

D-Link™ DGS-3024

Managed 24-Port Gigabit Ethernet Switch

Manual

Information in this document is subject to change without notice.

© 2005 D-Link Computer Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Computer Corporation is strictly forbidden.

Trademarks used in this text: *D-Link* and the *D-Link* logo are trademarks of D-Link Computer Corporation; *Microsoft* and *Windows* are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

FCC Warning

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

CE Mark Warning

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

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen 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 caso, 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.

VCCI Warning

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

March 2005 P/N 6DGS3024..02

Table of Contents

<i>Preface</i>	<i>ix</i>
Intended Readers.....	<i>ix</i>
Notes, Notices, and Cautions.....	<i>ix</i>
<i>Safety Instructions</i>	<i>xi</i>
Introduction	1
<i>Features</i>	<i>1</i>
Ports.....	<i>1</i>
Performance Features.....	<i>1</i>
Management.....	<i>1</i>
Unpacking and Setup	3
<i>Packing List</i>	<i>3</i>
<i>Installation</i>	<i>3</i>
Desktop or Shelf Installation.....	<i>4</i>
Rack Installation.....	<i>4</i>
<i>Power on</i>	<i>5</i>
Power Failure.....	<i>5</i>
<i>External Redundant Power System</i>	<i>5</i>
Identifying External Components	7
<i>Front Panel</i>	<i>7</i>
<i>Rear Panel</i>	<i>7</i>
<i>Side Panels</i>	<i>7</i>
<i>LED Indicators</i>	<i>8</i>
Connecting the Switch	9
<i>Switch to End Node</i>	<i>9</i>
<i>Switch to Hub or Switch</i>	<i>10</i>
<i>Switch to Core Router Switch</i>	<i>10</i>
Introduction to Switch Management	12
Management Options	12
<i>Web-based Management Interface</i>	<i>12</i>
<i>SNMP-Based Management</i>	<i>12</i>
<i>Command Line Console Interface Through the Serial Port</i>	<i>12</i>
Connecting the Console Port (RS-232 DCE).....	<i>12</i>
<i>First Time Connecting to The Switch</i>	<i>14</i>
<i>Password Protection</i>	<i>14</i>
<i>SNMP Settings</i>	<i>15</i>

Traps	16
MIBs	16
<i>IP Address Assignment</i>	16
<i>Connecting Devices to the Switch</i>	18
Web-Based Network Management	19
Introduction	19
Login to Web Manager	19
<i>Web-based User Interface</i>	20
<i>Areas of the User Interface</i>	20
Configuration	22
IP Address	22
Switch Information	23
Advanced Settings	24
Port Configuration	26
Port Mirroring	28
Link Aggregation (Port Trunking)	29
IGMP Snooping	31
<i>IGMP Snooping</i>	32
<i>Static Router Ports Entry</i>	33
Spanning Tree	34
802.1s MSTP.....	34
802.1w Rapid Spanning Tree.....	35
Port Transition States	35
Edge Port.....	36
P2P Port	36
802.1d/802.1w/802.1s Compatibility	36
<i>STP Bridge Global Settings</i>	36
<i>MST Configuration Table</i>	38
<i>MSTI Settings</i>	41
<i>STP Instance Settings</i>	43
<i>STP Port Settings</i>	46
Forwarding	48

<i>Unicast Forwarding</i>	48
<i>Multicast Forwarding</i>	48
VLANs	49
Understanding IEEE 802.1p Priority	49
VLAN Description.....	50
Notes About VLANs on the DGS-3024	50
IEEE 802.1Q VLANs	50
802.1Q VLAN Tags.....	52
Port VLAN ID.....	53
Tagging and Untagging.....	54
Ingress Filtering	54
Default VLANs.....	55
VLAN and Trunk Groups	55
<i>Static VLAN Entry</i>	55
<i>8021Q Port Settings</i>	57
SNTP Settings	59
<i>Time Setting</i>	59
<i>Time Zone and DST</i>	61
QoS	62
Advantages of QoS	63
Understanding QoS.....	63
<i>Traffic Control</i>	65
<i>802.1p Default Priority</i>	66
<i>802.1p User Priority</i>	67
<i>QoS Scheduling Mechanism</i>	67
<i>QoS Output Scheduling</i>	68
MAC Notification	68
<i>MAC Notification Global Settings</i>	68
<i>MAC Notification Port Settings</i>	69
System Log Server	71
Port Access Entity	73
802.1x Port-Based Access Control	73
Authentication Server	73
Authenticator.....	74
Client.....	75
Authentication Process.....	75
Port-Based Network Access Control	75
<i>Configure Authenticator</i>	76
<i>Local users</i>	79
<i>802.1x Capability Settings</i>	79
Initialize Port(s).....	81

Reauthenticate Port(s).....	82
<i>RADIUS Server</i>	83
Static ARP Settings.....	84
Security.....	85
Trusted Host.....	85
Secure Socket Layer (SSL).....	85
<i>Download Certificate</i>	86
<i>Configuration</i>	86
Secure Shell (SSH).....	88
<i>SSH Configuration</i>	88
<i>SSH Algorithm</i>	90
<i>SSH User Authentication</i>	92
Access Authentication Control.....	93
<i>Authentication Policy & Parameters</i>	94
<i>Application Authentication Settings</i>	95
<i>Authentication Server Group</i>	95
<i>Authentication Server Host</i>	97
<i>Login Method Lists</i>	98
<i>Enable Method Lists</i>	100
<i>Configure Local Enable Password</i>	102
<i>Enable Admin</i>	102
Management.....	104
User Accounts.....	104
Admin and User Privileges.....	105
SNMP Manager.....	106
<i>SNMP User Table</i>	107
<i>SNMP View Table</i>	108
<i>SNMP Group Table</i>	109
<i>SNMP Community Table</i>	111
<i>SNMP Host Table</i>	112
<i>SNMP Engine ID</i>	113
Monitoring.....	115

Port Utilization	115
Packets	116
<i>Received (RX)</i>	116
<i>UMB Cast (RX)</i>	118
<i>Transmitted (TX)</i>	120
Errors	121
<i>Received (RX)</i>	122
<i>Transmitted (TX)</i>	124
Size	126
MAC Address	128
Switch History Log	130
IGMP Snooping Group	132
IGMP Snooping Forwarding	133
VLAN Status	133
Router Port	134
Session Table	134
Port Access Control	135
<i>RADIUS Authentication</i>	135
Maintenance	136
TFTP Services	136
<i>Download Firmware</i>	136
<i>Download Configuration File</i>	136
<i>Save Settings</i>	137
<i>Save History Log</i>	137
Ping Test	137
Save Changes	138
Reboot Services	139
<i>Reboot</i>	139

<i>Reset</i>	139
<i>Reset Config</i>	140
<i>Reset System</i>	140
Logout	140
Technical Specifications	142
Cable Lengths	144
Glossary	145
Warranty and Registration Information	148
<i>Product Registration</i>	153

Preface

The *DGS-3024 Manual* is divided into chapters that describe the system installation and operating instructions with examples.

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

Section 2, “*Unpacking and Setup*” – Helps you get started with the basic installation of the Switch..

Section 3, “*Identifying External Components*” – Describes the front panel, rear panel, side panels, and LED indicators of the Switch.

Section 4, “*Connecting the Switch*” – Tells how you can connect the Switch to your Ethernet/Fast Ethernet network.

Section 5, “*Introduction to Switch Management*” – Introduces basic Switch management features, including password protection, SNMP settings, IP address assignment, and connecting devices to the Switch.

Section 6, “*Web-based Network Management*” – Talks about connecting to and using the Web-based Switch management feature on the Switch.

Section 7, “*Configuration*” – A detailed discussion about configuring some of the basic functions of the Switch, including accessing the Switch information, using the Switch's utilities and setting up network configurations, such as Quality of Service, Port Mirroring, and configuring the Spanning Tree.

Section 8, “*Security*” – Provides a description of the security features of the Switch, including Trusted Host, Secure Socket Layer (SSL), Secure Shell (SSH), and Access Authentication Control.

Section 9, “*Management*” – A discussion of the management features of the Switch, including User Accounts and SNMP.

Section 10, “*Monitoring*” – Features graphs and windows used in monitoring features and packets on the Switch.

Section 11, “*Maintenance*” – Features information on Switch utility functions, including TFTP Services, Ping History, Save Changes, Switch History, and Reboot Services.

Appendix A, “*Technical Specifications*” – The technical specifications of the DGS-3204.

Appendix B, “*Cable Lengths*” – Information on cable types and maximum distances.

Appendix C, “*Glossary*” – Lists definitions for terms and acronyms used in this document.

Intended Readers

The *DGS-3024 Manual* contains information for setup and management and of the DGS-3024 Switch. This guide is intended for network managers familiar with network management concepts and terminology.

Notes, Notices, and Cautions



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




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



CAUTION: 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 safety section, 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 the 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 a fire or an 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 selection Switch (if provided) 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.

Safety Instructions (continued)

- To help prevent an 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.



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 system/components in a rack, never 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 serious injury.

- 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.

Safety Instructions (continued)

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 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. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

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 and workbench pads and an antistatic grounding strap.

Battery Handling Reminder



CAUTION: This is danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Introduction

This section describes the features of the DGS-3024.

Features

The DGS-3024 was designed for departmental and enterprise connections. As an all-gigabit-port Switch, it is ideal for backbone and server connection. Powerful and versatile, the Switch eliminates network bottlenecks while giving users the capability to fine-tune performance

Switch features include:

Ports

- Twenty-four high performance 1000BASE-T ports for making 10/100/1000 connections to a backbone, end stations, and servers.
- Four mini-GBIC (SFP) combo ports to connect fiber optic media to another Switch, server or network backbone.
- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

Performance Features

- Store-and-forward Switching scheme.
- Switching fabric: 48Gbps
- Max. Forwarding Rate: 35.7 million packets per second
- High-speed data forwarding rate of 1,488,095 pps per port at 100% of wire-speed for 1000 Mbps speed.
- Supports 8K MAC address.
- Supports four priority queues per port.
- Supports 512Kbytes buffer memory per Switch.
- 802.1D Spanning Tree support. Can be disabled on the entire Switch or on a per-port basis.
- 802.1Q Tagged VLAN support, including GVRP (GARP VLAN Registration Protocol).
- Support for up to 255 VLANs.
- IGMP snooping support per Switch.
- Link aggregation support for up to four trunk groups and eight trunk members per group.
- Port-based 802.1x port access control.

Management

- RS-232 console port for out-of-band network management via a console terminal.
- Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops, including Multiple SpanningTree (MSTP) and Rapid Spanning Tree (RSTP).
- SNMP V.1, V2c1, and V3 network management, four groups of RMON.

- Flash memory for software upgrades. This can be done in-band via TFTP or out-of-band via the console.
- Built-in SNMP management:
 - Bridge MIB (RFC 1493)
 - MIB-II (RFC 1213)
 - 802.1P/Q MIB (RFC 2674)
 - Ethernet-like MIB (RFC 1643)
 - Private MIB
 - Mini-RMON MIB (RFC 1757) – four groups. The RMON specification defines the counters for the receive functions only. However, the DGS-3024 provides counters for both receive and transmit functions.
- Supports Web-based management.
- TFTP Client support.
- BOOTP Client support.
- DHCP Client support.
- Password enabled.
- Telnet remote control console.
- Broadcast storm control.
- Multicast storm control.
- Command Line Interface support.
- Syslog support.
- SNTP support.
- SNMP Trap on MAC Notification support.
- Jumbo frame support.
- SSH support.
- SSL support.
- TACACS+/RADIUS support.

Unpacking and Setup

This chapter provides unpacking and setup information for the Switch.

Packing List

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

- A DGS-3024 24-Port Gigabit Layer 2 Ethernet Switch
- A mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One or two AC power cords
- A printed Quick Installation Guide
- D-View 5.1 demo CD-ROM
- This Manual with Registration Card on CD-ROM

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

Installation

Use the following guidelines when choosing a place to install the Switch:

- The surface must support at least 4 kg.
- The power outlet should be within 1.82 meters (6 feet) of the device.
- Visually inspect the power cord and see that it is secured to the AC power connector.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Do not place heavy objects on the Switch.

Desktop or Shelf Installation

When installing the Switch on a desktop or shelf, the rubber feet included with the device should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow adequate space for ventilation between the device and the objects around it.

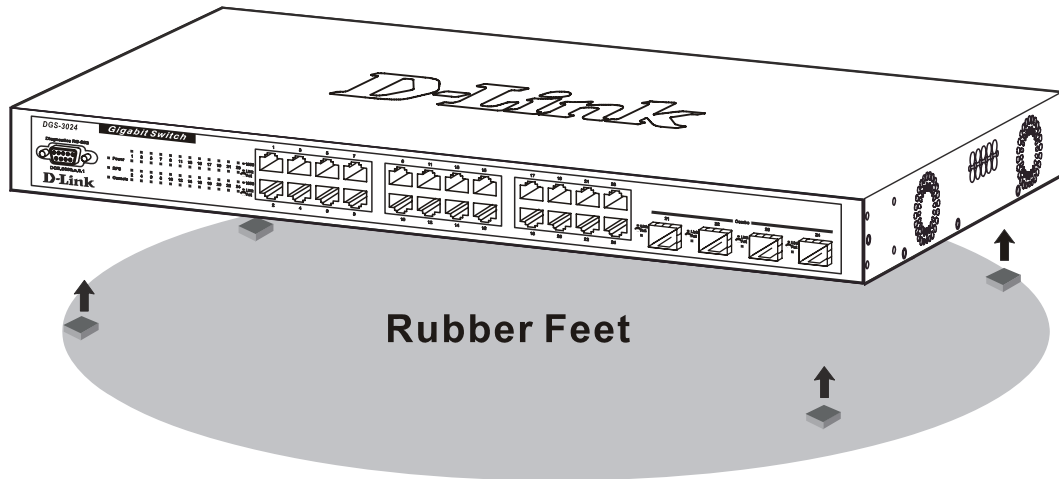


Figure 2-1. Installing rubber feet for desktop installation

Rack Installation

The DGS-3024 can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

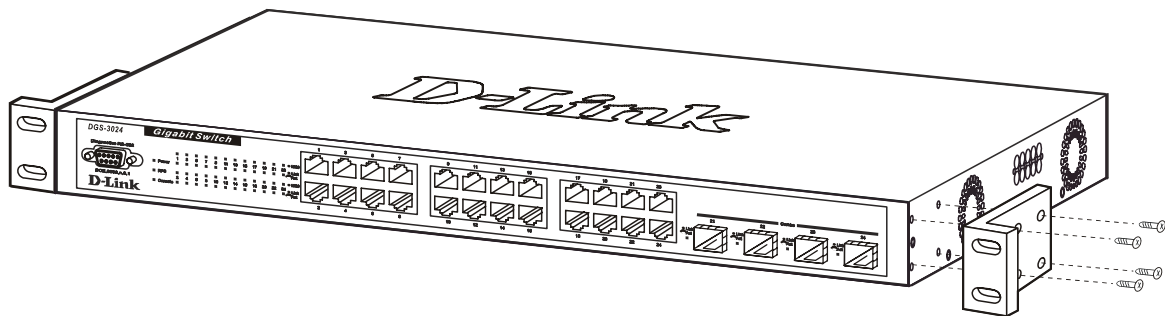


Figure 2- 2A. Attaching the mounting brackets

Then, use the screws provided with the equipment rack to mount the witch on the rack.

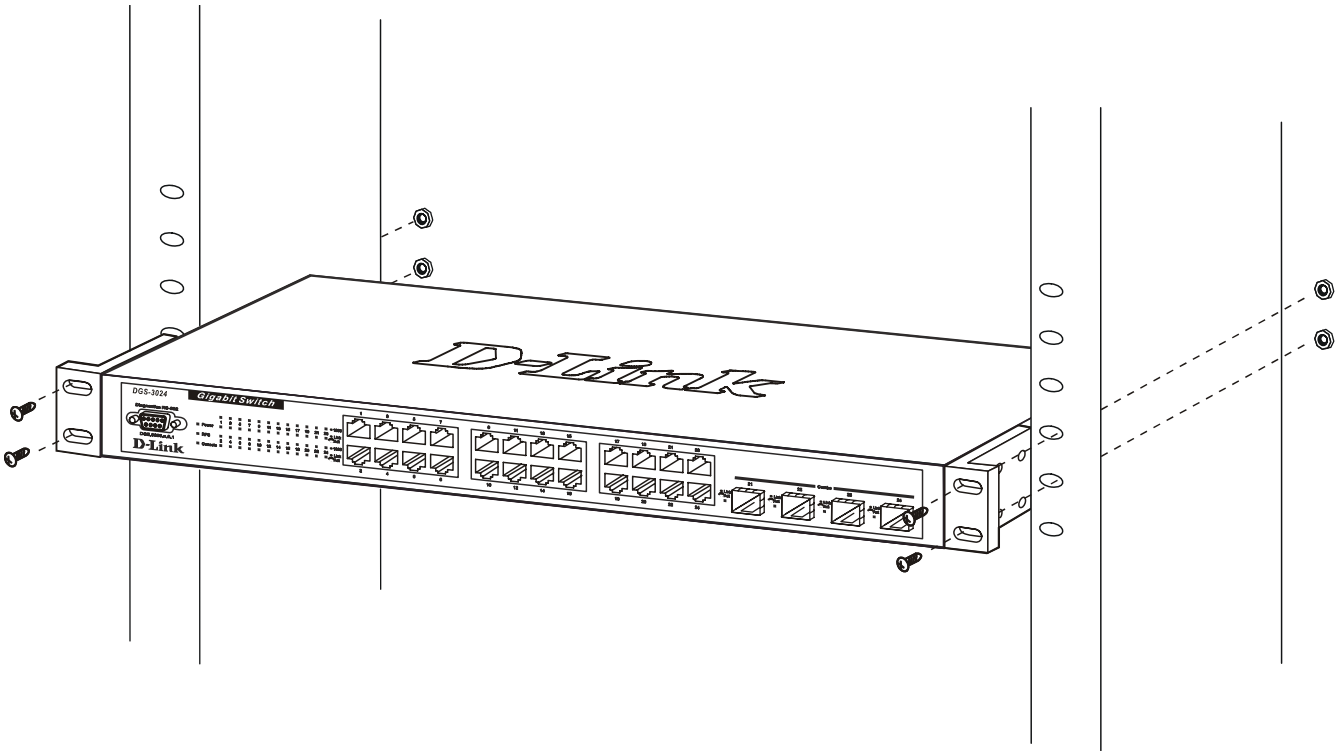


Figure 2- 2B. Installing in an equipment rack

Power on

The Switch can be used with AC power supply 100-240 VAC, 50 - 60 Hz. The Switch's power supply will adjust to the local power source automatically and may be powered on without having any or all LAN segment cables connected.

After the Switch is plugged in, the LED indicators should respond as follows:

- All LED indicators except console will momentarily blink. This blinking of the LEDs indicates a reset of the system.
- The console LED indicator will blink while the Switch loads onboard software and performs a self-test. When the POST is passed, the LED will become dark. If the POST fails, the indicator will light solid amber. This indicator lights solid green when the Switch is being logged-in via out-of-band/local console management through the RS-232 console port using a straight-through serial cable.

Power Failure

As a precaution in the event of a power failure, unplug the Switch. When power is resumed, plug the Switch back in.

External Redundant Power System

The Switch supports an external redundant power system.

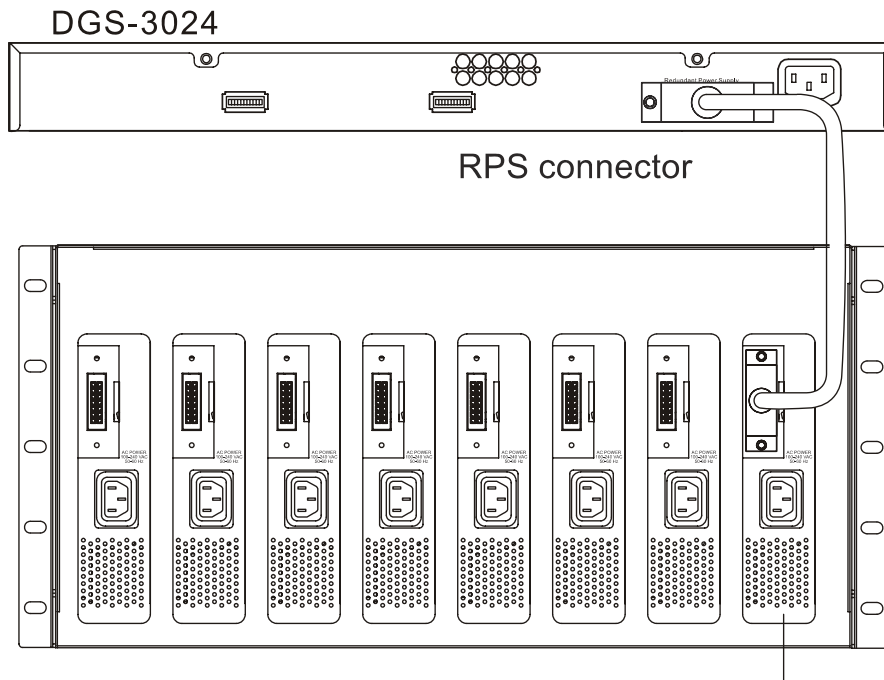


Figure 2-3. DPS-300 in DPS-900 case with DGS-3024

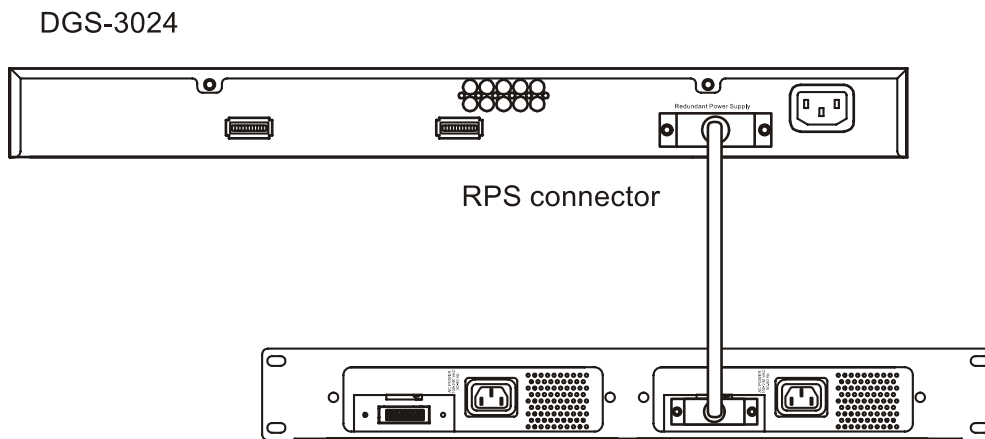


Figure 2-4. DPS-300 in DPS-800 case with DGS-3024



NOTE: See the DPS-300 documentation for more information.



CAUTION: Do not use the Switch with any redundant power system other than the DPS-300.

Identifying External Components

This chapter describes the front panel, rear panel, side panels, and LED indicators of the DGS-3024.

Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, 24 1000BASE-T ports, and four mini-GBIC combo ports.

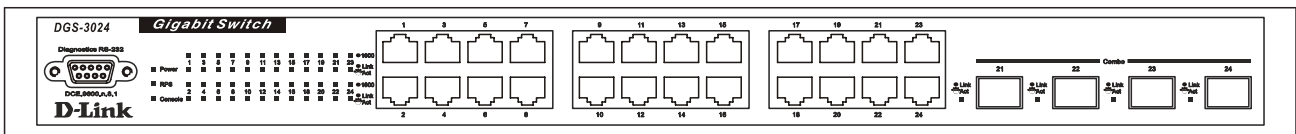


Figure 3-1. Front panel view

- An RS-232 DCE console port for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.
- Comprehensive LED indicators display the status of the Switch and the network (see the *LED Indicators* section below).
- Twenty-four 1000BASE-T Ethernet ports for 10/100/1000 connections to a backbone, end stations, and servers.
- Four mini-GBIC combo ports to connect fiber optic media to another Switch, server, core router Switch, or network backbone.

Rear Panel

The rear panel of the Switch contains an external Redundant Power Supply connector and an AC power connector.



Figure 3-2. Rear panel view

- The external Redundant Power Supply connector is used to connect the DGS-3024 to a DPS-300. An auto-Switch circuit automatically Switches to an external RPS once the internal power supply fails. Transition from internal to external supply shall not disturb normal operation.
- The AC power connector is a standard three-pronged connector that supports the power cord. Plug the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. Supported input voltages range from 100 ~ 240 VAC at 50 ~ 60 Hz.

Side Panels

The right side panel of the Switch contains two system fans (see the top part of the diagram below). The left side panel contains heat vents.

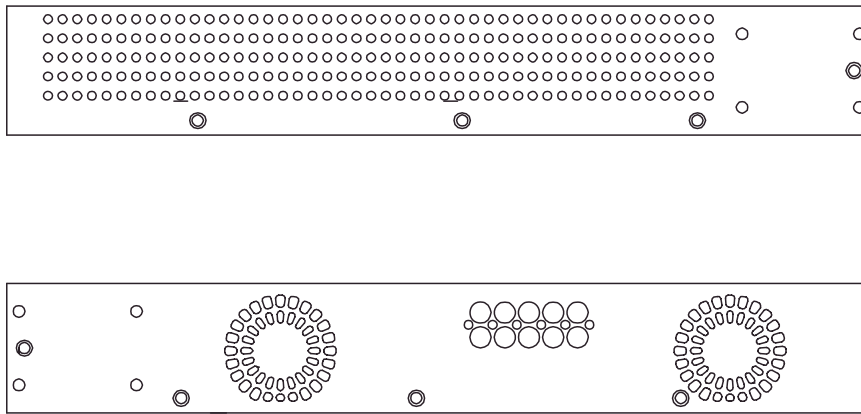


Figure 3-3. Side panel views of the Switch

- The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

LED Indicators

The LED indicators of the Switch include Power, Console, RPS, Speed, and Link/Activity. The following shows the LED indicators for the Switch along with an explanation of each indicator.

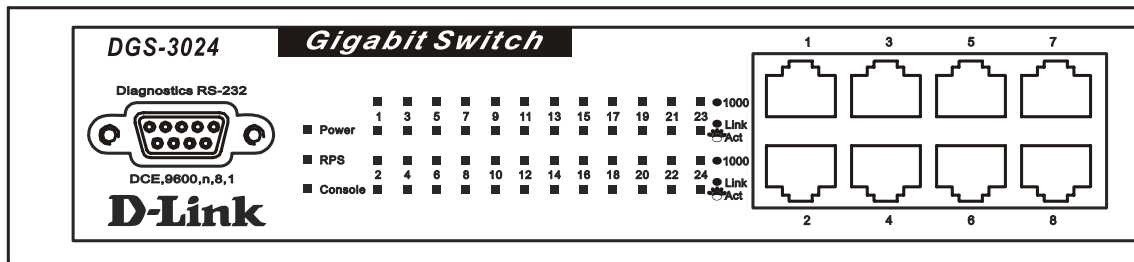


Figure 3-4. LED indicators

- **Power** – This indicator on the front panel lights solid green when the system is powered up and remains dark when the system is not powered on.
- **RPS** – This indicator is lit solid amber when the external Redundant Power Supply is in operation and remains dark when it is not in use or the main power is working normally.
- **Console** – This indicator blinks green when the system is booting up. It remains solid green when the system is operating properly. The LED is solid amber when the POST fails.
- **Speed** – This row of indicators will light solid green when the connection speed is operating at 1000 Mbps. An unlit LED indicates a connection speed of either 10 or 100 Mbps.
- **Link/Act** – This row of indicators for the 24 copper ports light solid green when there is a secure connection (or link) to a device on any of the ports. The LEDs blink green whenever there is reception or transmission (i.e. Activity--Act) of data occurring on a port.

Connecting the Switch

This chapter describes how to connect the DGS-3024 to your Gigabit Ethernet network.

Switch to End Node

End nodes include PCs outfitted with a 10, 100, or 1000 Mbps RJ-45 Ethernet/Fast Ethernet/Gigabit Ethernet Network Interface Card (NIC) and most routers.

An end node can be connected to the Switch via a Category 3, 4, 5, or 5e UTP/STP cable—for optimal performance, Category 5e is recommended. The end node should be connected to any of the ports of the Switch.

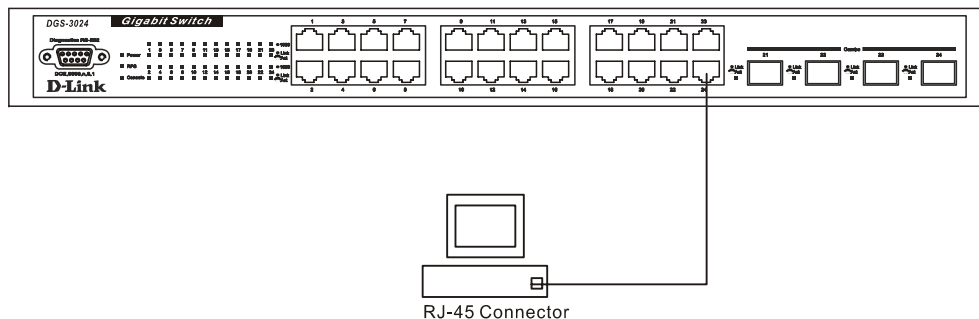


Figure 4- 1. Switch connected to an End Node

The Link/Act LEDs light green when the link is valid. A blinking green LED indicates packet activity on that port. The Speed LEDs indicate port speed and will light solid green for 1000 Mbps connections. They will remain off for 10 or 100 Mbps connections.

Switch to Hub or Switch

These connections can be accomplished in a number of ways using a normal cable.

- A 10BASE-T hub or Switch can be connected to the Switch via a two-pair Category 3, 4, 5, or 5e UTP/STP cable.
- A 100BASE-TX hub or Switch can be connected to the Switch via a two-pair Category 5 or 5e UTP/STP cable.
- A 1000BASE-T Switch can be connected to the Switch via four-pair straight Category 5 or 5e UTP/STP cable.

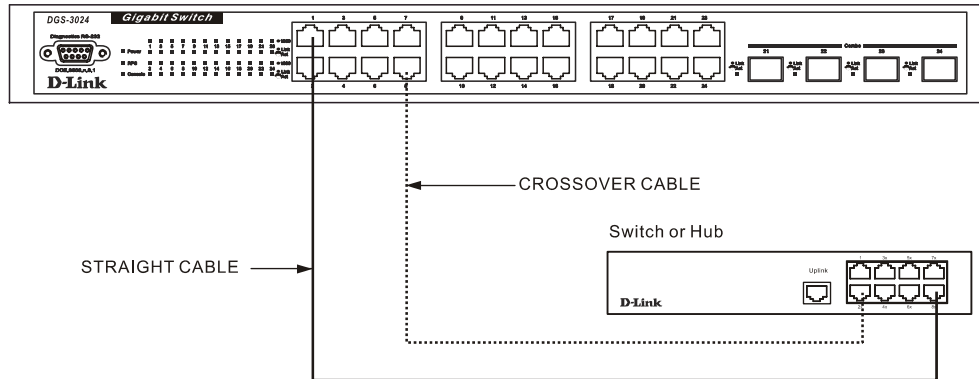


Figure 4- 2. Switch connected to a normal (non-Uplink) port on a hub or Switch using a straight or crossover cable

Switch to Core Router Switch

This connection can be accomplished using the following fiber optic media:

- SFP Transceiver for 1000BASE-LX Single-mode fiber module (10km)
- SFP Transceiver for 1000BASE-SX Multi-mode fiber module (550m)
- SFP Transceiver for 1000BASE-LHX Single-mode fiber module (40km)
- SFP Transceiver for 1000BASE-ZX Single-mode fiber module (80km)

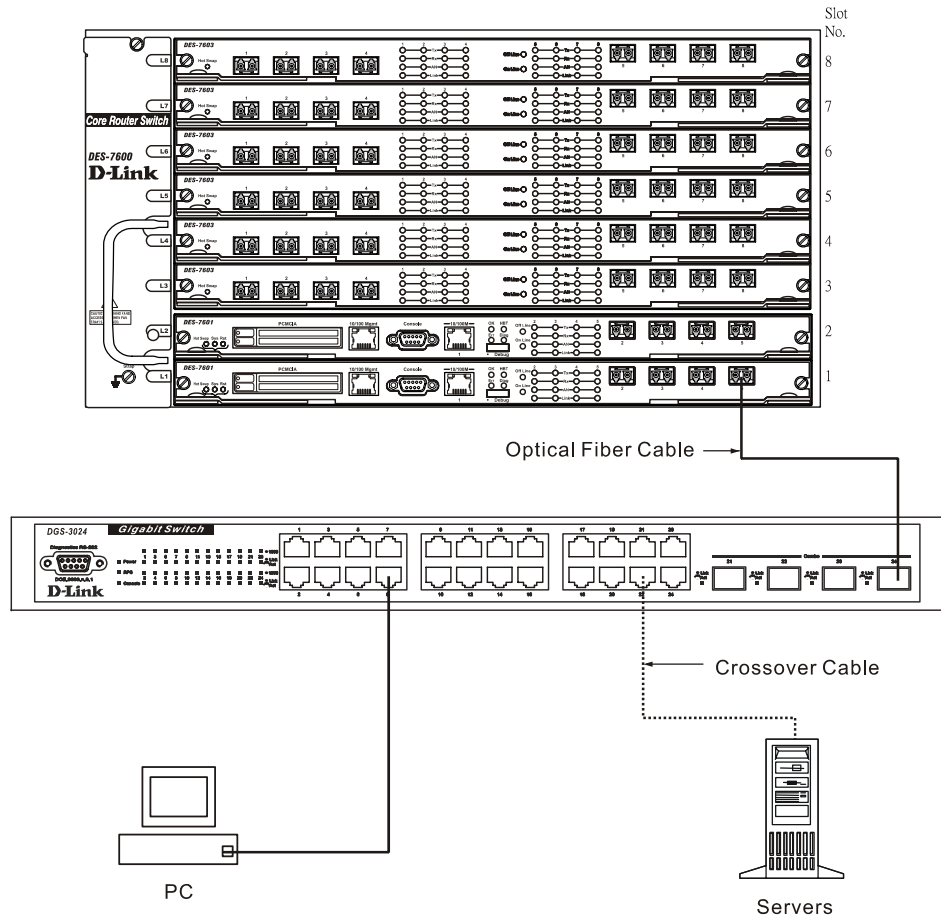


Figure 4- 3. Switch connected by optical fiber cable to a Core Router Switch, with a server connected by crossover cable and a PC connected by a Category 3, 4, 5, or 5e UTP/STP cable

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 and higher) or Microsoft® Internet Explorer (version 5.0).

SNMP-Based Management

You can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0 and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Command Line Console Interface Through the Serial Port

You can also connect a computer or terminal to the serial console port to access the Switch. The command-line-driven interface provides complete access to all Switch management features.

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 crossover 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 9600 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. User names and passwords must first be created by the administrator. 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 *DGS-3024 Command Line Interface Reference 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.

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 your 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 username and a password. Upon the initial connection, there is no username or password and therefore just press **Enter** twice to access the command line interface.

```
DGS-3024 Gigabit Ethernet Switch Command Line Interface
                          Firmware: Build 2.00-B12
                          Copyright(C) 2003-2004 D-Link Corporation. All rights reserved.
UserName:
```

Figure 5- 1. 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 (shown below).



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 **DGS-3024:4#** shown below:

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

```
DGS-3024 Gigabit Ethernet Switch Command Line Interface
                          Firmware: Build 2.00-B12
                          Copyright(C) 2003-2004 D-Link Corporation. All rights reserved.
UserName:
Password:
DGS-3024:4#_
```

Figure 5- 2. 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 DGS-3024 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, do the following:

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".

```
DGS-3024:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****

Success.

DGS-3024:4#
```



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 DGS-3024 supports SNMP versions 1, 2c, and 3. You can specify which version of SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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.

SNMP v.3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

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 SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.

Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v.3 in that SNMP messages may be encrypted. To read more about how to configure SNMP v.3 settings for the Switch read the section entitled Management.

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

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

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 10.90.90.90. 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.

```
DGS-3024:4#sh sw
Command: show switch

Device Type       : DGS-3024 Gigabit-Ethernet Switch
MAC Address       : 00-11-95-8D-F5-8B
IP Address        : 10.24.22.8 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 1.00.B02
Firmware Version  : Build 2.00-B12
Hardware Version  : 0A1
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
TELNET            : Enabled (TCP 23)
WEB               : Enabled (TCP 80)
RMON              : Disabled

DGS-3024:4#_
```

Figure 5- 3. Show Switch command

The Switch's MAC address can also be found from the Web management program on the **Switch Information (Basic Settings)** window on the **Configuration** menu.

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 System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**, where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the x's represent the IP address to be assigned to the IP interface named System and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask that can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

```
DGS-3024 Gigabit Ethernet Switch Command Line Interface
                          Firmware: Build 2.00-B12
                          Copyright(C) 2003-2004 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DGS-3024:4#config ipif System ipaddress 10.24.22.8/255.0.0.0
Command: config ipif System ipaddress 10.24.22.8/8

Success.

DGS-3024:4#save
Command: save

Saving all configurations to NV-RAM... Done.

DGS-3024:4#
```

Figure 5- 4. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.24.22.8 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. Please remember to save your new settings before you logout or they will be lost.

The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

Connecting Devices to the Switch

After you assign IP addresses to the Switch, you can connect devices to the Switch.

To connect a device to an SFP transceiver port:

Use your cabling requirements to select an appropriate SFP transceiver type.

Insert the SFP transceiver (sold separately) into the SFP transceiver slot.

Use the appropriate network cabling to connect a device to the connectors on the SFP transceiver.



NOTICE: When the SFP transceiver acquires a link, the associated integrated 10/100/1000BASE-T port is disabled.

Web-Based Network Management

Introduction

The DGS-3024 offers an embedded Web-based (HTML) interface allowing users to manage the Switch from anywhere on the network through a standard browser, such as Opera, Netscape Navigator/Communicator, or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol. Your browser window may vary with the screen shots (pictures) in this manual.

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.



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



NOTE: The Web browser needs to be upgraded to the latest Java version (Java™ Plug-in: version 1.5.0 or later).

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. Please note that the proxy for session connection should be turned off.



NOTE: The Factory default IP address for the Switch is 10.90.90.90.

In the page that opens, click on the **Login** to make a setup button:

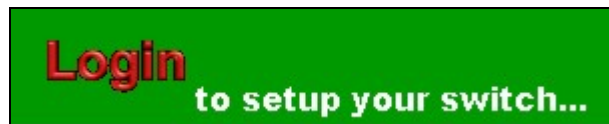


Figure 6- 1. Login button

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

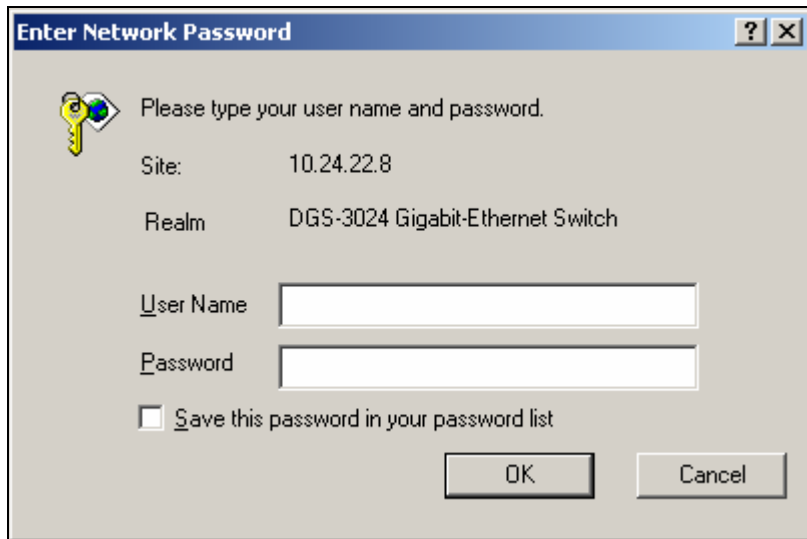


Figure 6- 2. Enter Network Password dialog box

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 windows, 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.

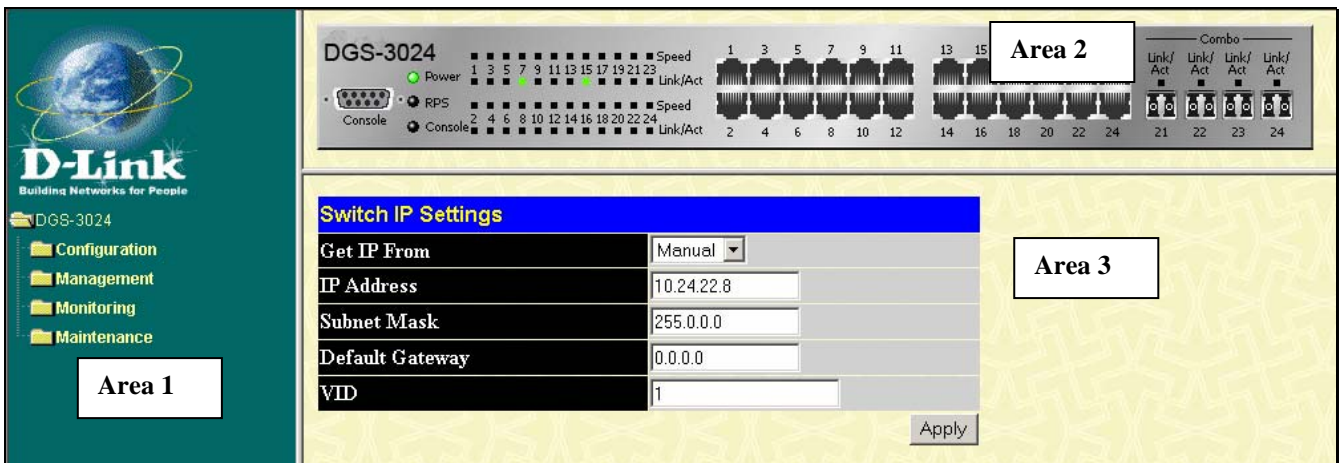


Figure 6- 3. Main Web-Manager window

Area	Function
Area 1	Select the folder or 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. This area displays the Switch's ports and expansion modules, showing port activity, duplex

	<p>mode, or flow control, depending on the specified mode.</p> <p>Various areas of the graphic can be selected for performing management functions, including port configuration.</p>
Area 3	<p>Presents Switch information based on your selection and the entry of configuration data.</p>



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



NOTE: Be sure to configure the user name and password in the **User Account Management** window (**Management** → **User Accounts**) before connecting the Switch to the greater network.

Configuration

The first Web Manager main folder is **Configuration** and includes the following windows and sub-folders: **IP Address**, **Switch Information**, **Advanced Settings**, **Port Configuration**, **Port Mirroring**, **Link Aggregation**, **IGMP Snooping**, **Spanning Tree**, **Forwarding & Filtering**, **VLANs**, **SNTP Settings**, **QoS**, **MAC Notification**, **System Log Server**, **Port Access Entity**, and **Static ARP Settings**, as well as secondary windows.

IP Address

Figure 7- 1. Switch IP Settings window

This window is used to determine whether the Switch should get its IP Address settings from the user (*Manual*), a *BOOTP* server, or a *DHCP* server. If you are not using either *BOOTP* or *DHCP*, enter the IP Address, Subnet Mask, and Default Gateway of the Switch. If you enable *BOOTP*, you do not need to configure any IP parameters because a *BOOTP* server automatically assigns IP configuration parameters to the Switch. If you enable *DHCP*, a Dynamic Host Configuration Protocol request will be sent when the Switch is powered up. Once you have selected a setting under Get IP From, click **Apply** to activate the new settings.

The information is described as follows:

Parameter	Description
Get IP From	There are three choices for how the Switch receives its IP Address settings: <i>Manual</i> , <i>BOOTP</i> , and <i>DHCP</i> .
IP Address	The host address for the device on the TCP/IP network.
Subnet Mask	The address mask that controls subnetting on your TCP/IP network.
Default Gateway	The IP address of the device—usually a router—that handles connections to other subnets and/or other TCP/IP networks.
VID	The VLAN ID number.

Switch Information

Switch Information (Basic Settings)	
Device Type	DGS-3024 Gigabit-Ethernet Switch
MAC Address	00:11:95:8d:f5:8b
Boot PROM Version	Build 1.00.B02
Firmware Version	Build 2.00-B12
Hardware Version	0A1
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Apply	

Figure 7- 2. Switch Information (Basic Settings) window

This window is used to enter name, location, and contact information. Click **Apply** to activate the new settings.

The information is described as follows:

Parameter	Description
Device Type	A description of the Switch type.
MAC Address	The Ethernet address for the device. Also known as the physical address.
Boot PROM Version	Version number for the firmware chip. This information is needed for new runtime software downloads.
Firmware Version	Version number of the firmware installed on the Switch. This can be updated by using the Download Firmware from TFTP Server window in the TFTP Services folder (Maintenance → TFTP Services → Download Firmware from TFTP Server).
Hardware Version	Version of the Switch hardware.
System Name	A user-assigned name for the Switch.
System Location	A user-assigned description for the physical location of the Switch.
System Contact	Name of the person to contact should there be any problems or questions with the system. You may also want to include a phone number or extension.

Advanced Settings

Switch Information (Advanced Settings)	
Serial Port Auto Logout	10 Minutes ▾
Serial Port Baud Rate	9600 ▾
MAC Address Aging Time (0-14400) Minutes	5
IGMP Snooping	Disabled ▾
Multicast router Only	Disabled ▾
Telnet Status	Enabled ▾
Telnet TCP Port Number(1-65535)	23
Web Status	Enabled ▾
Web TCP Port Number(1-65535)	80
RMON Status	Disabled ▾
GVRP	Disabled ▾
Link Aggregation Algorithm	MAC Source ▾
Switch 802.1x	Disabled ▾
Syslog state	Disabled ▾
Apply	

Figure 7- 3. Switch Information (Advanced Settings) window

The following fields can be set:

Parameter	Description
Serial Port Auto Logout	This setting for the restart of the console is 2 Minutes, 5 Minutes, 10 Minutes, 15 Minutes, or Never. The default is 10 Minutes.
Serial Port Baud Rate	Determines the serial port bit rate that will be used the next time the Switch is restarted. Available speeds are 9600, 19,200, 38,400, and 115,200 bits per second. The default setting is 9600.
MAC Address Aging Time (0-14400) Minutes	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this, type in a different value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between 0 and 14,400. The default setting is 5.
IGMP Snooping	This indicates if Internet Group Management Protocol (IGMP) Snooping is enabled on the Switch. When enabled, this feature instructs the Switch to read IGMP packets being forwarded through the Switch in order to obtain forwarding information from them (learn which ports contain Multicast members). The Switch's IGMP snooping state can be changed on the IGMP Snooping Settings window (Configuration → IGMP Snooping → IGMP Snooping). The default is <i>Disabled</i> .
Multicast Router Only	This field specifies that the Switch should only forward all multicast traffic to a multicast-enabled router, if enabled. Otherwise, the Switch will forward all multicast traffic to any

IP router. The default is *Disabled*.

Telnet Status	This indicates if a Telnet connection is currently enabled on the Switch. The default is <i>Enabled</i> .
Telnet TCP Port Number (1-65535)	The TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23.
Web Status	Web-based management is <i>Enabled</i> by default. If you choose to disable this by selecting <i>Disabled</i> , you will lose the ability to configure the system through the web interface as soon as these settings are applied
Web TCP Port Number (1-65535)	The TCP port number currently being utilized by the Switch to connect to the web interface. The "well-known" TCP port for the Web interface is 80.
RMON Status	This indicates if RMON is enabled on the Switch. The default is <i>Disabled</i> .
GVRP	This indicates if Group VLAN Registration Protocol (GVRP) is enabled on the Switch. GVRP is a protocol that allows members to dynamically join VLANs. The Switch's GVRP settings can be changed on the GVRP Settings window (Configuration → VLANs → 802.1Q Port Settings). The default is <i>Disabled</i> .
Link Aggregation Algorithm	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose <i>MAC Source</i> , <i>MAC Destination</i> , or <i>MAC Src & Dest</i> , (For further information, see the Link Aggregation section, under the Link Aggregation folder).
Switch 802.1x	The Switch's 802.1x function may be enabled by port; the default is <i>Disabled</i> . This field must be enabled to view and configure certain windows for 802.1x. More information regarding 802.1x, its functions and implementation can be found later in this section, under the Port Access Entity folder. Port-Based 802.1x specifies that ports configured for 802.1x are initialized based on the port number only and are subject to any authorization parameters configured.
Syslog State	This allows you to enable or disable the System Log State. The default is <i>Disabled</i> .

Port Configuration

Port Configuration						
From	To	State	Speed/Duplex	Flow Control	Learning	Apply
Port 1	Port 1	Disabled	Auto	Disabled	Disabled	Apply

The Port Information Table					
Port	State	Speed/Duplex	Flow Control	Connection	Learning
1	Enabled	Auto	Disabled	Link Down	Enabled
2	Enabled	Auto	Disabled	Link Down	Enabled
3	Enabled	Auto	Disabled	Link Down	Enabled
4	Enabled	Auto	Disabled	Link Down	Enabled
5	Enabled	Auto	Disabled	Link Down	Enabled
6	Enabled	Auto	Disabled	Link Down	Enabled
7	Enabled	Auto	Disabled	100M/Full/None	Enabled
8	Enabled	Auto	Disabled	Link Down	Enabled
9	Enabled	Auto	Disabled	Link Down	Enabled
10	Enabled	Auto	Disabled	Link Down	Enabled
11	Enabled	Auto	Disabled	Link Down	Enabled
12	Enabled	Auto	Disabled	Link Down	Enabled
13	Enabled	Auto	Disabled	Link Down	Enabled
14	Enabled	Auto	Disabled	Link Down	Enabled
15	Enabled	Auto	Disabled	100M/Full/None	Enabled
16	Enabled	Auto	Disabled	Link Down	Enabled
17	Enabled	Auto	Disabled	Link Down	Enabled
18	Enabled	Auto	Disabled	Link Down	Enabled
19	Enabled	Auto	Disabled	Link Down	Enabled
20	Enabled	Auto	Disabled	Link Down	Enabled
21	Enabled	Auto	Disabled	Link Down	Enabled
22	Enabled	Auto	Disabled	Link Down	Enabled
23	Enabled	Auto	Disabled	Link Down	Enabled
24	Enabled	Auto	Disabled	Link Down	Enabled

Figure 7- 4. Port Configuration window

To configure Switch ports:

1. Choose the port or sequential range of ports using the From and To pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:

Parameter	Description
State <Enabled>	Toggle the State field to either enable or disable a given port or group of ports.
Speed/Duplex <Auto>	Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. <i>Auto</i> denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex. The <i>Auto</i> setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and

	<p>then to use those settings. The other options are <i>10M/Half</i>, <i>10M/Full</i>, <i>100M/Half</i> and <i>100M/Full</i>, <i>1000M/Full_M</i> and <i>1000M/Full_S</i>. There is no automatic adjustment of port settings with any option other than <i>Auto</i>.</p> <p>The Switch allows the user to configure two types of gigabit connections; <i>1000M/Full_M</i> and <i>1000M/Full_S</i>. Gigabit connections are only supported in full duplex connections and take on certain characteristics that are different from the other choices listed.</p> <p>The <i>1000M/Full_M</i> (master) and <i>1000M/Full_S</i> (slave) parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (<i>1000M/Full_M</i>) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (<i>1000M/Full_S</i>) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for <i>1000M/Full_M</i>, the other side of the connection must be set for <i>1000M/Full_S</i>. Any other configuration will result in a link down status for both ports.</p>
Flow Control	<p>Displays 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 <i>Auto</i> ports use an automatic selection of the two. The default is <i>Disabled</i>.</p>
Learning	<p>Enable or disable MAC address learning for the selected ports. When <i>Enabled</i>, destination and source MAC addresses are automatically listed in the forwarding table. When learning is <i>Disabled</i>, MAC addresses must be manually entered into the forwarding table. This is sometimes done for security or efficiency reasons. See the section on Forwarding for information on entering MAC addresses into the forwarding table. The default setting is <i>Disabled</i>.</p>

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

Port Mirroring

Setup Port Mirroring

SourcePort	<input type="text" value="Port 1"/>																								
Status	<input type="text" value="Disabled"/>																								
Target Port																									
Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ingress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.

Note(2): The target port should be a non-trunked port.

Figure 7- 5. Setup Port Mirroring window

To configure a mirror port:

1. Select the Source Port from where you want to copy frames and the Target Port, which receives the copies from the source port.
2. Select Ingress, Egress, or None and change the Status drop-down menu to *Enabled*.
3. Click **Apply** to let the changes take effect.



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

Link Aggregation (Port Trunking)

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.



NOTE: In the current DGS-3024 firmware version, only Static Type Link Aggregation is supported. LACP Type Link Aggregation (802.3ad) is not yet supported.

Static Type Link Aggregation is usually referred as “Port Trunking.” In this section, the terms “Link Aggregation” and “Port Trunking” will be used synonymously.

The DGS-3024 supports up to four port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

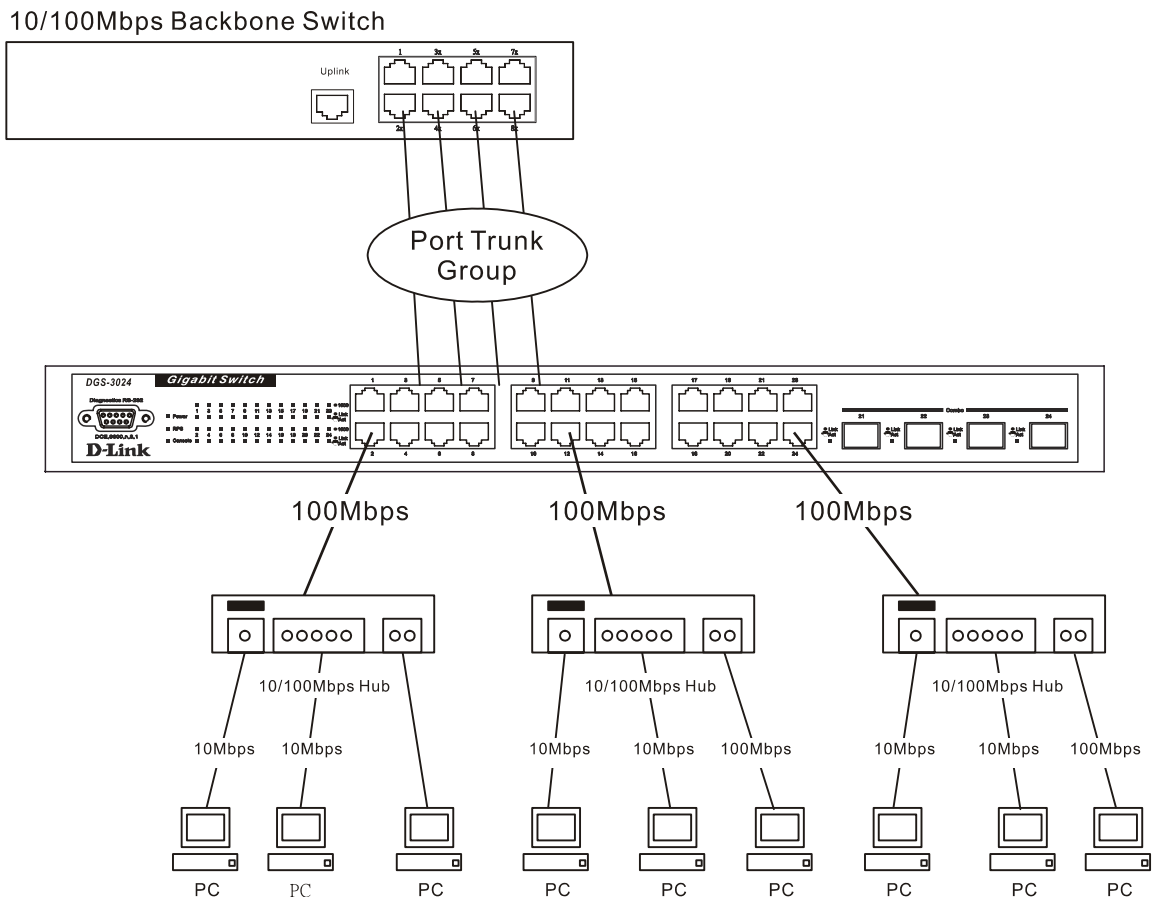


Figure 7- 6. Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other uplinked ports of the port trunking group.

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

Port trunking is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to four port trunking groups, each group consisting of 2 to 8 links (ports). The aggregated links must be contiguous (they must have sequential port numbers) except the two (optional) Gigabit ports, which can only belong to a single port trunking group. All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control, traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1x must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire port trunking group.

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

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

To configure port trunking, click on the **Link Aggregation** hyperlink in the **Configuration** folder to bring up the following window:

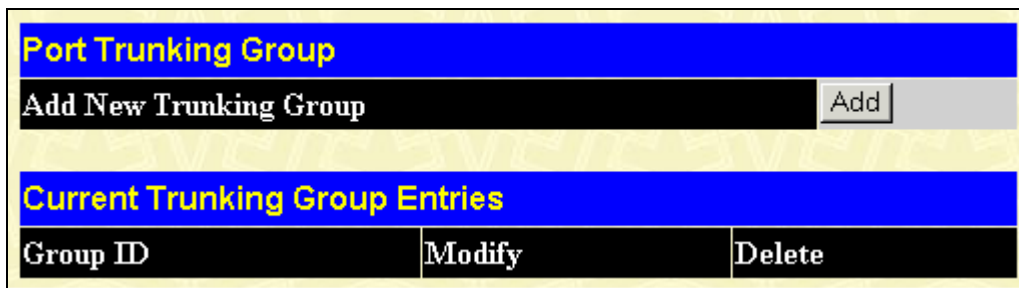



Figure 7- 7. Port Trunking Group window

To configure port trunk groups, click the **Add** button to add a new trunk group and use the **Port Trunking Configuration** window to set up trunk groups. To modify a port trunk group, click the **Modify** button corresponding to the entry you wish to alter. To delete a port trunk group, click the corresponding  under the Delete heading in the Current Trunking Group Entries table.

Port Trunking Configuration																								
Group ID [1-4]	<input type="text"/>																							
State	Disabled ▾																							
Type	Static ▾																							
Master Port	Port 1 ▾																							
Port Map	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Active Port																								
Apply																								
<p>Note: It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Port Trunking Group Entries</p>																								

Figure 7- 8. Port Trunking Configuration window

The user-changeable parameters are as follows:

Parameter	Description
Group ID [1-4]	Select an ID number for the group, between 1 and 4.
State	Trunk groups can be toggled between <i>Enabled</i> and <i>Disabled</i> . This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Type	The type of port trunking supported by the DGS-3024 is Static.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
Port Map	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Active Port	Shows the port that is currently forwarding packets.

After setting the previous parameters, click **Apply** to allow your changes to be implemented. Successfully created trunk groups will be show in the Current Trunking Group Entries table.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

In order to use IGMP Snooping it must first be enabled for the entire Switch on the **Switch Information (Advanced Settings)** window (**Configuration > Advanced Settings**). You may then fine-tune the settings for each VLAN by clicking the **IGMP Snooping** link in the **Configuration** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

IGMP Snooping

Use the **Current IGMP Snooping Group Entries** window to view **IGMP Snooping** settings. To modify the settings, click the **Modify** button of the VLAN ID you want to change.

Current IGMP Snooping Group Entries					
VLAN ID	VLAN Name	State	Querier State	Querier Router Behavior	Modify
1	default	Disabled	Disabled	Non-Querier	Modify

Figure 7- 9. Current IGMP Snooping Group Entries window

Clicking the **Modify** button will open the **IGMP Snooping Settings** window, shown below:

IGMP Snooping Settings	
VLAN ID	<input type="text" value="1"/>
VLAN Name	<input type="text" value="default"/>
Query Interval	<input type="text" value="125"/>
Max Response Time	<input type="text" value="10"/>
Robustness Value	<input type="text" value="2"/>
Last Member Query Interval	<input type="text" value="1"/>
Host Timeout	<input type="text" value="260"/>
Route Timeout	<input type="text" value="260"/>
Leave Timer	<input type="text" value="2"/>
Querier State	<input type="text" value="Disabled"/>
State	<input type="text" value="Disabled"/>
<input type="button" value="Apply"/>	
Show All IGMP Group Entries	

Figure 7- 10. IGMP Snooping Settings window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
Query Interval	Allows the entry of a value between 1 and 65535 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.
Max Response Time	Sets the maximum amount of time allowed before sending an IGMP response report.

	A value between 1 and 25 seconds can be entered, with a default of 10 seconds.
Robustness Value	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 2 and 255 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets. The default is 2 seconds.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. A value between 1 and 25. The default is 1 second.
Host Timeout	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. The default is 260.
Route Timeout	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. The default is 260.
Leave Timer	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted. The default is 2
Querier State	Choose <i>Enabled</i> to enable transmitting IGMP Query packets or <i>Disabled</i> to disable. The default is <i>Disabled</i> .
State	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> and enables or disables IGMP for the VLAN. The default is <i>Disabled</i> .

Click **Apply** to implement the new settings. Click the [Show All IGMP Group Entries](#) link to return to the **Current IGMP Snooping Group Entries** window.

Static Router Ports Entry

Total Entries: 1		
Current Static Router Ports Entries		
VLAN ID	VLAN Name	Modify
1	default	<input type="button" value="Modify"/>

Figure 7- 11. Current Static Router Ports Entries window

Select an entry and click **Modify** to access the following window:

Figure 7- 12. Static Router Ports Settings window

The following parameters can be viewed or set:

Parameter	Description
VID (VLAN ID)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN where the multicast router is attached.
VLAN Name	This is the name of the VLAN where the multicast router is attached.
Member Ports	These are the ports on the Switch that will have a multicast router attached to them.

Click **Apply** to implement the new settings, Click the [Show All Static Router Port Entries](#) link to return to the **Current Static Router Port Entries** window.

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 either 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. These instances will be classified by an MSTI ID. 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 **Current MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level (0-65535) and found in the **Current MST Configuration Identification** window) and;
3. A 4096-element table (defined here as a VID List in the **Current MST Configuration Identification** window) that 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 *MSTP* (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 Table** window when configuring the settings for an MSTI ID).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **Current MST Configuration Identification** window when configuring the settings for an MSTI ID).

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 6-1 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.

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

Table 7- 1. 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 open the following window, open the **Spanning Tree** folder in the **Configuration** menu and click the **STP Bridge Global Settings** link.

STP Bridge Global Settings	
STP Status	Enabled ▾
STP Version	STP compatible ▾
Hello Time(1-10 Sec)	2
Max Age(6-40 Sec)	20
Forward Delay(4-30 Sec)	15
Max Hops(1-20)	20
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled ▾
Apply	

Figure 7- 13. STP Bridge Global Settings window – STP compatible

STP Bridge Global Settings	
STP Status	Enabled ▾
STP Version	RSTP ▾
Hello Time(1-10 Sec)	2
Max Age(6-40 Sec)	20
Forward Delay(4-30 Sec)	15
Max Hops(1-20)	20
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled ▾
Apply	

Figure 7- 14. STP Bridge Global Settings window - RSTP (default)

STP Bridge Global Settings	
STP Status	Enabled ▾
STP Version	MSTP ▾
Max Age(6-40 Sec)	20
Forward Delay(4-30 Sec)	15
Max Hops(1-20)	20
TX Hold Count(1-10)	3
Forwarding BPDU	Enabled ▾
Apply	

Figure 7- 15. STP Bridge Global Settings window - MSTP

The following parameters can be set:

Parameter	Description
STP Status	Use the pull-down menu to enable or disable STP globally on the Switch. The default is <i>Disabled</i> .
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices: <i>STP</i> - Select this parameter to set the Spanning Tree Protocol (STP) globally on the Switch. <i>RSTP</i> - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. <i>MSTP</i> - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Hello Time (1-10 Sec)	The Hello Time 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. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. See the STP Port Settings section for further details.
Max Age (6-40 Sec)	The Max Age 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.
Forward Delay (4 - 30 Sec)	The Forward Delay 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.
Max Hops (1-20)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 1 to 20. The default is 20.
TX Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is 3.
Forwarding BPDU	This field can be <i>Enabled</i> or <i>Disabled</i> . When <i>Enabled</i> , it allows the forwarding of STP BPDU packets from other network devices. The default is Enabled.

Click **Apply** to implement changes made.



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 $\leq 2 \times$ (Forward Delay - 1 second)

Max. Age $\geq 2 \times$ (Hello Time + 1 second)

MST Configuration Table

The following windows allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one *CIST* or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted. To view the **Current MST Configuration Identification** window, click **Configuration > Spanning Tree > MST Configuration Table**:

Add

Current MST Configuration Identification

Configuration Name	Revision Level
00:11:95:8D:F5:8B	0

MSTI ID	VID List	Delete
CIST	1-4094	Can't be Deleted!

MST Configuration Identification Settings


Configuration Name	<input type="text" value="00:11:95:8D:F5:8B"/>
Revision Level(0-65535)	<input type="text" value="0"/>

Apply

Figure 7- 16. Current MST Configuration Identification window

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	This value, along with the Configuration Name will identify the MSTP region configured on the Switch.
MSTI ID	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
VID List	This field displays the VLAN IDs associated with the specific MSTI.

To delete a previously set MSTI Instance ID, click the corresponding  under the Delete heading in the **Current MST Configuration Identification** window. Clicking the **Add** button will reveal the following window to configure:

Instance ID Settings

MSTI ID	<input type="text"/>
Type	Create ▾
VID List (1-4094)	<input type="checkbox"/> <input type="text"/>

Apply

[Show MST Configuration Table](#)

Figure 7- 17. Instance ID Settings window - Add

The user may configure the following parameters to create a MSTI in the Switch.

Parameter	Description
MSTI ID	Enter a number between 1 and 15 to set a new MSTI on the Switch.
Type	<i>Create</i> is selected to create a new MSTI. No other choices are available for this field when creating a new MSTI.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.

Click **Apply** to implement changes made.

To configure the settings for the CIST, click on its hyperlinked **MSTI ID** number in the **Current MST Configuration Identification** window, which will reveal the following window to configure:

Figure 7- 18. Instance ID Settings window - CIST modify

The user may configure the following parameters to configure the CIST on the Switch.

Parameter	Description
MSTI ID	The MSTI ID of the CIST is 0 and cannot be altered.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices. <i>Add VID</i> - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. <i>Remove VID</i> - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.

Click **Apply** to implement changes made.

To configure the parameters for a previously set MSTI, click on its hyperlinked MSTI ID number, which will reveal the following window for configuration.

Figure 7- 19. Instance ID Settings window - Modify

The user may configure the following parameters for a MSTI on the Switch.

Parameter	Description
MSTI ID	Displays the MSTI ID previously set by the user.
Type	<p>This field allows the user to choose a desired method for altering the MSTI settings. The user has two choices.</p> <p><i>Add VID</i> - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter.</p> <p><i>Remove VID</i> - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.</p>
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch that the user wishes to add to this MSTI ID. Supported VIDs on the Switch range from ID number 1 to 4094. This parameter can only be utilized if the Type chosen is <i>Add</i> or <i>Remove</i> .

Click **Apply** to implement changes made.

MSTI Settings

This window displays the current MSTI configuration settings and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest port number into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **Configuration > Spanning Tree > MSTI Settings**:

Port	Apply
Port 1	Apply

MSTI Port Information-Port 1					
Msti	Designated Bridge	Internal PathCost	Prio	Status	Role
0	N/A	200000	128	Disabled	Disabled

Figure 7- 20. MSTI Port Information window

To view the MSTI settings for a particular port, select the Port number, located in the top left hand corner of the window and click **Apply**. To modify the settings for a particular MSTI Instance, click on its hyperlinked MSTI ID, which will reveal the following window.

MSTI Settings-Port 1 of Unit 1	
Instance ID	<input type="text" value="1"/>
Internal cost(0=Auto)	<input type="text" value="0"/>
Priority	<input type="text" value="128"/>
<input type="button" value="Apply"/>	
Show MSTP Port Information Table-Port 1 of Unit 1	

Figure 7- 21. MSTI Settings window

Parameter	Description
Instance ID	Displays the MSTI ID of the instance being configured. An entry of 0 in this field denotes the CIST (default MSTI).
Internal cost	<p>This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto). There are two options:</p> <p><i>0 (auto)</i> - Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.</p> <p><i>value 1-2000000</i> - Selecting this parameter with a value in the range of 1-2000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.</p>
Priority	Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority. This entry must be divisible by 16. The default priority setting is 128.

Click **Apply** to implement changes made.

STP Instance Settings

The following window displays MSTIs currently set on the Switch. To view the following table, click **Configuration > Spanning Tree > STP Instance Settings**:

STP Instance Settings			
Instance Type	Instance Status	Instance Priority	Priority
CIST	Enabled	32768(bridge priority : 32768, sys ID ext : 0)	<input type="button" value="Modify"/>
MSTI(1)	Enabled	32769(bridge priority : 32768, sys ID ext : 1)	<input type="button" value="Modify"/>

Figure 7- 22. STP Instance Settings window

The following information is displayed:

Parameter	Description
Instance Type	Displays the instance type(s) currently configured on the Switch. Each instance type is classified by an MSTI ID. CIST refers to the default MSTI configuration set on the Switch.
Instance Status	Displays the current status of the corresponding MSTI ID
Instance Priority	Displays the priority of the corresponding MSTI Instance Type. The lowest priority will be the root bridge.
Priority	Click the Modify button to change the priority of the MSTI. This will open the Instance ID Settings window to configure. The Type field in this window will be permanently set to <i>Set Priority Only</i> . Enter the new priority in the Priority field and click Apply to implement the new priority setting.

Click **Apply** to implement changes made.

Clicking the hyperlinked name will allow the user to view the current parameters set for the MSTI Instance.

STP Instance Operational Status	
Designated Root Bridge	4096/00-01-27-32-26-95
External Root Cost	200004
Regional Root Bridge	32768/00-53-13-1a-33-24
Internal Root Cost	0
Designated Bridge	32768/00-50-ba-71-20-d6
Root Port	1
Max Age	20
Forward Delay	15
Last Topology Change	177
Topology Changes Count	157
Show STP Instance Table	

Figure 7- 23. STP Instance Operational Status window – CIST

STP Instance Operational Status	
Regional Root Bridge	32770/00-53-13-1a-33-24
Internal Root Cost	0
Designated Bridge	32770/00-53-13-1a-33-24
Root Port	None
Remaining Hops	20
Last Topology Change	288
Topology Changes Count	3
Show STP Instance Table	

Figure 7- 24. STP Instance Operational Status window – Previously Configured MSTI

The following parameters may be viewed in the **STP Instance Operational Status** windows:

Parameter	Description
Designated Root Bridge	This field will show the priority and MAC address of the Root Bridge.
External Root Cost	<p>This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</p> <p><i>0 (auto)</i> - Setting 0 for the external cost will 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.</p> <p><i>value 1-200000000</i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p>
Regional Root Bridge	This field will show the priority and MAC address of the Regional (Internal) Root Bridge. This MAC address should be the MAC address of the Switch.
Internal Root Cost	<p>This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto). There are two options:</p> <p><i>0 (auto)</i> - Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.</p> <p><i>value 1-2000000</i> - Selecting this parameter with a value in the range of 1 to 2000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.</p>
Designated Bridge	This field will show the priority and MAC address of the Designated Bridge. The information shown in this table comes from a BPDU packet originating from this bridge.
Root Port	This is the port on the Switch that is physically connected to the Root Bridge.

Max Age	The Max Age 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.
Forward Delay	The Forward Delay 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.
Last Topology Change	This field shows the time, in seconds, since the last spanning tree topology change.
Topology Changes Count	This field displays the number of times that the spanning tree topology has changed since the original initial boot up of the Switch.

STP Port Settings

STP can be set up on a port per port basis. To view the following window click **Configuration > Spanning Tree > STP Port Settings**:

STP Port Settings								
Unit	From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	P2P	State
1	Port 1	Port 1	0	1	Yes	False	True	Enabled
								Apply
STP Port Settings Table-Unit 1								
Port	External Cost		Hello Time		Edge		P2P	Port STP
1	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
2	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
3	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
4	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
5	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
6	AUTO/200000		2/2		No/No		Auto/Yes	Enabled
7	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
8	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
9	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
10	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
11	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
12	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
13	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
14	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
15	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
16	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
17	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
18	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
19	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
20	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
21	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
22	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
23	AUTO/20000		2/2		No/No		Auto/Yes	Enabled
24	AUTO/20000		2/2		No/No		Auto/Yes	Enabled

Figure 7- 25. STP Port Settings window

In addition to setting Spanning Tree parameters for use on the Switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the Switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the Switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the Switch level.

The STP on the Switch level blocks redundant links between Switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following fields can be set:

Parameter	Description
From/To	A consecutive group of ports may be configured starting with the selected port.
External Cost (0 = Auto)	<p>This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</p> <p><i>0 (auto)</i> - Setting 0 for the external cost will 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.</p> <p><i>value 1-200000000</i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p>
Hello Time	The time interval between the transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 10 seconds. The default is 2 seconds. This field is only operable when the Switch is enabled for MSTP.
Migration	Setting this parameter as Yes will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1d STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1d network connects to an 802.1w or 802.1s enabled network. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.
Edge	Choosing the <i>True</i> parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the <i>False</i> parameter indicates that the port does not have edge port status.
P2P	Choosing the <i>True</i> parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of <i>false</i> indicates that the port cannot have p2p status. <i>Auto</i> allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were <i>False</i> . The default setting for this parameter is

	<i>True.</i>
State	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is <i>Enabled</i> .

Click **Apply** to implement changes made.

Forwarding


Unicast Forwarding

Open the **Forwarding** folder in the **Configuration** menu and click on the **Unicast Forwarding** link. This will open the **Setup Static Unicast Forwarding Table** window, as shown below:

Figure 7- 26. Setup Static Unicast Forwarding Table window

To add or edit an entry, define the following parameters and then click **Add/Modify**:

Parameter	Description
VID (VLAN ID)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Allowed to go port	Allows the selection of the port number on which the MAC address entered above resides.

Click **Apply** to implement the changes made. To delete an entry in the Static Unicast Forwarding Table, click the corresponding  under the Delete heading.

Multicast Forwarding

The following window describes how to set up Multicast Forwarding on the Switch. Open the **Forwarding** folder and click on the **Multicast Forwarding** link to see the entry window below:

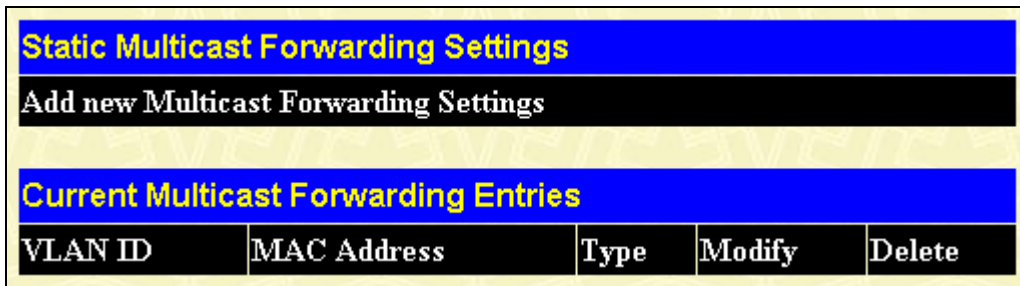


Figure 7- 27. Static Multicast Forwarding Settings window

The **Static Multicast Forwarding Settings** window displays all of the entries made into the Switch's static multicast forwarding table. Click the **Add** button to open the **Setup Static Multicast Forwarding Table** window, as shown below:

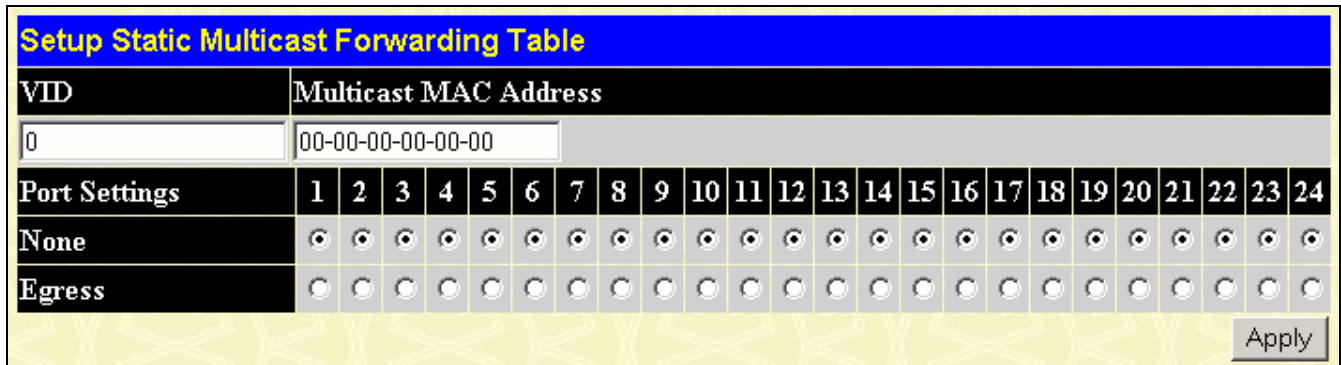



Figure 7- 28. Setup Static Multicast Forwarding Table window

The following parameters can be set:

Parameter	Description
VID	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	<p>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:</p> <p><i>None</i> - No restrictions on the port dynamically joining the multicast group. When <i>None</i> is chosen, the port will not be a member of the Static Multicast Group.</p> <p><i>Egress</i> - The port is a static member of the multicast group.</p>

Click **Apply** to implement the changes made. To delete an entry in the Static Multicast Forwarding Table, click the corresponding  under the Delete heading. Click the **Show All Multicast Forwarding Entries** link to return to the **Static Multicast Forwarding Settings** window.

VLANs

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 1, 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.

A weighted round robin system is 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 1, 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.

Notes About VLANs on the DGS-3024

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The DGS-3024 supports IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

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 the receiving port is a member of.

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.

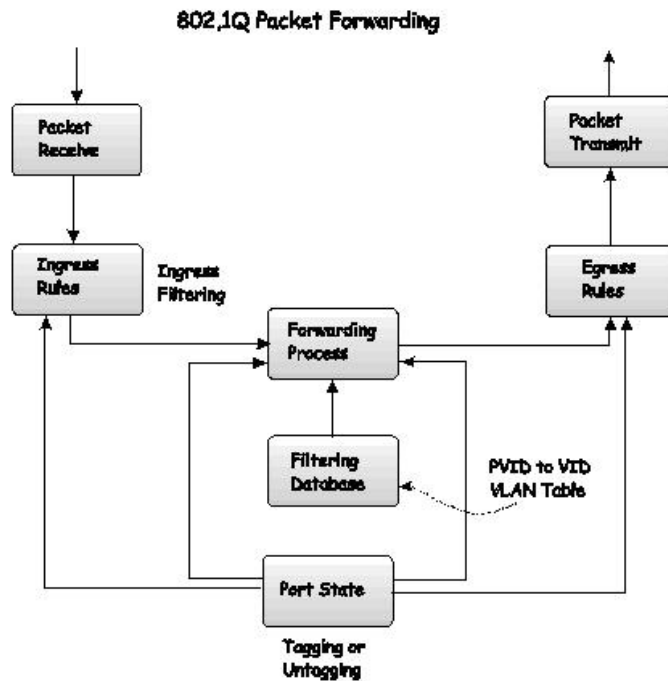


Figure 7- 29. IEEE 802.1Q Packet Forwarding

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.

IEEE 802.1Q Tag

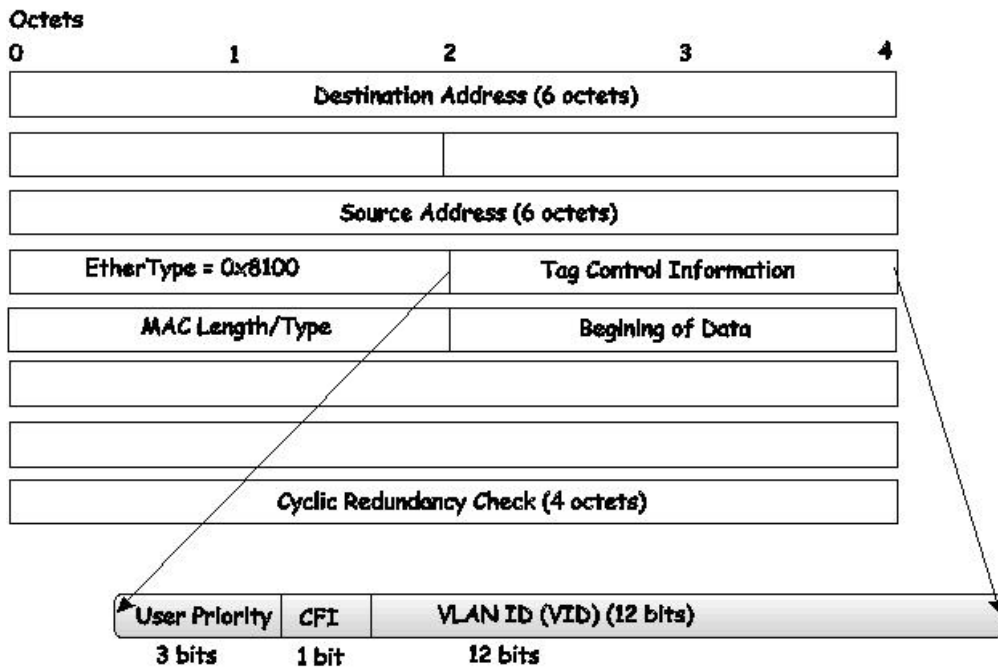


Figure 7- 30. IEEE 802.1Q Tag

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.

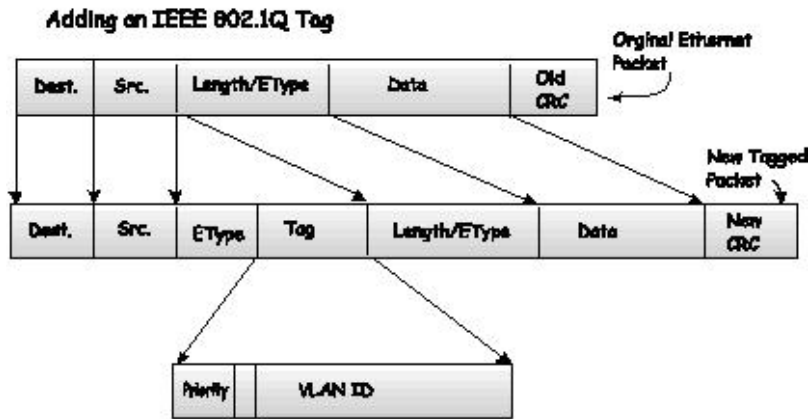


Figure 7- 31. Adding an IEEE 802.1Q Tag

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). Therefore, 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. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

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

Ingress Filtering

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

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

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

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

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."

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

Table 7- 2. VLAN Example - Assigned Ports

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.

Static VLAN Entry

In the **Configuration** folder, open the **VLANs** folder and click the **Static VLAN Entry** link to open the following window:

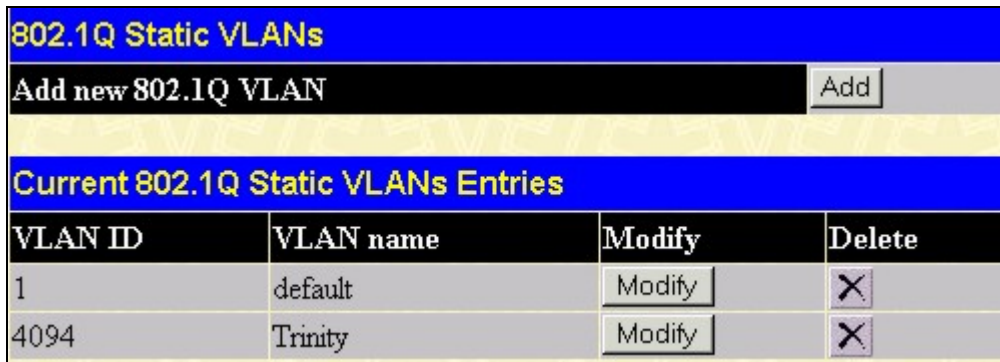



Figure 7- 32. first 802.1Q Static VLANs window

The first **802.1Q Static VLANs** window lists all previously configured VLANs by VLAN ID and VLAN Name. To delete an existing 802.1Q VLAN, click the corresponding  button under the Delete heading.

To create a new 802.1Q VLAN, click the **Add** button in the first **802.1Q Static VLANs** window. A new window will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.

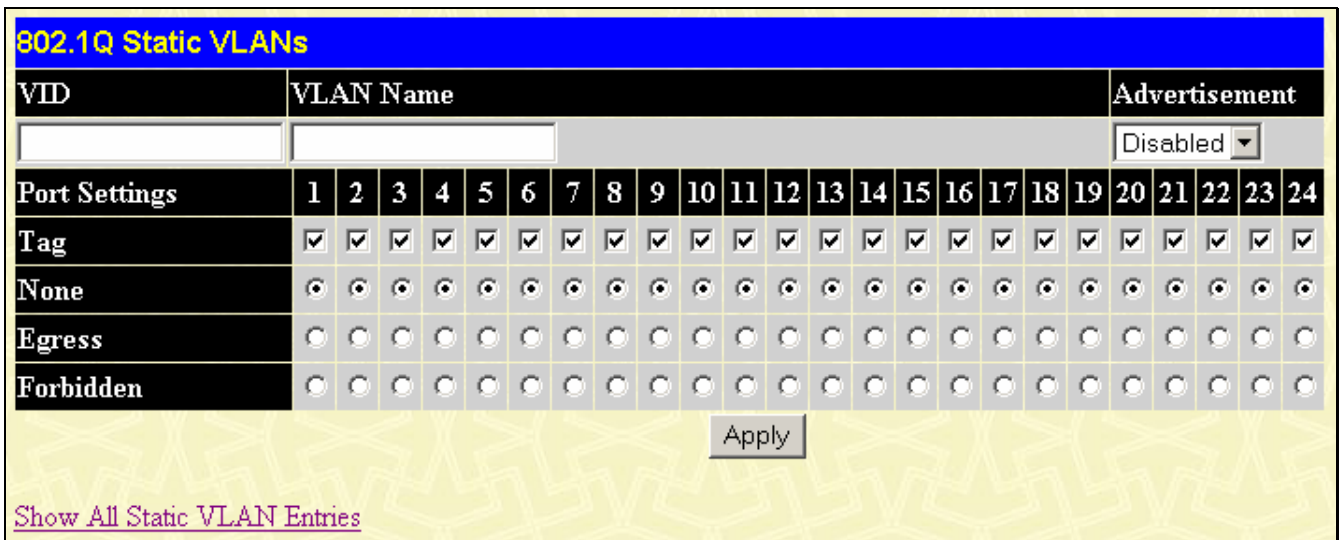


Figure 7- 33. second 802.1Q Static VLANs window (Add)

To return to the first **802.1Q Static VLANs** window, click the [Show All Static VLAN Entries](#) link. To change an existing 802.1Q VLAN entry, click the **Modify** button of the corresponding entry you wish to modify. A new window will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.

802.1Q Static VLANs																									
VID	VLAN Name																								Advertisement
4094	Ichiro																								Disabled ▾
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
Tag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Egress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Forbidden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Apply																									
Show All Static VLAN Entries																									

Figure 7- 34. second 802.1Q Static VLANs window (Modify)

The following fields can then be set in either the Add or Modify 802.1Q Static VLANs windows:

Parameter	Description
VID (VLAN ID)	Allows the entry of a VLAN ID in the Add window, or displays the VLAN ID of an existing VLAN in the Modify window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the Add window, or for editing the VLAN name in the Modify window.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
None	Allows an individual port to be specified as a non-VLAN member.
Egress	Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Click **Apply** to implement changes made.

8021Q Port Settings

In the **Configuration** menu, open the **VLANs** folder and click **8021Q Port Settings**.

This **GVRP Settings** window (shown below), allows you to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled Switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

GVRP Settings						
From	To	Ingress Check	Frame Type	PVID	GVRP	Apply
Port 1	Port 1	Disabled	Admit_all	1	Disabled	Apply

GVRP Table				
Port	PVID	Ingress	Frame Type	GVRP
1	1	Enabled	All frames	Disabled
2	1	Enabled	All frames	Disabled
3	1	Enabled	All frames	Disabled
4	1	Enabled	All frames	Disabled
5	1	Enabled	All frames	Disabled
6	1	Enabled	All frames	Disabled
7	1	Enabled	All frames	Disabled
8	1	Enabled	All frames	Disabled
9	1	Enabled	All frames	Disabled
10	1	Enabled	All frames	Disabled
11	1	Enabled	All frames	Disabled
12	1	Enabled	All frames	Disabled
13	1	Enabled	All frames	Disabled
14	1	Enabled	All frames	Disabled
15	1	Enabled	All frames	Disabled
16	1	Enabled	All frames	Disabled
17	1	Enabled	All frames	Disabled
18	1	Enabled	All frames	Disabled
19	1	Enabled	All frames	Disabled
20	1	Enabled	All frames	Disabled
21	1	Enabled	All frames	Disabled
22	1	Enabled	All frames	Disabled
23	1	Enabled	All frames	Disabled
24	1	Enabled	All frames	Disabled

Figure 7- 35. GVRP Settings window

The following fields can be set:

Parameter	Description
From/To	These two fields allow you to specify the range of ports that will be included in the VLAN that you are creating using the GVRP Settings window.
Ingress Check	This field can be toggled using the space bar between <i>Enabled</i> and <i>Disabled</i> . <i>Enabled</i> enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. <i>Disabled</i> disables ingress filtering. Ingress Checking is <i>Disabled</i> by default.

Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between <i>Tagged Only</i> , which means only VLAN tagged frames will be accepted, and <i>Admit All</i> , which means both tagged and untagged frames will be accepted. <i>Admit All</i> is enabled by default.
PVID	This field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and Ingress filtering is <i>Enabled</i> , the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is <i>Disabled</i> by default.

Click **Apply** to implement changes made.

SNTP Settings

Time Setting

To configure the time settings for the Switch, open the **Configuration** folder, then the **SNTP Settings** folder and click on the **Time Setting** link, revealing the following window for the user to configure.

Current Time: Status	
Current Time	18 Jan 2000 19:07:07
Time Source	System Clock
Current Time: SNTP Settings	
SNTP State	Disabled ▾
SNTP Primary Server	0.0.0.0
SNTP Secondary Server	0.0.0.0
SNTP Poll Interval in Seconds	720
Apply	
Current Time: Set Current Time	
Year	▾
Month	▾
Day	▾
Time in HH MM SS	▾ ▾ ▾
Apply	

Figure 7- 36. Current Time: Status window

The following parameters can be set or are displayed:

Parameter	Description
Current Time: Status	
Current Time	Displays the time when the Switch was initially started for this session.
Time Source	Displays the time source for the system.
Current Time: SNTP Settings	
SNTP State	Use this pull-down menu to <i>Enabled</i> or <i>Disabled</i> SNTP.
SNTP Primary Server	This is the IP address of the primary server the SNTP information will be taken from.
SNTP Secondary Server	This is the IP address of the secondary server the SNTP information will be taken from.
SNTP Poll Interval in Seconds	This is the interval, in seconds, between requests for updated SNTP information.
Current Time: Set Current Time	
Year	Enter the current year, if you want to update the system clock.

Month	Enter the current month, if you would like to update the system clock.
Day	Enter the current day, if you would like to update the system clock.
Time in HH MM SS	Enter the current time in hours and minutes, if you would like to update the system clock.

Click **Apply** to implement your changes.

Time Zone and DST

The following are windows used to configure time zones and Daylight Savings time settings for SNTP. Open the **Configuration** folder, then the **SNTP Setting** folder and click on the **Time Zone and DST** link, revealing the following window.

Time Zone and DST Settings

Daylight Saving Time State	Disabled ▾
Daylight Saving Time Offset in Minutes	60 ▾
Time Zone Offset from GMT in +/-HH:MM	- ▾ 06 ▾ 00 ▾

DST Repeating Settings

From Which Week of the month	First ▾
From Which Day of the Week	Sunday ▾
From Which Month	April ▾
From What Time HH:MM	00 ▾ 00 ▾
To Which Week	Last ▾
To Which Day	Sunday ▾
To Which Month	October ▾
To What Time HH:MM	00 ▾ 00 ▾

DST Annual Settings

From What Month	April ▾
From What Date	29 ▾
From What Time	00 ▾ 00 ▾
To What Month	October ▾
To What Date	12 ▾
To What Time	00 ▾ 00 ▾

Figure 7- 37. Time Zone and DST Settings window

The following parameters can be set:

Parameter	Description
Time Zone and DST Settings	

Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-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	Enter the week of the month that DST will start.
From Which Day of the Week	Enter the day of the week that DST will start on.
From Which Month	Enter the month DST will start on.
From What Time HH MM	Enter the time of day that DST will start on.
To Which Week	Enter the week of the month the DST will end.
To Which Day	Enter the day of the week that DST will end.
To Which Month	Enter the month that DST will end.
To What Time HH MM	Enter 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 What Month	Enter the month DST will start on, each year.
From What Date	Enter the day of the week DST will start on, each year.
From What Time	Enter the time of day DST will start on, each year.
To What Month	Enter the month DST will end on, each year.
To What Date	Enter the day of the week DST will end on, each year.
To What Time	Enter the time of day that DST will end on, each year.

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

QoS

The DGS-3024 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 DGS-3024 implements 802.1P priority queuing.

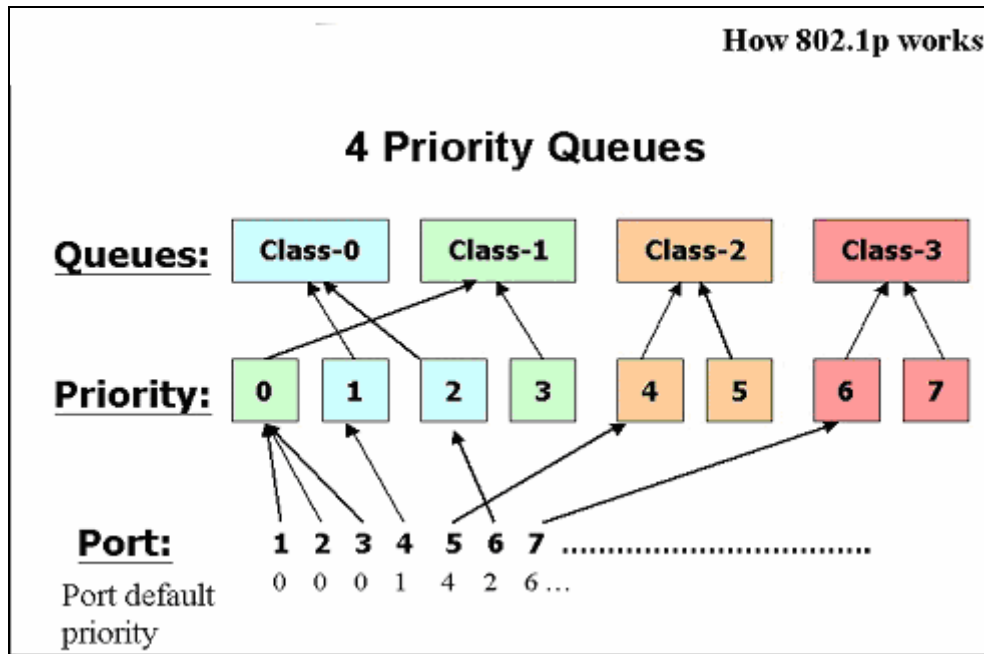


Figure 7- 38. Mapping QoS on the Switch

The picture above shows the default priority setting for the Switch. Class-3 has the highest priority of the four 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, lets 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 results 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 four priority queues. These priority queues are labeled as 3, the highest 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 Q1 queue.

Priority 1 is assigned to the Switch's Q0 queue.

Priority 2 is assigned to the Switch's Q0 queue.

Priority 3 is assigned to the Switch's Q1 queue.

Priority 4 is assigned to the Switch's Q2 queue.

Priority 5 is assigned to the Switch's Q2 queue.

Priority 6 is assigned to the Switch's Q3 queue.

Priority 7 is assigned to the Switch's Q3 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 eight 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 DGS-3024 has four priority queues (and four Classes of Service) for each port on the Switch.

Traffic Control

Use the **Traffic Control** window to enable or disable storm control and adjust the threshold for multicast/broadcast/DLF (Destination Look Up Failure) storms. Traffic control settings are applied to individual Switch modules. To view the following window, click **Configuration > QOS > Traffic Control**.

Storm Control Type Setting

Storm Control Type	broadcast_multicast_dlf ▾
Threshold	15000 ▾ Packet/Sec

Traffic Control Setting

From	To	Traffic control State	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	<input type="button" value="Apply"/>

Traffic Control Information Table

Port	Traffic Control State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled

Figure 7- 39. Storm Control Type Setting window

The purpose of this window is to limit too many broadcast, multicast or unknown unicast packets flooding the network. The Storm Control Type Settings you can choose from are: *broadcast*, *broadcast_multicast*, *broadcast_dlf*, and *broadcast_multicast_dlf*.

The Threshold value is the upper threshold at which the specified traffic control is Switched on. This is the number of Broadcast, Broadcast/Multicast, Broadcast/DLF, and Broadcast/Multicast/DLF packets received by the Switch that will

trigger the storm traffic control measures. The Threshold value can be set from 10 to 15000 packets per second. The default setting is 15000. The settings of each port may be viewed in the Traffic Control Information Table in the same window.

To configure the Storm Control Type Setting, select the desired Storm Control Type from the pull-down menu, select the threshold from the drop-down menu, and click **Apply**.

To configure the Traffic Control Setting, select the beginning and ending ports by using the From/To pull-down menu. Now, change the Traffic control State to *Enabled* and click **Apply**.

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. In the **Configuration** folder open the **QoS** folder and click **802.1p Default Priority**, to view the window shown below.

Port Default Priority assignment			
From	To	Priority	Apply
Port 1 ▾	Port 1 ▾	0 ▾	Apply

The Port Priority Table	
Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0

Figure 7- 40. Port Default Priority assignment window

This window allows you to assign a default 802.1p priority to any given port on the Switch. The priority queues are numbered from 0, the lowest priority, to 7, the highest priority. Click **Apply** to implement your settings.

802.1p User Priority

The DGS-3024 allows the assignment of a user priority to each of the 802.1p priorities. In the **Configuration** folder open the **QoS** folder and click **802.1p User Priority**, to view the window shown below.

User Priority Configuration	
Priority-0	Class-1
Priority-1	Class-0
Priority-2	Class-0
Priority-3	Class-1
Priority-4	Class-2
Priority-5	Class-2
Priority-6	Class-3
Priority-7	Class-3

Apply

Figure 7- 41. User Priority Configuration window

Once you have assigned a priority to the port groups on the Switch, you can then assign this Class to each of the four levels of 802.1p priorities. Click **Apply** to set your changes.

QoS Scheduling Mechanism

This window allows you to select between a *RoundRobin* and a *Strict* mechanism for emptying the priority classes. In the **Configuration** menu open the **QoS** folder and click **QoS Scheduling Mechanism**, to view the window shown below

QoS Scheduling Mechanism	
Scheduling Mechanism	Strict

Apply

QoS Scheduling Mechanism Table	
Class ID	Mechanism
Class-0	Round robin
Class-1	Round robin
Class-2	Round robin
Class-3	Round robin

Figure 7- 42. QoS Scheduling Mechanism window

The Scheduling Mechanism has the following parameters.

Parameter	Description
-----------	-------------

Strict	The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.
RoundRobin	Use the weighted round-robin (<i>WRR</i>) algorithm to handle packets in an even distribution in priority classes of service.

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



NOTE: The settings you assign to the queues, numbers 0-7, represent the IEEE 802.1p priority tag number. Do not confuse these settings with port numbers.

QoS Output Scheduling

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

Class ID	Max. Packets
Class-0	0
Class-1	1
Class-2	2
Class-3	3

Figure 7- 43. QoS Output Scheduling window

You may assign the following values to the QoS classes to set the scheduling.

Parameter	Description
Max. Packets	Specifies the maximum number of packets the above specified hardware priority class of service will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 15 can be specified.

Click **Apply** to implement changes made.

MAC Notification

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database.

MAC Notification Global Settings

To globally set MAC notification on the Switch, open the following window by opening the **MAC Notification** folder and clicking the **MAC Notification Global Settings** link:

Figure 7- 44. MAC Notification Global Settings window

The following parameters may be modified:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval (sec) [1~2147483647]	The time in seconds between notifications.
History size [1~500]	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

MAC Notification Port Settings

To change MAC notification settings for a port or group of ports on the Switch, click **MAC Notification Port Settings** in the **MAC Notification** folder, which will display the following window:

MAC Notification Port Settings			
From	To	State	Apply
Port 1 ▾	Port 1 ▾	Disabled ▾	Apply

MAC Notification Port State Table	
Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled

Figure 7- 45. MAC Notification Port Settings window

The following parameters may be set:

Parameter	Description
From and To	Select a port or group of ports to enable for MAC notification using the pull-down menus.
State	Enable MAC Notification for the ports selected using the pull-down menu.

Click **Apply** to implement changes made.

System Log Server

The Switch can send Syslog messages to up to four designated servers using the System Log Server. In the **Configuration** folder, click **System Log Server**, to view the window shown below.

System Log Servers						
Add New System Log Server						Add
Current System Log Servers						
Index	Server IP	Severity	Facility	UDP Port	Status	Delete
1	10.53.13.94	all	Local0	514	Enabled	X

Figure 7- 46. System Log Servers window

The parameters configured for adding and editing System Log Server settings are the same. To add a new Syslog Server, click the **Add** button. To modify a current entry, click the hyperlinked number of the server in the Index field. Both actions will result in the same window to configure. See the table below for a description of the parameters in the following window.


System Log Server-Add	
Index	1
Server IP	10.53.13.94
Severity	ALL
Facility	Local0
UDP Port	514
Status	Enabled
Apply	
Show All System Log Servers	

Figure 7- 47. System Log Server – Add window

The following parameters can be set:

Parameter	Description
Index	Syslog server settings index.
Server IP	The IP address of the Syslog server.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are <i>Warning</i> , <i>Informational</i> , and <i>ALL</i> .
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. Those Facilities that have been designated are shown in the following. Bold font denotes the facility values that the Switch currently implements.

	<p>Numerical Facility</p> <p>Code</p> <p>0 kernel messages</p> <p>1 user-level messages</p> <p>2 mail system</p> <p>3 system daemons</p> <p>4 security/authorization messages</p> <p>5 messages generated internally by Syslog line printer subsystem</p> <p>7 network news subsystem</p> <p>8 UUCP subsystem</p> <p>9 clock daemon</p> <p>10 security/authorization messages</p> <p>11 FTP daemon</p> <p>12 NTP subsystem</p> <p>13 log audit</p> <p>14 log alert</p> <p>15 clock daemon</p> <p>16 local use 0 (local0)</p> <p>17 local use 1 (local1)</p> <p>18 local use 2 (local2)</p> <p>19 local use 3 (local3)</p> <p>20 local use 4 (local4)</p> <p>21 local use 5 (local5)</p> <p>22 local use 6 (local6)</p> <p>23 local use 7 (local7)</p>
UDP Port	Enter the UDP port number used for sending Syslog messages. The default is <i>514</i> .
Status	Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate.

To set the System Log Server configuration, click **Apply**. To delete an entry from the **System Log Servers** window, click the corresponding  under the Delete heading of the entry to delete. To return to the **System Log Servers** window, click the [Show All System Log Servers](#) link.

Port Access Entity

802.1x Port-Based Access Control

The IEEE 802.1x standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

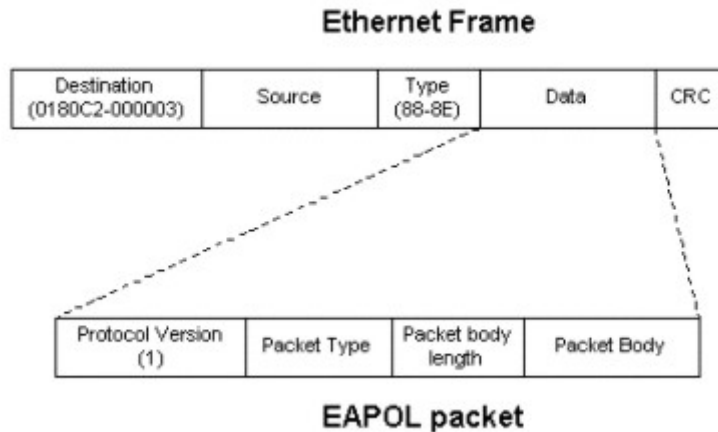


Figure 7- 48. EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1x Access Control protocol consists of three components, each of which is vital to creating and maintaining a stable and working Access Control security method.

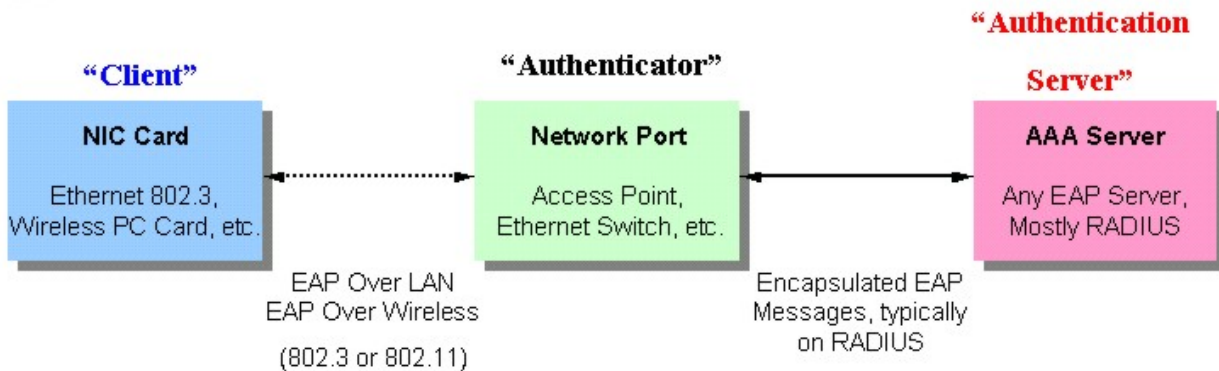


Figure 7- 49. Three Functions of 802.1x

The following section will explain Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the

network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or Switch services.

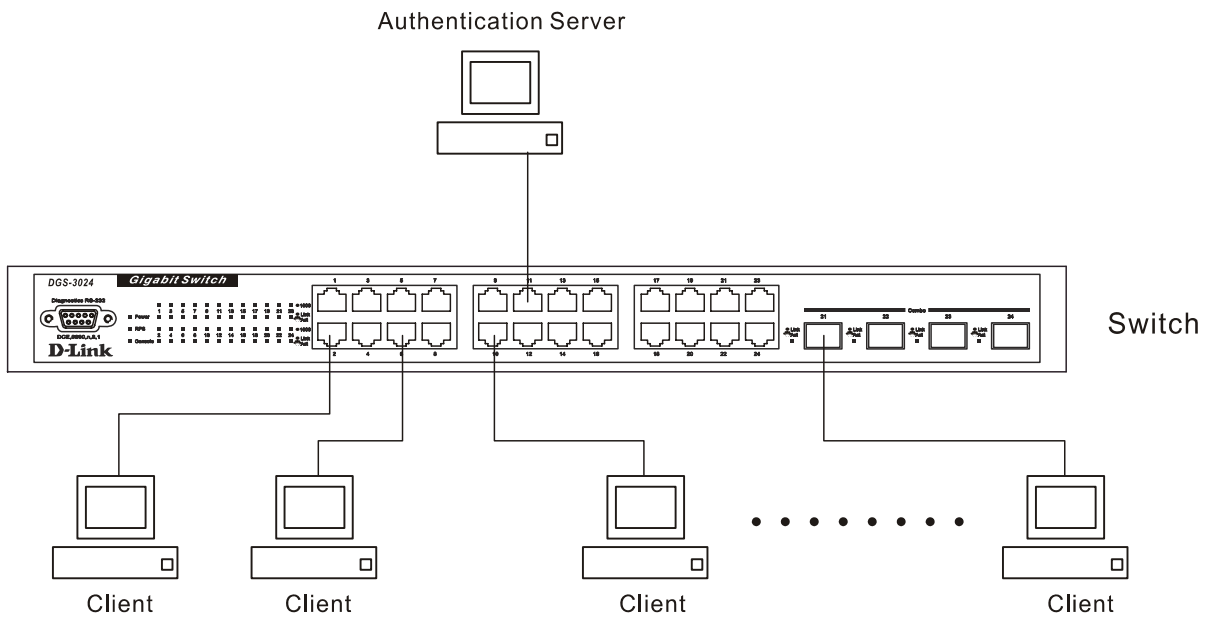


Figure 7- 50. Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing 802.1x. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1x State must be enabled to *Port Base* on the **Switch Information (Advanced Settings)** window under Switch 802.1x (**Configuration > Advanced Settings**).
2. The 802.1x settings must be implemented by port. (**Configuration > Port Access Entity > 802.1x Capability Settings**).
3. A RADIUS server must be configured on the Switch on the **Authentic RADIUS Server Setting** window (**Configuration > Port Access Entity > RADIUS Server**).

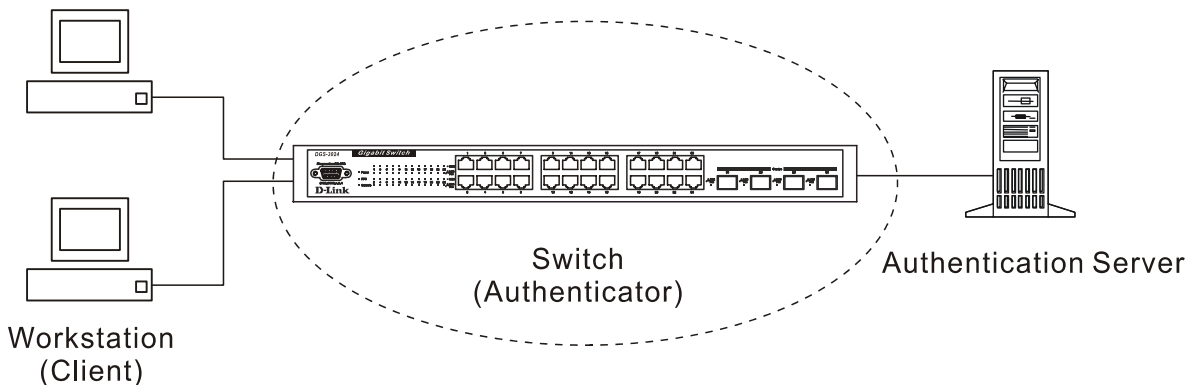


Figure 7- 51. Authenticator

Client

The Client is simply the workstation that wishes to gain access to the LAN or Switch services. All workstation must be running software that is compliant with the 802.1x protocol. For users running Windows XP, the software is included within the operating system. All other users are required to attain 802.1x client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

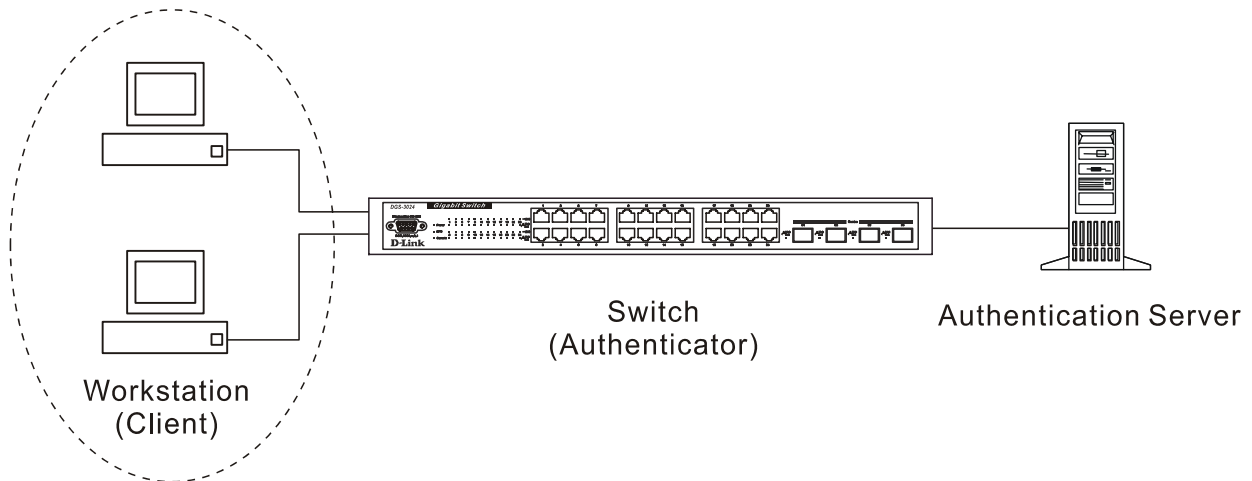


Figure 7- 52. Client

Authentication Process

Utilizing the three components stated above, the 802.1x protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password is granted access and therefore successfully “unlocks” the port. Once unlocked, normal traffic is allowed to pass through the port. The implementation of 802.1x allows network administrators to choose Port-Based Access Control. This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.

Port-Based Network Access Control

The original intent behind the development of 802.1x was to leverage the characteristics of point-to-point in LANs. Any single LAN segment in such an infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

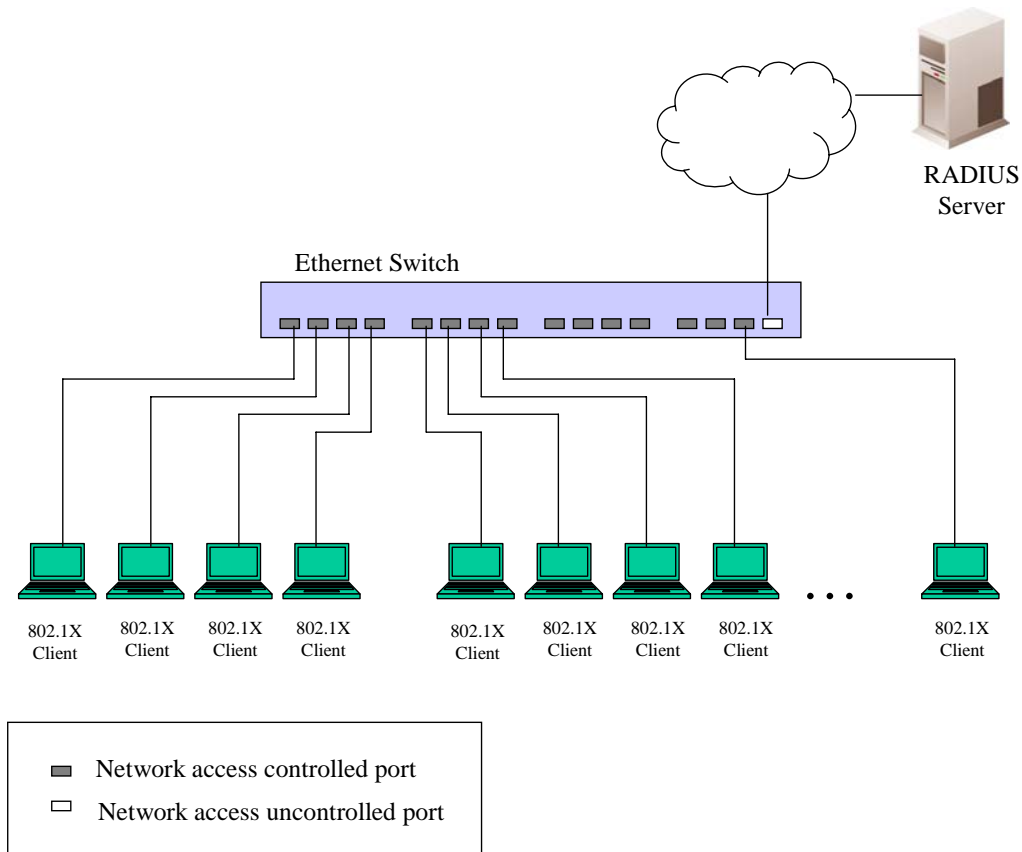


Figure 7- 53. Example of Typical Port-Based Configuration

Once the connected Client has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

Configure Authenticator

To configure the 802.1x Authenticator Settings, click **Configure Authenticator**:

802.1X Authenticator Settings									
Port	AdmDir	Ctrl Stat	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	auto	30	60	30	30	2	3600	no
2	both	auto	30	60	30	30	2	3600	no
3	both	auto	30	60	30	30	2	3600	no
4	both	auto	30	60	30	30	2	3600	no
5	both	auto	30	60	30	30	2	3600	no
6	both	auto	30	60	30	30	2	3600	no
7	both	auto	30	60	30	30	2	3600	no
8	both	auto	30	60	30	30	2	3600	no
9	both	auto	30	60	30	30	2	3600	no
10	both	auto	30	60	30	30	2	3600	no
11	both	auto	30	60	30	30	2	3600	no
12	both	auto	30	60	30	30	2	3600	no
13	both	auto	30	60	30	30	2	3600	no
14	both	auto	30	60	30	30	2	3600	no
15	both	auto	30	60	30	30	2	3600	no
16	both	auto	30	60	30	30	2	3600	no
17	both	auto	30	60	30	30	2	3600	no
18	both	auto	30	60	30	30	2	3600	no
19	both	auto	30	60	30	30	2	3600	no
20	both	auto	30	60	30	30	2	3600	no
21	both	auto	30	60	30	30	2	3600	no
22	both	auto	30	60	30	30	2	3600	no
23	both	auto	30	60	30	30	2	3600	no
24	both	auto	30	60	30	30	2	3600	no

Figure 7- 54. First 802.1x Authenticator Settings window

To configure the settings by port, click on the hyperlinked port number under the Port heading, which will display the following table to configure:

802.1X Authenticator Settings	
From	Port 1 ▾
To	Port 1 ▾
AdmDir	both ▾
PortControl	auto ▾
TxPeriod	30
QuietPeriod	60
SuppTimeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled ▾
Show Authenticators Setting Apply	

Figure 7- 55. Second 802.1x Authenticator Settings window

This window allows you to set the following features:

Parameter	Description
From and To	Enter the port or ports to be set.
AdmDir	<p>Sets the administrative-controlled direction to either <i>in</i> or <i>both</i>.</p> <p>If <i>in</i> is selected, control is only exerted over incoming traffic through the port you selected in the first field.</p> <p>If <i>both</i> is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.</p>
PortControl	<p>This allows you to control the port authorization state.</p> <p>Select <i>forceAuthorized</i> to disable 802.1x and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1x-based authentication of the client.</p> <p>If <i>forceUnauthorized</i> is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.</p> <p>If <i>auto</i> is selected, it will enable 802.1x and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.</p> <p>The default setting is <i>auto</i>.</p>

TxPeriod	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is 30 seconds.
QuietPeriod	This allows you to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is 60 seconds.
SuppTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
ServerTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is 30 seconds.
MaxReq	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is 2.
ReAuthPeriod	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.
ReAuth	Determines whether regular reauthentication will take place on this port. The default setting is <i>Disabled</i> .

Click **Apply** to implement your configuration changes. To view configurations for the 802.1x Authenticator Settings, click [Show Authenticators Setting](#).

Local users

Figure 7- 56. 802.1x Local User Table Configuration window

Enter a User Name, Password, and confirmation of that password. Properly configured local users will be displayed in the 802.1x Local User Table in the same window.

802.1x Capability Settings

Click **802.1x Capability Settings** to view the following window:

802.1X Capability Settings			
From	To	Capability	Apply
Port 1 ▾	Port 1 ▾	None ▾	Apply

802.1X Capability Table	
Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None
13	None
14	None
15	None
16	None
17	None
18	None
19	None
20	None
21	None
22	None
23	None
24	None

Figure 7- 57. 802.1x Capability Settings window

To set up the Switch's 802.1x port-based authentication, select which ports are to be configured in the From and To fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under Capability. Click **Apply** to make your change take effect.

Configure the following 802.1x capability settings:

Parameter	Description
From and To	Ports being configured for 802.1x settings.
Capability	Two role choices can be selected: <i>Authenticator</i> - A user must pass the authentication process to gain access to the

network.

None - The port is not controlled by the 802.1x functions.

Initialize Port(s)

To initialize ports for the port-based side of 802.1x, the user must first enable 802.1x by *Port Base* under Switch 802.1x in the **Switch Information (Advanced Settings)** window.

Existing 802.1x port and MAC settings are displayed and can be configured using the window below.

Click **Initialize Port(s)** to open the following window:

Initialize Port					
From	To	Apply			
Port 1	Port 1	Apply			
Initialize Port Table					
Port	MAC Address	Auth PAE State	Backend_State	Oper Dir	PortStatus

Figure 7- 58. Initialize Port window

This window allows you to initialize a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s).

This window displays the following information:

Parameter	Description
From and To	Select ports to be initialized.
Port	A read-only field indicating a port on the Switch.
MAC Address	The MAC address of the Switch connected to the corresponding port, if any.
Auth PAE State	The Authenticator PAE State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,</i> and <i>N/A</i> .
Backend_State	The Backend Authentication State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize,</i> and <i>N/A</i> .
Oper Dir	Operational Controlled Directions are <i>both</i> and <i>in</i>
PortStatus	The status of the controlled port can be <i>Authorized, Unauthorized,</i> or <i>N/A</i> .



NOTE: The user must first globally enable 802.1x in the **Switch Information (Advanced Settings)** window in the **Configuration** folder before initializing ports. Information in the Initialize Ports Table cannot be viewed before enabling 802.1x.

Reauthenticate Port(s)

This window allows you to reauthenticate a port or group of ports by choosing a port or group of ports by using the pull down menus From and To and clicking **Apply**. The Reauthenticate Port Table displays the current status of the reauthenticated port(s) once you have clicked **Apply**.

Click **Configuration > Port Access Entity > Reauthenticate Port(s)** to open the **Reauthenticate Port(s)** window:

Reauthenticate Port					
From	To	Apply			
Port 1 ▾	Port 1 ▾	Apply			
Reauthenticate Port Table					
Port	MAC Address	Auth State	BackendState	OperDir	PortStatus
1	---	N/A	N/A	both	Authorized
2	---	N/A	N/A	both	Authorized
3	---	N/A	N/A	both	Authorized
4	---	N/A	N/A	both	Authorized
5	---	N/A	N/A	both	Authorized
6	---	N/A	N/A	both	Authorized
7	---	N/A	N/A	both	Authorized
8	---	N/A	N/A	both	Authorized
9	---	N/A	N/A	both	Authorized
10	---	N/A	N/A	both	Authorized

Figure 7- 59. Reauthenticate Port window

This window displays the following information:

Parameter	Description
Port	The port number of the reauthenticated port.
MAC Address	Displays the physical address of the Switch where the port resides.
Auth State	The Authenticator State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth,</i> and <i>N/A</i> .
BackendState	The Backend State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize,</i> and <i>N/A</i> .
OpenDir	Operational Controlled Directions are <i>both</i> and <i>in</i> .
PortStatus	The status of the controlled port can be <i>Authorized, Unauthorized,</i> or <i>N/A</i> .

RADIUS Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

Click **Port Access Entity > RADIUS Server** to open the **Authentic RADIUS Server Setting** window shown below:

Authentic Radius Server Setting					
Succession	First				
Radius Server	0.0.0.0				
Authentic Port	1812				
Accounting Port	1813				
Key					
Confirm Key					
Status	Valid				
Apply					
Current Radius Server(s) Settings Table					
Succession	Radius Server	Auth UDP Port	Acct UDP Port	Key	Status
First					
Second					
Third					

Figure 7- 60. Authentic RADIUS Server Setting window

This window displays the following information:

Parameter	Description
Succession <First>	Choose the desired RADIUS server to configure: <i>First</i> , <i>Second</i> or <i>Third</i> .
RADIUS Server <0.0.0.0>	Set the RADIUS server IP.
Authentic Port <1812>	Set the RADIUS authentic server(s) UDP port. The default port is <i>1812</i> .
Accounting Port <1813>	Set the RADIUS account server(s) UDP port. The default port is <i>1813</i> .
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Status	This allows you to set the RADIUS authentic server to <i>Valid</i> or <i>Invalid</i> .

Static ARP Settings

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices.

Static entries can be defined in the ARP Table. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses.

To open the **Static ARP Table** open the **Configuration** folder and click on the **Static ARP Settings** link.



Interface Name	IP Address	MAC Address	Type	Modify	Delete
----------------	------------	-------------	------	--------	--------

Figure 7- 61. Static ARP Settings window

To add a new entry, click the **Add** button, revealing the following window to configure:

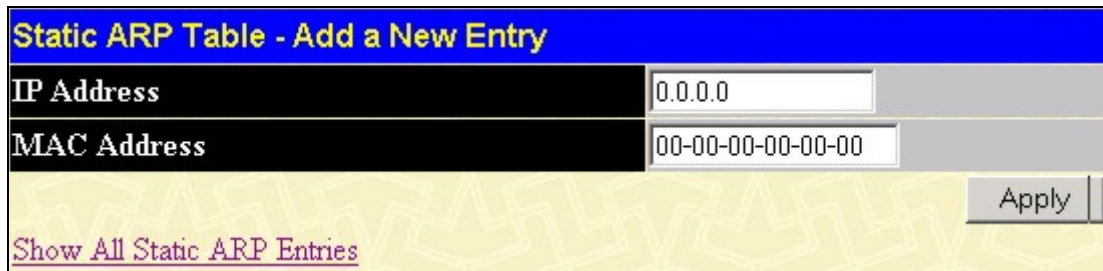


Figure 7- 62. Static ARP Table – Add a New Entry window

The following fields can be set:

Parameter	Description
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.

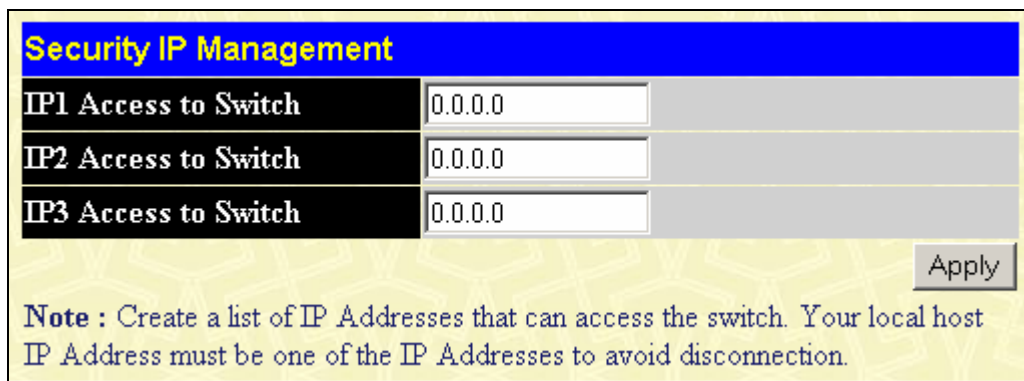
After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To completely clear the Static ARP Settings, click the **Clear All** button.

Security

The second Web Manager main folder is **Security** and includes the following windows and sub-folders: **Trusted Host**, **Secure Socket Layer (SSL)**, **Secure Shell (SSH)**, and **Access Authentication Control**, as well as secondary windows.

Trusted Host

Go to the **Security** folder and click on the **Trusted Host** link; the following window will appear.



Security IP Management	
IP1 Access to Switch	<input type="text" value="0.0.0.0"/>
IP2 Access to Switch	<input type="text" value="0.0.0.0"/>
IP3 Access to Switch	<input type="text" value="0.0.0.0"/>

Apply

Note : Create a list of IP Addresses that can access the switch. Your local host IP Address must be one of the IP Addresses to avoid disconnection.

Figure 8- 1. Security IP Management window

Use security IP management to permit remote stations to manage the Switch. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address and click the **Apply** button.

Secure Socket Layer (SSL)

Secure Sockets Layer or *SSL* is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the ciphersuite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

3. **Hash Algorithm:** This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Download Certificate

This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. Currently, all members of the xStack family come with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

To view the following window, click **Security > Secure Socket Layer (SSL) > Download Certificate**:

Figure 8- 2. Download Certificate window

To download certificates, set the following parameters and click **Apply**.

Parameter	Description
Server IP	Enter the IP address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click **Apply** to implement changes made.

Configuration

This window will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the Switch. A *ciphersuite* is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible ciphersuites for the

SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web-based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://10.90.90.90) Any other method will result in an error and no access can be authorized for the web-based management.

To view the following window, click **Security > Secure Socket Layer (SSL) > Configuration**:

SSL Configuration		
Ciphersuite		
RSA with RC4 128 MD5	Enabled	0x0004
RSA with 3DES EDE CBC SHA	Enabled	0x000a
DHE DSS with 3DES EDE CBC SHA	Enabled	0x0013
RSA EXPORT with RC4 40 MD5	Enabled	0x0003
Status		
Disabled		Apply

Figure 8- 3. SSL Configuration window

To set up the SSL function on the Switch, configure the following parameters and click **Apply**.

Parameter	Description
Status	Use the pull-down menu to enable or disable the SSL status on the Switch. The default is <i>Disabled</i> .
RSA with RC4 128 MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
DHS DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.



NOTE: Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface. For more information on SSL and its functions, see the ***DGS-3024 Command Line Interface Reference Manual***, located on the documentation CD of this product.



NOTE: Enabling the SSL command will disable the web-based Switch management. To log on to the Switch again, the header of the URL must begin with `https://`. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

Secure Shell (SSH)

SSH is an abbreviation of *Secure Shell*, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1. Create a user account with admin-level access using the **User Accounts** window in the **Security** folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
2. Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **Current Accounts** window (**Security > Secure Shell (SSH) > SSH User Authentication**). There are three choices for the method SSH will use to authorize the user: *HostBased*, *Password*, and *Public Key*. Otherwise choose the fourth option, *None*.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the **Encryption Algorithm** window.
4. Finally, enable SSH on the Switch using the **SSH Configuration** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Configuration

The following window is used to configure and view settings for the SSH server and can be opened by clicking **Security > Secure Shell (SSH) > SSH Configuration**:

Current SSH Configuration Settings	
SSH Server Status	Disabled
Max Session	8
Time Out	300
Auth. Fail	2
Session Rekeying	Never
Ports	22

New SSH Configuration Settings	
SSH Server Status	Disabled ▾
Max Session(1-8)	8
Time Out(120-600)	300
Auth. Fail(2-20)	2
Session Rekeying	Never ▾
Port(1-65535)	22

Apply

Figure 8- 4. Current SSH Configuration Settings window

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

Parameter	Description
SSH Server Status	Use the pull-down menu to enable or disable SSH on the Switch. The default is <i>Disabled</i> .
Max Session (1-8)	Enter a value between 1 and 8 to set the number of users that may simultaneously access the Switch. The default setting is 8.
Time Out (120-600)	Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default setting is 120 seconds.
Auth. Fail (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between 2 and 20. The default setting is 2.
Session Rekeying	This field is used to set the time period that the Switch will change the security shell encryptions by using the pull-down menu. The available options are <i>Never</i> , <i>10 min</i> , <i>30 min</i> , and <i>60 min</i> . The default setting is <i>Never</i> .
Port (1-65535)	The TCP port number currently being utilized by the Switch to connect to the SSH server. The "well-known" TCP port for SSH management is 22.

SSH Algorithm

This window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by using their corresponding pull-down menus. All algorithms are enabled by default. To open the following window, click **Security > Secure Shell (SSH) > SSH Algorithm**:

Encryption Algorithm	
3DES-CBC	Enabled ▾
Blow-fish-CBC	Enabled ▾
AES128-CBC	Enabled ▾
AES192-CBC	Enabled ▾
AES256-CBC	Enabled ▾
ARC4	Enabled ▾
Cast128-CBC	Enabled ▾
Twofish128	Enabled ▾
Twofish192	Enabled ▾
Twofish256	Enabled ▾
Data Integrity Algorithm	
HMAC-SHA1	Enabled ▾
HMAC-MD5	Enabled ▾
Public Key Algorithm	
HMAC-RSA	Enabled ▾
HMAC-DSA	Enabled ▾
Authentication Algorithm	
Password	Enabled ▾
Publickey	Enabled ▾
Host-based	Enabled ▾
Apply	

Figure 8- 5. Encryption Algorithm window

The following algorithms may be set:

Parameter	Description
Encryption Algorithm	
3DES-CBC	Use the pull-down to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Blow-fish CBC	Use the pull-down to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .

AES128-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES192-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES256-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
ARC4	Use the pull-down to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Cast128-CBC	Use the pull-down to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Twofish128	Use the pull-down to enable or disable the twofish128 encryption algorithm. The default is <i>Enabled</i> .
Twofish192	Use the pull-down to enable or disable the twofish192 encryption algorithm. The default is <i>Enabled</i> .
Twofish256	Use the pull-down to enable or disable the twofish256 encryption algorithm. The default is <i>Enabled</i> .
Data Integrity Algorithm	
HMAC-SHA1	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is <i>Enabled</i> .
HMAC-MD5	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is <i>Enabled</i> .
Public Key Algorithm	
HMAC-RSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is <i>Enabled</i> .
HMAC-DSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm (DSA) encryption. The default is <i>Enabled</i> .
Authentication Algorithm	
Password	This field may be enabled or disabled to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This field is <i>Enabled</i> by default.
Public Key	This field may be enabled or disabled to choose if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. This field is <i>Enabled</i> by default.
Host-based	This field may be enabled or disabled to choose if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. This field is <i>Enabled</i> by default.

Click **Apply** to implement changes made.

SSH User Authentication

The following windows are used to configure parameters for users attempting to access the Switch through SSH. To access the following window, click **Security Management > Secure Shell > SSH User Authentication Mode**.

Current Accounts			
User Name	Auth. Mode	Host Name	Host IP
DFlint	Password		

Figure 8- 6. Current Accounts window

In the example screen above, the User Account “DFlint” has been previously set using the User Accounts window in the **Management** folder. A User Account **MUST** be set in order to set the parameters for the SSH user. To configure the parameters for a SSH user, click on the hyperlinked User Name in the **Current Accounts** window, which will reveal the following window to configure.

User Name	<input type="text" value="DFlint"/>
Auth. Mode	<input type="text" value="Password"/>
Host Name	<input type="text"/>
Host IP	<input type="checkbox"/> <input type="text" value="0.0.0.0"/>

[Show All User Authntication Entries](#)

Figure 8- 7. untitled SSH User window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Auth. Mode	<p>The administrator may choose one of the following to set the authorization for users attempting to access the Switch.</p> <p><i>Host Based</i> – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.</p> <p style="padding-left: 40px;"><i>Host Name</i> – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user.</p> <p style="padding-left: 40px;"><i>Host IP</i> – Enter the corresponding IP address of the SSH user.</p> <p><i>Password</i> – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.</p> <p><i>Public Key</i> – This parameter should be chosen if the administrator wishes to use the</p>

	publickey on a SSH server for authentication.
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the <i>Host Based</i> choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the <i>Host Based</i> choice in the Auth. Mode field.

Click **Apply** to implement changes made.



NOTE: To set the SSH User Authentication parameters on the Switch, a User Account must be previously configured. For more information on configuring local User Accounts on the Switch, see the User Accounts section of this manual located in this section.

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands let you secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

TACACS (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

Extended TACACS (XTACACS) - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.

TACACS+ (Terminal Access Controller Access Control System plus) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in **Authentication Server Groups**, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set **Authentication Server Hosts** in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no

authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.



NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Authentication Policy & Parameters

This feature will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

To access the following window, click **Security > Access Authentication Control > Policy and Parameters**:

Figure 8- 8. Policy & Parameter Settings window

The following parameters can be set:

Parameters	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 0 and 255 seconds. The default setting is 30 seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 3.

Click **Apply** to implement changes made.

Application Authentication Settings

This window is used to configure Switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list. To view the following window, click **Security > Access Authentication Control > Application Authentication Settings**:

Application Authentication Settings		
Application	Login Method List	Enable Method List
Console	default ▾	default ▾
Telnet	default ▾	default ▾
SSH	default ▾	default ▾
HTTP	default ▾	default ▾
		Apply

Figure 8- 9. Application Authentication Settings window

The following parameters can be set:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH and the Web (HTTP) application.
Login Method List	Using the pull down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Login Method Lists window, in this section, for more information.
Enable Method List	Using the pull down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Enable Method Lists window, in this section, for more information

Click **Apply** to implement changes made.

Authentication Server Group

This window will allow users to set up *Authentication Server Groups* on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view the following window, click **Security > Access Authentication Control > Authentication Server Group**:

Authentication Server Group Settings	
Group Name	Delete
radius	X
tacacs	X
tacacs+	X
xtacacs	X

Figure 8- 10. Authentication Server Group Settings window

This window displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click its hyperlinked Group Name, which will then display the following window.

Add a Server Host to Server Group (xtacacs)		
IP Address	<input type="text" value="0.0.0.0"/>	
Protocol	<input type="text" value="XTACACS"/>	
<input type="button" value="Add"/>		
Server Group (xtacacs)		
IP Address	Protocol	Delete
Show All Server Group Entries		

Figure 8- 11. Add a Server Host to Server Group (XTACACS) window.

To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host and click **Add to Group** to add this Authentication Server Host to the group.

To add a server group other than the ones listed, click the add button, revealing the following window to configure.

Authentication Server Group Table Add Settings	
Group Name	<input type="text"/>
<input type="button" value="Apply"/>	
Show All Server Group Table Entries	

Figure 8- 12. Authentication Server Group Table Add Settings window

Enter a group name of up to 15 characters into the Group Name field and click **Apply**. The entry should appear in the **Authentication Server Group Settings** window.



NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.



NOTE: The three built in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

Authentication Server Host

This window will set user-defined *Authentication Server Hosts* for the TACACS / XTACACS / TACACS+ / RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS / XTACACS / TACACS+ / RADIUS server host on a remote host. The TACACS / XTACACS / TACACS+ / RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS / XTACACS / TACACS+ / RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Security > Access Authentication Control > Authentication Server Host:**

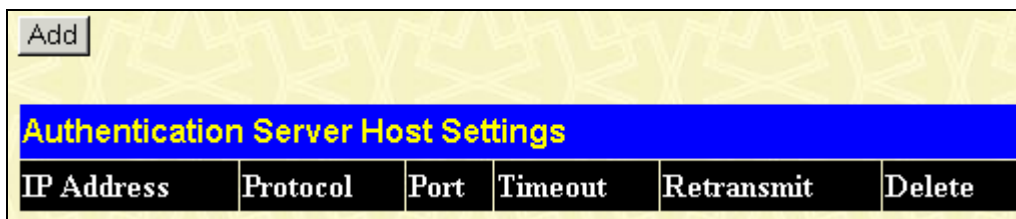


Figure 8- 13. Authentication Server Host Settings window

To add an Authentication Server Host, click the **Add** button, revealing the following window:

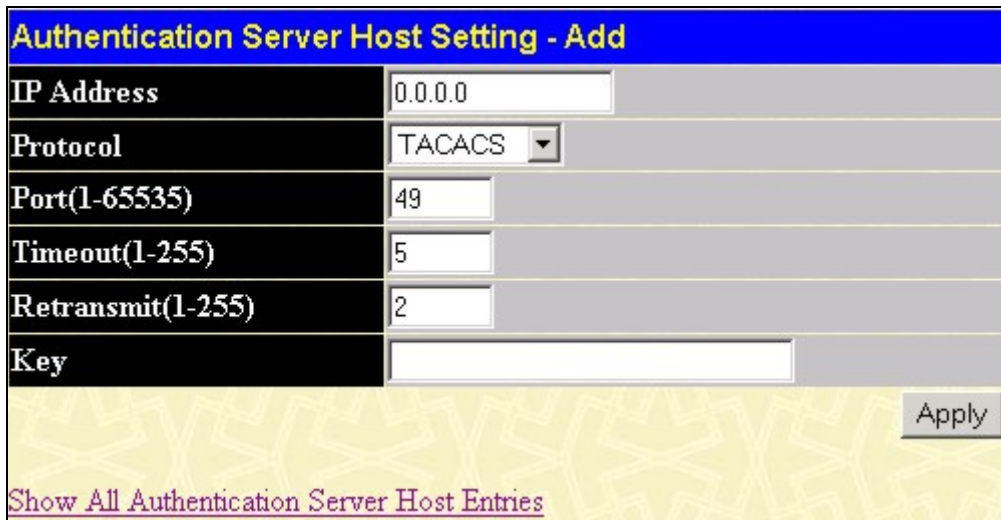


Figure 8- 14. Authentication Server Host Setting - Add window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
-----------	-------------

IP Address	The IP address of the remote server host the user wishes to add.
Protocol	The protocol used by the server host. The user may choose one of the following: <i>TACACS</i> - Enter this parameter if the server host utilizes the TACACS protocol. <i>XTACACS</i> - Enter this parameter if the server host utilizes the XTACACS protocol. <i>TACACS+</i> - Enter this parameter if the server host utilizes the TACACS+ protocol. <i>RADIUS</i> - Enter this parameter if the server host utilizes the RADIUS protocol.
Port (1-65535)	Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1813 for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.

Click **Apply** to add the server host.



NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other

Login Method Lists

This command will configure a user-defined or default *Login Method List* of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS - XTACACS- local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a "User" privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator. (See the Enable Admin part of this section for more detailed information concerning the Enable Admin command.)

To view the following screen click **Security > Access Authentication Control > Login Method Lists:**

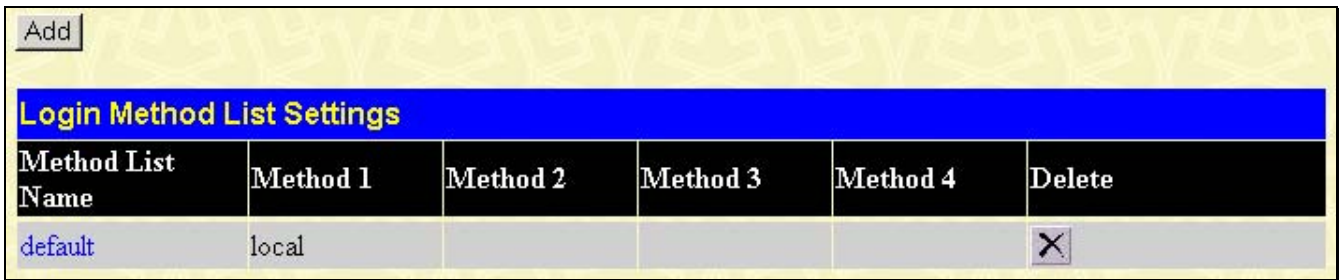



Figure 8- 15. Login Method List Settings window

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the  under the **Delete** heading corresponding to the entry desired to be deleted. To modify a Login Method List, click on its hyperlinked Method List Name. To configure a new Method List, click the **Add** button.

Both actions will result in the same screen to configure:

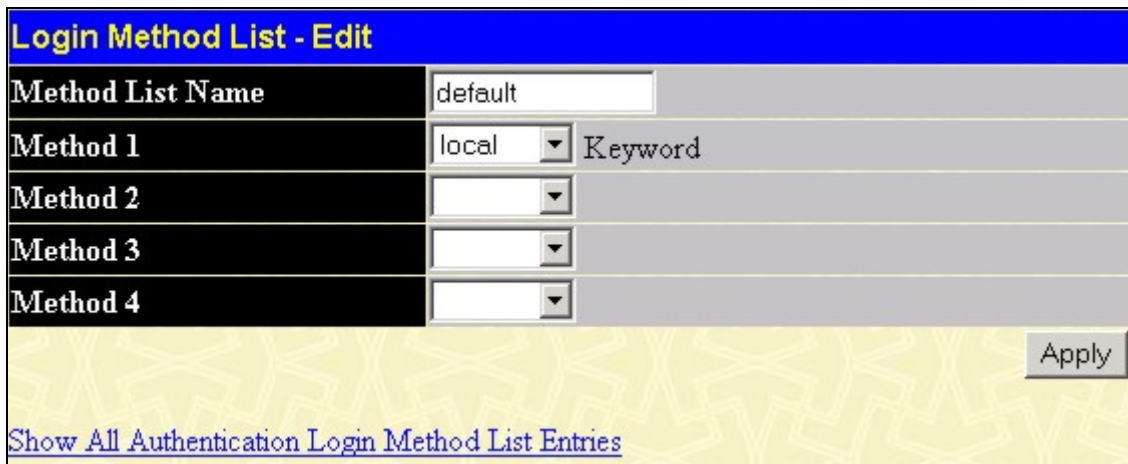


Figure 8- 16. Login Method List - Edit window (default)

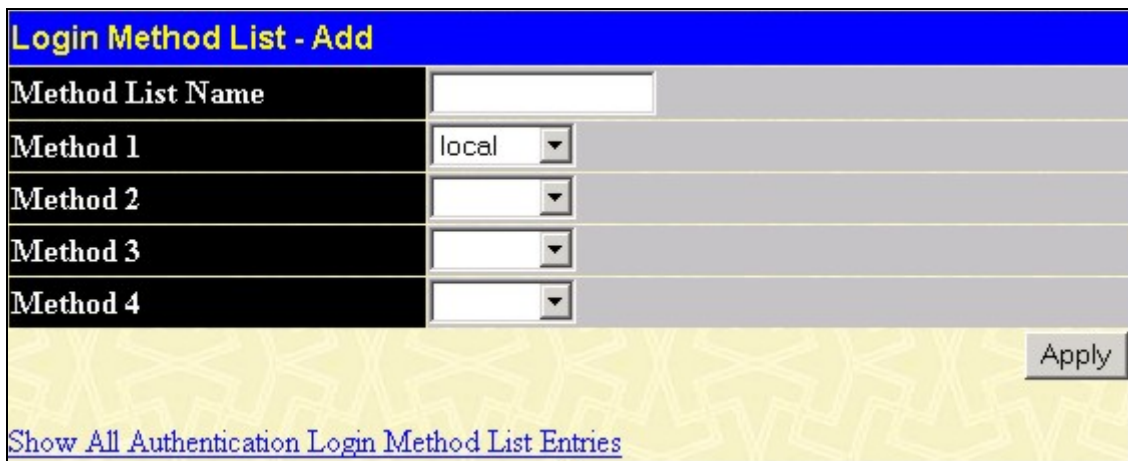


Figure 8- 17. Login Method List – Add window

To define a Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	The user may add one, or a combination of up to four of the following authentication

	<p>methods to this method list:</p> <p><i>tacacs</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>xtacacs</i> - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p> <p><i>tacacs+</i> - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.</p> <p><i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><i>server_group</i> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.</p> <p><i>local</i> - Adding this parameter will require the user to be authenticated using the local user account database on the Switch.</p> <p><i>none</i> - Adding this parameter will require no authentication to access the Switch.</p>
--	--

Enable Method Lists

The **Enable Method Lists** window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.




NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following table, click **Security > Access Authentication Control > Enable Method Lists**:

Add					
Enable Method List Settings					
Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local_enable				✕

Figure 8- 18. Enable Method List Settings window

To delete an Enable Method List defined by the user, click the  under the Delete heading corresponding to the entry desired to be deleted. To modify an Enable Method List, click on its hyperlinked Method List Name. To configure a Method List, click the **Add** button.

Both actions will result in the same window to configure:

Figure 8- 19. Enable Method List - Edit window

Figure 8- 20. Enable Method List - Add window

To define an Enable Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><i>local_enable</i> - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section entitled Local Enable Password.</p> <p><i>none</i> - Adding this parameter will require no authentication to access the Switch.</p> <p><i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p>

	<p><i>tacacs</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>xtacacs</i> - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p> <p><i>tacacs+</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>server_group</i> - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.</p>
--	---

Configure Local Enable Password

This window will configure the locally enabled password for the Enable Admin command. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security > Access Authentication Control > Configure Local Enable Password**:

Figure 8- 21. Configure Local Enable Password window

To set the Local Enable Password, set the following parameters and click **Apply**.

Parameter	Description
Old Local Enable Password	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable Password	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable Password	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Click **Apply** to implement changes made.

Enable Admin

The **Enable Admin** window is for users who have logged on to the Switch on the normal user level, and wish to be promoted to the administrator level. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and

a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

To view the following window, click **Security > Access Authentication Control > Enable Admin:**

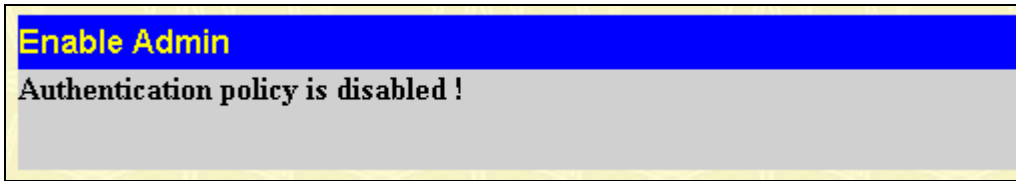


Figure 8- 22. Enable Admin window

When this window appears, click the **Enable Admin** button revealing a dialog box for the user to enter authentication (password, username), as seen below. A successful entry will promote the user to Administrator level privileges on the Switch.

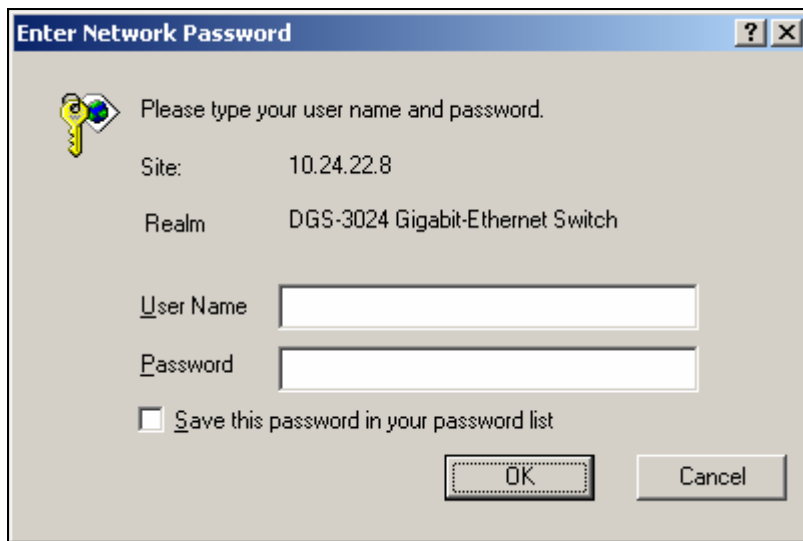


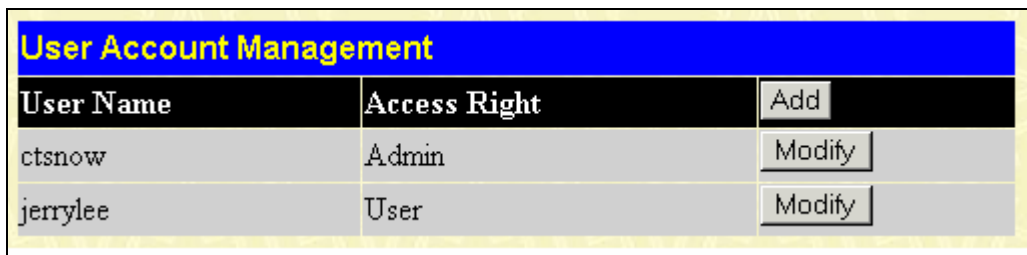
Figure 8- 23. Enter Network Password dialog box

Management

The third Web Manager main folder is **Management** and includes the following windows and sub-folders: **User Accounts** and **SNMPV3**, as well as secondary windows.

User Accounts

The Switch allows you to set up and manage user accounts in the following windows.



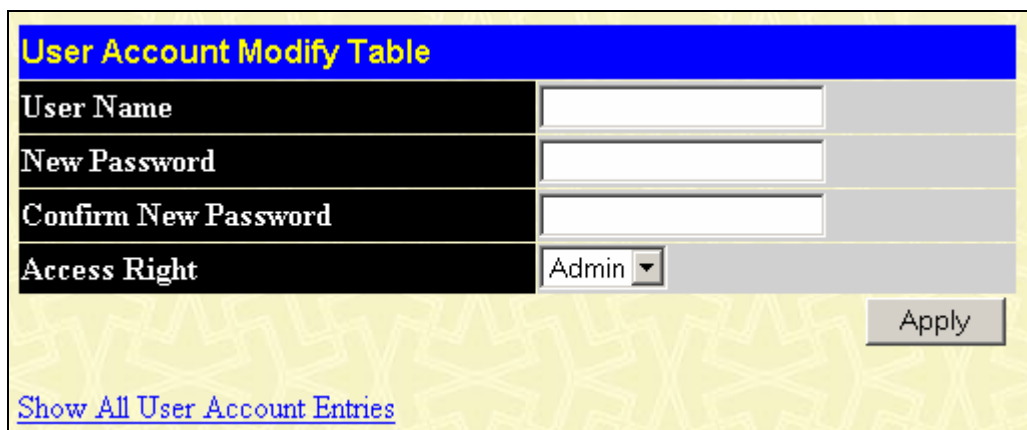
User Account Management		
User Name	Access Right	
ctsnow	Admin	Add Modify
jerrylee	User	Modify

Figure 9- 1. User Account Management window

The information on the window is described as follows:

The following fields can be set:

Parameter	Description
User Name	Displays all current users for the Switch.
Access Right	Displays the current access level assigned to each corresponding user. There are two access levels: <i>User</i> and <i>Admin</i> . <i>Admin</i> has full read/write access, while a <i>User</i> has read-only access.



User Account Modify Table	
User Name	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Access Right	Admin ▾
<input type="button" value="Apply"/>	
Show All User Account Entries	

Figure 9- 2. User Account Modify Table window (Add)

To add a User Account, fill in the appropriate information in the Username, New Password, and Confirm New Password fields. Then select the desired access, *Admin* or *User*, in the Access Right drop-down menu and click **Apply**.

The information on the window is described as follows:

Parameter	Description
User Name	Enter a user name in this field.
New Password	Enter the desired new password in this field.
Confirm New Password	Enter the new password a second time.
Access Right	Displays the current access level assigned to each corresponding user. There are two access levels: <i>Admin</i> and <i>User</i> . An <i>Admin</i> user has full read/write access, while a <i>User</i> has read-only access.

Figure 9- 3. User Account Modify Table window (Edit)

To edit a User Account, fill in the appropriate information in the Old Password, New Password, and Confirm New Password fields. Click **Apply** to make your change take effect.

The information on the window is described as follows:

Parameter	Description
User Name	The user name being edited.
Old Password	Enter the last password used in this field.
New Password	Enter the desired new password in this field.
Confirm New Password	Enter the new password a second time.

Admin and User Privileges

There are two levels of user privileges, *Admin* and *User*. Some menu selections available to users with *Admin* privileges may not be available to those with *User* privileges.

The following table summarizes the *Admin* and *User* privileges:

Management	Admin	User
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only
Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	No
Factory Reset	Yes	No
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Table 9- 1. Admin and User Privileges

After establishing a User Account with Admin-level privileges, be sure to save the changes by opening the **Maintenance** folder, opening the **Save Configuration** window and clicking the **Save Configuration** button.

SNMP Manager

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 DGS-3204 supports the SNMP versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

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.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

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 SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

SNMP User Table

Use the **SNMP User Table** window to create a new SNMP user and add the user to an existing SNMP group or to a newly created group.

User Name	Group Name	SNMP Version	Delete
initial	initial	V3	

Figure 9- 4. SNMP User Table window

To delete an existing entry, click the Delete icon in the right-hand column that corresponds to the port you want to remove.

To create a new entry, click the **Add** button, a separate window will appear.

Figure 9- 5. SNMP User Table Configuration window

The following parameters can be set:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP V3 Encryption	Check to use encryption.
Auth-Protocol	<i>MD5</i> - Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when the Encryption field has been checked. This field will require the user to enter a password.

	<i>SHA</i> - Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when the Encryption field has been checked. This field will require the user to enter a password.
Priv-Protocol	<p><i>None</i> - Specifies that no authorization protocol is in use.</p> <p><i>DES</i> - Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when the Encryption field has been checked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.</p>

To implement changes made, click **Apply**. To return to the SNMP User Table, click the [Show All SNMP User Table Entries](#) link.

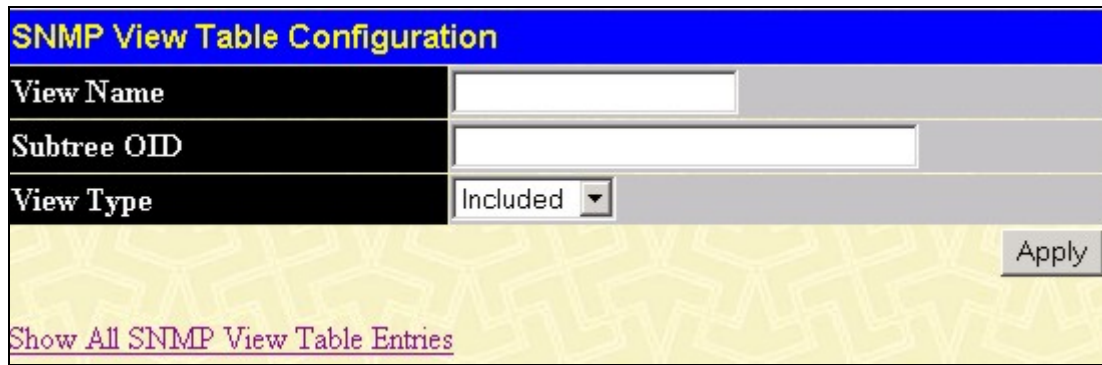
SNMP View Table

The SNMP View Table is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. To view the **SNMP View Table** window, open the **SNMP Manager** folder under **Management** and click the **SNMP View Table** entry. The following window should appear:

View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	<input type="checkbox"/>
restricted	1.3.6.1.2.1.11	Included	<input type="checkbox"/>
restricted	1.3.6.1.6.3.10.2.1	Included	<input type="checkbox"/>
restricted	1.3.6.1.6.3.11.2.1	Included	<input type="checkbox"/>
restricted	1.3.6.1.6.3.15.1.1	Included	<input type="checkbox"/>
CommunityView	1	Included	<input type="checkbox"/>
CommunityView	1.3.6.1.6.3	Excluded	<input type="checkbox"/>
CommunityView	1.3.6.1.6.3.1	Included	<input type="checkbox"/>

Figure 9- 6. SNMP View Table window

To delete an existing SNMP View Table entry, click the in the Delete column corresponding to the entry you wish to delete. To create a new entry, click the **Add** button and a separate window will appear.



The image shows a web-based configuration window titled "SNMP View Table Configuration". It has a blue header bar with the title. Below the header, there are three input fields: "View Name" (a text box), "Subtree OID" (a text box), and "View Type" (a dropdown menu currently set to "Included"). To the right of these fields is an "Apply" button. At the bottom left of the window, there is a link that says "Show All SNMP View Table Entries".

Figure 9- 7. SNMP View Table Configuration window

The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

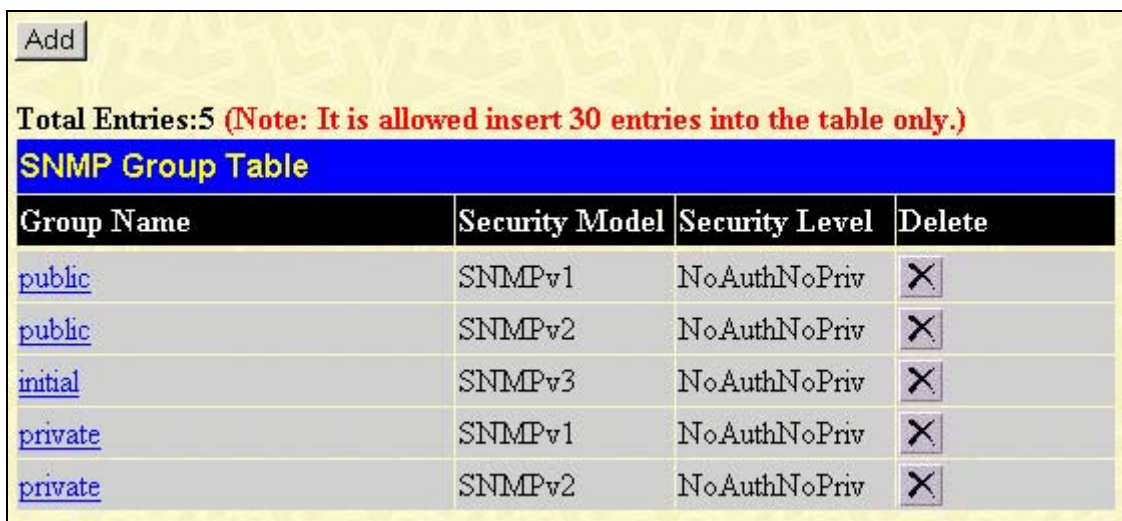
The following parameters can be set:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

To implement your new settings, click **Apply**. To return to the SNMP View Table, click the [Show All SNMP View Table Entries](#) link.

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous menu. To view the **SNMP Group Table** window, open the **SNMP Manager** folder in the **Management** folder and click the **SNMP Group Table** entry. The following window should appear:



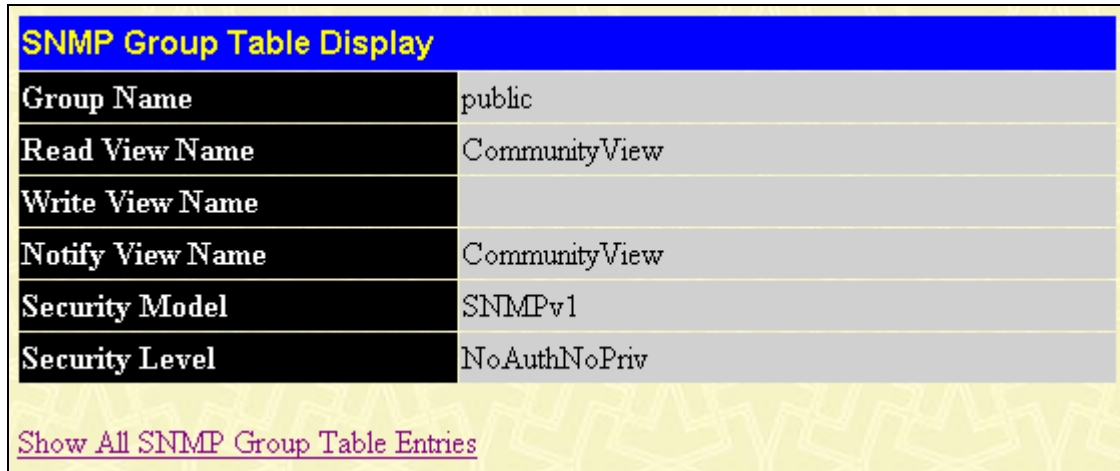
The image shows a web-based window titled "SNMP Group Table". At the top left is an "Add" button. Below it, the text "Total Entries:5 (Note: It is allowed insert 30 entries into the table only.)" is displayed. The main content is a table with a blue header bar containing the title "SNMP Group Table". The table has four columns: "Group Name", "Security Model", "Security Level", and "Delete". There are five rows of data, each with a blue underlined link in the "Group Name" column and an "X" icon in the "Delete" column.

Group Name	Security Model	Security Level	Delete
public	SNMPv1	NoAuthNoPriv	X
public	SNMPv2	NoAuthNoPriv	X
initial	SNMPv3	NoAuthNoPriv	X
private	SNMPv1	NoAuthNoPriv	X
private	SNMPv2	NoAuthNoPriv	X

Figure 9- 8. SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding  under the Delete heading.

To display the current settings for an existing SNMP Group Table entry, click the hyperlink for the entry under the Group Name.



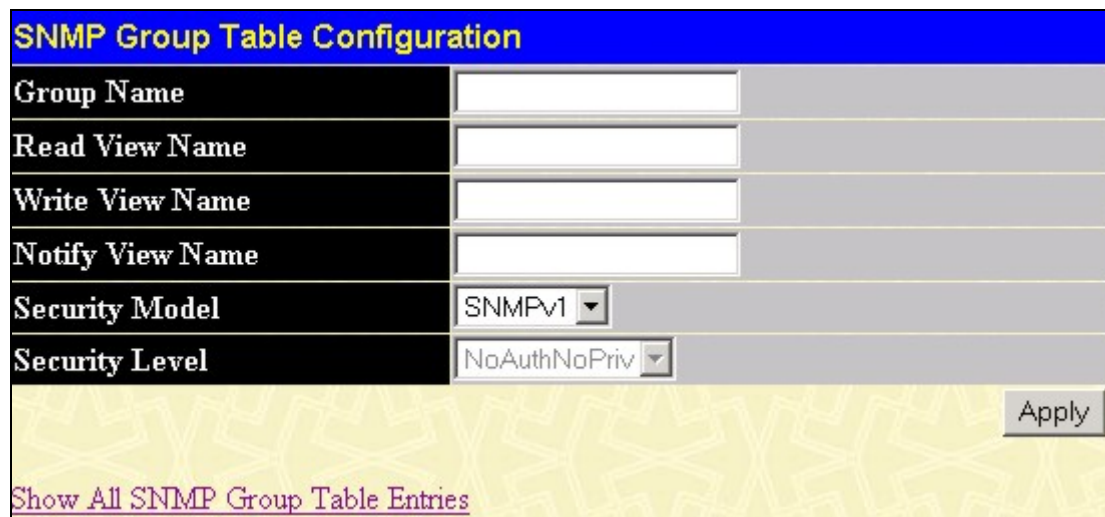
The image shows a window titled "SNMP Group Table Display" with a blue header. It contains a table with the following data:

Group Name	public
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv

At the bottom of the window, there is a link: [Show All SNMP Group Table Entries](#).

Figure 9- 9. SNMP Group Table Display window

To add a new entry to the Switch's SNMP Group Table, click the **Add** button in the upper left-hand corner of the **SNMP Group Table** window. This will open the **SNMP Group Table Configuration** window, as shown below.



The image shows a window titled "SNMP Group Table Configuration" with a blue header. It contains a form with the following fields:

Group Name	<input type="text"/>
Read View Name	<input type="text"/>
Write View Name	<input type="text"/>
Notify View Name	<input type="text"/>
Security Model	SNMPv1 <input type="button" value="v"/>
Security Level	NoAuthNoPriv <input type="button" value="v"/>

At the bottom right of the form is an **Apply** button. At the bottom left of the window, there is a link: [Show All SNMP Group Table Entries](#).

Figure 9- 10. SNMP Group Table Configuration window

The following parameters can be set:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.

Security Model	<p><i>SNMPv1</i> – Specifies that SNMP version 1 will be used.</p> <p><i>SNMPv2</i> – Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>SNMPv3</i> – Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.</p>
Security Level	<p>The Security Level settings only apply to SNMPv3.</p> <p><i>NoAuthNoPriv</i> - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthNoPriv</i> - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthPriv</i> - Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p>

To implement your new settings, click **Apply**. To return to the SNMP Group Table, click the [Show All SNMP Group Table Entries](#) link.

SNMP Community Table

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.


To configure SNMP Community entries, open the **SNMP Manager** folder, located in the **Management** folder, and click the **SNMP Community Table** link, which will open the following window:

SNMP Community Table Configuration			
Community Name	View Name	Access Right	
<input type="text"/>	<input type="text"/>	Read Only ▾	
<input type="button" value="Apply"/>			
Total Entries:2 (Note: Insert a maximum of 10 entries into the table.)			
SNMP Community Table			
Community Name	View Name	Access Right	Delete
private	CommunityView	Read Write	<input type="button" value="X"/>
public	CommunityView	Read Only	<input type="button" value="X"/>

Figure 9- 11. SNMP Community Table Configuration window

The following parameters can be set:


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.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	<p><i>Read Only</i> – Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch.</p> <p><i>Read Write</i> – Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.</p>

To implement the new settings, click **Apply**. To delete an entry from the SNMP Community Table, click the  under the Delete heading, corresponding to the entry you wish to delete.

SNMP Host Table

Use the **SNMP Host Table** window to set up SNMP trap recipients.

Open the **SNMP Manager** folder, located in the **Management** folder and click on the **SNMP Host Table** link. This will open the **SNMP Host Table** window, as shown below.

To delete an existing SNMP Host Table entry, click the corresponding  under the Delete heading.

To display the current settings for an existing SNMP Group Table entry, click the blue link for the entry under the Host IP Address heading.

Add

Total Entries:0 (Note: It is allowed insert 10 entries into the table only.)

SNMP Host Table

Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete
-----------------	--------------	---------------------------------	--------

Figure 9- 12. SNMP Host Table window

To add a new entry to the Switch's SNMP Host Table, click the **Add** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below.

SNMP Host Table Configuration

Host IP Address: 0.0.0.0

SNMP Version: V1

Community String / SNMPv3 User Name:

Apply

[Show All SNMP Host Table Entries](#)

Figure 9- 13. SNMP Host Table Configuration window

The following parameters can be set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	<p>V1 - To specifies that SNMP version 1 will be used.</p> <p>V2 - To specify that SNMP version 2 will be used.</p> <p>V3-NoAuth-NoPriv - To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.</p> <p>V3-Auth-NoPriv - To specify that the SNMP version 3 will be used, with a Auth-NoPriv security level.</p> <p>V3-Auth-Priv - To specify that the SNMP version 3 will be used, with a Auth-Priv security level.</p>
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To implement your new settings, click **Apply**. To return to the SNMP Host Table, click the [Show All SNMP Host Table Entries](#) link.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.

To display the Switch's SNMP Engine ID, open the **SNMP Manager** folder, located in the **Management** folder and click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.

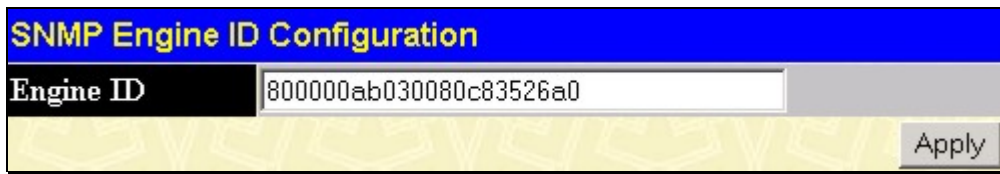


Figure 9- 14. SNMP Engine ID Configuration window

To change the Engine ID, type the new Engine ID in the space provided and click the **Apply** button

Monitoring

The fourth Web Manager main folder is **Monitoring** and includes the following windows and sub-folders: **Port Utilization**, **Packets**, **Errors**, **Size**, **MAC Address**, **Switch History Log**, **IGMP Snooping Group**, **IGMP Snooping Forwarding**, **VLAN Status**, **Router Port**, **Session Table**, and **Port Access Control**, as well as secondary windows.

Port Utilization

The **Utilization** window displays the percentage of the total available bandwidth being used on the port.

To view the port utilization, open the **Monitoring** folder and then click the **Port Utilization** link:

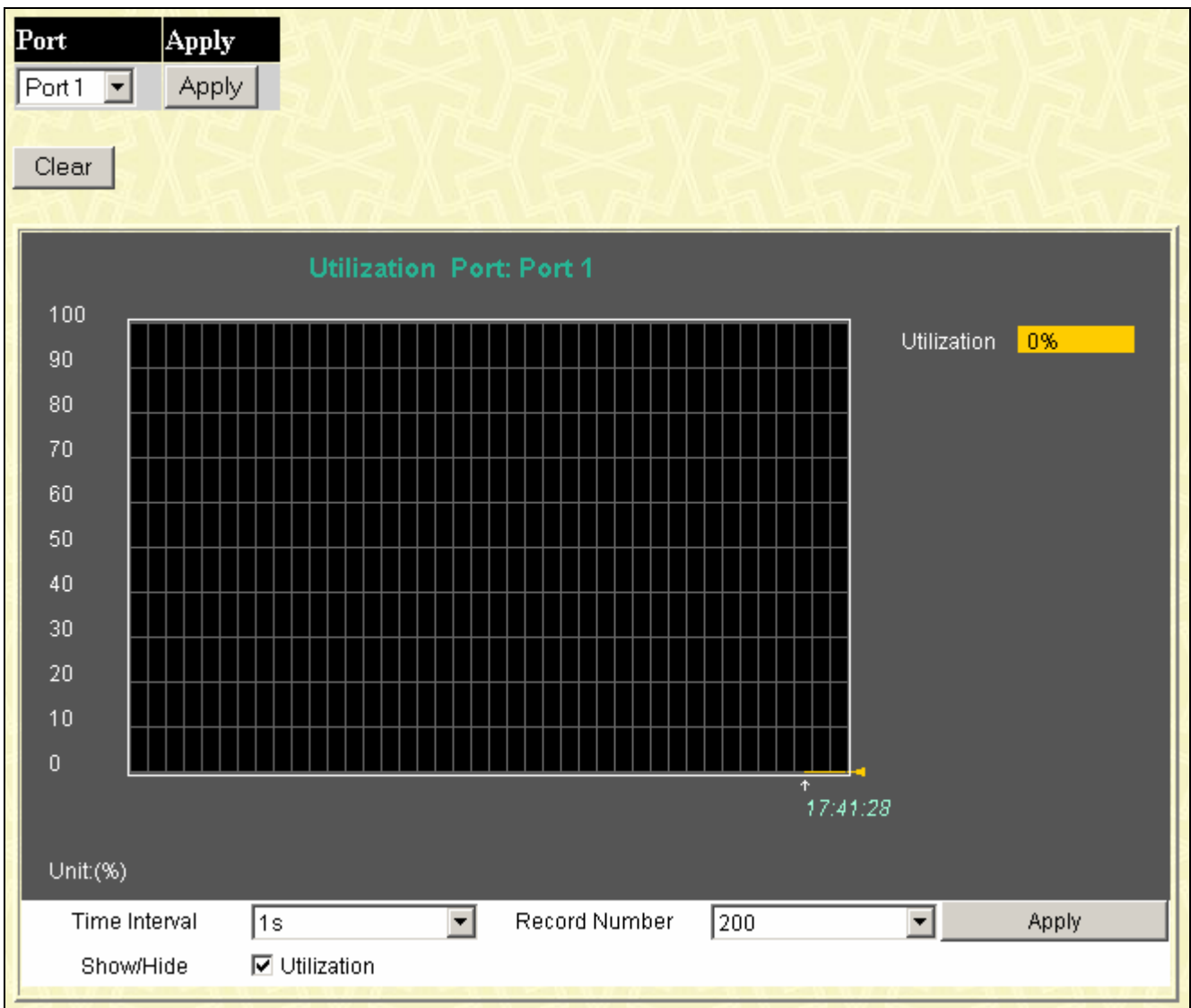


Figure 10- 1. Utilization window

The following fields can be set:

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

Click **Apply** to implement your changes.

Packets

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

Received (RX)

Click the **Received (RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets received on the Switch.

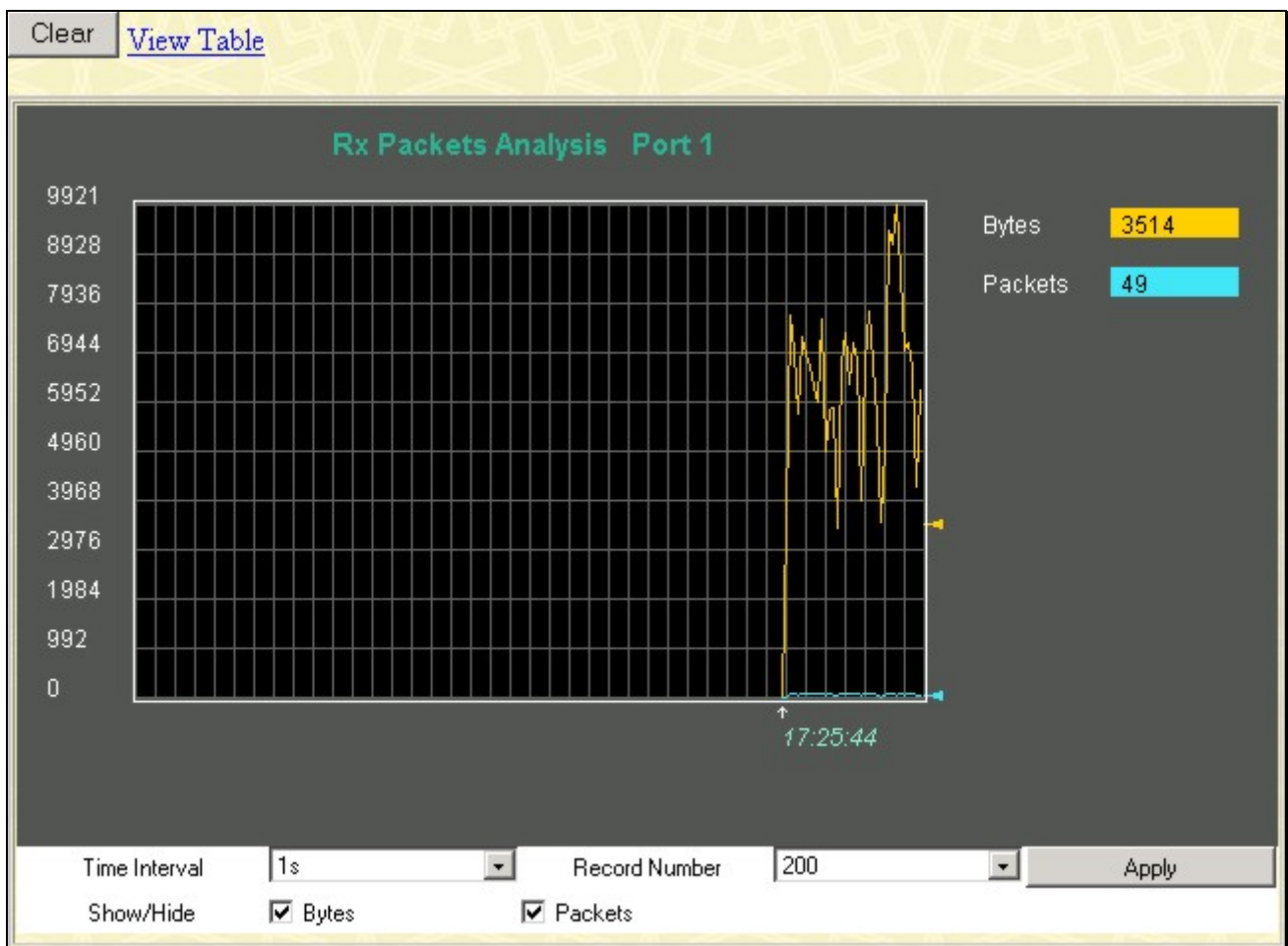


Figure 10- 2. Rx Packets Analysis window (line graph for Bytes and Packets)

To view the Received Packets Table, click the link [View Table](#), which will show the following table:

[View LineChart](#)

Packet Analysis of Port 1 Time Interval

Rx Packets	Total	Total/Sec
Bytes	0	0
Packets	0	0

Rx Packets	Total	Frames/Sec
Unicast	0	0
Multicast	0	0
Broadcast	0	0

Tx Packets	Total	Total/Sec
Bytes	0	0
Packets	0	0

Figure 10- 3. Rx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number	Select the number of times the Switch will be polled between 20 and 200. The default value is 20.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Show/Hide	Check whether to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB Cast (RX)

Click the **UMB Cast (RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of UMB cast packets received on the Switch.

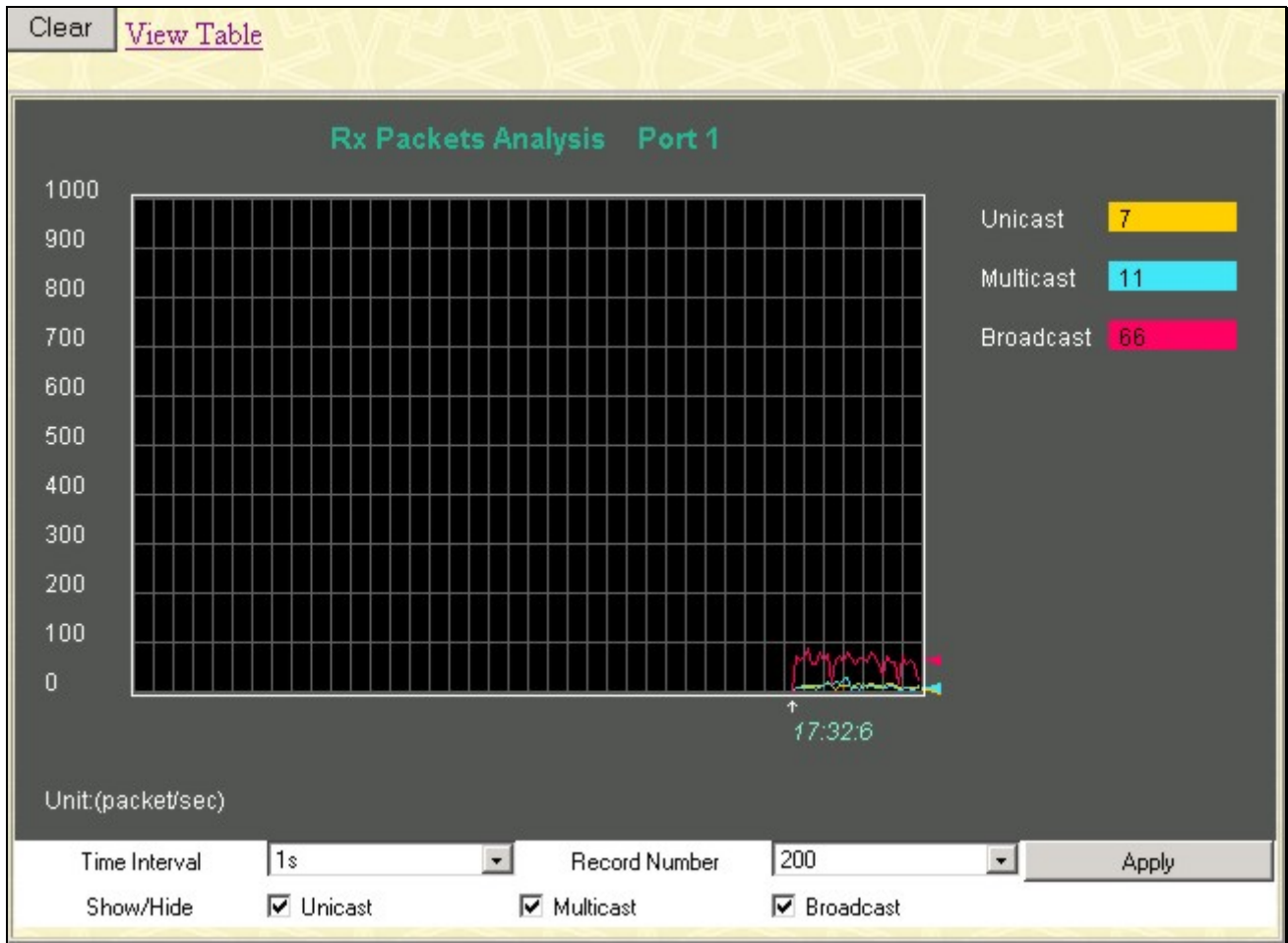


Figure 10- 4. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)

To view the UMB Cast Table, click the [View Table](#) link, which will show the following table:

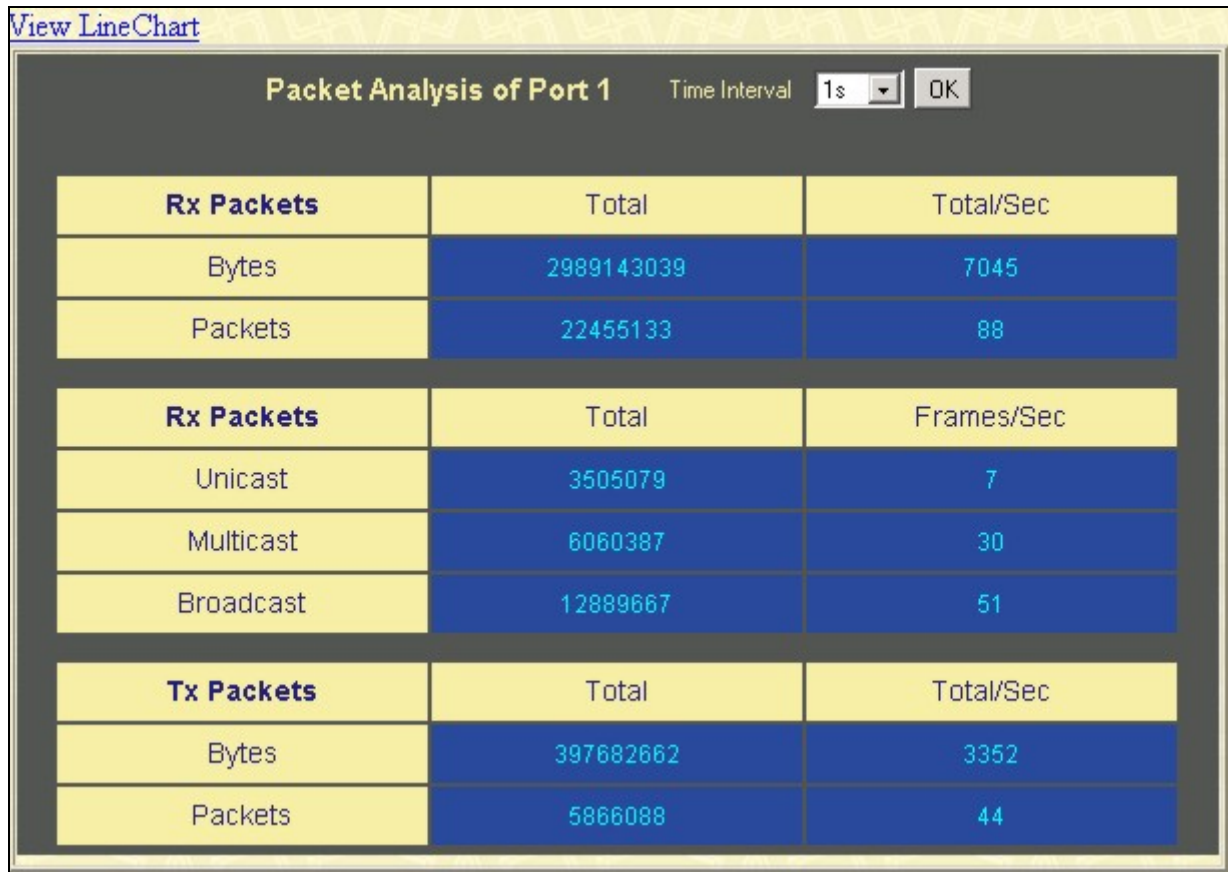


Figure 10- 5. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

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

Transmitted (TX)

Click the **Transmitted (TX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets transmitted from the Switch.

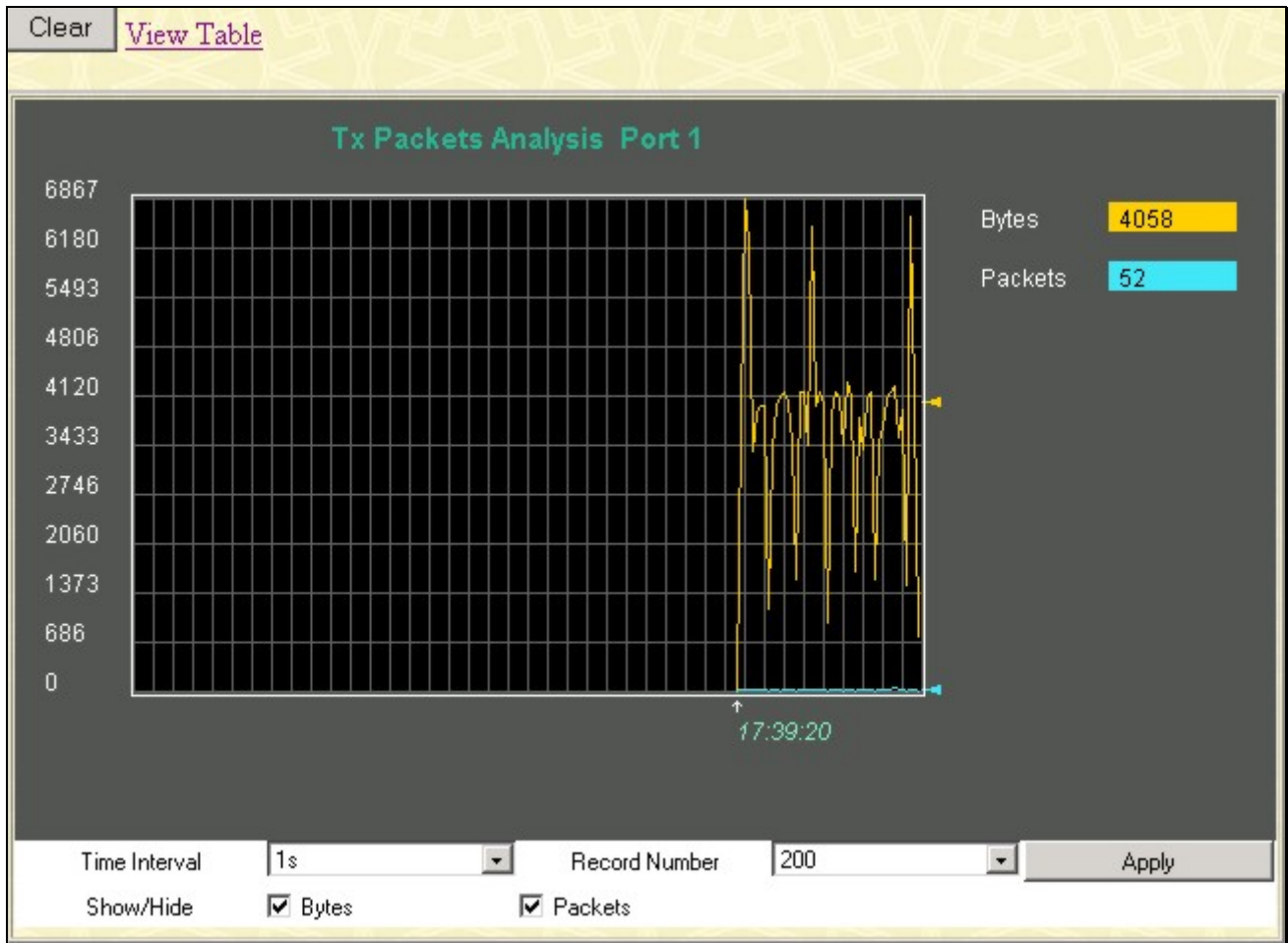


Figure 10- 6. Tx Packets Analysis window (line graph for Bytes and Packets)

To view the Transmitted (TX) Table, click the link [View Table](#), which will show the following table:

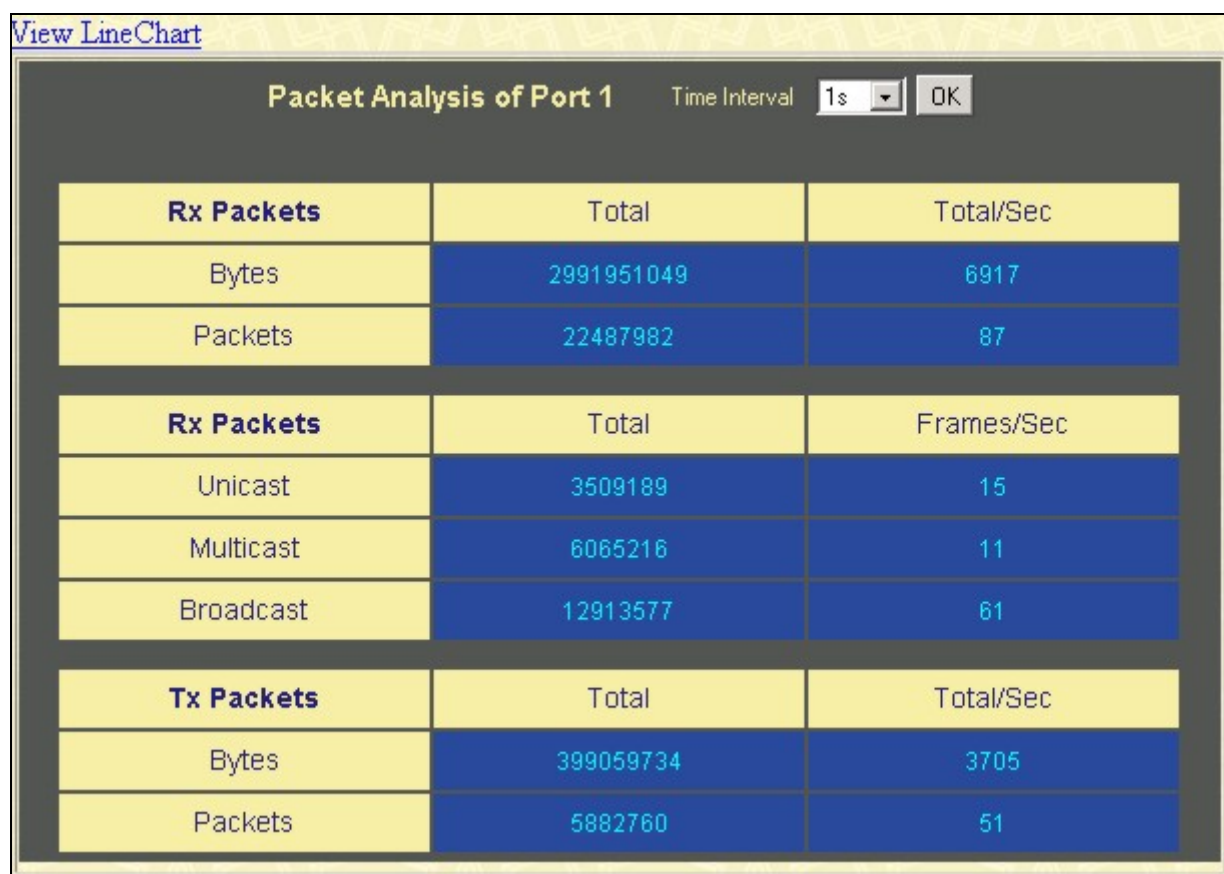


Figure 10- 7. Tx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

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

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. Four windows are offered.

Received (RX)

Click the **Received (RX)** link in the **Errors** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch.

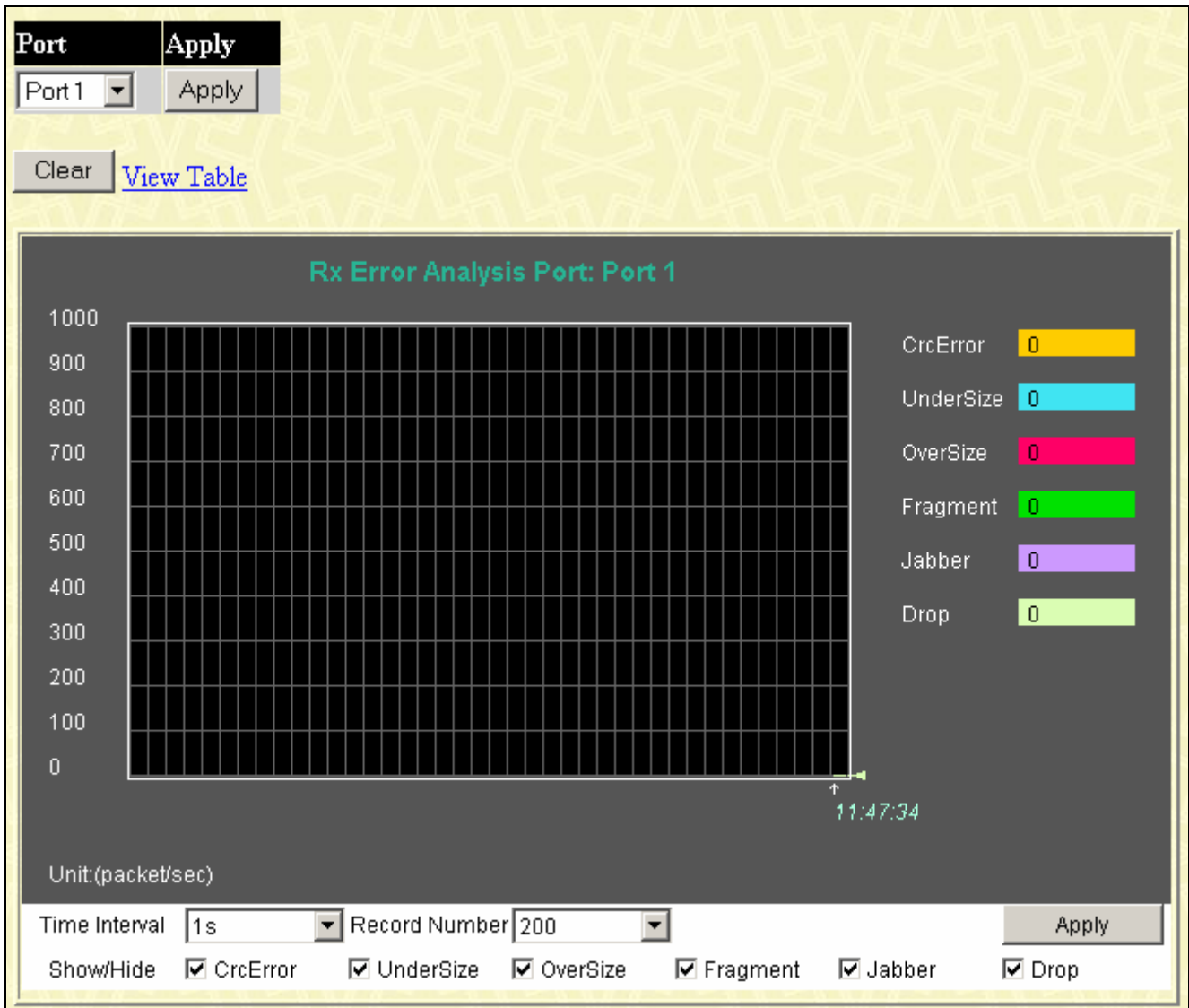


Figure 10- 8. Rx Error Analysis window (line graph)

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

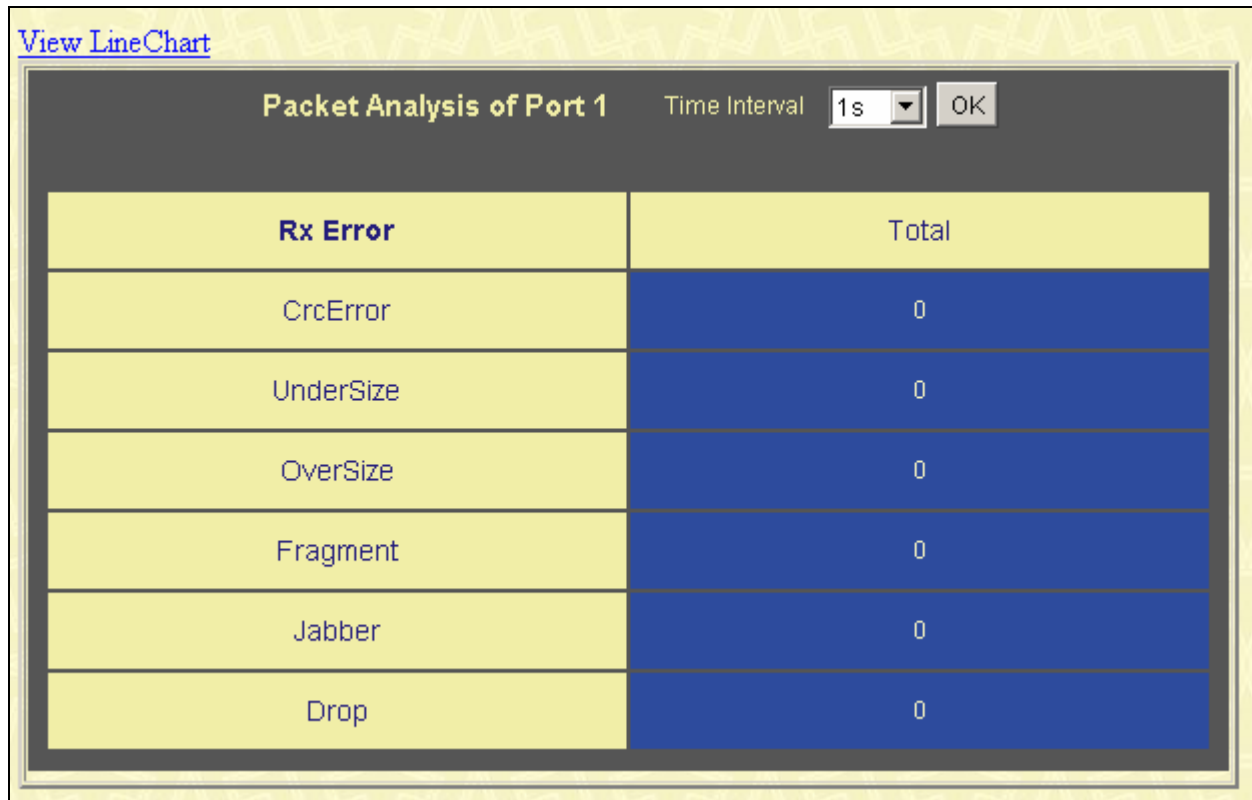


Figure 10- 9. Rx Error Analysis window (table)

The following fields can be set:

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

Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

Click the **Transmitted (TX)** link in the **Errors** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch.

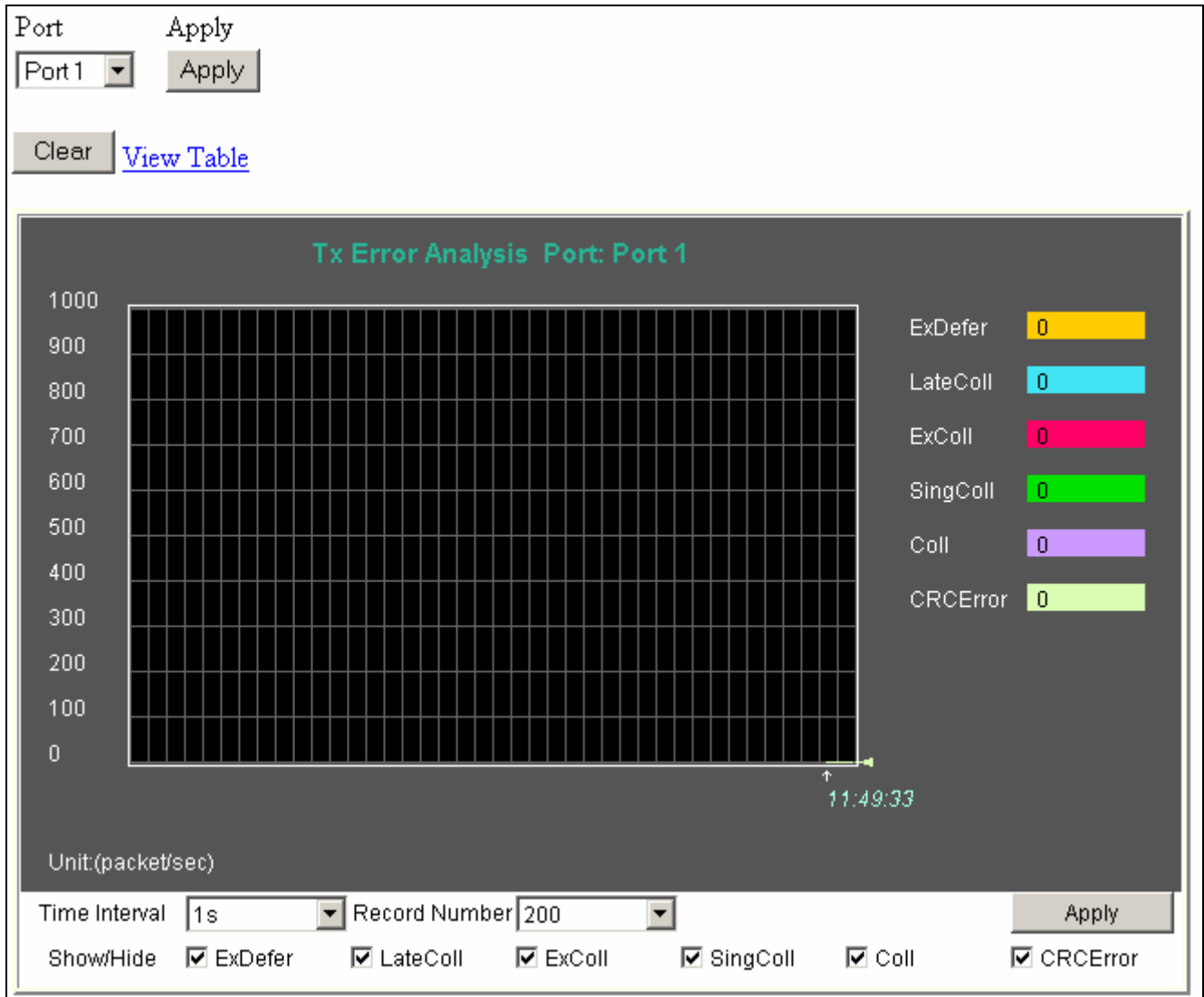


Figure 10- 10. Tx Error Analysis window (line graph)

To view the Transmitted Error Packets Table, click the link [View Table](#), which will show the following table:

[View LineChart](#)

Packet Analysis of Port 1 Time Interval

Tx Error	Total
ExDefer	0
LateColl	0
ExColl	0
SingColl	0
Coll	0
CRCError	0

Figure 10- 11. Tx Error Analysis window (table)

The following fields may be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number	Select the number of times the Switch will be polled between 20 and 200. The default value is 20.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Coll	An estimate of the total number of collisions on this network segment.
CRCError	Counts otherwise valid packets that did not end on a byte (octet) boundary.
Show/Hide	Check whether or not to display ExDefer, LateColl, ExColl, SingColl, Coll, and CRC errors.
Clear	Clicking this button clears all statistics counters on this window.

View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Size

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

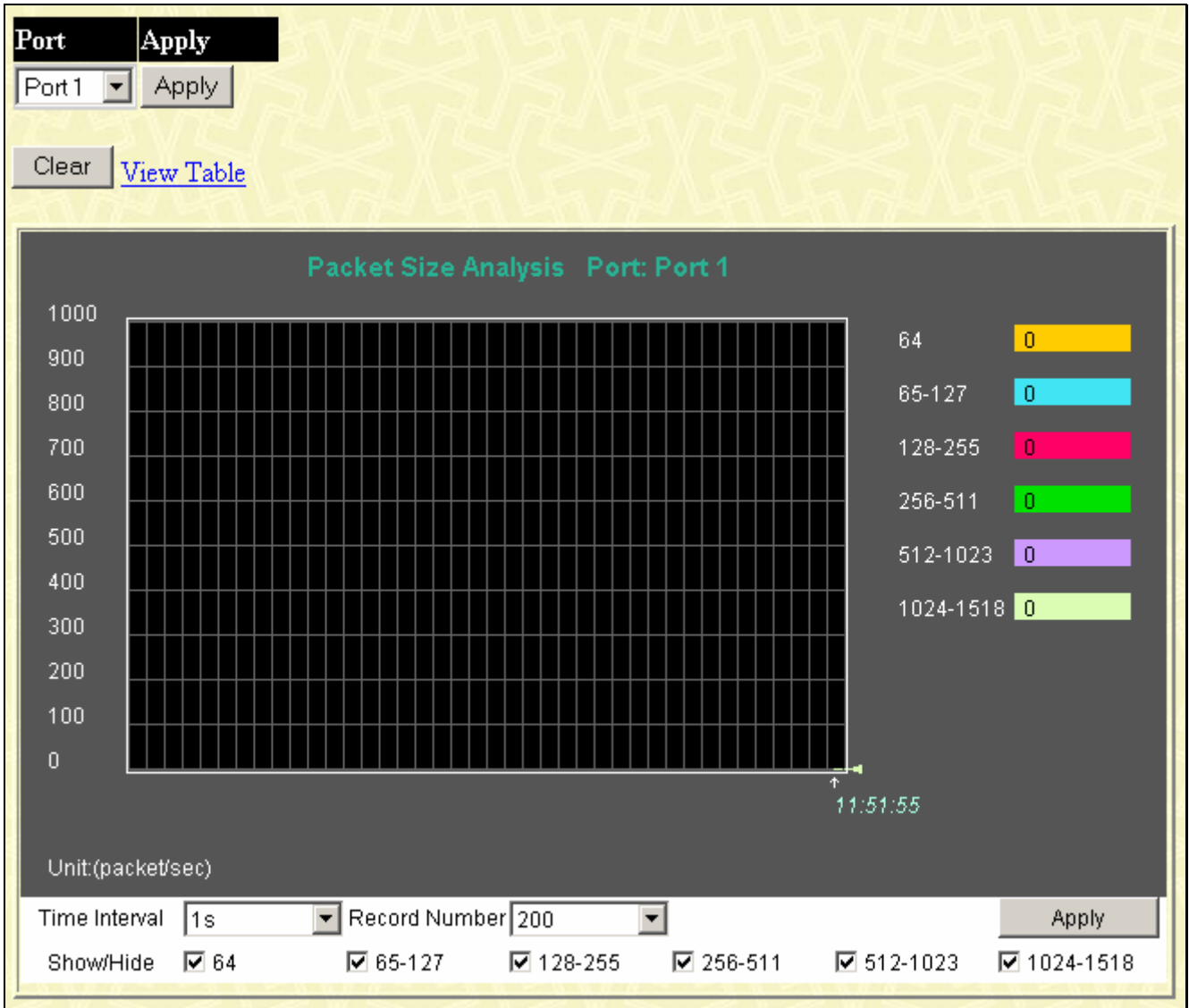


Figure 10- 12. Packet Size Analysis window (line graph)

To view the Packet Size Analysis Table, click the link [View Table](#), which will show the following table:

[View Line Chart](#)

Packet Analysis of Port 1 Time Interval

Packet Size	Total	Total/Sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0

Figure 10- 13. Packet Size Analysis window (table)

The following fields can be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between <i>1s</i> and <i>60s</i> , where "s" stands for seconds. The default value is one second.
Record Number	Select the number of times the Switch will be polled between <i>20</i> and <i>200</i> . The default value is <i>20</i> .
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

MAC Address

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view the MAC Address forwarding table, from the **Monitoring** menu, click the **MAC Address** link:

VLAN ID Find Delete

MAC Address Find

Port Find Delete

MAC Address Table

VID	MAC Address	Port	Type
1	00-00-01-02-03-a2	6	Dynamic
1	00-00-50-06-73-bd	6	Dynamic
1	00-00-5e-00-01-5f	6	Dynamic
1	00-00-e2-2f-44-ec	6	Dynamic
1	00-00-e2-58-db-cf	6	Dynamic
1	00-01-02-03-04-00	6	Dynamic
1	00-01-02-03-04-01	6	Dynamic
1	00-01-03-83-11-fd	6	Dynamic
1	00-01-06-30-10-63	6	Dynamic
1	00-01-30-11-00-5e	6	Dynamic
1	00-01-30-12-13-02	6	Dynamic
1	00-02-06-00-00-08	6	Dynamic
1	00-02-06-12-34-56	6	Dynamic
1	00-02-a5-fd-66-97	6	Dynamic
1	00-03-09-18-10-01	6	Dynamic
1	00-03-6d-1e-76-79	6	Dynamic
1	00-03-9d-73-32-f0	6	Dynamic
1	00-04-13-04-03-01	6	Dynamic
1	00-04-38-d5-64-01	6	Dynamic
1	00-04-38-d5-88-41	6	Dynamic

Total Entries: 382

Figure 10- 14. MAC Address Table window

The following fields can be viewed or set:

Parameter	Description
VLAN ID	Enter a VLAN ID for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
VID	The VLAN ID of the VLAN the port is a member of.

MAC Address	The MAC address entered into the address table.
Port	The port that the MAC address above corresponds to.
Learned	How the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.
Next	Click this button to view the next page of the address table.
View All Entry	Clicking this button will allow the user to view all entries of the address table.
Delete All Entry	Clicking this button will allow the user to delete all entries of the address table.

Switch History Log

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed. To view the Switch history log, open the **Monitoring** folder and click the **Switch History Log** link

Switch History		
Sequence	Time	Log Text
23	2040/04/03 01:26:11	Successful login through Console (Username: ctsnow)
22	2040/04/03 01:26:11	Login failed through Console (Username: Anonymous)
21	2040/04/03 01:26:11	Login failed through Console (Username: Anonymous)
20	2040/04/03 01:26:11	Login failed through Console (Username: Anonymous)
19	2040/04/03 01:26:11	Successful login through Web (Username: ctsnow)
18	2040/04/03 01:26:11	Console session timed out (Username: ctsnow)
17	2040/04/03 01:26:11	Successful login through Web (Username: ctsnow)
16	2040/04/03 01:26:11	Successful login through Console (Username: ctsnow)
15	2040/04/03 01:26:11	Login failed through Console (Username: Anonymous)
14	2040/04/03 01:26:11	Port 7 link up, 100Mbps FULL duplex
13	2040/04/03 01:26:11	Port 15 link up, 100Mbps FULL duplex
12	2040/04/03 01:26:11	System started up
11	2040/04/03 01:26:11	Spanning Tree Protocol is disabled
10	2040/04/03 01:26:05	Configuration saved to flash (Username: Anonymous)
9	2040/04/03 01:26:05	Configuration saved to flash (Username: Anonymous)
8	2040/04/03 01:26:05	Successful login through Console (Username: Anonymous)
7	2040/04/03 01:26:05	Console session timed out (Username: Anonymous)
6	2040/04/03 01:26:05	Successful login through Console (Username: Anonymous)

Figure 10- 15. Switch History window

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Click **Next** to go to the next page of the Switch History Log. Clicking **Clear** will allow the user to clear the Switch History Log.

The information is described as follows:

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

IGMP Snooping Group

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

To view the **IGMP Snooping Table**, click **IGMP Snooping Group** in the **Monitoring** menu:

VLAN ID	Multicast Group	MAC Address	Reports
0	0.0.0.0	00:00:00:00:00:00	0

Figure 10- 16. IGMP Snooping Table window

The user may search the IGMP Snooping Table by VLAN ID (VID) by entering the VID in the top left hand corner and clicking **Search**.

The following field can be viewed:

Parameter	Description
VLAN ID	The VLAN ID (VID) of the multicast group.
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Queries	A read-only field showing the status of the Querier State. Disabled implies that the Switch is not transmitting IGMP Snooping Query packets, while Enabled means those packets are being transmitted.
Reports	The total number of reports received for this group.
Ports	These are the ports where the IGMP packets were snooped are displayed.



NOTE: To configure IGMP snooping for the DGS-3204, go to the **Configuration** folder and select **IGMP Snooping**. Configuration and other information concerning IGMP snooping may be found in this manual under IGMP.

IGMP Snooping Forwarding

This window will display the current IGMP snooping forwarding table entries currently configured on the Switch. To view the following screen, open the **Monitoring** folder and click the **IGMP Snooping Forwarding** link.

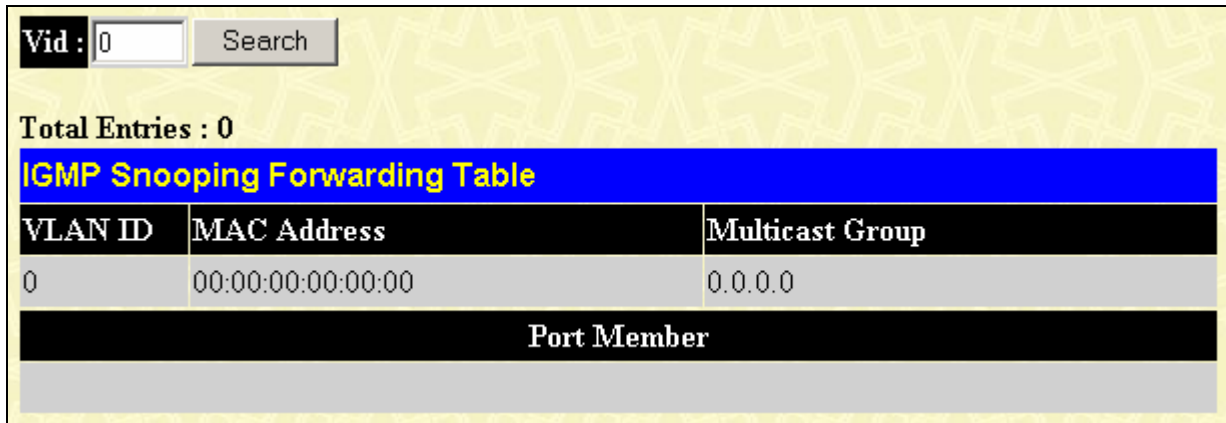


Figure 10- 17. IGMP Snooping Forwarding Table window

The user may search the IGMP Snooping Forwarding Table by VID clicking the top left hand corner **Search** button.

The following field can be viewed:

Parameter	Description
VLAN ID	The VLAN ID (VID) of the multicast group.
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Port Map	These are the ports where the IGMP packets were snooped are displayed.

VLAN Status

This allows the VLAN status for each of the Switch's ports to be viewed by VLAN. This window displays the ports on the Switch that are currently Egress or Tag ports. To view the following table, open the **Monitoring** folder and click the **VLAN Status** Link.

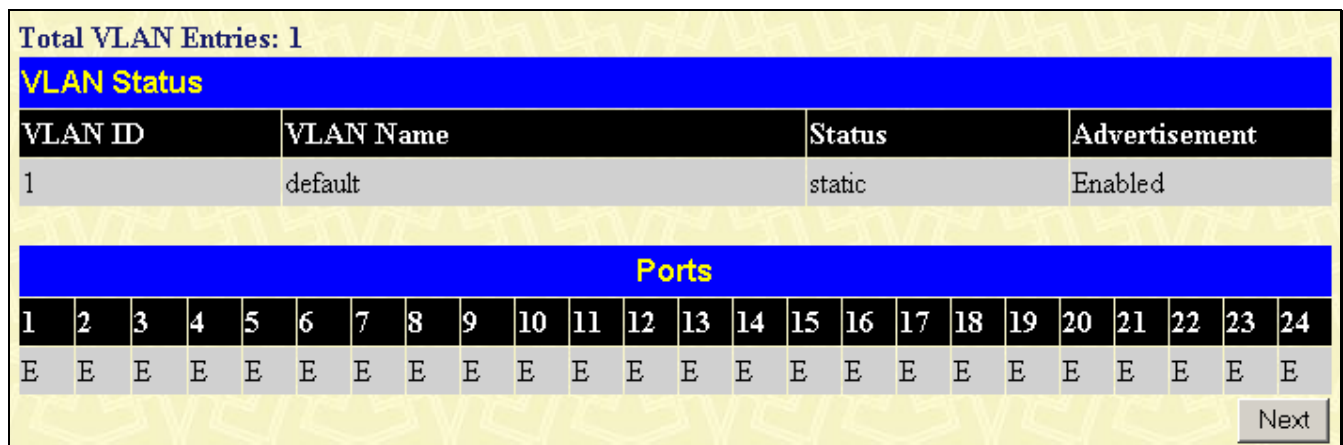


Figure 10- 18. VLAN Status window

Router Port

This displays the Switch's ports that are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by an S. A router port that is dynamically configured by the Switch is designated by D. To view the following window, open the **Monitoring** folder and click the **Router Port** link.

Browse Router Port																								
VLAN ID												VLAN Name												
1												default												
Ports																								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	

Figure 10- 19. Browse Router Port window

Session Table

Reload					
Total Entries : 1					
Current Session Table					
ID	Login Time	Live Time	From	Level	Name
8	2036/02/07 00:41:02	00:20:15.390	Serial Port	1	Anonymous

Figure 10- 20. Current Session Table window

This window displays a list of all the users that are currently logged-in.

Port Access Control

RADIUS Authentication

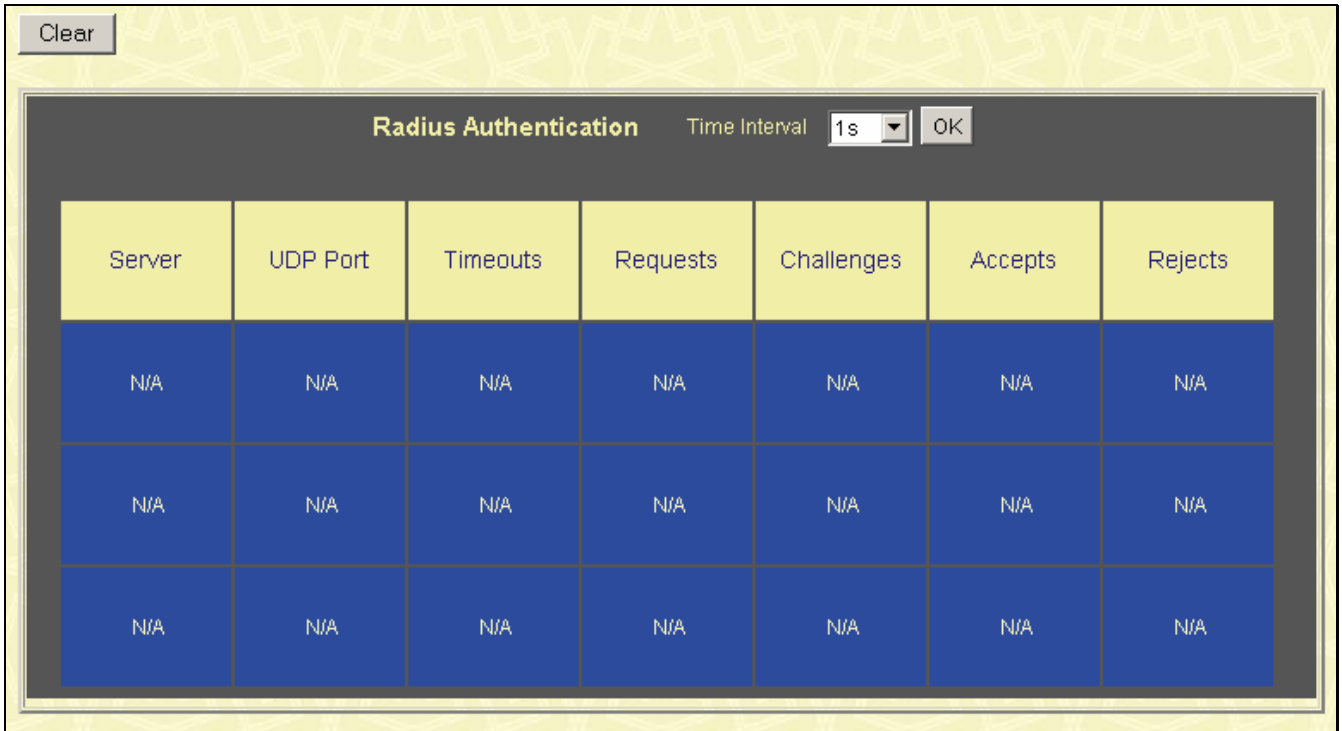


Figure 10- 21. RADIUS Authentication window

Maintenance

The fifth Web Manager main folder is **Maintenance** and includes the following windows and sub-folders: **TFTP Services**, **Ping Test**, **Save Changes**, **Reboot Services**, and **Logout**, as well as secondary windows.

TFTP Services

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

Download Firmware

To update the Switch's firmware, open the **TFTP Services** folder in the **Maintenance** folder and click the **Download Firmware** link:

Figure 11- 1. Download Firmware from TFTP Server window

To download firmware, configure the following fields and click **Start**.

Parameter	Description
Server IP Address	Enter the IP address of the server from which you wish to download firmware.
File Name	Specify the path and filename of the firmware on the Server.

Download Configuration File

To download a settings file from a TFTP server, click on the **TFTP Service** folder in the **Maintenance** folder and then the **Download Configuration File** link:

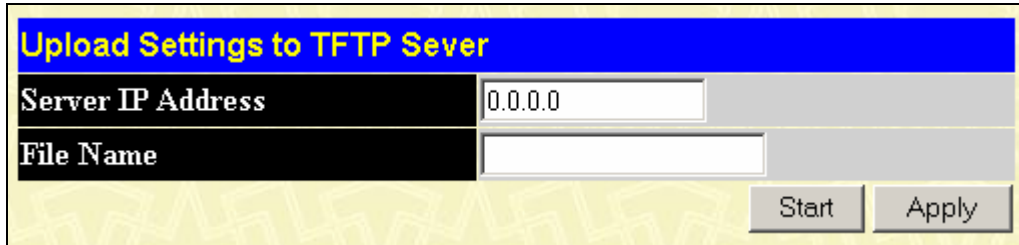
Figure 11- 2. Download Settings from TFTP Server window

Enter the IP address of the TFTP server and specify the location of the Switch settings file on the TFTP server.

Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Save Settings

To upload the Switch settings to a TFTP server, click on the **TFTP Services** folder in the **Maintenance** folder and then click the **Upload Settings to TFTP Server** link:



Upload Settings to TFTP Sever	
Server IP Address	0.0.0.0
File Name	
Start Apply	

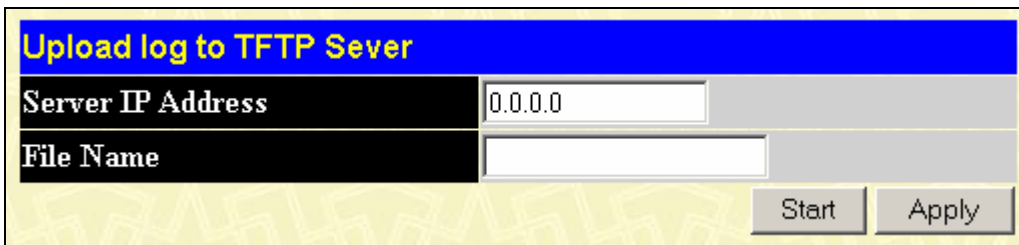
Figure 11- 3. Upload Settings to TFTP Server window

Enter the IP address of the TFTP server and the path and filename for the Switch settings on the TFTP server.

Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Save History Log

To upload the Switch history log file to a TFTP server, open the **TFTP Services** folder in the **Maintenance** folder and then click the **Upload Log to TFTP Server** link:



Upload log to TFTP Sever	
Server IP Address	0.0.0.0
File Name	
Start Apply	

Figure 11- 4. Upload Log to TFTP Server window

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.

Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Ping Test

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Figure 11- 5. Ping Test window

The user may use the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between 1 and 255. Click **Start** to initiate the Ping program.

Save Changes

The DGS-3204 has two levels of memory, normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by clicking the **Apply** button. When this is done, the settings will be immediately applied to the Switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the Switch.

To retain any configuration changes permanently, click the **Save Changes** link in the **Maintenance** folder. The following window will appear:

Figure 11- 6. Save Configuration window

Click the **Save Configuration** button to save the current Switch configuration in NV-RAM. The following dialog box will confirm that the configuration has been saved:



Figure 11- 7. Save Configuration Confirmation dialog box

Click the **OK** button to continue.

Once the Switch configuration settings have been saved to NV-RAM, they become the default settings for the Switch. These settings will be used every time the Switch is rebooted.

Reboot Services

Reboot

The following window is used to restart the Switch.

All of the configuration information entered from the last time **Save Changes** was executed will be lost. Click the **Reboot** button to restart the Switch.

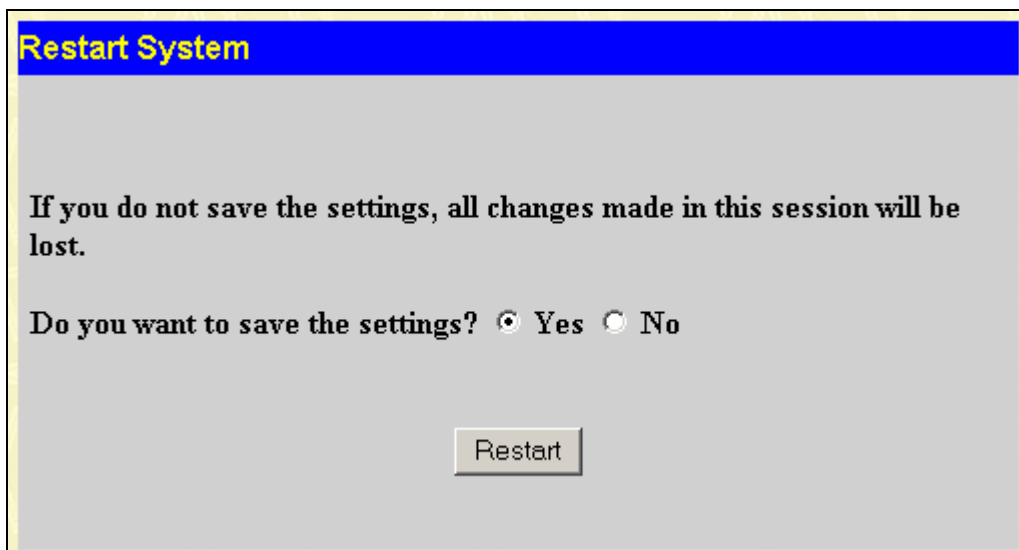


Figure 11- 8. Restart System window

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.



NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the state it was when it left the factory

Reset gives the option of retaining the Switch's User Accounts and History Log while resetting all other configuration parameters to their factory defaults. If the Switch is reset using this window, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

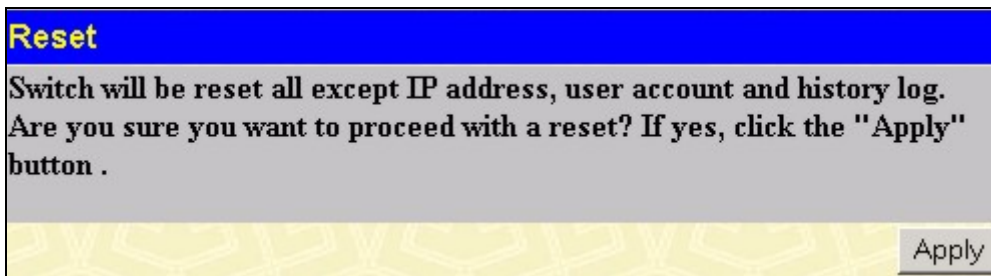


Figure 11- 9. Reset window

Reset Config

The Reset Config option will reset all of the Switch's configuration parameters to their factory defaults, without saving these default values to the Switch's non-volatile RAM. If the Switch is reset with this option enabled, and **Save Changes** is not executed, the Switch will return to the last saved configuration when rebooted.

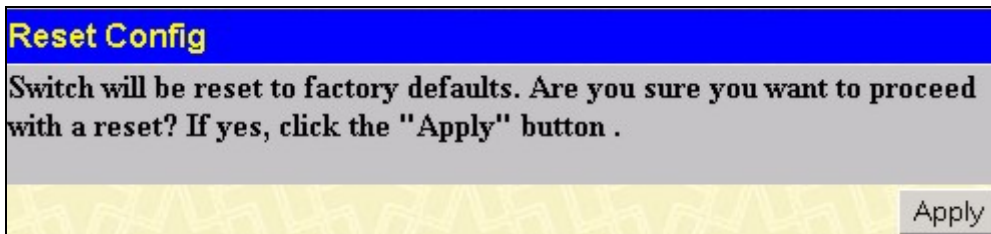


Figure 11- 10. Reset Config window

Reset System

In addition, the Reset System option is added to reset all configuration parameters to their factory defaults, save these parameters to the Switch's non-volatile RAM, and then restart the Switch. This option is equivalent to Reset Config followed by **Save Changes**.

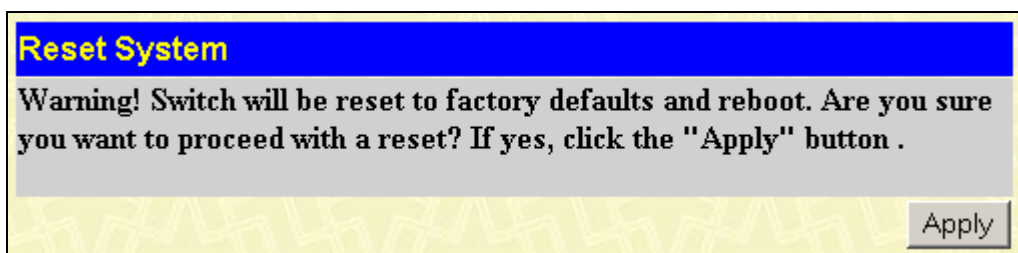


Figure 11- 11. Reset System window

Logout

Use the Logout page to logout of the Switch's Web-based management agent by clicking on the **Logout** button.

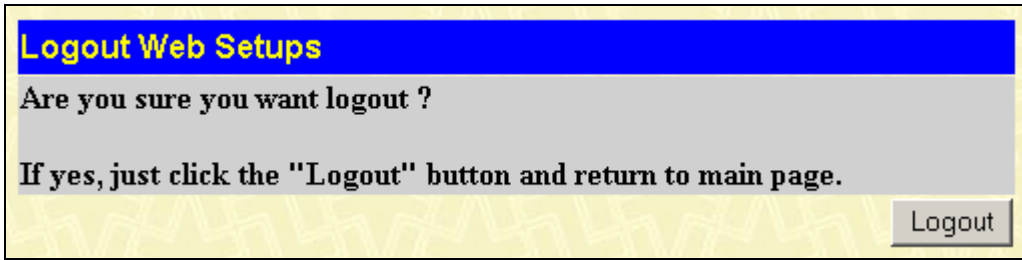


Figure 11- 12. Logout Web Setups window

Technical Specifications

Performance	
Transmission Method	Store-and-forward
RAM Buffer	512Kbytes per device
Packet Filtering/ Forwarding Rate	Full-wire speed for all connections. 1,488,095 pps per port (for 1000Mbps)
MAC Address Learning	Automatic update. Supports 8K MAC address.
Priority Queues	4 Priority Queues per port.
Forwarding Table Age Time	Max age: 10–1000000 seconds. Default = 300.

Physical and Environmental	
AC Inputs	100 – 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption	45 watts maximum
DC Fans	2 built-in 40 x 40 x 10 mm fans
Operating Temperature	0 to 40 degrees Celsius (32 to 104 degrees Fahrenheit)
Storage Temperature	-40 to 70 degrees Celsius (-40 to 158 degrees Fahrenheit)
Humidity	Storage: 5% to 95% non-condensing
Dimensions	441mm (W) x 309mm (D) x 44mm (H), 19-inch rack-mount width 1U height
Weight	3.8 kg (8.38 lb)
EMI	FCC, CE Mark
Safety	CSA International

General	
Standards	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z Gigabit Ethernet IEEE 802.1Q Tagged VLAN IEEE 802.1P Tagged Packets IEEE 802.3ab 1000BASE-T IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 NWay auto-negotiation
Protocols	CSMA/CD
Data Transfer Rates	
Ethernet:	Half-duplex Full-duplex
Fast Ethernet:	
Gigabit Ethernet:	10 Mbps 20 Mbps 100 Mbps 200 Mbps 2000 Mbps (Full duplex only)
Topology	Star
Network Cables	
10BASE-T:	UTP Category 3, 4, 5 (100 meters max.) EIA/TIA- 568 150-ohm STP (100 meters max.)
100BASE-TX:	UTP Cat. 5 (100 meters max.) EIA/TIA-568 150-ohm STP (100 meters max.)
1000BASE-T:	UTP Cat. 5e (100 meters max.) UTP Cat. 5 (100 meters max.) EIA/TIA-568B 150-ohm STP (100 meters max.)
1000BASE-LX:	Single-mode fiber module (10km)
1000BASE-SX:	Multi-mode fiber module (550m)
1000BASE-LHX:	Single-mode fiber module (40km)
1000BASE-ZX:	Single-mode fiber module (80km)
Mini-GBIC:	SFP Transceiver for 1000BASE-LX Single-mode fiber module (10km) SFP Transceiver for 1000BASE-SX Multi-mode fiber module (550m) SFP Transceiver for 1000BASE-LHX Single-mode fiber module (40km) SFP Transceiver for 1000BASE-ZX Single-mode fiber module (80km)
Number of Ports:	24 x 10/100/1000 Mbps ports 4 x GBIC combo ports

Cable Lengths

Use the following table to as a guide for the maximum cable lengths:

Standard	Media Type	Maximum Distance
Mini GBIC	DEM-310GT: SFP Transceiver for 1000BASE-LX, Single-mode fiber module	10km
	DEM-311GT: SFP Transceiver for 1000BASE-SX, Multi-mode fiber module	550m
	DEM-314GT: SFP Transceiver for 1000BASE-LHX, Single-mode fiber module	40km
	DEM-315GT: SFP Transceiver for 1000BASE-ZX, Single-mode fiber module	80km
1000BASE-T	Category 5e UTP Cable Category 5 UTP Cable (1000 Mbps)	100m
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m



Glossary

100BASE-T – A specification for Gigabit Ethernet over copper wire (IEEE Std. 802.3ab). The standard defines 1 Gb/s data transfer over distances of up to 100 meters using four pairs of CAT-5 balanced copper cabling and a 5-level coding scheme. Its benefits include compatibility with existing network protocols (i.e. IP, IPX, AppleTalk), existing applications, Network Operating Systems, network management platforms and applications.

100BASE-TX – 100Mbps Ethernet implementation over Category 5 and Type 1 twisted pair cabling.

10BASE-T – The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

aging – The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM – Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation – A feature on a port that allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone – The part of a network used as the primary path for transporting traffic

backbone port – A port that does not learn device addresses, and receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

bandwidth – Information capacity, measured in bits per second that a channel can transmit. The bandwidth of Ethernet is 10Mbps and the bandwidth of Fast Ethernet is 100Mbps.

baud rate – The Switching speed of a line. Also known as *line speed* between network segments.

BOOTP – The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge – A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast – A message sent to all destination devices on the network.

broadcast storm – Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port – The port on the Switch accepting a terminal. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD – Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center Switching – The point of aggregation within a corporate network where a Switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet – A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet – 100Mbps technology based on the Ethernet/CD network access method.

Flow Control – (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested Switch port.

forwarding The process of sending a packet toward its destination by an internetworking device.

full duplex – A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

GBIC – Gigabit interface converter, a transceiver that converts serial electric signals to serial optical signals and vice versa. In networking, a GBIC is used to interface a fiber optic system with an Ethernet system, such as Fiber Channel and Gigabit Ethernet.

A GBIC allows designers to design one type of device that can be adapted for either optical or copper applications. GBICs also are hot-swappable, which adds to the ease of upgrading electro-optical communication networks.

half-duplex – A system that allows packets to be transmitted and received, but not at the same time. Contrasts with full-duplex.

IP address – Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX – Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN – Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency – The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed – See *baud rate*.

main port – The port in a resilient link that carries data traffic in normal operating conditions.

MDI – Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X – Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB – Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast – Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol – A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link – A pair of ports that can be configured so that one will take over data transmission should the other fail. See also *main port* and *standby port*.

RJ-45 – Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON – Remote Monitoring. Subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS – Redundant Power System. A device that provides a backup source of power when connected to the Switch.

server farm – A cluster of servers in a centralized location serving a large user population.

SLIP – Serial Line Internet Protocol. A protocol that allows IP to run over a serial line connection.

SNMP – Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP Internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol – (STP) A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

stack – A group of network devices that are integrated to form a single logical device.

standby port – The port in a resilient link that will take over data transmission if the main port in the link fails.

Switch – A device that filters, forwards and floods packets based on the packet's destination address. The Switch learns the addresses associated with each Switch port and builds tables based on this information to be used for the Switching decision.

TCP/IP – A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet – A TCP/IP application protocol that provides virtual terminal service, allowing a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP – Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your Switch's local management capabilities.

UDP – User Datagram Protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN – Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT – Virtual LAN Trunk. A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100 – A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.

Warranty and Registration Information

(All countries and regions excluding USA)

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sint beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Originalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

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

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE,

FAILURE OR INTERRUPTION OF A D-LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Limited Warranty

Hardware:

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

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

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

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

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

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

Software:

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

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

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

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

Limited Lifetime Warranty for the product is defined as follows:

- Hardware: For as long as the original customer/end user owns the product, or five (5) years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power supplies and fans: Three (3) Year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, 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. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual 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 retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to 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. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. 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.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.
- 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. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

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: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, 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; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER 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, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, 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. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

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 you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement: No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2005 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

FCC Statement: 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 in a commercial 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 communication. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. 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.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration

Register your D-Link product online at <http://support.dlink.com/register/>

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Trademarks

Copyright 2005 D-Link Corporation. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/ D-Link Systems Inc. All other trademarks belong to their respective proprietors.

Copyright statement

No part of this publication may be reproduced in any form or by any means or used to make a derivative such as translation, transformation, or adaptation without permission from DLink Corporation/ D-Link Systems Inc as stipulated by the United States Copyright Act of 1976.

CE EMI class A 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.

D-Link Europe Limited Product Warranty

General Terms

The Limited Product Warranty set forth below is given by D-LINK (Europe) Ltd. (herein referred to as "D-LINK"). This Limited Product Warranty is only effective upon presentation of the proof of purchase. Upon further request by D-LINK, this warranty card has to be presented, too.

EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY, D-LINK MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. SOME STATES OR COUNTRIES DO NOT ALLOW A LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS. IN SUCH STATES OR COUNTRIES, SOME EXCLUSIONS OR LIMITATIONS OF THIS LIMITED WARRANTY MAY NOT APPLY TO YOU. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS THAT MAY VARY FROM STATE TO STATE OR FROM COUNTRY TO COUNTRY. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR A FULL DETERMINATION OF YOUR RIGHTS.

This limited warranty applies to D-LINK branded hardware products (collectively referred to in this limited warranty as "D-LINK Hardware Products") sold by from D-LINK (Europe) Ltd., its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this limited warranty as "D-LINK") with this limited warranty. The Term "D-LINK Hardware Product" is limited to the hardware components and all its internal components including firmware. The term "D-LINK Hardware Product" DOES NOT include any software applications or programs.

Geographical Scope of the Limited Product Warranty

This Limited Product Warranty is applicable in all European Countries as listed in the addendum "European Countries for D-LINK Limited Product Warranty". The term "European Countries" in this D-LINK Limited Product Warranty only include the countries as listed in this addendum. The Limited Product Warranty will be honored in any country where D-LINK or its authorized service providers offer warranty service subject to the terms and conditions set forth in this Limited Product Warranty. However, warranty service availability and response times may vary from country to country and may also be subject to registration requirements.

Limitation of Product Warranty

D-LINK warrants that the products described below under normal use are free from material defects in materials and workmanship during the Limited Product Warranty Period set forth below ("Limited Product Warranty Period"), if the product is used and serviced in accordance with the user manual and other documentation provided to the purchaser at the time of purchase (or as amended from time to time). D-LINK does not warrant that the products will operate uninterrupted or error-free or that all deficiencies, errors, defects or non-conformities will be corrected.

This warranty shall not apply to problems resulting from: (a) unauthorised alterations or attachments; (b) negligence, abuse or misuse, including failure to operate the product in accordance with specifications or interface requirements; (c) improper handling; (d) failure of goods or services not obtained from D-LINK or not subject to a then-effective D-LINK warranty or maintenance agreement; (e) improper

use or storage; or (f) fire, water, acts of God or other catastrophic events. This warranty shall also not apply to any particular product if any D-LINK serial number has been removed or defaced in any way.

D-LINK IS NOT RESPONSIBLE FOR DAMAGE THAT OCCURS AS A RESULT OF YOUR FAILURE TO FOLLOW THE INSTRUCTIONS FOR THE D-LINK HARDWARE PRODUCT.

Limited Product Warranty Period

The Limited Product Warranty Period starts on the date of purchase from D-LINK. Your dated sales or delivery receipt, showing the date of purchase of the product, is your proof of the purchase date. You may be required to provide proof of purchase as a condition of receiving warranty service. You are entitled to warranty service according to the terms and conditions of this document if a repair to your D-LINK branded hardware is required within the Limited Product Warranty Period.

This Limited Product Warranty extends only to the original end-user purchaser of this DLINK Hardware Product and is not transferable to anyone who obtains ownership of the DLINKHardware Product from the original end-user purchaser.

Product Type	Product Warranty Period
Managed Switches (i.e. Switches with built in SNMP agent)(including modules and management software)	Five (5) years
All other products	Two (2) years
Spare parts (i.e. External Power Adapters, Fans)	One (1) year

The warranty periods listed above are effective in respect of all D-LINK products sold in European Countries by D-LINK or one of its authorized resellers or distributors from 1st of January 2004. All products sold in European Countries by D-LINK or one of its authorized resellers or distributors before 1st January 2004 carry 5 years warranty, except power supplies, fans and accessories that are provided with 2 year warranty.

The warranty period stated in this card supersedes and replaces the warranty period as stated in the user's manual or in the purchase contract for the relevant products. For the avoidance of doubt, if you have purchased the relevant D-LINK product as a consumer your statutory rights remain unaffected.

Performance of the Limited Product Warranty

If a product defect occurs, D-LINK's sole obligation shall be to repair or replace any defective product free of charge to the original purchaser provided it is returned to an Authorized D-LINK Service Center during the warranty period. Such repair or replacement will be rendered by D-LINK at an Authorized D-LINK Service Center. All component parts or hardware products removed under this limited warranty become the property of D-LINK.

The replacement part or product takes on the **remaining** limited warranty status of the removed part or product. The replacement product need not be new or of an identical make, model or part; D-LINK may in its discretion replace the defective product (or any part thereof) with any reconditioned equivalent (or superior) product in all material respects to the defective product. Proof of purchase may be required by D-LINK.

Warrantor

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
London NW9 5 AB
United Kingdom
Telephone: +44-020-8731-5555
Facsimile: +44-020-8731-5511

www.dlink.co.uk

D-Link Europe Limited Produktgarantie

Allgemeine Bedingungen

Die hierin beschriebene eingeschränkte Garantie wird durch D-LINK (Europe) Ltd. Gewährt (im Folgenden: „D-LINK“). Diese eingeschränkte Garantie setzt voraus, dass der Kauf des Produkts nachgewiesen wird. Auf Verlangen von D-LINK muss auch dieser Garantieschein vorgelegt werden.

AUSSER IN DEM HIER AUSDRÜCKLICH BESCHRIEBENEN UMFANG GEWÄHRT D-LINK KEINE WEITEREN GARANTIEEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND. INSBESONDERE WIRD NICHT STILLSCHWEIGEND EINE GARANTIE FÜR DIE ALLGEMEINE GEBRAUCHSTAUGLICHKEIT ODER DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ERKLÄRT. D-LINK LEHNT AUSDRÜCKLICH JEDE GARANTIE AB, DIE ÜBER DIESE EINGESCHRÄNKTE GARANTIE HINAUSGEHT. JEDE GESETZLICH ANGEORDNETE GARANTIE IST AUF DIE LAUFZEIT DER EINGESCHRÄNKTEN GARANTIE BESCHRÄNKT. IN EINIGEN STAATEN ODER LÄNDERN IST DIE ZEITLICHE BESCHRÄNKUNG EINER STILLSCHWEIGEND ERKLÄRTEN GARANTIE SOWIE AUSSCHLUSS ODER BESCHRÄNKUNG VON SCHADENERSATZ FÜR NEBEN- ODER FOLGESCHÄDEN BEIM VERBRAUCHSGÜTERKAUF UNTERSAGT. SOWEIT SIE IN SOLCHEN STAATEN ODER LÄNDERN LEBEN, ENTFALTEN MÖGLICHERWEISE EINIGE AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN DIESER EINGESCHRÄNKTEN GARANTIE GEGENÜBER IHNEN KEINE WIRKUNG. DIESE EINGESCHRÄNKTE GARANTIE GEWÄHRT IHNEN SPEZIFISCHE RECHTE. DARÜBER HINAUS STEHEN IHNEN MÖGLICHERWEISE NOCH WEITERE RECHTE ZU, DIE SICH JEDOCH VON STAAT ZU STAAT ODER VON LAND ZU LAND UNTERSCHIEDEN KÖNNEN. UM DEN UMFANG IHRER RECHTE ZU BESTIMMEN, WIRD IHNEN EMPFOHLEN, DIE ANWENDBAREN GESETZE DES JEWEILIGEN STAATES ODER LANDES ZU RATE ZU ZIEHEN.

Diese eingeschränkte Garantie ist auf Hardware-Produkte der Marke D-LINK (insgesamt im Folgenden: „D-LINK Hardware-Produkte“) anwendbar, die von D-LINK (Europe) Ltd. Oder dessen weltweiten Filialen, Tochtergesellschaften, Fachhändlern oder Länderdistributoren (insgesamt im Folgenden: „D-LINK“) mit dieser eingeschränkten Garantie verkauft wurden. Der Begriff „D-LINK Hardware-Produkte“ beinhaltet nur Hardwarekomponenten und deren Bestandteile einschließlich Firmware. Der Begriff „D-LINK Hardware-Produkte“ umfasst KEINE Software-Anwendungen oder -programme.

Räumlicher Geltungsbereich der eingeschränkten Garantie

Diese eingeschränkte Garantie gilt für alle genannten europäischen Staaten gemäß dem Anhang „Eingeschränkte Garantie von D-LINK in europäischen Staaten“. Im Rahmen dieser eingeschränkten Garantie sind mit dem Begriff „europäische Staaten“ nur die im Anhang genannten Staaten gemeint. Die eingeschränkte Garantie findet überall Anwendung, wo D-LINK oder dessen autorisierte Servicepartner Garantiedienste gemäß den Bestimmungen dieser eingeschränkten Garantie erbringen. Gleichwohl kann sich die Verfügbarkeit von Garantiediensten und die Bearbeitungszeit von Land zu Land unterscheiden und von Registrierungsanforderungen abhängig sein.

Einschränkung der Garantie

D-LINK gewährleistet, dass die nachstehend aufgeführten Produkte bei gewöhnlicher Verwendung für die unten angegebene Laufzeit der eingeschränkten Garantie („Garantielaufzeit“) frei von wesentlichen Verarbeitungs- und Materialfehlern sind. Voraussetzung hierfür ist jedoch, dass das Produkt entsprechend dem Benutzerhandbuch und den weiteren Dokumentationen, die der Benutzer beim Kauf (oder später) erhalten hat, genutzt und gewartet wird. D-LINK garantiert nicht, dass die Produkte störungs- oder fehlerfrei arbeiten oder dass alle Mängel, Fehler, Defekte oder Kompatibilitätsstörungen beseitigt werden können. Diese Garantie gilt nicht für Probleme wegen: (a) unerlaubter Veränderung oder Hinzufügung, (b) Fahrlässigkeit, Missbrauch oder Zweckentfremdung, einschließlich des Gebrauchs des Produkts entgegen den Spezifikationen oder den durch Schnittstellen gegebenen Vorgaben, (c) fehlerhafter Bedienung, (d) Versagen von Produkten oder Diensten, die nicht von D-LINK stammen oder nicht Gegenstand einer zum maßgeblichen Zeitpunkt gültigen Garantie- oder Wartungsvereinbarung sind, (e) Fehlgebrauch oder fehlerhafter Lagerung oder (f) Feuer, Wasser, höherer Gewalt oder anderer Katastrophen. Diese Garantie gilt ebenfalls nicht für Produkte, bei denen eine D-LINK-Seriennummer entfernt oder auf sonstige Weise unkenntlich gemacht wurde.

D-LINK STEHT NICHT FÜR SCHÄDEN EIN, DIE DADURCH ENTSTEHEN, DASS DIE ANLEITUNG FÜR DAS D-LINK HARDWARE-PRODUKT NICHT BEFOLGT WIRD.

Laufzeit der eingeschränkten Garantie

Die Laufzeit der eingeschränkten Garantie beginnt mit dem Zeitpunkt, zu dem das Produkt von D-LINK gekauft wurde. Als Nachweis für den Zeitpunkt des Kaufs gilt der datierte Kauf- oder Lieferbeleg. Es kann von Ihnen verlangt werden, dass Sie zur Inanspruchnahme von Garantiediensten den Kauf des Produkts nachweisen. Wenn Ihre Hardware-Produkte der Marke D-LINK innerhalb der Laufzeit der

eingeschränkten Garantie eine Reparatur benötigen, so sind Sie berechtigt, gemäß den Bedingungen dieser eingeschränkten Garantie Garantiedienste in Anspruch zu nehmen.

Diese eingeschränkte Garantie gilt nur für denjenigen, der das D-LINK Hardware-Produkt ursprünglich als originärer Endbenutzer gekauft hat. Sie ist nicht auf Dritte übertragbar, die das D-LINK-Produkt von dem ursprünglichen originären Endbenutzer erworben haben.

Produkttyp	Gewährleistungslaufzeit
Verwaltete Switches (d. h. Switches mit eingebauten SNMP-Agents) (einschließlich Modulen und Verwaltungssoftware)	Fünf (5) Jahre
Alle weiteren Produkte	Zwei (2) Jahre
Ersatzteile (z.B. externe Netzteile, Lüfter)	Ein (1) Jahr

Die oben aufgeführten Garantielaufzeiten gelten für alle D-LINK-Produkte, die in europäischen Staaten ab dem 1. Januar 2004 von D-LINK oder einem autorisierten Fachhändler oder Distributor verkauft werden. Alle vor dem 1. Januar 2004 von D-LINK oder einem autorisierten Vertragshändler oder Distributor verkauften Produkte haben eine Gewährleistung von 5 Jahren; ausgenommen sind Netzteile, Lüfter und Zubehör, diese haben eine Garantie von 2 Jahren.

Die durch diesen Garantieschein festgelegte Garantielaufzeit tritt an die Stelle der im Benutzerhandbuch oder im Kaufvertrag für das jeweilige Produkt angegebenen Laufzeit. Sollten Sie das betreffende D-LINK-Produkt als Verbraucher erworben haben, so sei klargestellt, dass Ihre gesetzlichen Rechte hiervon unberührt bleiben.

Leistungsumfang der eingeschränkten Garantie

Bei Auftreten eines Produktfehlers besteht die einzige Verpflichtung von D-LINK darin, dem ursprünglichen Käufer das defekte Produkt kostenlos zu reparieren oder es auszutauschen. Voraussetzung hierfür ist, dass das Produkt während der Garantielaufzeit einem autorisierten D-LINK-Servicecenter übergeben wird. Reparatur oder Austausch werden von D-LINK durch ein autorisiertes D-LINK-Servicecenter durchgeführt. Bauteile oder Hardware-Produkte, die gemäß dieser eingeschränkten Garantie entfernt werden, gehen in das Eigentum von D-LINK über. Die **verbliebene** eingeschränkte Garantie des entfernten Teils oder Produkts wird auf das Ersatzteil oder -produkt übertragen. Das Austauschprodukt muss weder neu sein noch dem defekten Produkt ganz oder in Teilen entsprechen. D-LINK darf dieses nach eigenem Ermessen gegen ein entsprechendes wiederaufbereitetes Produkt austauschen, welches dem defekten Produkt im Wesentlichen entspricht (oder höherwertig ist). D-LINK kann verlangen, dass der Kauf des Produkts nachgewiesen wird.

DIE VORSTEHENDE GARANTIE WURDE IN DIE DEUTSCHE SPRACHE AUS DEM ENGLISCHEN ÜBERSETZT. BEI ABWEICHUNGEN ZWISCHEN DER ENGLISCHEN VERSION UND DER DEUTSCHEN ÜBERSETZUNG GELTEN DIE BESTIMMUNGEN DER ENGLISCHEN VERSION.

Garantiegeber

D-Link (Europe) Ltd.

4th Floor, Merit House

Edgware Road

Colindale

London NW9 5 AB

Vereinigtes Königreich

Telefon: +44-020-8731-5555

Fax: +44-020-8731-5511

www.dlink.com

D-Link Europe a limité la garantie des produits

Conditions Générales

La Garantie Produit Limitée énoncée ci-dessous émane de D-LINK (Europe) Ltd. (ci-après « D-LINK »). Cette Garantie Produit Limitée n'est valable que sur présentation de la preuve d'achat. D-LINK peut également exiger la présentation du présent bon de garantie.

SAUF INDICATION EXPLICITE DES PRESENTES, D-LINK NE FOURNIT AUCUNE AUTRE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS UNE GARANTIE IMPLICITE DE VALEUR MARCHANDE OU D'ADAPTATION DU PRODUIT A UN USAGE PRECIS. D-LINK DECLINE EXPLICITEMENT TOUTE GARANTIE NON ENONCEE DANS LES PRESENTES. TOUTE GARANTIE IMPLICITE IMPOSEE PAR LA LOI, LE CAS ECHEANT, EST LIMITEE DANS SA DUREE A CELLE DE LA GARANTIE LIMITEE. CERTAINS ETATS OU PAYS NE PERMETTENT PAS DE LIMITER LA DUREE DE LA GARANTIE IMPLICITE OU INTERDISENT D'EXCLURE OU DE LIMITER LA COUVERTURE DES DOMMAGES DIRECTS OU INDIRECTS OCCASIONNES AUX PRODUITS GRAND PUBLIC. DANS LES ETATS OU PAYS EN QUESTION, CERTAINES EXCLUSIONS OU LIMITATIONS DE LA PRESENTE GARANTIE PEUVENT NE PAS S'APPLIQUER A VOTRE CAS. LA PRESENTE GARANTIE LIMITEE VOUS OCTROIE CERTAINS DROITS LEGAUX SPECIFIQUES. VOUS POUVEZ EGALEMENT BENEFICIER D'AUTRES DROITS VARIABLES D'UN ETAT OU D'UN PAYS A L'AUTRE. NOUS VOUS RECOMMANDONS DE CONSULTER LA LEGISLATION EN VIGUEUR DANS VOTRE LIEU DE RESIDENCE POUR CONNAITRE L'ETENDUE DE VOS DROITS.

La présente garantie limitée s'applique aux produits matériels commercialisés sous la marque D-LINK (collectivement ici « les Produits Matériels D-LINK ») vendus par D-LINK (Europe) Ltd., ses filiales, sociétés affiliées, revendeurs agréés ou distributeurs locaux à travers le monde (collectivement ici « D-LINK ») avec la présente garantie limitée. Le terme de « Produit Matériel D-LINK » se limite aux composants matériels et à l'ensemble de leurs composants internes, notamment le firmware. Le terme de « Produit Matériel D-LINK » N'englobe PAS les applications ou programmes logiciels.

Etendue géographique de la Garantie Produit Limitée

La présente Garantie Produit Limitée s'applique à tous les pays européens figurant dans l'annexe « Pays européens où s'applique la Garantie Produit Limitée D-LINK ». Le terme de « pays européens » utilisé dans la présente Garantie Produit Limitée D-LINK englobe uniquement les pays figurant dans la liste en annexe. La Garantie Produit Limitée sera honorée dans tout pays où D-LINK ou ses prestataires agréés proposent le service de garantie, sous réserve des modalités énoncées dans la présente Garantie Produit Limitée. Cependant, la disponibilité du service de garantie et les temps de réponse varient d'un pays à l'autre et peuvent également être assujettis à un enregistrement.

Limitation de la Garantie Produit

D-LINK garantit que les produits décrits ci-dessous, dans le cadre d'une utilisation normale, sont dénués de défauts conséquents, tant au niveau de leurs composants matériels que de leur fabrication, et ce pendant toute la Période de Garantie Produit Limitée indiquée ci-dessous (« Période de Garantie Produit Limitée »), sous réserve qu'ils soient utilisés et entretenus conformément au manuel utilisateur et aux autres documents remis au client lors de l'achat (ou amendés de temps à autre). D-LINK ne garantit pas le fonctionnement ininterrompu ou sans erreur de ses produits. D-LINK ne s'engage pas non plus à corriger tous les défauts, erreurs ou non conformités.

La présente garantie ne s'applique pas aux problèmes qui sont la conséquence : (a) d'altérations ou d'ajouts non autorisés ; (b) d'une négligence, d'un abus ou d'une mauvaise utilisation, notamment une utilisation du produit non conforme à ses spécifications ou aux interfaces requises ; (c) d'une mauvaise manipulation ; (d) d'une panne de biens ou de services acquis auprès d'une société tierce (non D-LINK) ou qui ne font pas l'objet d'un contrat D-LINK de garantie ou de maintenance en bonne et due forme ; (e) d'une mauvaise utilisation ou d'un rangement dans des conditions inadaptées ; ou (f) du feu, de l'eau, d'une catastrophe naturelle ou autre. La présente garantie ne s'applique pas non plus à un produit dont le numéro de série D-LINK aurait été retiré ou altéré de quelque manière que ce soit.

D-LINK N'EST NULLEMENT RESPONSABLE DE DOMMAGES RESULTANT DE VOTRE INOBSERVATION DES INSTRUCTIONS FOURNIES POUR L'UTILISATION DE SON PRODUIT MATERIEL.

Période de Garantie Produit Limitée

La Période de Garantie Produit Limitée court à compter de la date d'achat auprès de D-LINK. La date de votre reçu ou bon de livraison correspond à la date d'achat du produit et constitue la date de votre preuve d'achat. Il est possible que le service de garantie ne vous soit accordé que sur production de votre preuve d'achat. Vous avez droit à un service de garantie conforme aux modalités énoncées dans les

présentes dès lorsque que votre matériel de marque D-LINK nécessite une réparation pendant la Période de Garantie Produit Limitée.

La présente Garantie Produit Limitée s'applique uniquement à l'acheteur utilisateur final initial du Produit Matériel D-LINK. Elle est non cessible à quiconque se procure le Produit Matériel D-LINK auprès de l'acheteur utilisateur final initial.

Type de produit	Période de Garantie
Switches gérés (Switches comportant un agent SNMP intégré)(y compris modules et logiciel de gestion)	Cinq (5) ans
Tous autres produits	Deux (2) ans
Pièces détachées (adaptateurs d'alimentation externes, ventilateurs)	Un (1) an

Les périodes de garantie indiquées ci-dessus s'appliquent à tous les produits D-LINK vendus depuis le 1er janvier 2004 dans les pays européens par D-LINK ou l'un de ses revendeurs ou distributeurs agréés. Tous les produits vendus avant le 1er janvier 2004 dans les pays européens par D-LINK ou l'un de ses revendeurs ou distributeurs agréés bénéficient d'une garantie de 5 ans, excepté les fournitures électriques, ventilateurs et accessoires, qui sont couverts par une garantie de 2 ans.

La période de garantie indiquée sur ce bon annule et remplace celle qui figure dans le manuel utilisateur ou dans le contrat d'achat des produits considérés. Pour éviter le doute, si vous avez acheté votre produit D-LINK en tant que consommateur, vos droits légaux demeurent inchangés.

Exécution de la Garantie Produit Limitée

En cas de défaut ou d'erreur d'un produit, l'unique obligation de D-LINK se limite à la réparation ou au remplacement gratuit du produit défectueux, au bénéfice de l'acheteur initial, sous réserve que le produit soit rapporté à un Centre de Service Agréé D-LINK pendant la période de garantie. D-LINK assure la réparation ou le remplacement dans un Centre de Service Agréé D-LINK. Les composants, pièces ou produits retirés dans le cadre de cette garantie limitée deviennent propriété de D-LINK. La pièce ou le produit de remplacement est couvert par la garantie limitée de la pièce ou du produit d'origine pendant la **période restante**.

Le produit de remplacement n'est pas nécessairement neuf, ni d'une marque ou d'un modèle identique ; D-LINK peut décider, de manière discrétionnaire, de remplacer le produit défectueux (ou ses pièces) par un équivalent (ou un article supérieur) reconditionné ayant toutes les fonctionnalités du produit défectueux. D-LINK peut exiger la preuve d'achat.

Garant

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
London NW9 5 AB
Royaume-Uni
Tél : +44-020-8731-5555
Fax : +44-020-8731-5511

www.dlink.co.uk

Garantía limitada del producto D-LINK Europa

Condiciones generales

Esta garantía la ofrece D-LINK (Europe) Ltd. (en este documento, "D-LINK"). La garantía limitada del producto sólo es válida si se acompaña del comprobante de la compra. También deberá presentarse la tarjeta de garantía si D-LINK lo solicita.

EXCEPTO EN LO EXPRESAMENTE INDICADO EN ESTA GARANTÍA LIMITADA, D-LINK NO CONCEDE OTRAS GARANTÍAS, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIDAD Y APTITUD A UN FIN DETERMINADO. D-LINK RECHAZA EXPLÍCITAMENTE CUALQUIER GARANTÍA QUE NO FIGURE EN ESTA GARANTÍA LIMITADA. LA DURACIÓN DE CUALQUIER GARANTÍA IMPLÍCITA QUE PUEDA SER IMPUESTA POR LEY QUEDA LIMITADA AL PERÍODO DE LA GARANTÍA LIMITADA. ALGUNOS ESTADOS O PAÍSES NO PERMITEN QUE EN LA GARANTÍA LIMITADA DE PRODUCTOS DE CONSUMO SE RESTRINJA LA DURACIÓN TEMPORAL, NI QUE SE EXCLUYAN O LIMITEN LOS DAÑOS INCIDENTALES O RESULTANTES PARA EL CONSUMIDOR DE LOS PRODUCTOS. EN ESTOS ESTADOS O PAÍSES, A USTED NO LE PUEDEN APLICAR ALGUNAS EXCLUSIONES O LIMITACIONES DE LA GARANTÍA LIMITADA. ESTA GARANTÍA LIMITADA LE CONCEDE DETERMINADOS DERECHOS. PUEDE, TAMBIÉN, TENER OTROS DERECHOS, QUE PUEDEN SER DISTINTOS DE UN ESTADO A OTRO O DE UN PAÍS A OTRO. SE RECOMIENDA QUE CONSULTE LAS LEYES PERTINENTES DE UN ESTADO O PAÍS A FIN DE QUE CONOZCA SUS DERECHOS.

Esta garantía limitada se aplica a los productos de hardware de la marca D-LINK (llamados en esta guía "Productos de hardware D-LINK") comprados a D-LINK (Europe) Ltd., a sus filiales en el mundo, a sus proveedores autorizados o a sus distribuidores locales (llamados en este documento "D-LINK") con esta garantía limitada. El término "producto de hardware D-LINK" se restringe a los componentes de hardware y a los componentes internos de estos, incluyendo el firmware. El término "producto de hardware D-LINK" NO incluye ni las aplicaciones ni los programas de software.

Cobertura geográfica de la garantía limitada del producto

Esta garantía limitada del producto es válida en todos los países europeos que figuran en el apéndice "Países europeos de la garantía limitada del producto D-LINK". En esta garantía limitada del producto D-Link, el término "países europeos" sólo incluye los países que figuran en el apéndice. La garantía limitada del producto será válida en cualquier país en el que D-LINK o sus proveedores autorizados de servicios ofrezcan un servicio de garantía sujeto a los términos y condiciones recogidos en esta garantía limitada del producto. Sin embargo, la disponibilidad del servicio de garantía, así como el tiempo de respuesta, pueden variar de un país a otro y pueden estar sujetos a requisitos de registro.

Limitación de la garantía del producto

D-LINK garantiza que los productos descritos más adelante están libres de defectos de fabricación y materiales, en condiciones normales de uso, a lo largo del período de la garantía limitada del producto que se indica en este documento ("período de la garantía limitada del producto"), si el producto se ha utilizado y mantenido conforme a lo recogido en el manual del usuario o en otra documentación que se haya proporcionado al comprador en el momento de la compra (o que se haya corregido). D-LINK no garantiza que los productos funcionarán sin interrupciones o sin errores, ni que se corregirán todas las deficiencias, errores, defectos o disconformidades.

Esta garantía no cubre problemas derivados de: (a) modificaciones o conexiones no autorizadas; (b) negligencia, abuso o mal uso, incluyendo el incumplimiento de las especificaciones y de los requisitos de la interfaz en el funcionamiento del producto; (c) manejo incorrecto; (d) errores en artículos o servicios ajenos a D-LINK o no sujetos a una garantía o un contrato de mantenimiento vigentes de D-LINK; (e) uso o almacenamiento incorrecto; o (f) fuego, agua, casos fortuitos u otros hechos catastróficos. Esta garantía tampoco es válida para aquellos productos a los que se haya eliminado o alterado de algún modo el número de serie D-LINK.

D-LINK NO SE RESPONSABILIZA DE LOS DAÑOS CAUSADOS COMO CONSECUENCIA DEL INCUMPLIMIENTO DE LAS INSTRUCCIONES DEL PRODUCTO DE HARDWARE D-LINK.

Período de la garantía limitada del producto

El período de la garantía limitada del producto se inicia en la fecha en que se realizó la compra a D-LINK. Para el comprador, el comprobante de la fecha de la compra es el recibo de la venta o de la entrega, en el que figura la fecha de la compra del producto. Puede ser necesario tener que presentar el comprobante de la compra a fin de que se preste el servicio de garantía. El comprador tiene derecho al servicio de garantía conforme a los términos y condiciones de este documento, si requiere una reparación del hardware de la marca D-LINK dentro del período de garantía limitada del producto.

Esta garantía limitada del producto cubre sólo al originario comprador-usuario final de este producto de hardware D-LINK, y no es transferible a otras personas que reciban el producto de hardware D-LINK del originario comprador-usuario final.

Tipo de producto	Período de garantía del producto
Conmutadores gestionados (p. ej., conmutadores con agente SNMP integrado) (incluyendo módulos y software de gestión)	Cinco (5) años
Resto de productos	Dos (2) años
Piezas de repuesto (p. ej., adaptadores de alimentación externos, ventiladores)	Un (1) año

Estos períodos de garantía están en vigor para todos los productos D-LINK que hayan sido comprados en países europeos a D-LINK o a alguno de sus proveedores o distribuidores autorizados a partir del 1 de enero del 2004. Todos los productos comprados en países europeos a D-LINK o a uno de sus proveedores o distribuidores autorizados antes del 1 de enero del 2004 cuentan con 5 años de garantía, excepto las fuentes de alimentación, los ventiladores y los accesorios, que cuentan con 2 años de garantía.

El período de garantía que figura en esta tarjeta sustituye y reemplaza al período de garantía que consta en el manual del usuario o en el contrato de compra de los productos correspondientes. Para evitar dudas: si usted ha comprado el producto D-LINK correspondiente como consumidor, sus derechos legales no se ven afectados.

Uso de la garantía limitada del producto

Si un producto presenta algún defecto, la obligación exclusiva de D-LINK será reparar o reemplazar, sin coste alguno para el comprador originario, cualquier producto defectuoso siempre y cuando éste sea entregado en un centro autorizado de servicio D-LINK durante el período de garantía. D-LINK realizará la reparación o sustitución para un centro autorizado de servicio D-LINK. Todos los productos de hardware o componentes que se eliminen bajo esta garantía limitada serán propiedad de D-LINK. La parte o el producto de repuesto adquiere, para el resto de la garantía limitada, el estatus de parte o producto eliminado. El producto de repuesto no ha de ser nuevo o de la misma marca, modelo o parte; D-LINK puede sustituir a discreción el producto defectuoso (o cualquier parte) con un producto equivalente reacondicionado (o superior) en cualquier material respecto al producto defectuoso. D-LINK puede pedir el comprobante de compra.

Garante

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
London NW9 5 AB
United Kingdom
Teléfono: +44-020-8731-5555
Fax: +44-020-8731-5511

www.dlink.co.uk

D-Link Europe Termini di Garanzia dei Prodotti

Generalità

La presente Garanzia viene fornita da D-LINK (Europe) Ltd. (di seguito denominata "DLINK"). Essa viene riconosciuta solo se accompagnata dalla prova di acquisto. D-LINK può richiedere anche l'esibizione della presente cartolina di garanzia.

SALVO QUANTO ESPRESSAMENTE STABILITO NELLA PRESENTE GARANZIA LIMITATA, D-LINK NON FORNISCE NESSUN'ALTRA GARANZIA NE' ESPRESSA NE' IMPLICITA, COMPRESSE EVENTUALI GARANZIE DI COMMERCIALIZZABILITÀ O DI IDONEITÀ PER UN PARTICOLARE SCOPO. D-LINK NEGA ESPRESSAMENTE QUALUNQUE ALTRA GARANZIA CHE NON RIENTRI NELLA PRESENTE GARANZIA LIMITATA. QUALSIASI GARANZIA IMPLICITA, CHE DOVESSE ESSERE IMPOSTA PER LEGGE, SARÀ CIRCOSCRITTA ALLA DURATA DELLA PRESENTE GARANZIA. ALCUNI PAESI VIETANO QUALSIASI LIMITAZIONE DEL PERIODO DI VALIDITÀ DELLE GARANZIE IMPLICITE OPPURE L'ESCLUSIONE O LA LIMITAZIONE DEI DANNI INCIDENTALI O CONSEGUENZIALI PER I PRODOTTI. IN TALI PAESI, EVENTUALI ESCLUSIONI O LIMITAZIONI DELLA PRESENTE GARANZIA NON POTRANNO APPLICARSI AL VOSTRO CASO. LA PRESENTE GARANZIA VI CONFERISCE DIRITTI LEGALI SPECIFICI. INOLTRE POTRETE GODERE DI ULTERIORI DIRITTI CHE POSSONO VARIARE A SECONDA DEL PAESE. SIETE INVITATI A CONSULTARE LE LEGGI APPLICABILI DEL VOSTRO PAESE AL FINE DI DETERMINARE CON PRECISIONE I VOSTRI DIRITTI.

La presente garanzia trova applicazione su tutti i prodotti hardware recanti il marchio D-LINK (di seguito denominati collettivamente "Prodotti hardware D-LINK") venduti da D-LINK (Europe) Ltd., dalle sue controllate, dalle sue affiliate, dai rivenditori autorizzati o dai distributori nazionali (di seguito denominati collettivamente "D-LINK"), accompagnati dalla presente garanzia limitata. Il termine "Prodotto hardware D-LINK" si riferisce esclusivamente ai componenti hardware e a tutte le parti interne compreso il firmware. Il termine "Prodotto hardware D-LINK" NON comprende eventuali applicazioni o programmi software.

Ambito geografico della Garanzia limitata

La presente Garanzia è estesa a tutti i Paesi europei elencati nell'appendice "Paesi europei - Garanzia limitata dei prodotti D-LINK". Il termine "Paesi europei" si riferisce esclusivamente ai paesi nominati in questa appendice. La Garanzia verrà riconosciuta in tutti i paesi nei quali D-LINK o i suoi Centri di Assistenza autorizzati offrono assistenza conformemente alle condizioni e ai termini stabiliti nella presente Garanzia. Tuttavia, la disponibilità all'assistenza e i tempi di intervento variano da paese a paese e possono essere soggetti a eventuali requisiti di registrazione.

Limitazione della Garanzia

D-LINK garantisce che i prodotti sotto descritti in condizioni di normale utilizzo non presentano difetti di fabbricazione o vizi di materiale durante il Periodo di garanzia sotto specificato ("Periodo di garanzia"), a condizione che vengano utilizzati e sottoposti a manutenzione in conformità con il manuale d'uso e con ogni altra documentazione fornita all'acquirente all'atto dell'acquisto (e relativi emendamenti). D-LINK non garantisce che il funzionamento del prodotto sarà ininterrotto o esente da errori né tanto meno che tutti gli eventuali errori, carenze, difetti o non conformità potranno essere corretti.

La presente garanzia non copre eventuali problemi derivanti da: (a) alterazioni o aggiunte non autorizzate; (b) negligenza, abuso o utilizzo improprio, compresa l'incapacità di far funzionare il prodotto in conformità con le specifiche e i requisiti di connessione; (c) movimentazione impropria; (d) guasto di prodotti o servizi non forniti da D-LINK o non soggetti a una garanzia successiva di D-LINK o a un accordo di manutenzione; (e) impiego o conservazione impropri; (f) incendio, inondazione, cause di forza maggiore o altro evento catastrofico accidentale. La presente garanzia non si applica altresì ad alcun prodotto particolare qualora il numero di serie di D-LINK sia stato rimosso o reso illeggibile in altro modo.

D-LINK DECLINA OGNI RESPONSABILITÀ PER EVENTUALI DANNI RISULTANTI DAL MANCATO RISPETTO DELLE ISTRUZIONI RELATIVE AL PRODOTTO HARDWARE D-LINK.

Periodo di garanzia

Il Periodo di garanzia ha decorrenza dalla data dell'acquisto presso D-LINK. Prova della data di acquisto è il documento fiscale (scontrino fiscale o ricevuta) recante la data di acquisto del prodotto. Per avere diritto alla garanzia può esservi richiesto di esibire la prova di acquisto. Potete beneficiare delle prestazioni di assistenza previste dalla garanzia in conformità con i termini e le condizioni di cui sotto nel momento in cui il Vostro prodotto hardware D-LINK necessita di una riparazione durante il Periodo di garanzia.

La presente Garanzia si applica esclusivamente al primo acquirente del Prodotto hardware D-LINK e non può essere trasferita a terzi che abbiano ottenuto la proprietà del Prodotto hardware D-LINK dal primo acquirente.

Tipo de producto	Período de garantía del producto
Switch (solo Switch dotati di agente SNMP incorporato) (inclusi moduli e software di gestione)	5 (cinque) anni
Tutti gli altri prodotti	2 (due) anni
Pezzi di ricambio (es. adattatori esterni di potenza, alimentatori esterni, ventole)	1 (Un) anno

Il periodo di garanzia sopra specificato relativamente a tutti i prodotti D-LINK venduti nei Paesi europei da D-LINK o da qualsiasi suo rivenditore o distributore autorizzato decorre dal 1° gennaio 2004. Tutti i prodotti venduti nei Paesi europei da D-LINK o da uno qualsiasi dei suoi rivenditori o distributori autorizzati prima del 1° gennaio 2004 sono coperti da una garanzia di 5 anni fatto salvo per alimentatori, ventole e accessori che hanno 2 anni di garanzia.

Il periodo di garanzia qui menzionato sostituisce qualsiasi altro periodo di garanzia definito nel manuale d'uso o nel contratto di acquisto del prodotto. Se avete acquistato un prodotto D-LINK in qualità di consumatore i Vostri diritti rimangono invariati.

Prestazioni della Garanzia limitata

Qualora comparisse un difetto o una non conformità, D-LINK avrà l'unico obbligo di riparare o sostituire il prodotto non conforme senza alcun costo per l'acquirente a condizione che il prodotto venga restituito a un Centro di Assistenza autorizzato D-LINK entro il periodo di garanzia. La riparazione o la sostituzione verranno eseguite da D-LINK presso un Centro di Assistenza autorizzato D-LINK. Tutti i componenti o i prodotti hardware rimossi conformemente ai termini e alle condizioni della presente garanzia divengono di proprietà di D-LINK. Il pezzo o il prodotto in sostituzione beneficerà della garanzia per il tempo residuo della parte o del prodotto originale. Il prodotto in sostituzione non deve necessariamente essere nuovo o di identica fattura, modello o composizione; D-LINK può a sua discrezione sostituire il prodotto non conforme (o qualsiasi parte di esso) con un prodotto che risulti essere equivalente (o di valore superiore) al prodotto non conforme. D-LINK può richiedere che venga esibita la prova di acquisto.

Garante

D-Link (Europe) Ltd.
4th Floor, Merit House
Edgware Road
Colindale
Londra NW9 5 AB
Regno Unito
Telefono: +44-020-8731-5555
Fax: +44-020-8731-5511

www.dlink.co.uk

D-Link® Offices

U.S.A

17595 Mt. Herrmann Street
Fountain Valley, CA. 92708
TEL: 714-885-6000
FAX: 866-743-4905
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.)

4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
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

Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr

Netherlands

Weena 290
3012 NJ Rotterdam
Netherlands
TEL: +31-10-282-1445
FAX: +31-10-282-1331
URL: www.dlink-benelux.com

Belgium

Rue des Colonies 11
B-1000 Brussels
Belgium
Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL: www.dlink-benelux.com

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

Norway

Karihaugveien 89, 1086 Oslo
Norway
TEL: 47-23-897189
FAX: 47-22-309085
URL: www.dlink.no

Finland

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

Iberia

C/Sabino De Arana,, 56 Bajos
08028 Barcelona
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es

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

Regus Offices
Beybi Giz Plaza, Ayazaga Mah. Meydan Sok.
No.28
Maslak 34396, Istanbul-Turkiye
TEL: +90 212 335 2553
FAX: +90 212 335 2500
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.B 2148, Hertzelia-Pituach 46120
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

Latin America

Isidora Goyechea 2934 of 702, Las Condes
Santiago, Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brazil

Av das Nacoes Unidas,
11857 - 14 - andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000
TEL: +55 11 55039320
FAX: +55 11 55039322
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: 7-095-744-0099
FAX: 7-095-744-0099 #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

2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw

Headquarters

2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL: www.dlink.com
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
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 No.	Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

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

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

1. Where and how will the product primarily be used?

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 DECnet Pathwork Windows NT 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®