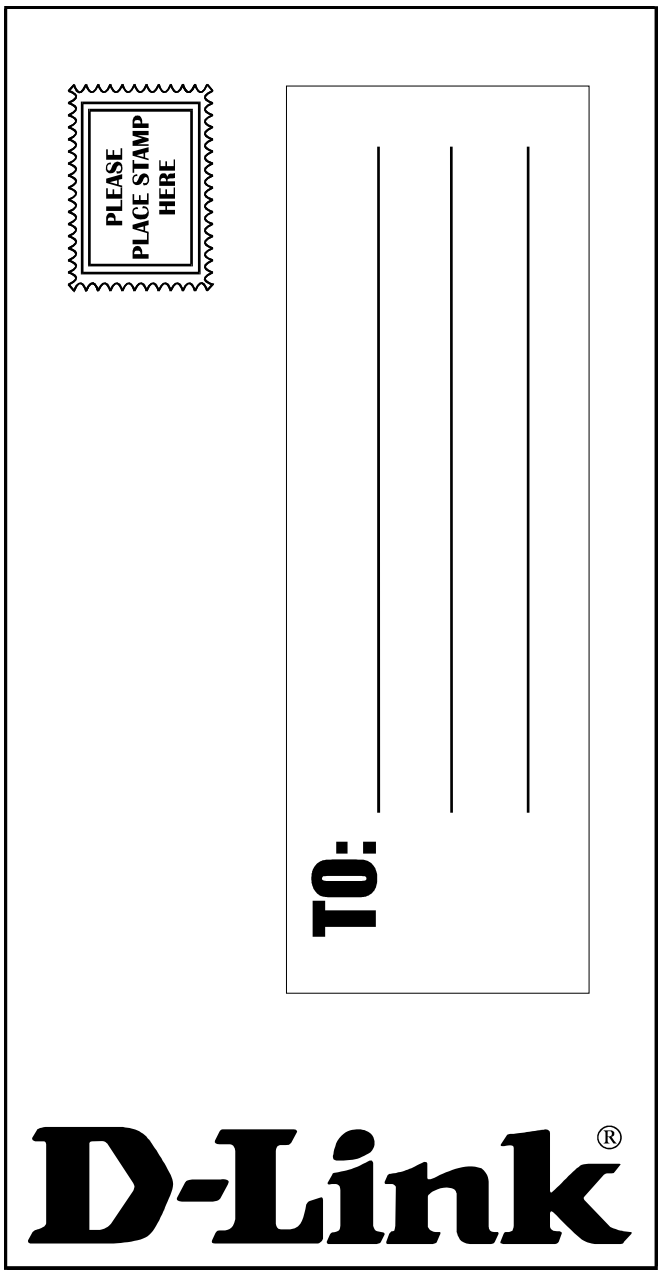
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR

☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10.Your comments on this product?


PLEASE
PLACE STAMP
HERE
TO:
D-Link®