GS-3012/GS-3012F

Gigabit Ethernet Switch

Version 3.60 (LH.1, LR.1)

12/2005

User's Guide

ZyXEL

Copyright

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two (2) years from the date of purchase. During the warranty period and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online for free future product updates and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Interference Statements and Warnings

FCC Interference Statement

This switch complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This switch may not cause harmful interference.

(2) This switch must accept any interference received, including interference that may cause undesired operations.

FCC Warning

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

CE Mark Warning:

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

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者

這是甲類的資訊產品，在居住的環境使用時，

可能造成射頻干擾，在這種情況下，

使用者會被要求採取某些適當的對策.

Certifications

Go to www.zyxel.com

Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

Select the certification you wish to view from this page.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways:

Contacting Customer Support

When you contact your customer support representative, have the following information ready:

Product model and serial number.

Firmware version information.

Warranty information.

Date you received your product.

Brief description of the problem and the steps you took to solve it.

7METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[1] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 – Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de/	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	mailto:support@zyxel.hu	+36-1-3361649	www.zyxel.hu/	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	mailto:info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz/	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

[1] "+" is the (prefix) number you enter to make an international telephone call.

7METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[1] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
POLAND	info@pl.zyxel.com 	+48-22-5286603 +48-22-5206701	www.pl.zyxel.com/ 	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
RUSSIA	http://zyxel.ru/support sales@zyxel.ru	+7-095-542-89-29 +7-095-542-89-25	www.zyxel.ru/ 	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es 	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se 	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
UKRAINE	support@ua.zyxel.com sales@ua.zyxel.com	+380-44-247-69-78 +380-44-494-49-32	www.ua.zyxel.com/ 	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
UNITED KINGDOM	support@zyxel.co.uk sales@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only) +44 (0) 1344 303034	www.zyxel.co.uk ftp.zyxel.co.uk	ZyXEL Communications UK Ltd., 11, The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

Table of Contents

List of Figures

List of Tables

List of Charts

Preface

Congratulations on your purchase of a GS-3012 series switch.

This preface introduces you to the GS-3012 models and discusses the conventions of this User's Guide. It also provides information on other related documentation.

About the GS-3012 Series

The GS-3012 Gigabit Ethernet Switches are managed switches with features ideally suited in an enterprise environment. They can deliver broadband IP services to:

- Multi-tenant unit (MTU) buildings (hotels, motels, resorts, residential multi-dwelling units, office buildings, educational establishments, etc.)
- Public facilities (convention centers, airports, plazas, train stations, etc.)
- Enterprises.

They can also be deployed as a mini-POP (point-of-presence) in a building basement delivering 10/100/1000Mbps data service over Category 5 wiring to each customer.

About the GS-3012

There are two GS-3012 models. The GS-3012 DC model requires DC power supply input of -48 VDC to -60 VDC, 1.84A Max. The GS-3012 AC model requires 100~240VAC/1.5A power.

About the GS-3012F

There are two GS-3012F models. The GS-3012F DC model requires DC power supply input of -48 VDC to -60 VDC, 1.2A Max. The GS-3012F AC model requires 100~240VAC/1.5A power.

All figures in this guide display the GS-3012F AC model unless specifically noted otherwise.

General Syntax Conventions

- This guide shows you how to configure the switch using the web configurator and CLI commands. See the online HTML help for information on individual web configurator screens.
- Mouse action sequences are denoted using a comma. For example, click **Start, Settings, Control Panel, Network** means first you click **Start**, click or move the mouse pointer over **Settings**, then click or move the mouse pointer over **Control Panel** and finally click (or double-click) **Network**.
- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Predefined choices are in **Bold Arial** font.
- Button and field labels, links and screen names in are in **Bold Times New Roman** font.
- For brevity's sake, we will use "e.g." as shorthand for "for instance", and "i.e." as shorthand for "that is" or "in other words" throughout this manual.
- This User's Guide will refer to both the GS-3012 and the GS-3012F as the "GS" or "the switch" in this User's Guide. Distinctions between the models will be made where needed.

Firmware Naming Conventions

A firmware version includes the network operating system platform version, model code and release number as shown in the following example.

GS-3012 Firmware Version: V3.60 (LH.1)
"V3.60" is the network operating system platform version.
"LH" is the model code.
"1" is this firmware's release number. This varies as new firmware is released. Your firmware's release number may not match what is displayed in this *User's Guide*.

Graphics Icons Key

 The GS	 Switch	 Server
 Computer	 Printer	 Gateway

Related Documentation

Web Configurator Online HTML help

The online HTML help shows you how to use the web configurator to configure individual screens. More background information can be found in this UG.

ZyXEL Web Site

The ZyXEL download library at www.zyxel.com contains additional support documentation as well as an online glossary of networking terms.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Part I

Features and Applications

This part acquaints you with the features and applications of the switches.

Chapter 1
Getting to Know the GS-3012 Series

This chapter describes the key features, benefits and applications of the GS-3012 series.

1.1 Introduction

The GS-3012 and GS-3012F are layer 2 stand-alone Gigabit Ethernet switches. There are 100/1000 Mbps ports for electrical Ethernet connections and mini GBIC slots for optical uplink connections. See the appendices for details on the number of 100/1000 Mbps ports and mini GBIC slots on each model.

There is a console port and RJ-45 port for local management. With the built-in web configurator, managing and configuring the switch is easy. From cabinet management to port-level control and monitoring, you can visually configure and manage your network via the web browser. Just click your mouse instead of typing cryptic command strings. In addition, the switch can also be managed via Telnet, the console port, or third-party SNMP management.

1.2 Features

These sections describe the hardware and firmware features of the GS-3012 series.

1.2.1 Hardware Features

100/1000 Mbps Gigabit Ports (Some Paired With Mini GBIC Slots)

Connect computers or switches directly to the 100/1000Mbps auto-negotiating, automatic cable sensing (auto-MDIX) RJ-45 Gigabit ports. All ports support:

- IEEE 802.3/3u/3z/3ab standards
- Back pressure flow control in half duplex mode
- IEEE 802.3x flow control in full duplex mode

Mini GBIC Slots

These are slots for mini GBIC (Gigabit Interface Converter) transceivers. These allow the switch to connect to another WAN switch or daisy-chain to other switches.

Console Port

Use the console port for local management of the switch.

One Management Port

Use the RJ-45 management port for local switch management only.

Fans

The fans provide sufficient cooling to allow reliable operation even in poorly ventilated rooms or basements.

1.2.2 Firmware Features

IP Protocols

- IP Host (No routing)
- Telnet for configuration and monitoring
- SNMP for management
  - SNMP MIB II (RFC 1213)
  - SNMP v1 RFC 1157
  - Ethernet MIBs RFC 1643
  - Bridge MIBs RFC 1493
  - SMI RFC 1155
  - RMON RFC 1757
  - SNMPv2 or SNMPv2c
  - Bridge extension MIBs RFC 2674
  - Interface MIB RFC 2863
  - Ping and Trace Route RFC 2925

Management

- Web configurator
- Command-line interface locally via console port or remotely via Telnet
- Out-of-band RJ-45 management port
- SNMP

System Monitoring

- System status (link status, rates, statistics counters)
- Syslog
- SNMP
- Temperatures, voltage, fan speed reports and alarms
- Port Mirroring allows you to analyze one port's traffic from another.

Security

- System management password protection
- IEEE 802.1Q VLAN
- Limit dynamic port MAC address learning
- Secure SHell communication protocol
- Port-based VLAN
- 802.1x Authentication
- Static MAC address filtering

Port Link Aggregation

The GS adheres to the IEEE 802.3ad standard for static and dynamic port link aggregation.

Bandwidth Control

- You can set the amount of bandwidth that an individual port can use. The switch allows you to define a maximum allowable bandwidth for incoming and/or out-going traffic on a port.
- The switch supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your switch.
- Broadcast storm control.

Quality of Service

- Eight priority queues so you can ensure mission-critical data gets delivered on time.
- Follows the IEEE 802.1p priority setting.
- Advanced policy-based traffic shaping.

STP (Spanning Tree Protocol) / RSTP (Rapid STP)

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

Cluster Management

Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

1.3 Applications

This section shows a few examples of using the switch in various network environments.

1.3.1 Backbone Application

In this application, the switch is an ideal solution for small networks where rapid growth can be expected in the near future.

The switch can be used standalone for a group of heavy traffic users. You can connect computers directly to the switch's ports or connect other switches to the GS.

In this example, all computers connected directly or indirectly to the GS can share super high-speed applications on the Gigabit server.

To expand the network, simply add more networking devices such as switches, routers, firewalls, print servers etc.

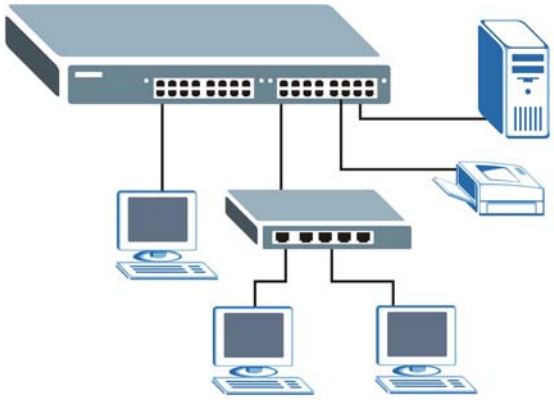


Figure 1-1 Backbone Application

1.3.2 Bridging Example

In this example application the switch is the ideal solution for different company departments to connect to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the switch. You can provide a super-fast uplink connection by installing the transceiver(s) in the mini GBIC slots.

Moreover, the switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

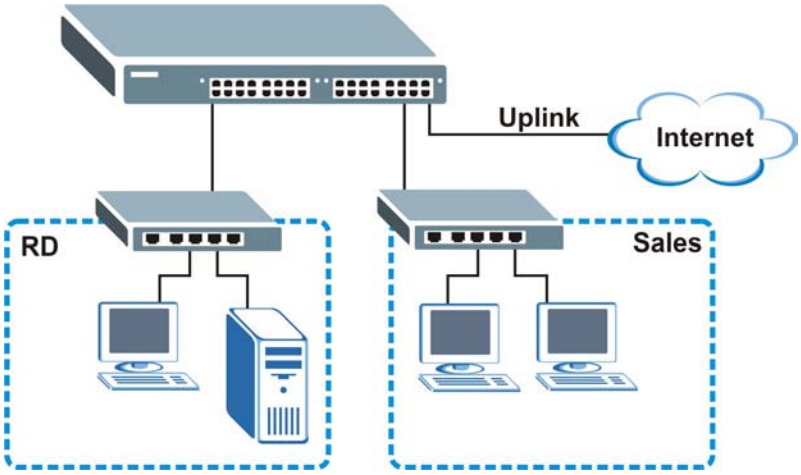


Figure 1-2 Bridging Application

Full-duplex mode operation only applies to point-to-point access (for example, when attaching the switch to a workstation, server, or another switch). When connecting to hubs, use a standard cascaded connection set at half-duplex operation.

1.3.3 High Performance Switched Workgroup Example

The switch is ideal for connecting two power workgroups that need high bandwidth. In the following example, use trunking to connect these two power workgroups.

Switching to higher-speed LANs such as FDDI or ATM is not feasible for most people due to the expense of replacing all existing Ethernet cables and adapter cards, restructuring your network and complex maintenance.

The GS can provide the same bandwidth as FDDI and ATM at much lower cost while still being able to use existing adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

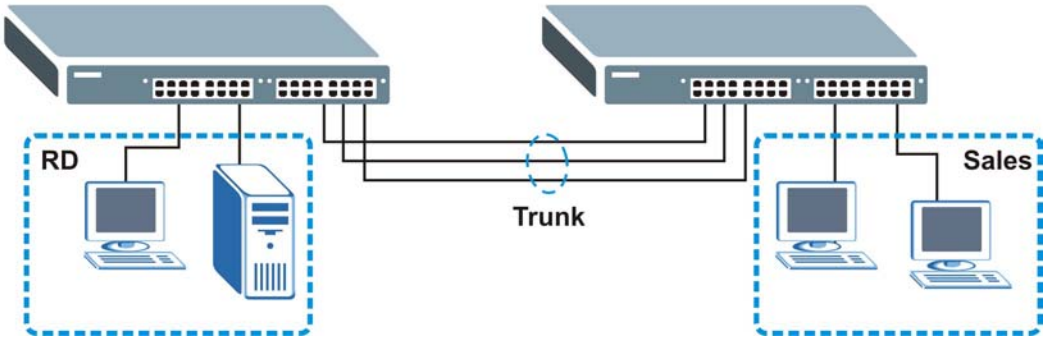


Figure 1-3 High Performance Switched Workgroup Application

1.3.4 IEEE 802.1Q VLAN Application Examples

This section shows a workgroup and a shared server example using 802.1Q tagged VLANs. For more information on VLANs, see the *Switch Setup* section and the *VLAN Setup* chapter in this User's Guide. A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

Tag-based VLAN Workgroup Example

Ports in the same VLAN group share the same broadcast domain thus increase network performance through reduced broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

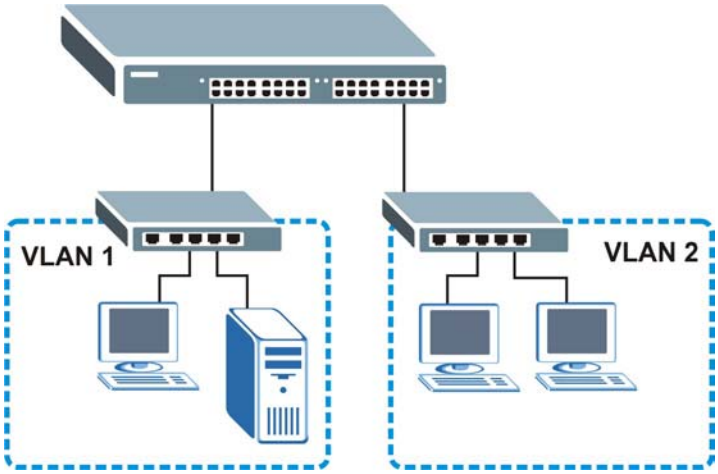


Figure 1-4 VLAN Workgroup Application

VLAN Shared Server Example

Shared resources such as a server can be used by all ports in the same VLAN as the server, as shown in the following example. In this example, only ports that need access to the server need belong to VLAN 1 while they can belong to other VLAN groups too.

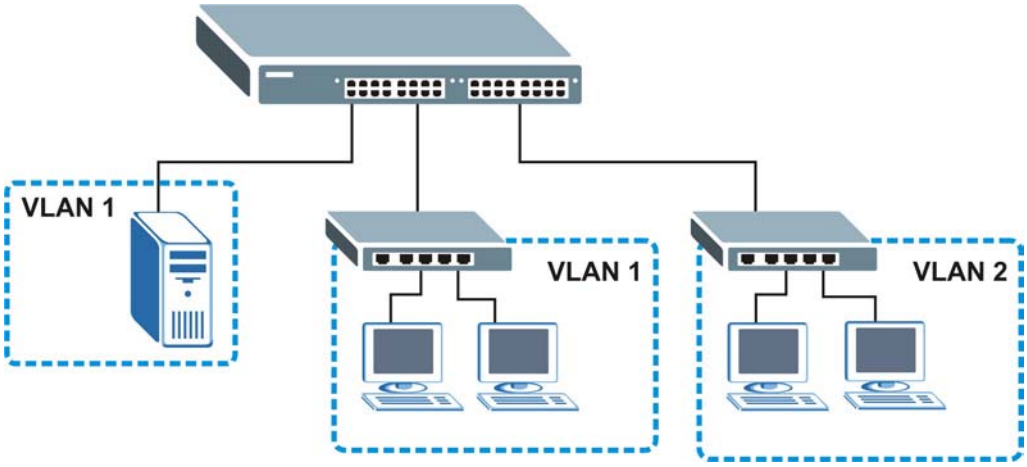


Figure 1-5 Shared Server Using VLAN Example

Part II

Hardware Installation and Connections

This part acquaints you with installing the switch, instructs you on how to make the hardware connections and explains the front panel LEDs.

Chapter 2 Hardware Installation

This chapter shows two switch installation scenarios.

2.1 Installation Scenarios

The switch can be placed on a desktop or rack-mounted on a standard EIA rack. Use the rubber feet in a desktop installation and the brackets in a rack-mounted installation.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and 3.4 inches (8 cm) at the back of the switch. This is especially important for enclosed rack installations.

2.1.1 Desktop Installation Procedure

1. Make sure the switch is clean and dry.
2. Set the switch on a smooth, level surface strong enough to support the weight of the switch and the connected cables. Make sure there is a power outlet nearby.
3. Make sure there is enough clearance around the switch to allow air circulation and the attachment of cables and the power cord.
4. Remove the adhesive backing from the rubber feet.
5. Attach the rubber feet to each corner on the bottom of the switch. These rubber feet help protect the switch from shock or vibration and ensure space between switches when stacking.

Figure 2-1 Attaching Rubber Feet

Do not block the ventilation holes. Leave space between switches when stacking.

2.1.2 Rack-Mounted Installation

The switch can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your switch on a standard EIA rack using a rack-mounting kit.

1. Align one bracket with the holes on one side of the switch and secure it with the bracket screws smaller than the rack-mounting screws.
2. Attach the other bracket in a similar fashion.

Figure 2-2 Attaching Mounting Brackets and Screws

3. After attaching both mounting brackets, position the switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the switch to the rack with the rack-mounting screws.

Figure 2-3 Mounting the ES to an EIA standard 19-inch rack

Chapter 3
Hardware Connections

This chapter acquaints you with the front and rear panels, shows you how to make the connections, install/remove (optional) modules and explains the LEDs.

3.1 Safety Warnings

- The length of exposed (bare) power wire should not exceed 7mm.
- Do not use this product near water, for example, in a wet basement.
- Only a qualified technician should service or disassemble this device.

3.2 Front Panel

The following figure shows the front panel of the GS-3012. The front panel contains the switch LEDs, RJ-45 gigabit ports, mini GBIC ports and a console and management port for local management.

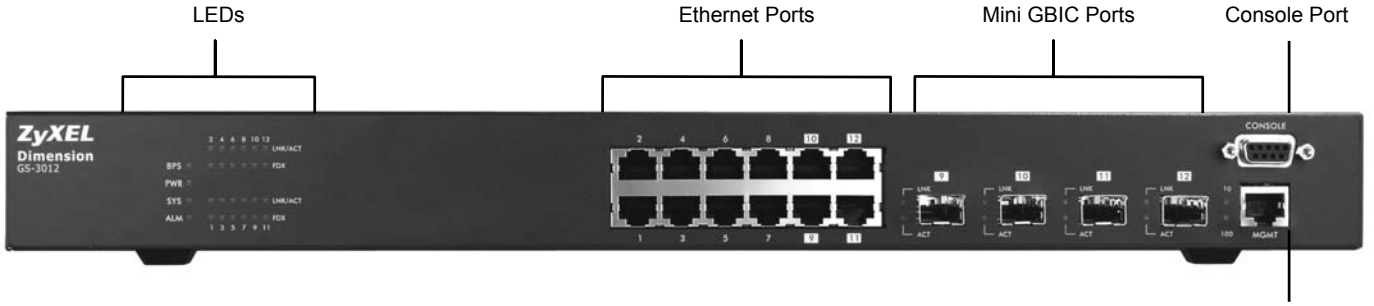


Figure 3-1 GS-3012 Front Panel

The following figure shows the front panel of the GS-3012F. The front panel contains the switch LEDs, mini GBIC ports, RJ-45 Gigabit ports, and a console and management port for local management.

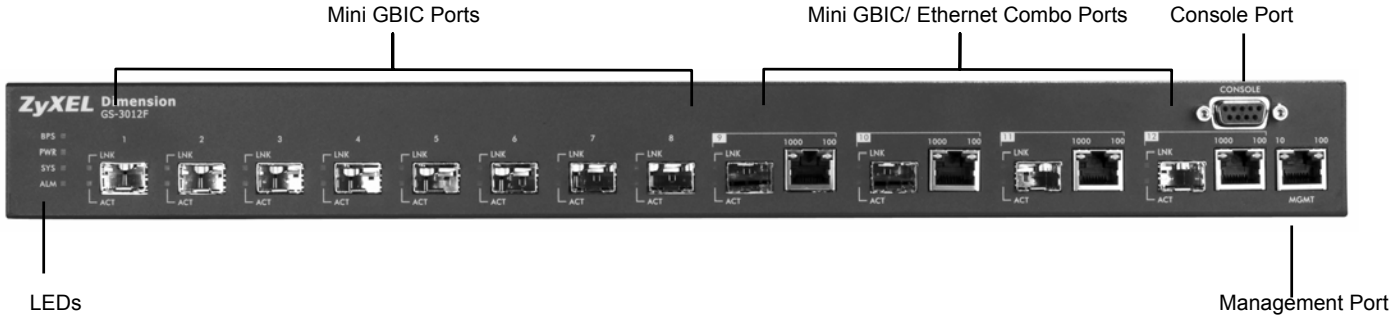


Figure 3-2 GS-3012F Front Panel

Table 3-1 Front Panel Connections

CONNECTOR	DESCRIPTION
100/1000 Mbps RJ-45 Ethernet Ports	Connect these 1Gbps Electrical Ethernet ports to high-bandwidth backbone network Ethernet switches or use them to daisy-chain other switches.
Mini GBIC Ports	Use mini GBIC transceivers in these slots for fiber-optical connections to backbone Ethernet switches.
Console Port	The console port is for local configuration of the switch.
Management Port	Connect to a computer using an RJ-45 Ethernet cable for local configuration of the switch.

3.2.1 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port on the switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.2.2 Gigabit Interfaces

The switch has 100/1000Mbps auto-negotiating, auto-crossover Gigabit ports. The speed of the Gigabit ports can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (for 100 Mbps) or full duplex. The GS-3012's mini GBIC slots are paired with Gigabit ports. The GS-3012F's Gigabit ports are paired with mini GBIC slots.

The switch uses up to one connection for each mini GBIC slot and Gigabit port pair. The mini GBIC ports have priority over the Gigabit ports. This means that if a mini GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

When auto-negotiation is turned on, a Gigabit port negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a Gigabit port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

Default Ethernet Negotiation Settings

The factory default negotiation settings for the Gigabit ports are:

Speed: Auto — Duplex: Auto

Flow control: On — Link Aggregation: Disabled

Auto-crossover

All ports are auto-crossover, that is auto-MDIX ports (Media Dependent Interface Crossover), so you may use either a straight-through Ethernet cable or crossover Ethernet cable for all Gigabit port connections. Auto-crossover ports automatically sense whether they need to function as crossover or straight ports, so crossover cables can connect both computers and switches/hubs.

3.2.3 Mini GBIC Slots

These are slots for mini GBIC (Gigabit Interface Converter) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The switch does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

- Type: SFP connection interface
- Connection speed: 1 Gigabit per second (Gbps)

Transceiver Installation

Use the following steps to install a mini GBIC transceiver (SFP module).

1. Insert the transceiver into the slot with the exposed section of PCB board facing down.
2. Press the transceiver firmly until it clicks into place.
3. The switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

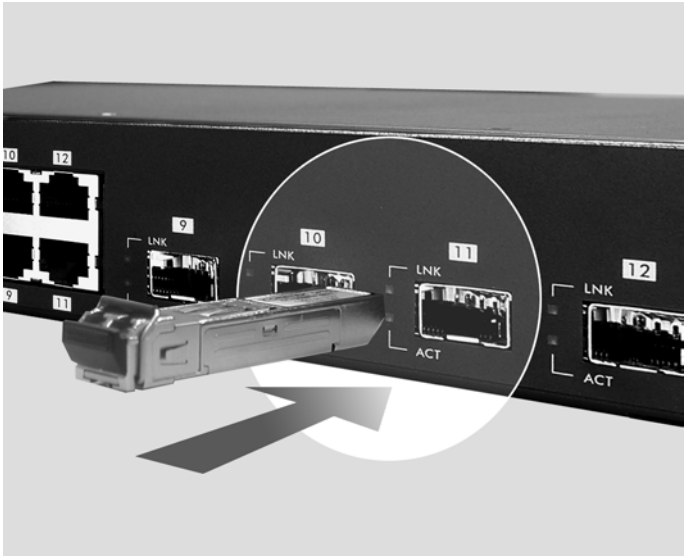


Figure 3-3 Transceiver Installation Example

Figure 3-4 Installed Transceiver

Transceiver Removal

Use the following steps to remove a mini GBIC transceiver (SFP module).

1. Open the transceiver's latch (latch styles vary).
2. Pull the transceiver out of the slot.

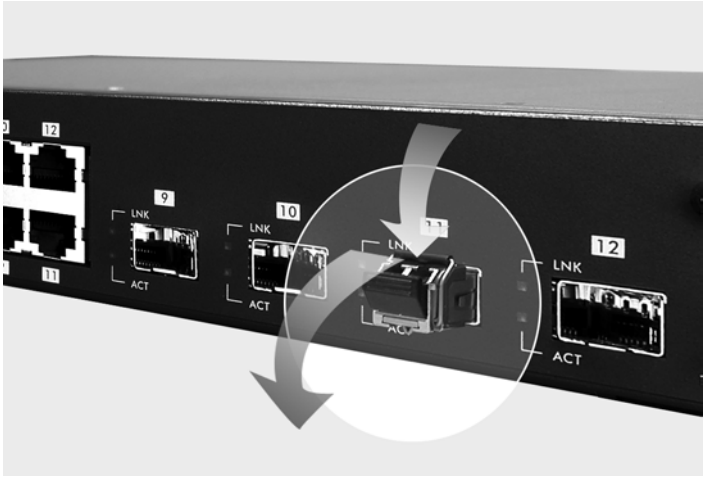


Figure 3-5 Opening the Transceiver's Latch Example

Figure 3-6 Transceiver Removal Example

3.2.4 Management Port

The **MGMT** (management) port is used for local management. Connect directly to this port using an Ethernet cable. You can configure the switch via Telnet or the web configurator.

The default IP address of the management port is 192.168.0.1 with a subnet mask of 255.255.255.0.

3.3 Rear Panel

The following figure shows the rear panel of the GS-3012F. The rear panel contains the ventilation holes, a connector for external backup power supply (BPS), the power receptacle and the power switch (for DC model). The GS-3012 rear panels are similar.

Figure 3-7 GS-3012F Rear Panel: AC Model

Figure 3-8 GS-3012F Rear Panel: DC Model

3.3.1 Power Connector

Make sure you are using the correct power source as shown on the panel.

To connect the power to the AC power model, insert the female end of power cord to the power receptacle on the rear panel. Connect the other end of the supplied power cord to an appropriate power outlet (see the appendix of product specifications for details). Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

The DC power model requires DC power supply input (see the appendix of product specifications for details). To connect the power to the unit, insert the one end of the supplied power cord to the power receptacle on the rear panel and the other end to a power outlet.

3.3.2 External Backup Power Supply Connector

The switch supports external backup power supply (BPS).

The backup power supply constantly monitors the status of the internal power supply. The backup power supply automatically provides power to the switch in the event of a power failure. Once the switch receives power from the backup power supply, it will not automatically switch back to using the internal power supply even when the power is resumed.

3.4 Front Panel LEDs

After you connect the power to the switch, view the LEDs to ensure proper functioning of the switch and as an aid in troubleshooting.

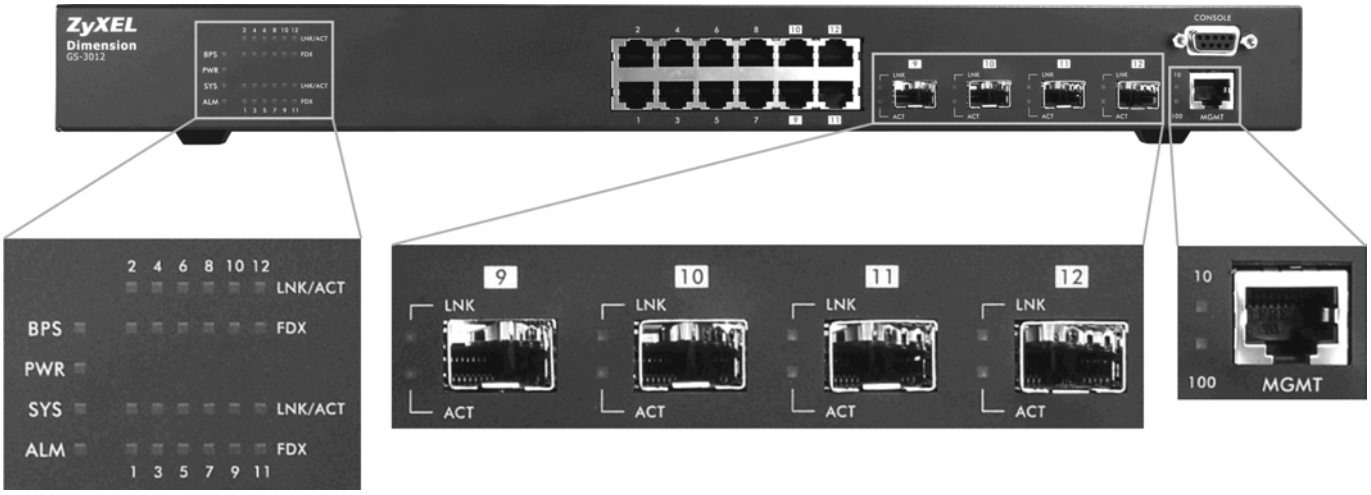


Figure 3-9 GS-3012 Front Panel LEDs

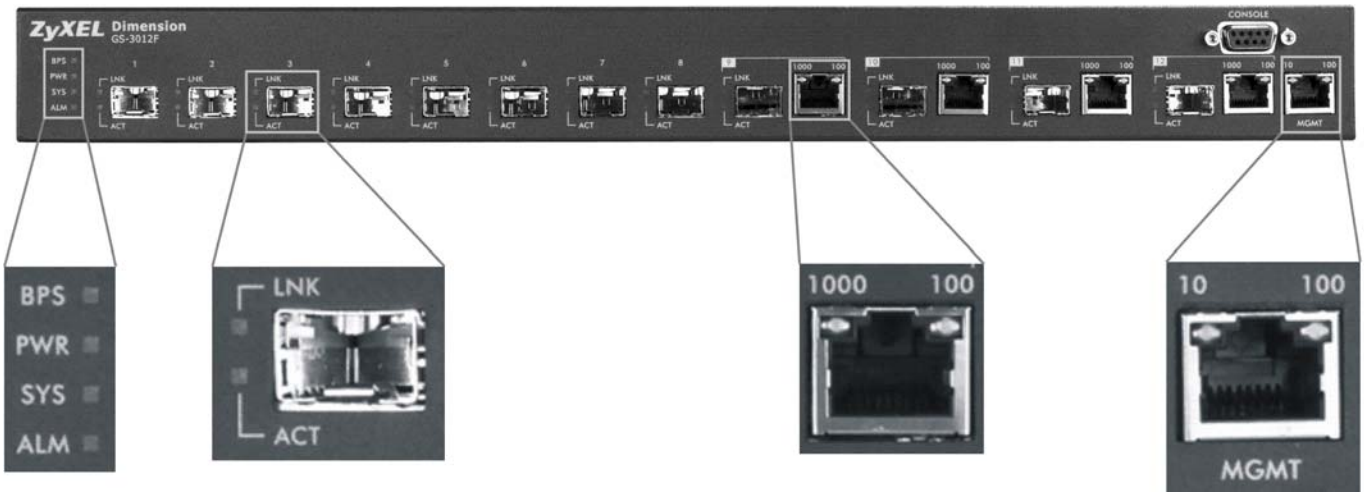


Figure 3-10 GS-3012F Front Panel LEDs

The following table describes the LEDs on the front panel.

Table 3-2 Front Panel LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
BPS	Green	Blinking	The system is receiving power from the backup power supply.
		On	The backup power supply is connected and active.
		Off	The backup power supply is not ready or not active.
PWR	Green	On	The system is turned on.
		Off	The system is off.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.

Table 3-2 Front Panel LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
Mini GBIC Slots			
LNK	Green	On	The link to this port is up.
		Off	The link to this port is not connected.
ACT	Green	Blinking	This port is receiving or transmitting data.
Gigabit Ports			
LNK/ACT (GS-3012)	Green	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
FDX (GS-3012)	Amber	On	The Gigabit port is negotiating in full-duplex mode.
		Off	The Gigabit port is negotiating in half-duplex mode and no collisions are occurring.
1000 (GS-3012F)	Green	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 1000 Mbps Ethernet network is up.
		Off	The link to a 1000 Mbps Ethernet network is down.
100 (GS-3012F)	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to a 100 Mbps Ethernet network is down.
MGMT			
10	Green	Blinking	The system is transmitting/receiving to/from an Ethernet device.
		On	The port is connected at 10Mbps.
		Off	The port is not connected at 10Mbps or to an Ethernet device.
100	Amber	Blinking	The system is transmitting/receiving to/from an Ethernet device.
		On	The port is connected at 100Mbps.
		Off	The port is not connected at 100Mbps or to an Ethernet device.

3.5 Configuring the Switch

You may use the embedded web configurator or command line interface to configure the switch. If you're using the web configurator, you need Internet Explorer 5.5 and later or Netscape Navigator 6 and later.

You can access the command line interface using a terminal emulation program on a computer connected to the switch console port (see *Section 3.2.1*) or access the switch using Telnet.

The next part of this guide discusses configuring the switch using the web configurator.

Part III

Getting Started

This part introduces you to the web configurator, describes the Status and Port Details screens and shows you how to configure the Basic Setting screens.

Chapter 4
Introducing the Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The embedded web configurator allows you to manage the switch from anywhere through a standard browser such as Microsoft Internet Explorer or Netscape Navigator.

Use Internet Explorer 5.5 and later or Netscape Navigator 6 and later versions.

4.2 System Login

1. Start your Internet Explorer or Netscape Navigator web browser.
2. Type "http://" and the IP address of the switch (for example, the default is 192.168.1.1 for in-band management or 192.168.0.1 when connected to the management port) in the Location or Address field. Press **Enter**.
3. The login screen appears. The default username is **admin** and the associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 4-1 Web Configurator: login

4. Click **OK** to view the first web configurator screen.

4.3 Status Screen

The **Status** screen is the first web configurator screen you see after you log in. The following figure shows the navigating components of a web configurator screen.

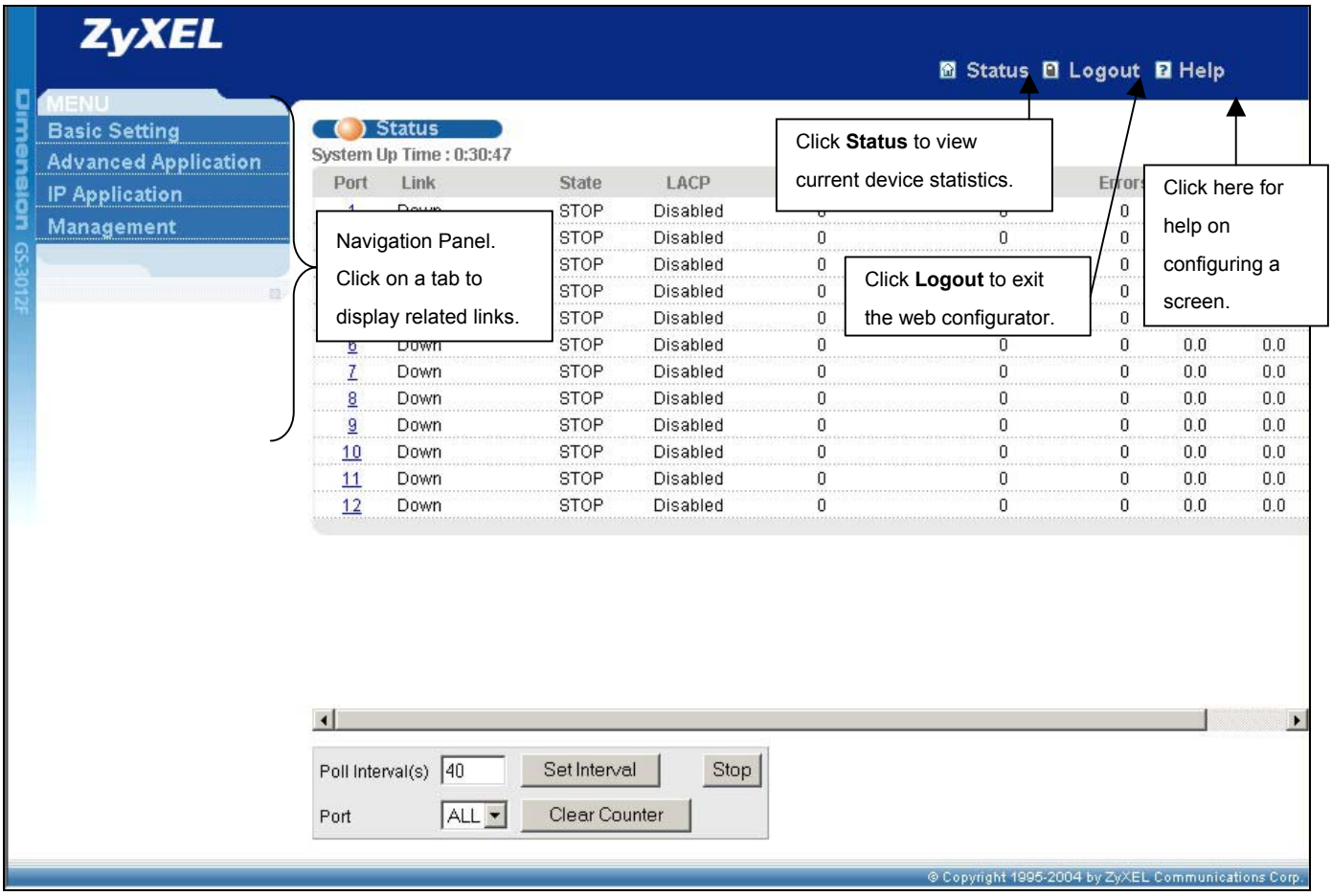


Figure 4-2 Web Configurator Home Screen (Status)

In the navigation panel, click a main link to reveal a list of submenu links.

Table 4-1 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table lists the various web configurator screens within the sub-links.

Table 4-2 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
System Info	VLAN Status	Static Routing	Maintenance
General Setup	VLAN Port Setting	DHCP Relay	Firmware Upgrade
Switch Setup	Static VLAN		Restore Configuration
IP Setup	Static MAC Forwarding		Backup Configuration
Port Setup	Filtering		Load Factory Default
	Spanning Tree Protocol		Reboot System
	Status		Access Control
	Spanning Tree Protocol Configuration		SNMP
	Bandwidth Control		Logins
	Broadcast Storm Control		Service Access Control
	Mirroring		Remote Management
	Link Aggregation		Diagnostic
	Status		Syslog
	Link Aggregation Configuration		Syslog Setup
			Syslog Server Setup
			Cluster Management

Table 4-2 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
	Port Authentication RADIUS 802.1x Port Security Queuing Method Classifier Policy Rule Multicast Multicast Status Multicast Setting IGMP Filtering Profile MVR		Status Cluster Management Configuration MAC Table ARP Table

The following table summarizes these sub-links in the navigation panel.

Table 4-3 Navigation Panel Sub-link Descriptions

LABEL	DESCRIPTION
Basic Setting Screens	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the switch.
Switch Setup	This link takes you to a screen where you can set up global switch parameters such as VLAN type, MAC address learning, IGMP snooping, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for switch management) and DNS (domain name server).
Port Setup	This link takes you to screens where you can configure settings for individual switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the **Switch Setup** menu).
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the STP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can define a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.

Table 4-3 Navigation Panel Sub-link Descriptions

LABEL	DESCRIPTION
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference
Link Aggregation	This link takes you to a screen where you can logically trunk physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure RADIUS (Remote Authentication Dial-In User Service), a protocol for user authentication that allows you to use an external server to validate an unlimited number of users.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Queuing Method	This link takes you to a screen where you can configure SPQ or WRR with associated queue weights for each port.
Classifier	This link takes you to a screen where you can configure classifiers.
Policy Rule	This link takes you to a screen where you can configure policy rules.
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
IP Application	
Static Routing	This link takes you to screens where you can configure static routes. A static route defines how the switch should forward traffic by configuring the TCP/IP parameters manually.
DHCP Relay	This link takes you to a screen where you can configure DHCP relay information.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and test port(s).
Syslog	This link takes you to screens where you can configure the device's system logging settings.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default Administrator password in the **Logins** screen. Click **Advanced Application**, **Access Control** and then **Logins** to display the next screen.

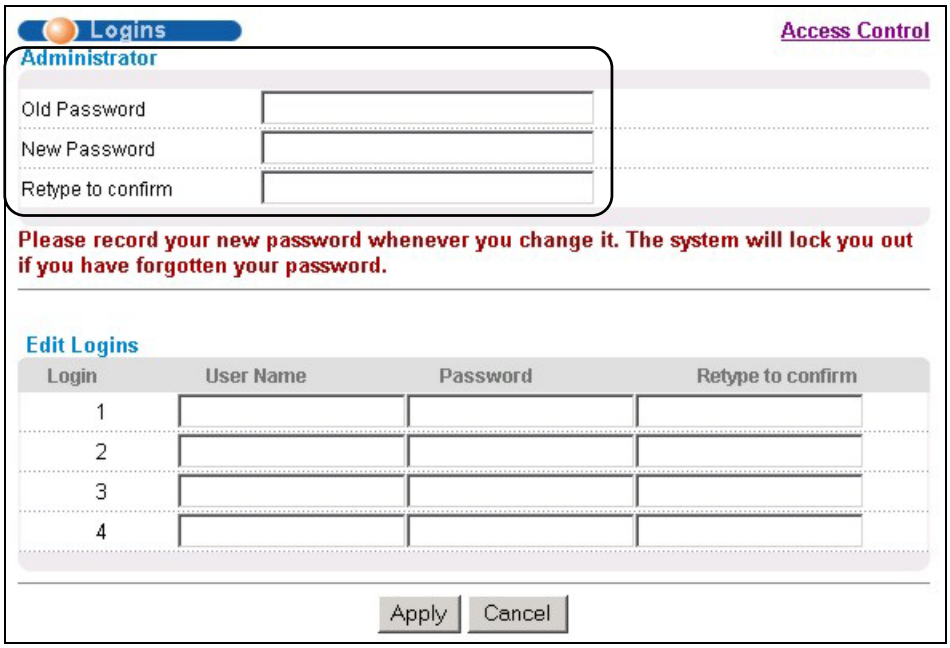


Figure 4-3 Web Configurator: Change Password at Login

4.4 Switch Lockout

You can be locked out from managing the switch if another administrator is currently logged in. You must wait until the other administrator has logged out before you can log in.

Any of the following could also lock you (and others) out from using in-band management to manage the switch.

1. Deleting the management VLAN (default is VLAN 1).
2. With port-based VLAN, disabling the CPU in-band switch management port option for all ports.
3. Incorrectly configuring the access control settings (this could also lock you out from performing out-of-band management).
4. Disabling all ports.
5. Assigning minimum bandwidth to the CPU port. If you limit bandwidth to the CPU port, you may find that the switch performs sluggishly or not at all.

Be careful not to lock yourself and others out of the switch.

4.5 Resetting the Switch

If you lock yourself (and others) out of the switch, you can try using the **MGMT** out-of-band management port or the console port. If you still cannot correct the situation or forgot the password, you will need to reload the factory-default configuration file.

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will

be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to "1234" and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

1. Connect to the console port using a computer with terminal emulation software. See the chapter on hardware connections for details.
2. Disconnect and reconnect the switch's power to begin a session. When you reconnect the switch's power, you will see the initial screen.
3. When you see the message "`Press any key to enter Debug Mode within 3 seconds`" press any key to enter debug mode.
4. Type `atlc` after the "`Enter Debug Mode`" message.
5. Wait for the "`Starting XMODEM upload`" message before activating XMODEM upload on your terminal.
6. After a successful configuration file upload, type `atgo` to finish starting the switch.

```
Bootbase Version: V1.0 | 04/25/2003 10:01:06
RAM: Size = 32768 Kbytes
FLASH: Intel 32M

ZyNOS Version: V3.60(LH.1) | 10/17/2005 14:08:00

Press any key to enter debug mode within 3 seconds.
.....................
Enter Debug Mode
GS-3012F> atlc

Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total  393216 bytes received.

Erasing..
.............................................................
OK

GS-3012F> atgo
```

Figure 4-4 Resetting the Switch: Via Console Port

The switch is now reinitialized with a default configuration file including the default password of "1234".

4.5.1 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so as you don't lock out other switch administrators.

Figure 4-5 Web Configurator: Logout Screen

4.5.2 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

Chapter 5
System Status and Port Details

This chapter describes the system status (web configurator home page) and port details screens.

5.1 About System Statistics and Information

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

5.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

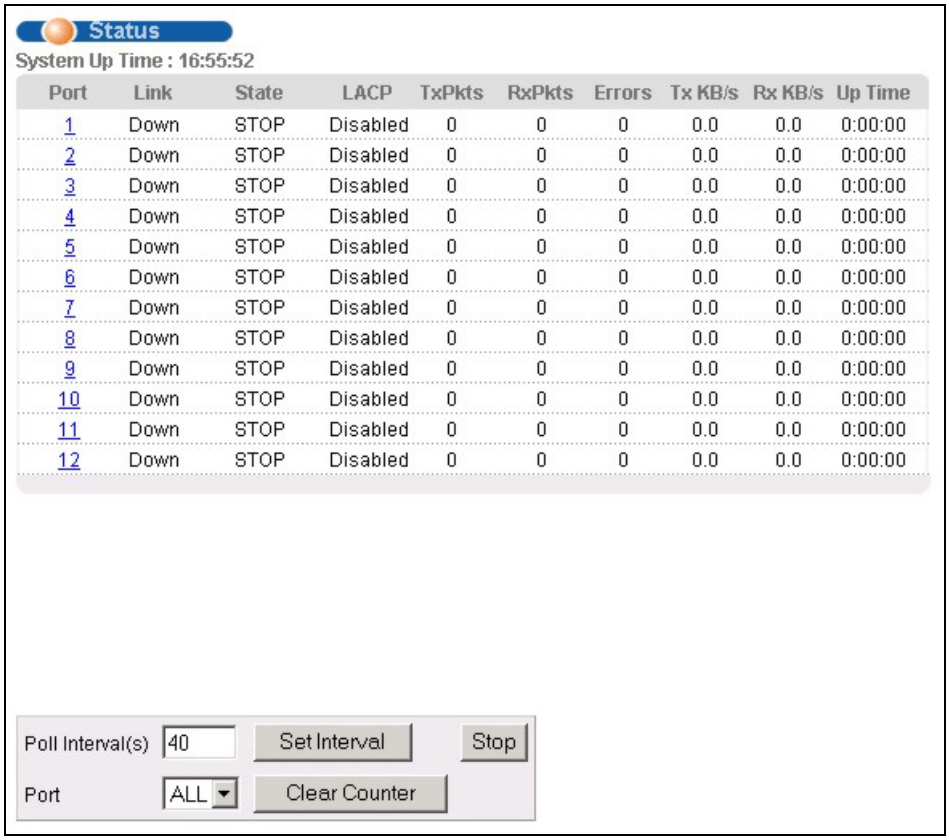


Figure 5-1 Status

The following table describes the labels in this screen.

Table 5-1 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.

Table 5-1 Status

LABEL	DESCRIPTION
Port	This identifies the Gigabit port. Click a port number to display the **Port Details** screen (refer to *Section 5.2.1*).
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half duplex).
State	This field displays the STP state of the port. See the *Spanning Tree Protocol* chapter for details on STP port states.
LACP	This fields displays whether the Link Aggregation Control Protocol (LACP) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.

5.2.1 Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the switch.

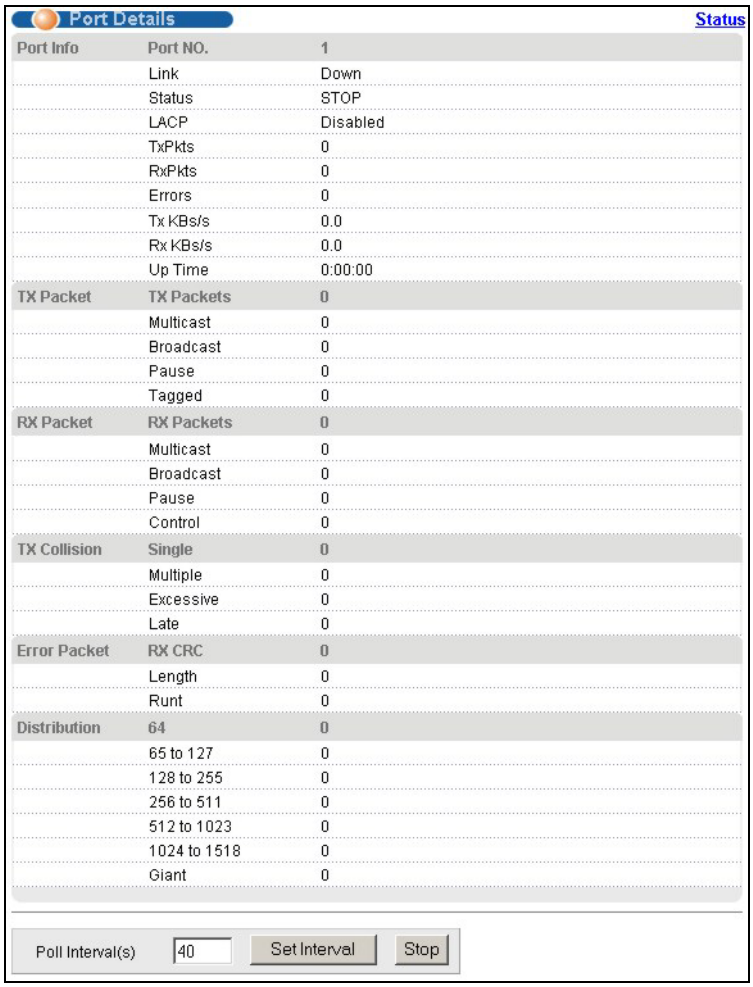


Figure 5-2 Status: Port Details

The following table describes the labels in this screen.

Table 5-2 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field identifies the Gigabit port described in this screen.
Link	This field shows whether the port connection is down, and the speed/duplex mode.
Status	This field shows the training state of the ports. The states are **FORWARDING** (forwarding), which means the link is functioning normally or **STOP** (the port is stopped to break a loop or duplicate path).
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.

Table 5-2 Status: Port Details

LABEL	DESCRIPTION
Tx KB/s	This field shows the number kilobytes per second transmitted on this port.
Rx KB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about frames transmitted.	
TX Packets	This field shows the number of good frames (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast frames transmitted.
Broadcast	This field shows the number of good broadcast frames transmitted.
Pause	This field shows the number of 802.3x Pause frames transmitted.
Tagged	This field shows the number of frames with VLAN tags transmitted.
Rx Packet The following fields display detailed information about frames received.	
RX Packets	This field shows the number of good frames (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast frames received.
Broadcast	This field shows the number of good broadcast frames received.
Pause	This field shows the number of 802.3x Pause frames received.
Control	This field shows the number of control received (including those with CRC error) but it does not include the 802.3x Pause frames.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frame have already been transmitted.
Error Packet	The following fields display detailed information about frames received that were in error.
RX CRC	This field shows the number of frames received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of frames received with a length that was out of range.

Table 5-2 Status: Port Details

LABEL	DESCRIPTION
Runt	This field shows the number of frames received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	This field shows the distribution of good packets (unicast, multicast and broadcast) received.
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to stop port statistic polling.

Chapter 6 Basic Setting

*This chapter describes how to configure the **System Info, General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.*

6.1 Introducing the Basic Setting Screens

The **System Info** screen displays general switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your switch. The real time is then displayed in the switch logs. The **Switch Setup** screen allows you to set up and configure global switch features. The **IP Setup** screen allows you to configure a switch IP address, subnet mask and DNS (domain name server) for management purposes.

6.2 System Information

In the navigation panel, click **Basic Setting** and then **System Info** to display the screen as shown. You can check the firmware version number and monitor the switch temperature, fan speeds and voltage in this screen.

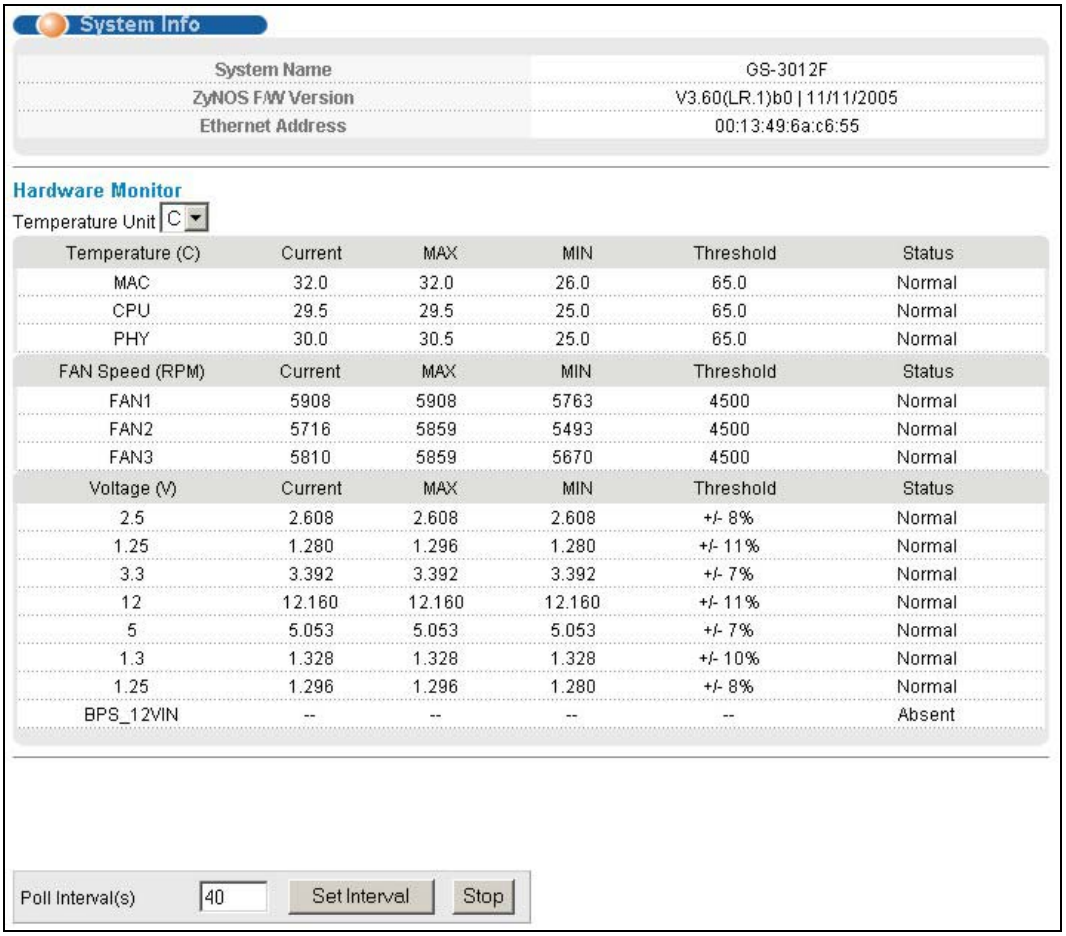


Figure 6-1 System Info

The following table describes the labels in this screen.

Table 6-1 System Info

LABEL	DESCRIPTION
System Name	This field displays the switch 's model name.
ZyNOS F/W Version	This field displays the version number of the switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the switch.
Hardware Monitor	
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**MAC**, **CPU** and **PHY** refer to the location of the temperature sensors on the switch printed circuit board.
Current	This field displays the current temperature measured at this sensor.

Table 6-1 System Info

LABEL	DESCRIPTION
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the minimum voltage at which the switch should work.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

6.3 General Setup

Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

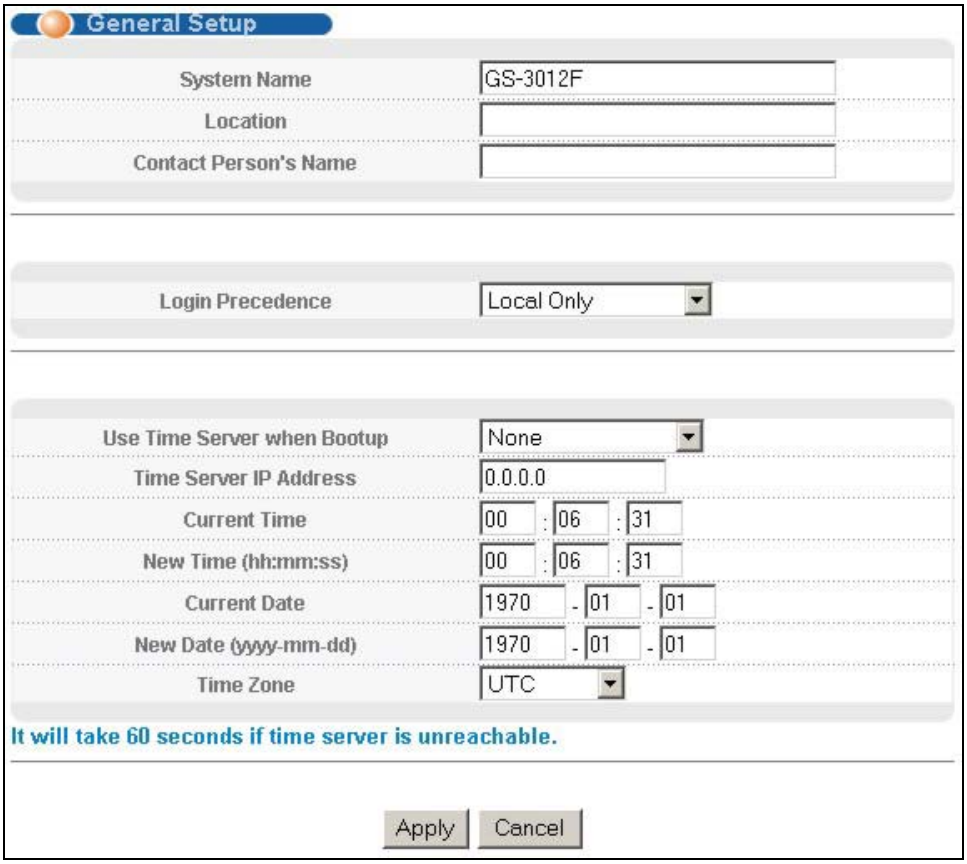


Figure 6-2 General Setup

Table 6-2 General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 32 printable characters; spaces are allowed.
Location	Enter the geographic location (up to 32 characters) of your switch.
Contact Person's Name	Enter the name (up to 32 characters) of the person in charge of this switch.

Table 6-2 General Setup

LABEL	DESCRIPTION
Login Precedence	Configure the local user accounts in the **Access Control Logins** screen. The RADIUS is an external server. Use this drop-down list box to select which database the switch should use (first) to authenticate a user. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local Only** to have the switch just check the local user accounts configured in the **Access Control Logins** screen. Select **Local then RADIUS** to have the switch check the local user accounts configured in the **Access Control Logins** screen. If the user name is not found, the switch then checks the user database on the specified RADIUS server. You need to configure the **Port Authentication Radius** screen first. Select **RADIUS Only** to have the switch just check the user database on the specified RADIUS server for a login username and password.
Use Time Server When Bootup	Enter the time service protocol that a timeserver sends when you turn on the switch. Not all timeservers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format, it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the switch, the time and date will be reset to 1970-1-1 0:0.
Time Server IP Address	Enter the IP address of your timeserver. The switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring the screen again.

6.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that VLAN is unidirectional; it only governs outgoing traffic.

See the *VLAN* chapter for information on port-based and 802.1Q tagged VLANs.

6.5 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLANs.

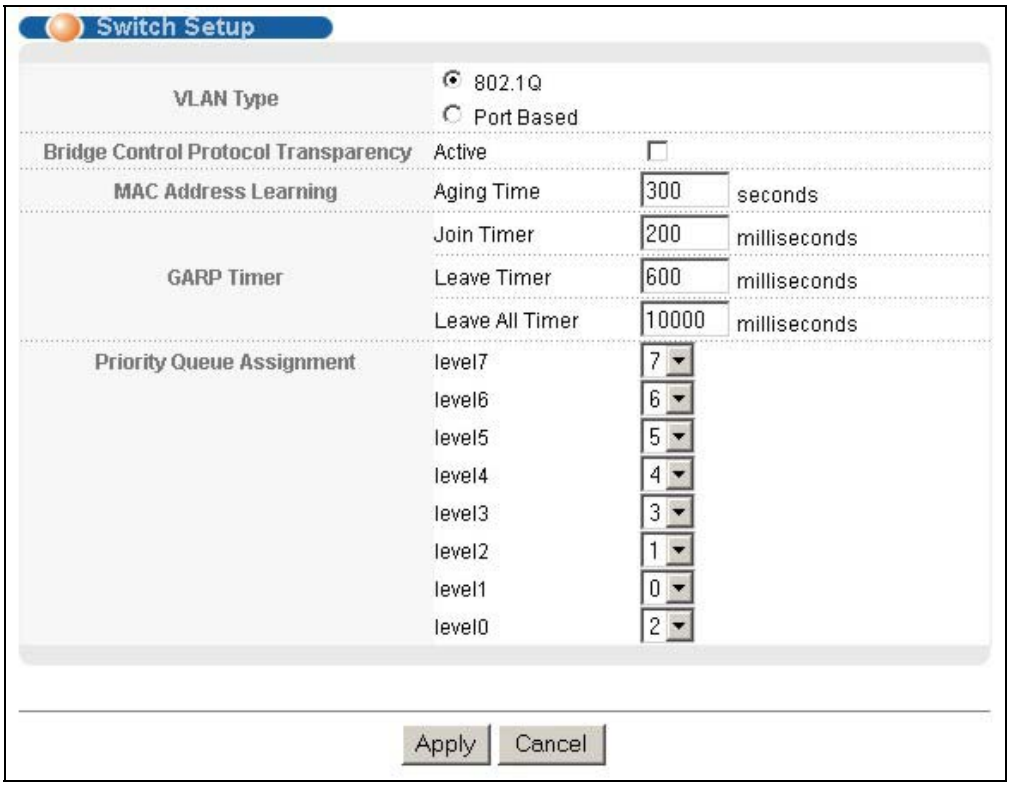


Figure 6-3 Switch Setup

The following table describes the labels in this screen.

Table 6-3 Switch Setup

LABEL	DESCRIPTION	EXAMPLE
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q VLAN Type** or **Port Based VLAN Type** in this screen. See *Section 6.4* and the *VLAN* chapter for more information on VLANs.	802.1Q
Bridge Control Protocol Transparency	Select **Active** to allow the switch to handle bridging control protocols (STP for example). You also need to define how to treat a BPDU in the **Port Setup** screen.	
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.	
Aging Time	Enter a time from 10 to 3000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).	300
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.		
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.	200 milliseconds (default)
Leave Timer	Leave Timer sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.	600 milliseconds (default)
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.	10000 milliseconds (default)
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping. The switch has eight physical queues that you can map to the eight priority levels. On the switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested. See also **Queuing Method** and **802.1p Priority** in **Port Setup** for related information.		
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).		
Level 7	Typically used for network control traffic such as router configuration messages.	
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).	
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.	

Table 6-3 Switch Setup

LABEL	DESCRIPTION	EXAMPLE
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.	
Level 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.	
Level 2	This is for "spare bandwidth".	
Level 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.	
Level 0	Typically used for best-effort traffic.	
Apply	Click **Apply** to save your changes back to the switch.	
Cancel	Click **Cancel** to begin configuring this screen afresh.	

6.6 IP Setup

Use the **IP Setup** screen to configure the switch IP address, default gateway device, the default domain name server and the management VLAN ID. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

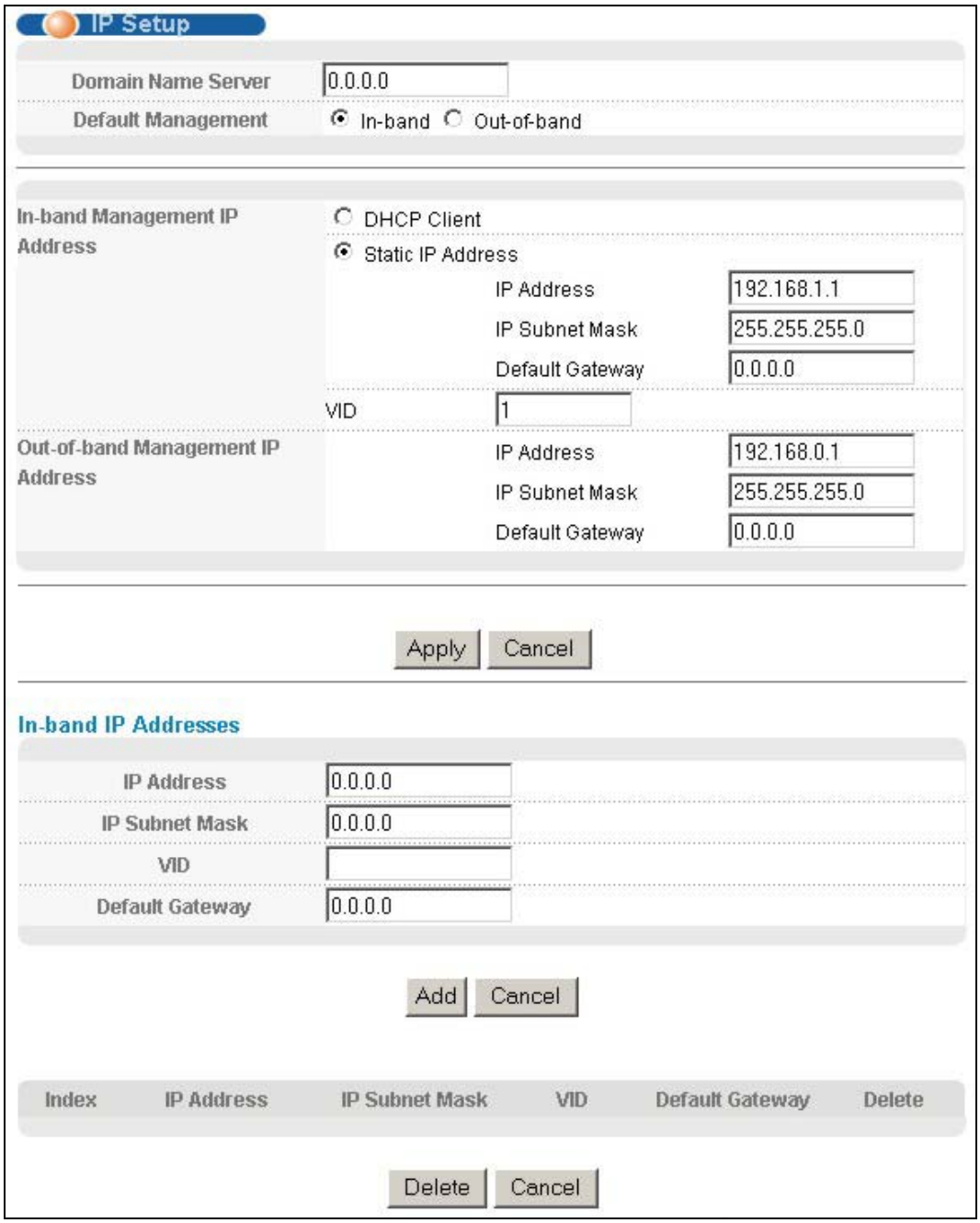


Figure 6-4 IP Setup

The following table describes the labels in this screen.

Table 6-4 IP Setup

LABEL	DESCRIPTION
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.

Table 6-4 IP Setup

LABEL	DESCRIPTION
Default Management	Select which traffic flow (**In-Band** or **Out-of-band**) the switch use to send packets with an unknown source or originate from the switch itself (such as SNMP traps). Select **Out-of-band** to have the switch send the packets to the out-of-band management port. This means that device(s) connected to the other port(s) do not receive these packets. Select **In-Band** to have the switch send the packets to all ports except the out-of-band management port. This means that device(s) connected to out-of-band management port do not receive these packets.
In-Band Management IP Address	
DHCP Client	Select this option if you have a DHCP server that can assign the switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
VID	Enter the VLAN identification number associated with the switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the switch make sure the port that you are connected to is a member of Management VLAN.
Out-of-band Management IP Address	
IP Address	Enter the IP address of the management port in dotted decimal notation for example 192.168.0.1. If you change this IP address, make sure the computer connected to this management port is in the same subnet before accessing the GS.
Subnet Mask	Enter the IP subnet mask in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring the fields again.
In-band IP Addresses You can create up to 128 IP addresses, which are used to access and manage the switch from the ports belonging to the pre-defined VLAN(s). You must configure a VLAN first.	
IP Address	Enter the IP address for managing the switch by the members of the VLAN specified in the **VID** field below.

Table 6-4 IP Setup

LABEL	DESCRIPTION
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation.
VID	Type the VLAN group identification number.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This field displays the index number of the rule. Click an index number to edit the rule.
IP Address	This field displays the IP address.
IP Subnet Mask	This field displays the subnet mask.
VID	This field displays the ID number of the VLAN group.
Default Gateway	This field displays the IP address of the default gateway.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

6.7 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to enter the port configuration screen.

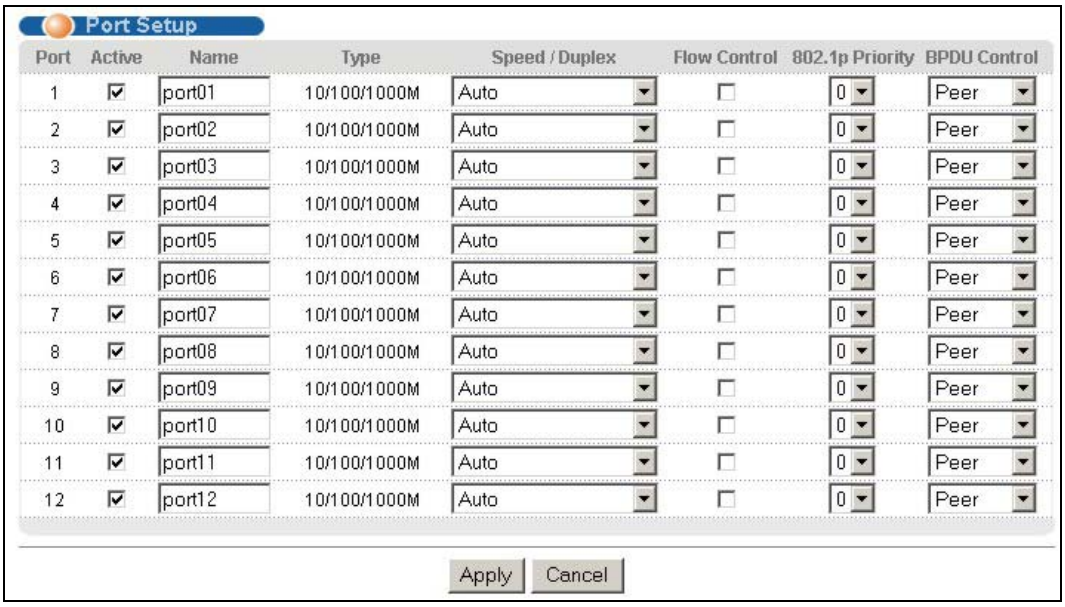


Figure 6-5 Port Setup

The following table describes the fields in this screen.

Table 6-5 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Enter a descriptive name that identifies this port.
Type	This field displays **10/100/1000M** for this connection.
Speed/Duplex	Select the speed and the duplex mode of the connection on this port. For mini GBIC slots, select **Auto** or **1000M/Full Duplex**. For mini Gigabit Ethernet or GBIC/Gigabit Ethernet combo ports, select **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **100M/Full Duplex** or **1000M/Full Duplex.** Selecting **Auto** (auto-negotiation) makes one Gigabit port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a Gigabit port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer Ethernet port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a Gigabit port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer Ethernet port are the same in order to connect.

Table 6-5 Port Setup

LABEL	DESCRIPTION
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select this option to enable flow control.
802.1P Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in *Table 6-3* for more information. See also **Priority Queue Assignment** in **Switch Setup** and **Queuing Method** for related information.
BPDU Control	Configure the way to treat BPDUs received on this port. **You must activate bridging control protocol transparency in the** Switch Setup **screen first.** Select **Peer** to process any BPDU (Bridge Protocol Data Units) received on this port. Select **Tunnel** to forward BPDUs received on this port. Select **Discard** to drop any BPDU received on this port. Select **Network** to process a BPDU with no VLAN tag and forward a tagged BPDU.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Part IV

Advanced Application 1

This part shows you how to configure the VLAN, Static MAC Forwarding, Filtering, STP and Bandwidth Control Advanced Application screens.

Chapter 7 VLAN

*The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs. See the General, Switch and IP Setup chapter for more information.*

7.1 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (212) VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

7.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

7.1.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

Please refer to the following table for common GARP terminology.

Table 7-1 GARP Terminology

VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

7.1.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

Refer to the following figure. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking,** you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

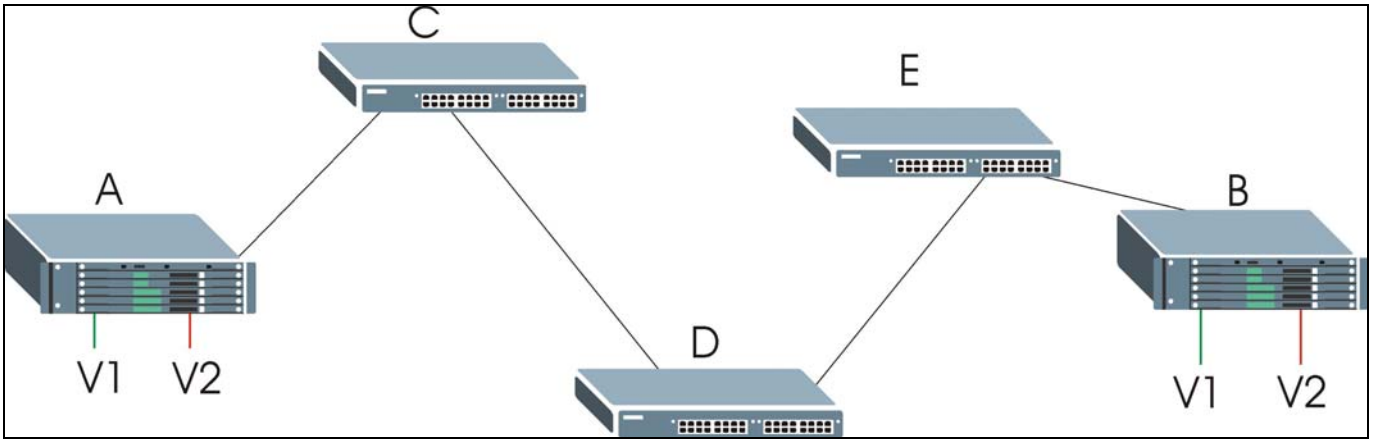


Figure 7-1 Port VLAN Trunking

7.2 802.1Q VLAN

Follow the steps below to set the **802.1Q VLAN Type** on the switch.

1. Select **802.1Q** as the **VLAN Type** in the **Switch Setup** screen (under **Basic Setting**) and click **Apply**.

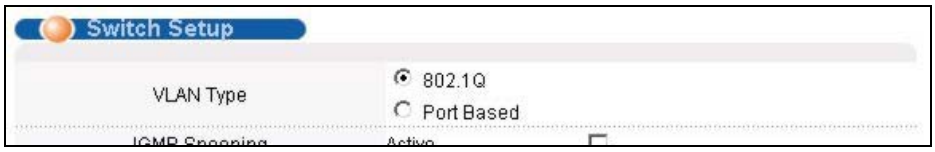


Figure 7-2 Selecting a VLAN Type

2. Click **VLAN** under **Advanced Application** to display the **VLAN Status** screen as shown next.

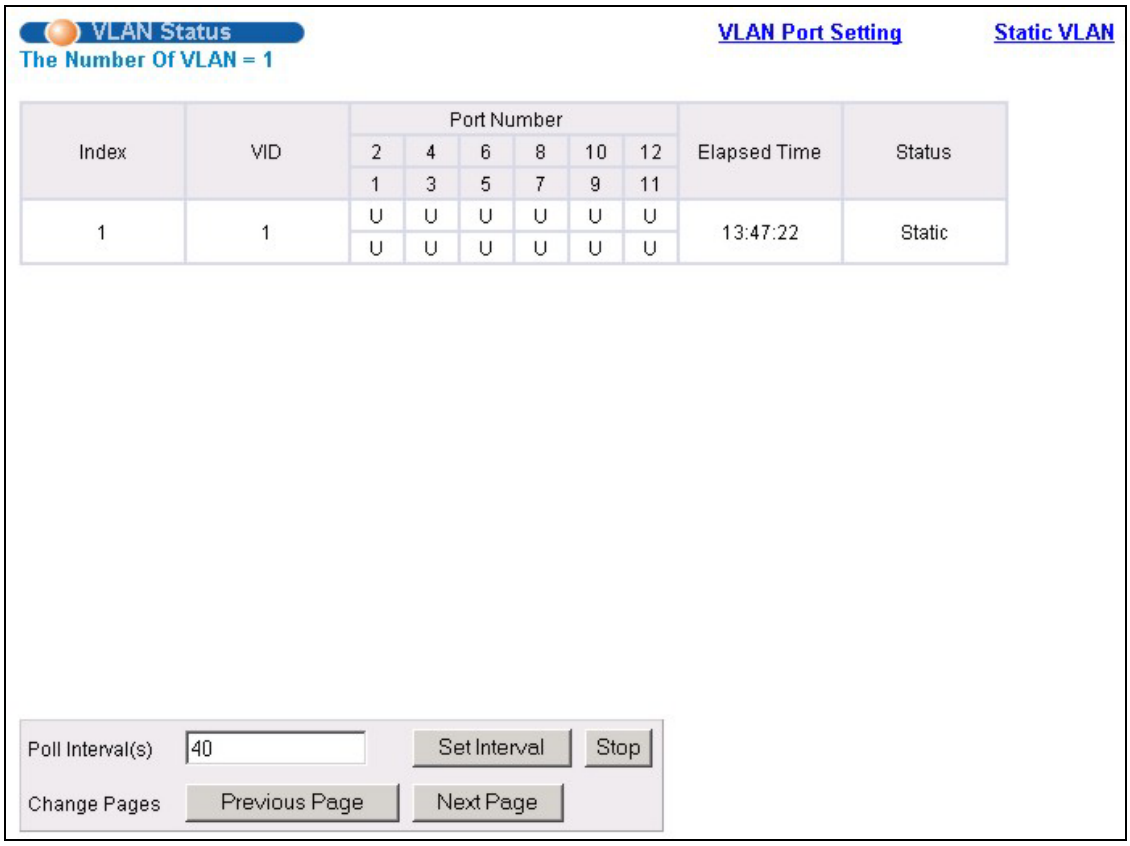


Figure 7-3 802.1Q VLAN Status

The following table describes the labels in this screen.

Table 7-2 802.1Q VLAN Status

LABEL	DESCRIPTION
The Number of VLAN	This is the number of VLANs configured on the switch.
Index	This is the VLAN index number.
VID	VID is the PVID, the Port VLAN ID assigned to untagged frames or priority-tagged frames received on this port that you configure in the **VLAN Port Setting** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN in marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the switch; dynamically using GVRP or statically, that is, added as a permanent entry.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.

Table 7-2 802.1Q VLAN Status

LABEL	DESCRIPTION
Previous/Next Page	Click one of these buttons to show the previous/next screen if all status information cannot be seen in one screen.

7.2.1 802.1Q VLAN Port Settings

To configure the 802.1Q VLAN settings on a port, click the **VLAN Port Settings** link in the **VLAN Status** screen.

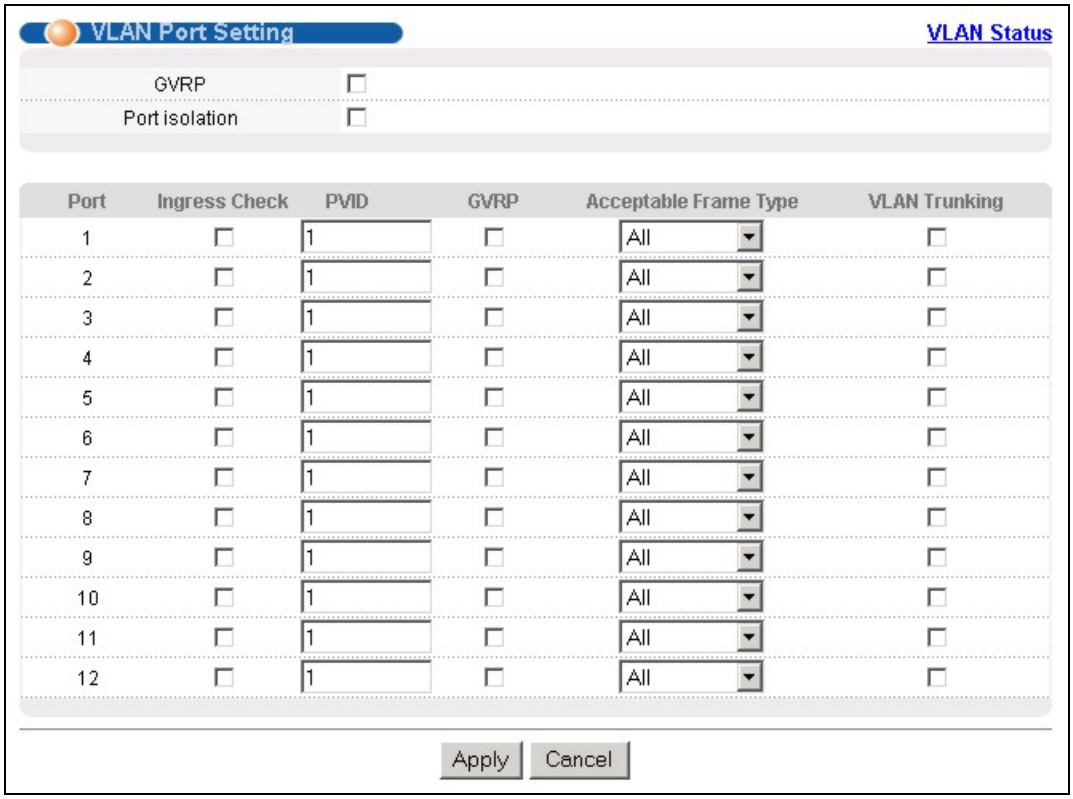


Figure 7-4 802.1Q VLAN Port Settings

The following table describes the labels in this screen.

Table 7-3 802.1Q VLAN Port Settings

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to dynamically register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local switch.
Port Isolation	**Port Isolation** allows interfaces 1 to 8 to communicate with the CPU port (in-band switch management) and interfaces 9 to 12. Interfaces 1 to 8 are isolated and cannot communicate with each other. However, interfaces 9 to 12 and the CPU port can communicate with all ports. This option is the most limiting but also the most secure.
Port	This field displays the port numbers.

Table 7-3 802.1Q VLAN Port Settings

LABEL	DESCRIPTION
Ingress Check	If this check box is selected for a port, the device discards incoming frames for VLANs that do not include this port in its member set.
PVID	Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the default ingress port's VLAN ID, the PVID. The default PVID is VLAN 1 for all ports, but this can be changed to any number between 0 and 4094.
GVRP	Select this check box to permit VLANs groups beyond the local switch on this port. GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All** and **Tag Only**. Select **All** to accept all frames with untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames are dropped.
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring the screen again.

7.2.2 802.1Q Static VLAN

You can dynamically have a port join a VLAN group using GVRP, permanently assign a port to be a member of a VLAN group or prohibit a port from joining a VLAN group in this screen. Click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

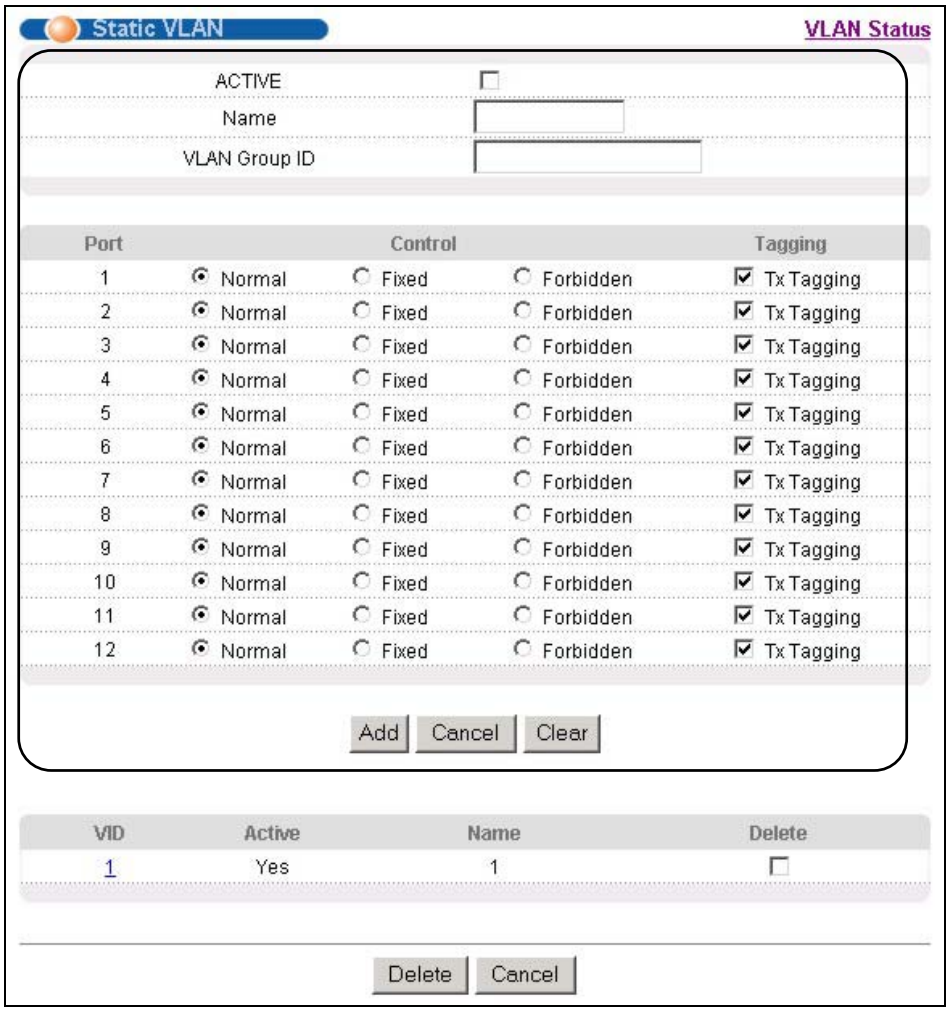


Figure 7-5 802.1Q Static VLAN

The following table describes the labels in this screen.

Table 7-4 802.1Q Static VLAN

LABEL	DESCRIPTION
Active	Select this check box to enable the VLAN.
Name	Enter a descriptive name for this VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static VLAN entry; the valid range is between 1 and 4094.
Port	The port number identifies the port you are configuring.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.

Table 7-4 802.1Q Static VLAN

LABEL	DESCRIPTION
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

7.2.3 Viewing and Editing VLAN Settings

To view a summary of the VLAN configuration, scroll down to the summary table at the bottom of the **Static VLAN** screen.

To change the settings of a rule, click a number in the **VID** field.

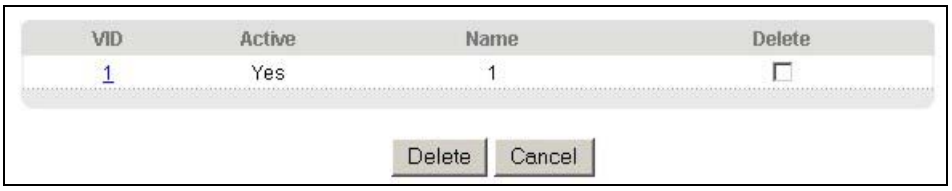


Figure 7-6 Static VLAN: Summary Table

The following table describes the labels in this screen.

Table 7-5 Static VLAN: Summary Table

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

VID1 Example Screen

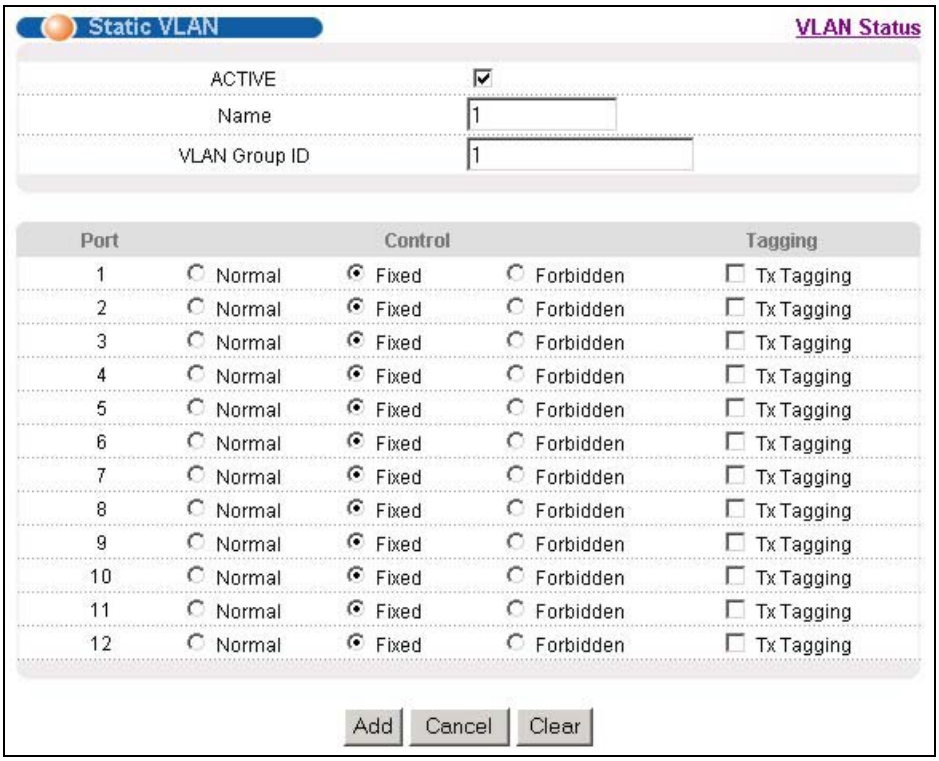


Figure 7-7 VID 1 Example Screen

7.3 Introduction to Port-based VLANs

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the switch on which they were created.

The port-based VLAN setup screen is shown next. The **CPU** port (for in-band switch management) forms a VLAN with all Gigabit ports.

7.3.1 Configuring a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen under **Basic Setting** and then click **VLAN** under **Advanced Application** to display the next screen.

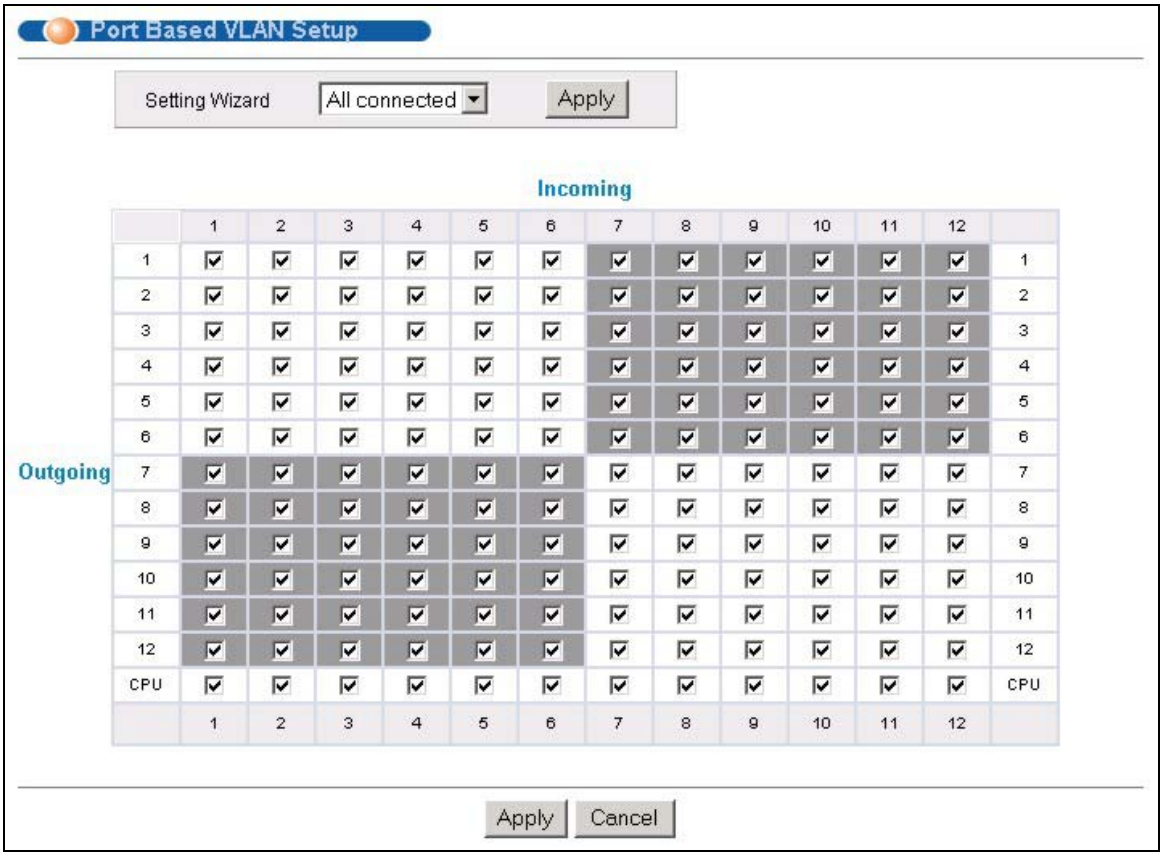


Figure 7-8 Port Based VLAN Setup (All Connected)

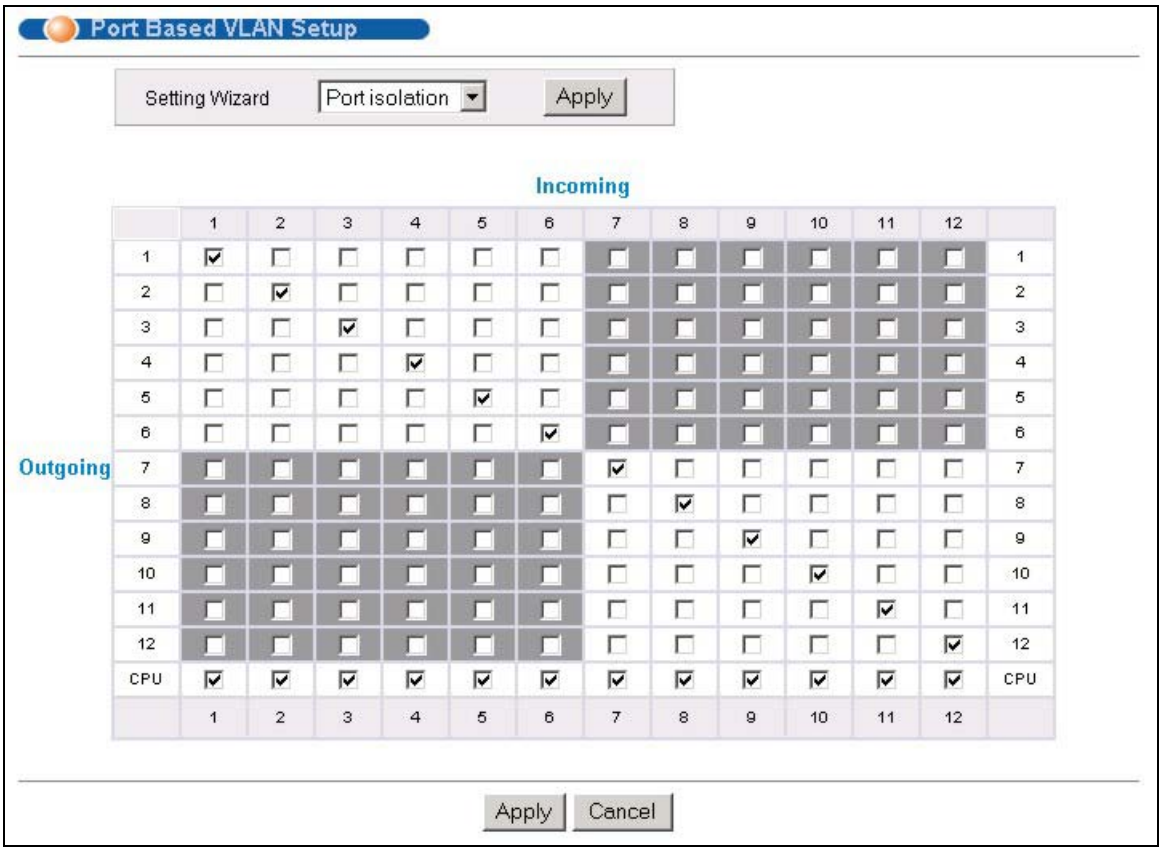


Figure 7-9 Port Based VLAN Setup (Port isolation)

The following table describes the labels in this screen.

Table 7-6 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose from **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected (*Figure 7-8*). This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU port (which is for in-band switch management) and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected (*Figure 7-9*). This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the in-band switch management port. By default it forms a VLAN with all Gigabit ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.

Table 7-6 Port Based VLAN Setup

LABEL	DESCRIPTION
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the in-band switch management port. By default it forms a VLAN with all Gigabit ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
Apply	Click **Apply** to save the changes, including the "wizard settings".
Cancel	Click **Cancel** to start configuring the screen again.

Chapter 8
Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

8.1 Introduction to Static MAC Forward Setup

A static MAC address entry is an address that has been manually entered in the MAC address learning table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. Devices that match static MAC address rules on a port can *only* receive traffic on that port and cannot receive traffic on other ports. This may reduce unicast flooding.

8.2 Configuring Static MAC Forwarding

Click **Static MAC Forwarding** to display the configuration screen as shown.

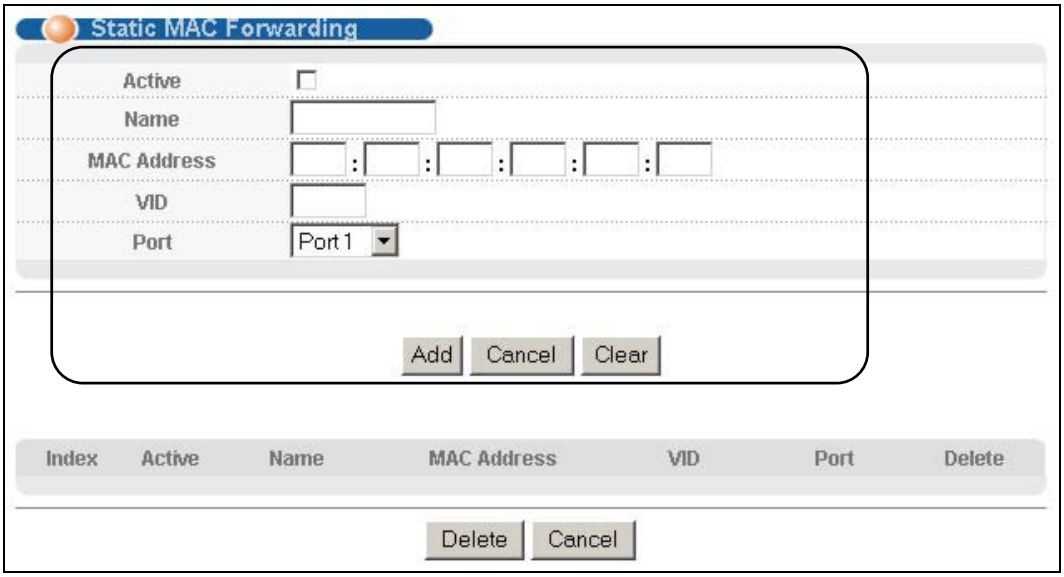


Figure 8-1 Static MAC Forwarding

The following table describes the labels in this screen.

Table 8-1 Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Static MAC addresses do not age out.
VID	Enter the VLAN identification number.

Table 8-1 Static MAC Forwarding

LABEL	DESCRIPTION
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

8.3 Viewing and Editing Static MAC Forwarding Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Static MAC Forwarding** screen.

To change the settings of a rule, click a number in the **Index** field.

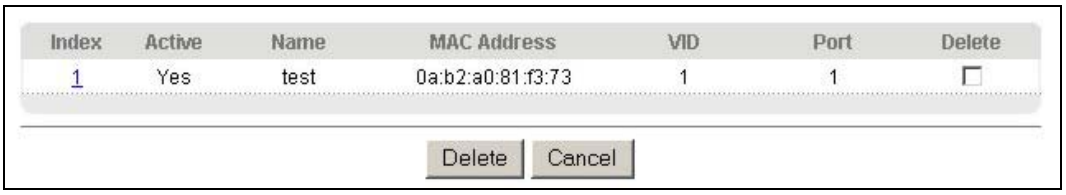


Figure 8-2 Static MAC Forwarding: Summary Table

The following table describes the labels in this screen.

Table 8-2 Static MAC Forwarding: Summary Table

LABEL	DESCRIPTION
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded.
VID	This field displays the VLAN identification number to which the MAC address belongs.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

Chapter 9 Filtering

This chapter discusses static IP and MAC address port filtering.

9.1 Introduction to Filtering

Filtering means sifting traffic going through the switch based on the source and/or destination MAC addresses and VLAN group (ID).

9.2 Configuring a Filtering Rule

Click **Advanced Application** and **Filtering** to display the screen as shown next.

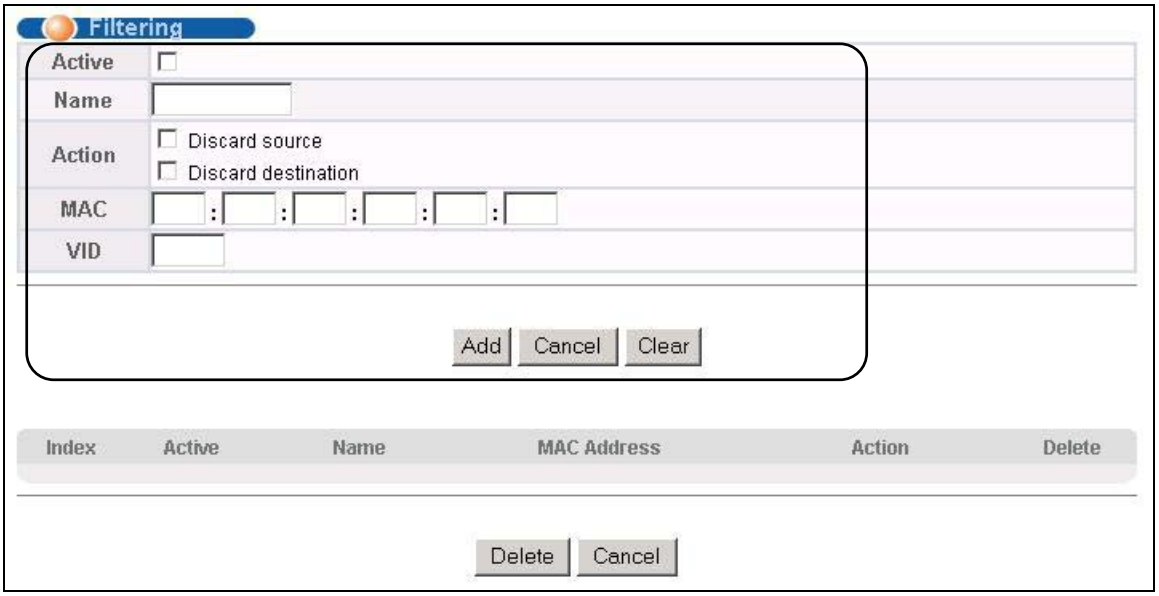


Figure 9-1 Filtering

The following table describes the related labels in this screen.

Table 9-1 Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name for this filter rule. This is for identification purpose only.

Table 9-1 Filtering

LABEL	DESCRIPTION
Action	Select **Discard source** to drop frame from the source MAC address (specified in the **MAC** field). The switch can still send frames to the MAC address. Select **Discard destination** to drop frames to the destination MAC address (specified in the **MAC** address). The switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

9.3 Viewing and Editing Filter Rules

To view a summary of the rule configuration, scroll down to the summary table at the bottom of the **Filtering** screen.

To change the settings of a rule, click a number in the **Index** field.

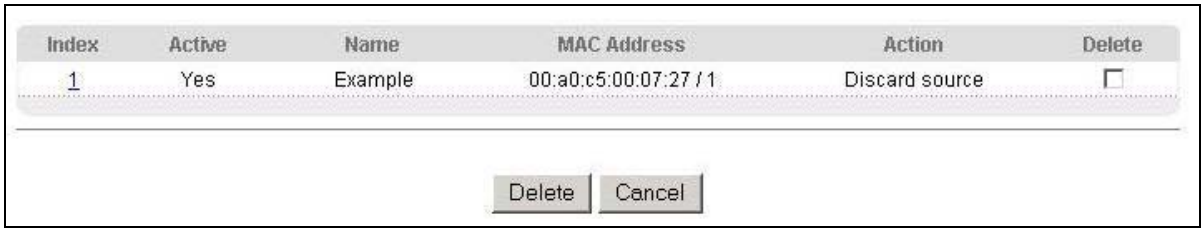


Figure 9-2 Filtering: Summary Table

The following table describes the labels in the summary table.

Table 9-2 Filtering: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.

Table 9-2 Filtering: Summary Table

LABEL	DESCRIPTION
Action	This field displays the filter action.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

Chapter 10
Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

10.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a switch to interact with other (R)STP -compliant switches in your network to ensure that only one path exists between any two stations on the network.

The switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge that then notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

In this user's guide, "STP" often refers to both STP and RSTP.

10.1.1 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

Table 10-1 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

10.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

In RSTP, the devices send BPDUs every Hello Time. If an RSTP-aware device does not get a Hello BPDU after three Hello Times pass (or the Max Age), the device assumes that the link to the neighboring bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

In STP, once a stable network topology has been established, all devices listen for Hello BPDUs transmitted from the root bridge. If an STP-aware device does not get a Hello BPDU after a predefined interval (Max Age), the device assumes that the link to the root bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

RSTP assigns three port states to eliminate packet looping while STP assigns five (see following table). A device port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 10-2 RSTP and STP Port States

RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Discarding	Disabled	RSTP or STP is disabled (default).
Discarding	Blocking	In RSTP, BPDUs are discarded. In STP, only configuration and management BPDUs are received and processed.
Discarding	Listening	In RSTP, BPDUs are discarded. In STP, all BPDUs are received and processed.
Learning	Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

See the IEEE 802.1w standard for more information on RSTP. See the IEEE 802.1D standard for more information on STP.

10.2 STP Status

Click **Advanced Application** and then **Spanning Tree Protocol** in the navigation panel to display the STP status as shown in the screen next.

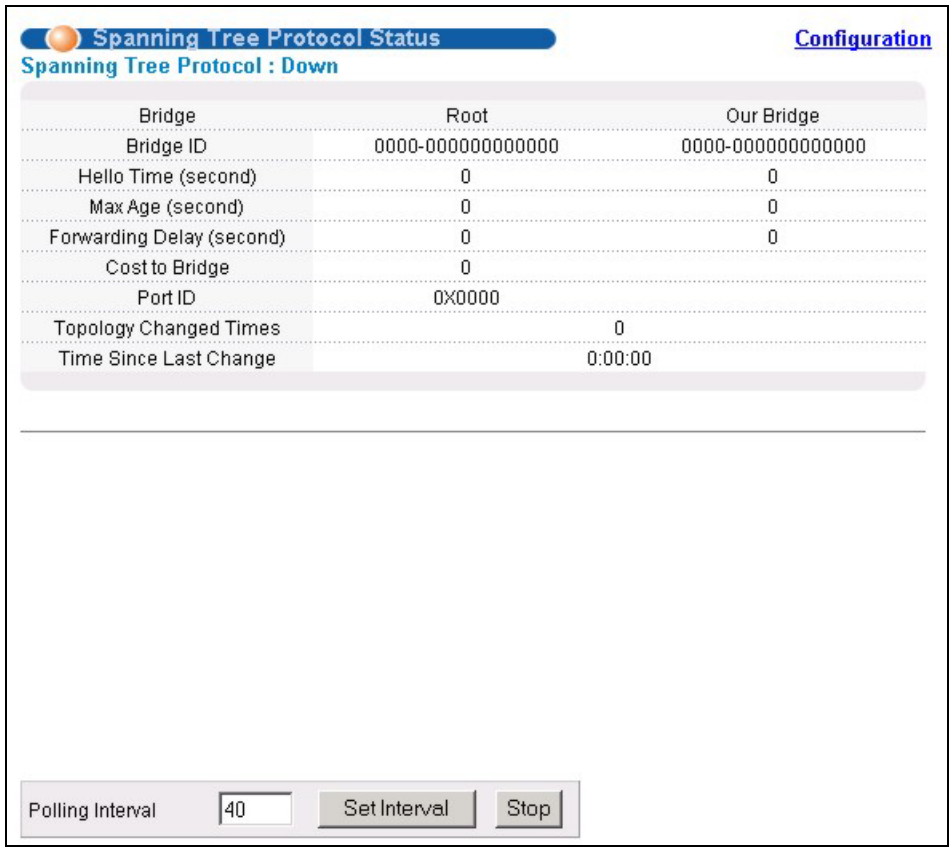


Figure 10-1 Spanning Tree Protocol: Status

The following table describes the labels in this screen.

Table 10-3 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays **Running** if STP is activated. Otherwise, it displays **Down**.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this switch. This switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time, Max Age** and **Forwarding Delay**
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this switch to the root switch.

Table 10-3 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt STP statistic polling.

10.2.1 Configuring STP

To configure STP, click the **Configuration** link in the **Spanning Tree Protocol** screen as shown next.

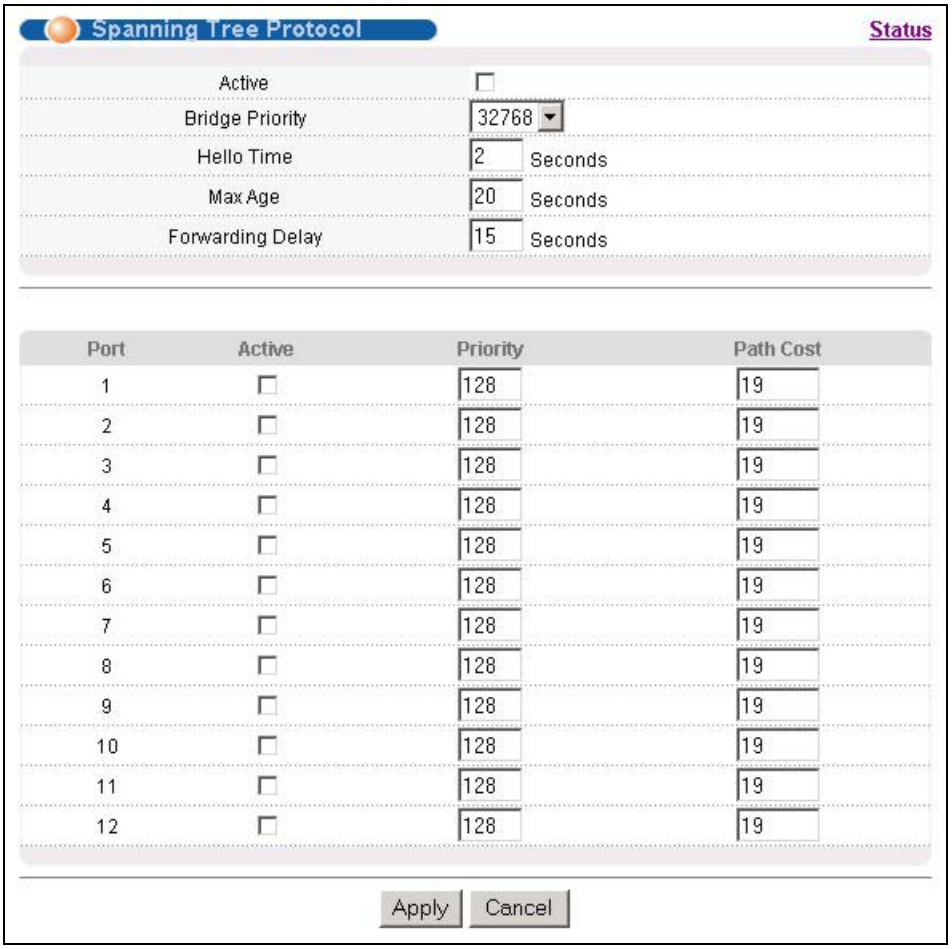


Figure 10-2 Spanning Tree Protocol: Configuration

The following table describes the labels in this screen.

Table 10-4 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Active	Select this check box to activate STP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. The allowed range is 0 to 61440. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: **2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)**
Port	This field displays the port number.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost - see *Table 10-1* for more information.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 11 Bandwidth Control

This chapter shows you how you can set the maximum bandwidth allowed for traffic flows on a port using the Bandwidth Control setup screens.

11.1 Introduction to Bandwidth Control

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

11.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

The CIR should be less than the PIR.

The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

11.1.2 Bandwidth Control Setup

Click **Advanced Application** and then **Bandwidth Control** in the navigation panel to bring up the screen as shown next.

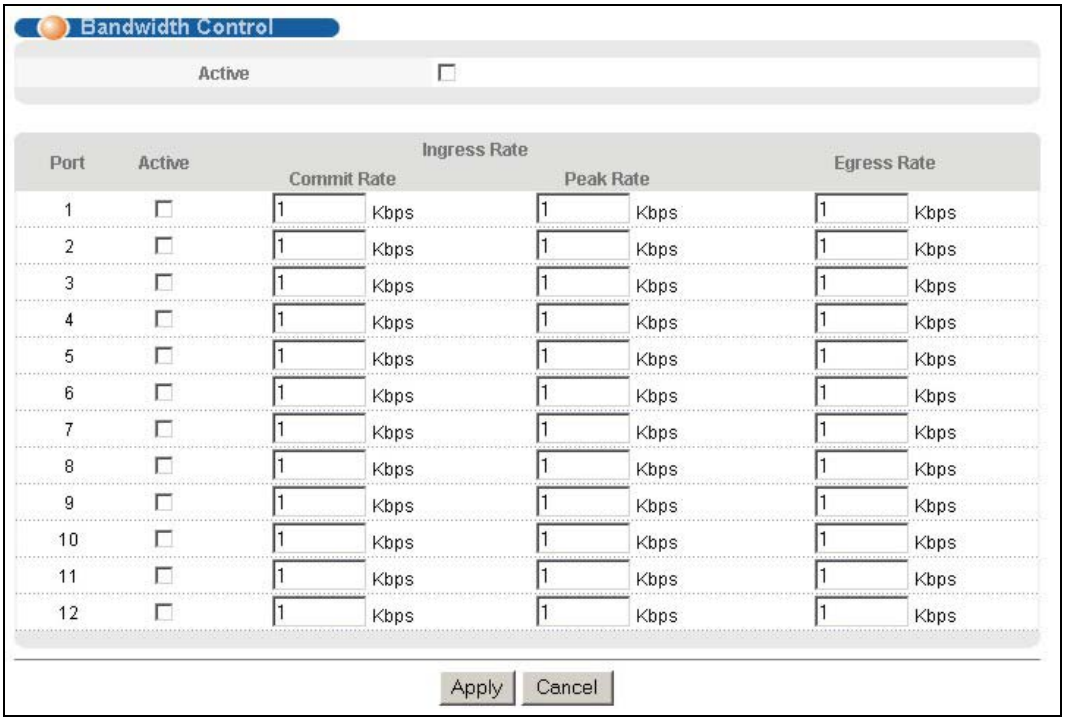


Figure 11-1 Bandwidth Control

The following table describes the labels in this screen.

Table 11-1 Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to activate bandwidth control.
Port	This field displays the port number.
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Egress Rate	Specify the maximum bandwidth allowed in megabits per second (Kbps) for the out-going traffic flow on a port. Enter a number between 1 and 1000.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

Part V

Advanced Application 2

This part shows you how to configure the Broadcast Storm Control, Mirroring, Link Aggregation, Port Authentication, Port Security, Queuing Method, Classifier, Policy Rule and Multicast Advanced Application screens.

Chapter 12
Broadcast Storm Control

12.1 Introducing Broadcast Storm Control

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

12.2 Configuring Broadcast Storm Control

Click **Advanced Application**, **Broadcast Strom Control** in the navigation panel to display the screen as shown next.

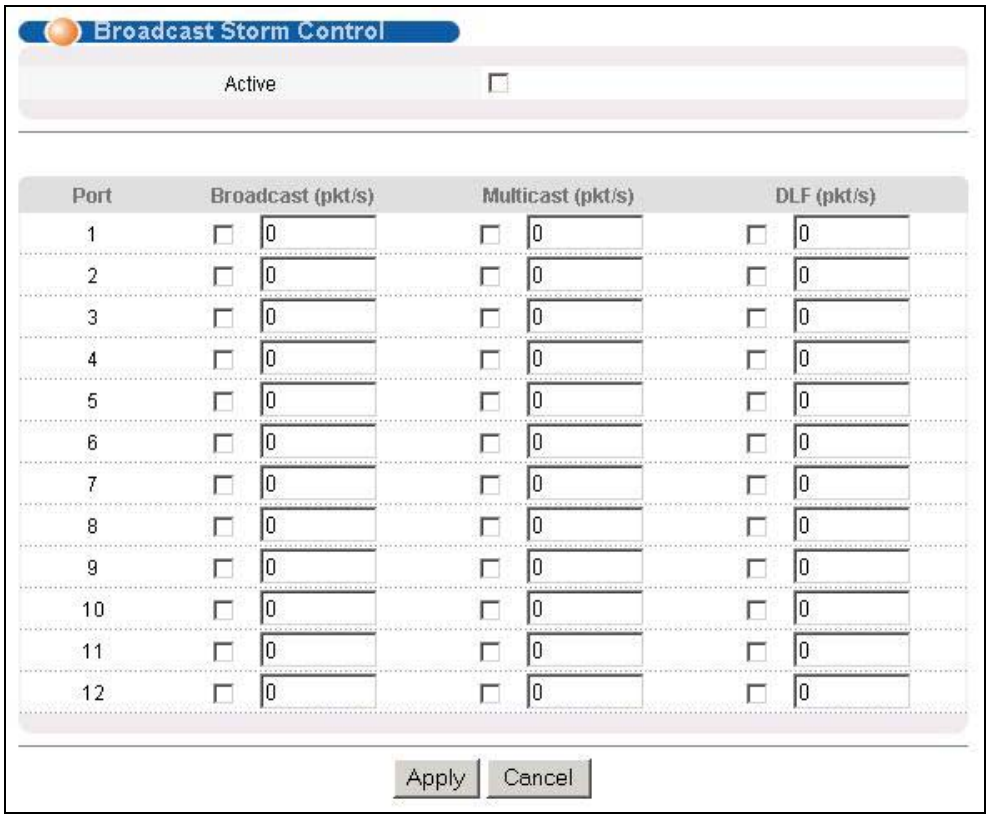


Figure 12-1 Broadcast Storm Control

The following table describes the labels in this screen.

Table 12-1 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control on the switch.
Port	This field displays a port number.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 13 Mirroring

This chapter discusses the Mirror setup screens.

13.1 Introduction to Port Mirroring

Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the monitor port (the port you copy the traffic to) without interference.

13.2 Port Mirroring Configuration

Click **Advanced Application**, **Mirroring** in the navigation panel to display the **Mirroring** screen.

You must first select a monitor port. A monitor port is a port that copies the traffic of another port. After you select a monitor port, configure a mirroring rule in the related fields.

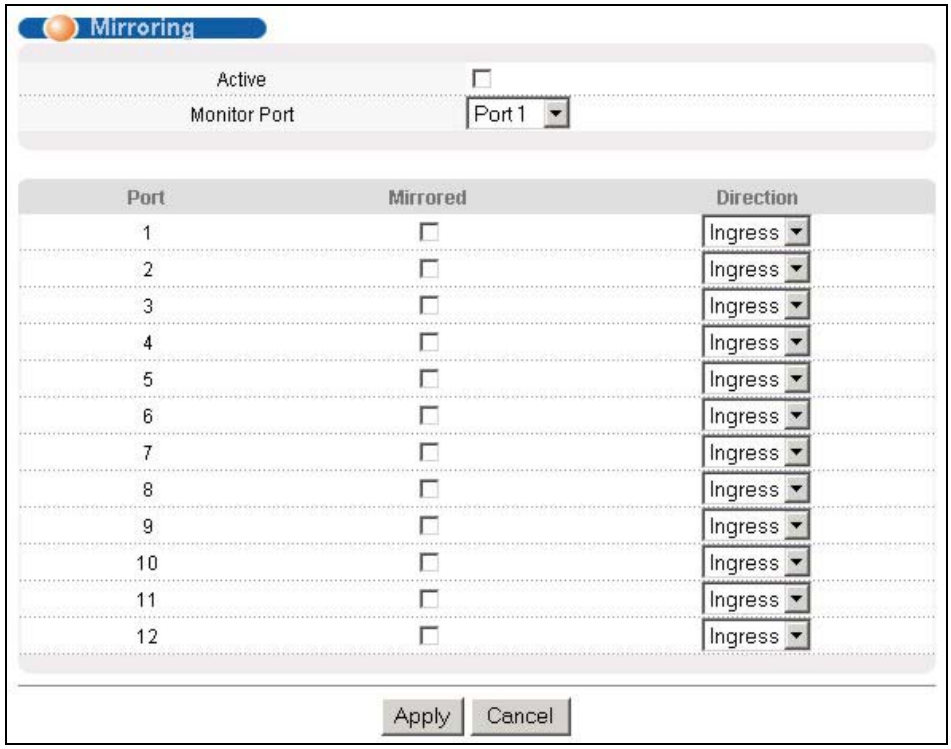


Figure 13-1 Mirroring

The following table describes the related labels in this screen.

Table 13-1 Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
Port	This field displays the port number.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields.

Chapter 14
Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

14.1 Introduction to Link Aggregation

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. Link aggregation also allows port redundancy, that is, if a port fails, the traffic automatically goes through another trunk group member port.

However, the more ports you aggregate then the fewer available ports you have. A link aggregation group is one logical link containing multiple ports.

14.1.1 Dynamic Link Aggregation

The switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The switch supports the link aggregation IEEE 802.3ad standard. This standard describes the Link Aggregate Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups.

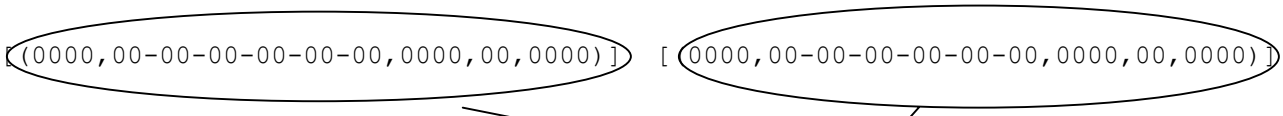
Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

14.1.2 Link Aggregation ID

LACP aggregation ID consists of the following information:



Local switch				
0000	00-00-00-00-00	0000	00	0000
System priority	Local switch MAC address	Key	Port Priority[1]	Port Number[1]

Peer switch				
0000	00-00-00-00-00	0000	00	0000
System priority	MAC address	Key	Port Priority[1]	Port Number[1]

Figure 14-1 Aggregation ID

14.2 Link Aggregation Protocol Status

Click **Advanced Application**, **Link Aggregation** in the navigation panel to display the **Link Aggregation Protocol Status** screen.

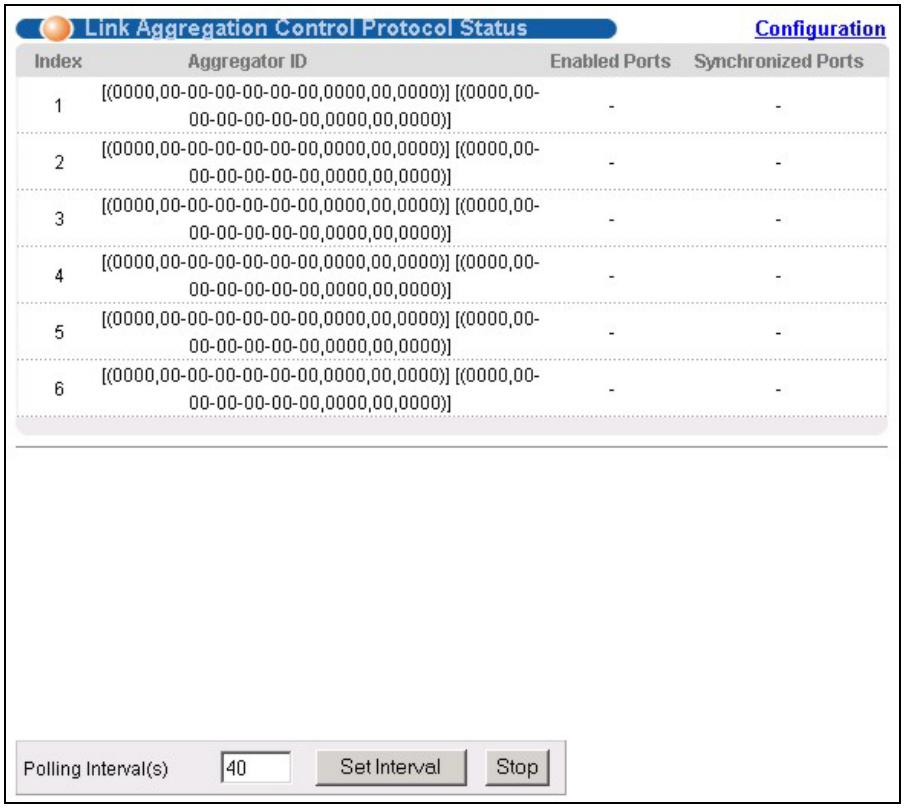


Figure 14-2 Link Aggregation: Link Aggregation Protocol Status

[1] This is "0" as it is the aggregator ID for the link aggregation group, not the individual port.

The following table describes the labels in this screen.

Table 14-1 Link Aggregation: Link Aggregation Protocol Status

LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	Refer to *Figure 14-1* for more information on this field.
Enabled Port	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

14.3 Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Protocol Status** screen to display the screen shown next.

You can configure up to six link aggregation groups and each group can aggregate up to six ports.

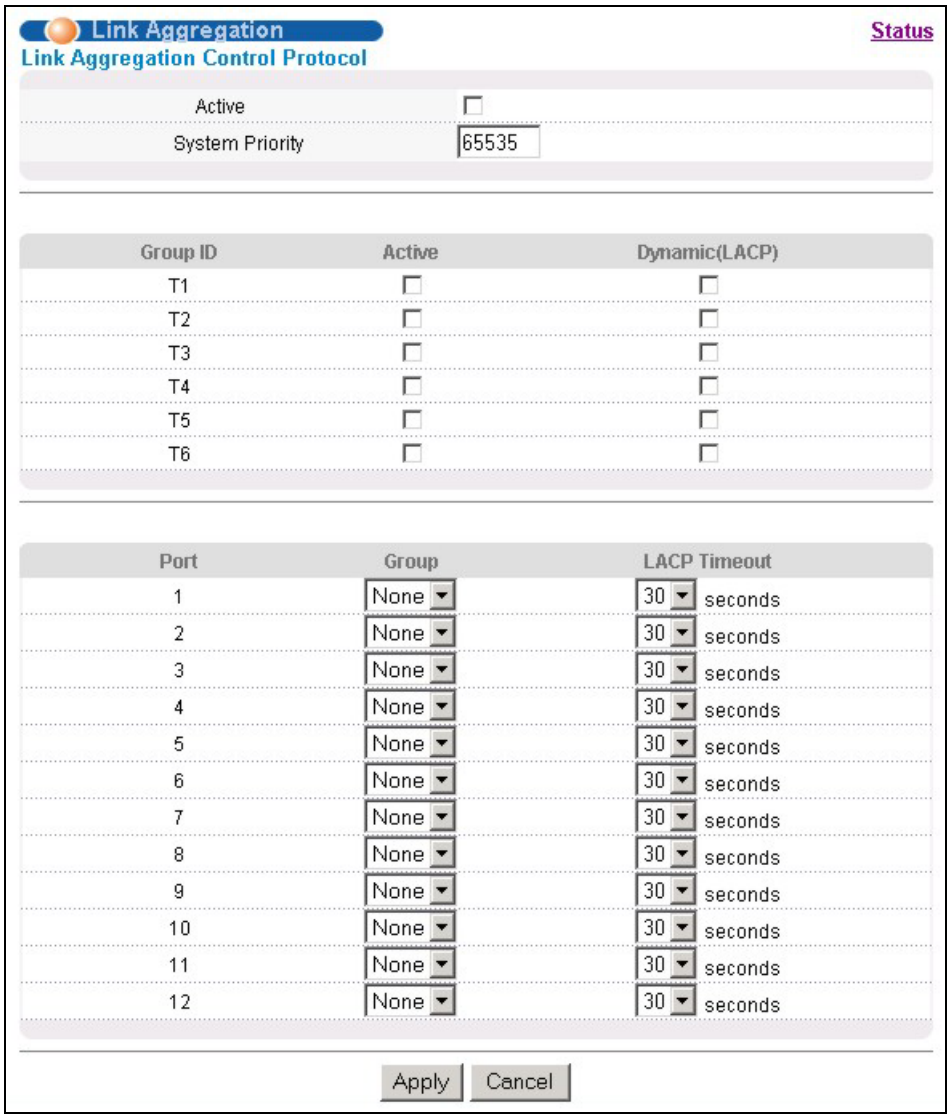


Figure 14-3 Link Aggregation: Configuration

The following table describes the labels in this screen.

Table 14-2 Link Aggregation: Configuration

LABEL	DESCRIPTION
Link Aggregation Control Protocol	
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65, 535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregate Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports
Active	Select this option to activate a trunk group.

Table 14-2 Link Aggregation: Configuration

LABEL	DESCRIPTION
Dynamic (LACP)	Select this check box to enable LACP for a trunk.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 15
Port Authentication

This chapter describes the IEEE 802.1x authentication method and RADIUS server connection setup.

15.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol[2] that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

15.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

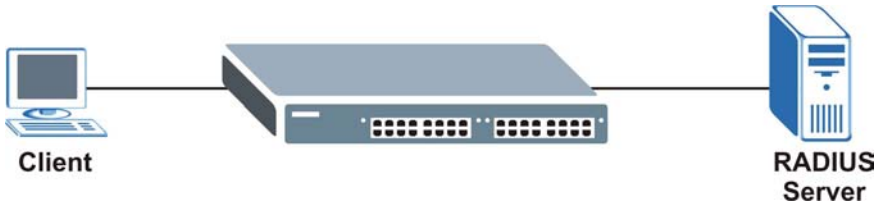


Figure 15-1 RADIUS Server

15.2 Configuring Port Authentication

To enable port authentication, first activate IEEE 802.1x security (both on the switch and the port(s)) then configure the RADIUS server settings.

Click **Port Authentication** under **Advanced Application** in the navigation panel to display the screen as shown.

Figure 15-2 Port Authentication

[2] At the time of writing, Windows XP of the Microsoft operating systems supports IEEE 802.1x. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support IEEE 802.1x, then you may need to install 802.1x client software.

15.2.1 Configuring RADIUS Server Settings

From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown.

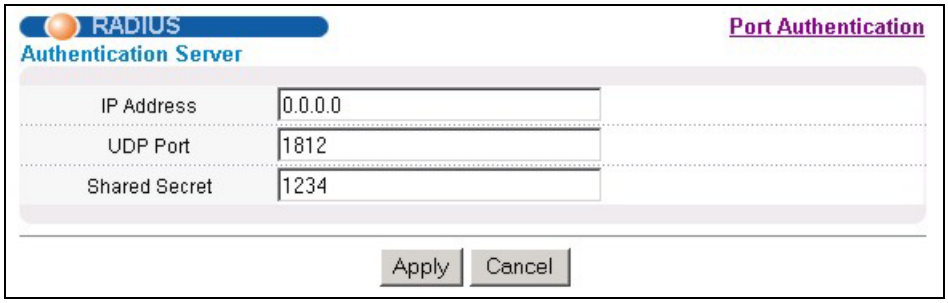


Figure 15-3 Port Authentication: RADIUS

The following table describes the labels in this screen.

Table 15-1 Port Authentication: RADIUS

LABEL	DESCRIPTION
Authentication Server	
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.2.2 Configuring IEEE 802.1x

From the **Port Authentication** screen, click **802.1x** to display the configuration screen as shown.

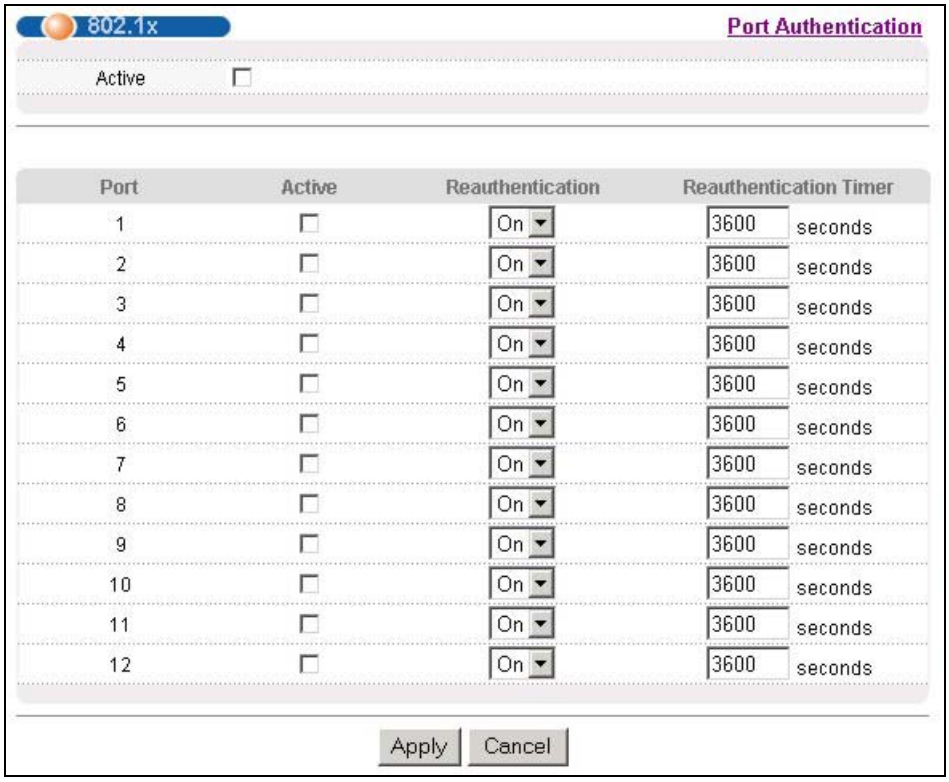


Figure 15-4 Port Authentication: 802.1x

The following table describes the labels in this screen.

Table 15-2 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit IEEE 802.1x authentication on the switch.
	You must first allow IEEE 802.1x authentication on the switch before configuring it on each port.
Port	This field displays a port number.
Active	Select this checkbox to permit IEEE 802.1x authentication on this port. You must first allow IEEE 802.1x authentication on the switch before configuring it on each port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Timer	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 16
Port Security

This chapter shows you how to set up port security.

16.1 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable **Port Security** together with MAC address learning as this will result in many broadcasts.

16.2 Port Security Setup

Click **Advanced Application**, **Port Security** in the navigation panel to display the screen as shown.

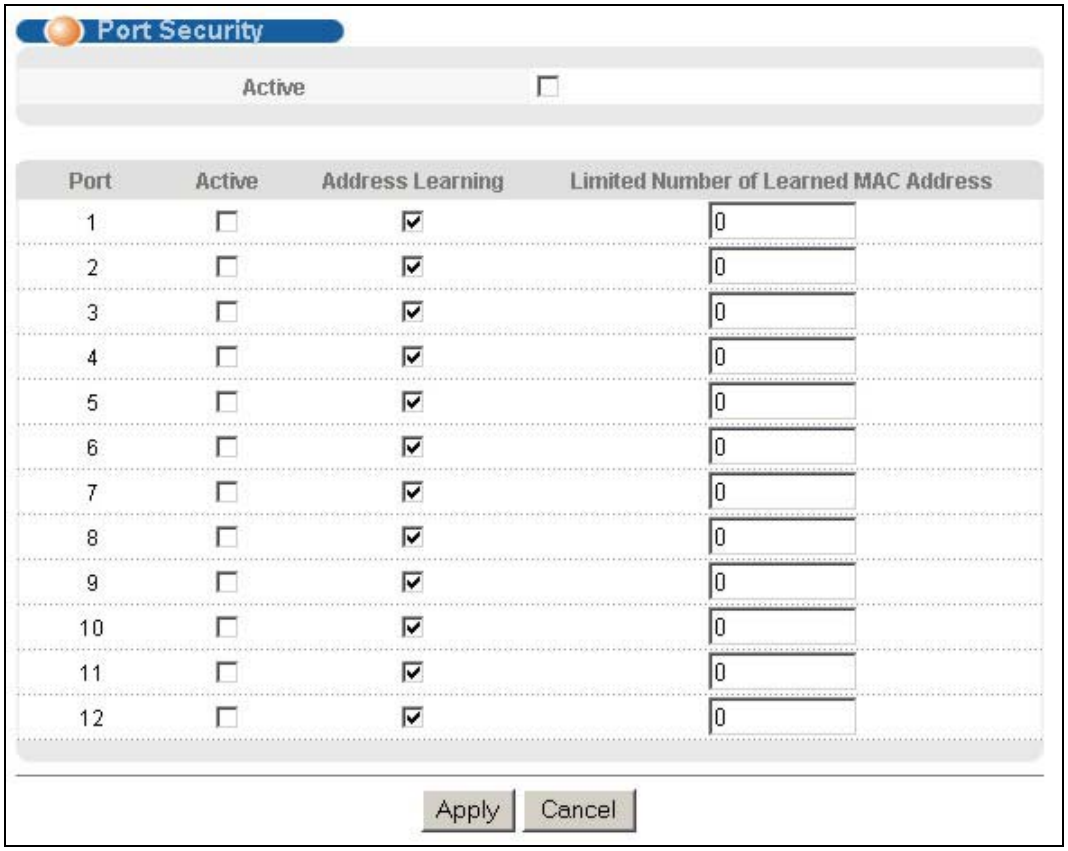


Figure 16-1 Port Security

The following table describes the labels in this screen.

Table 16-1 Port Security

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature.
Port	This field displays a port number.
Active	Select this check box to enable port security on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC-address aging out time can be set in the **Switch Setup** screen. The valid range is from 0 to 16K. The switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K. 0 means this feature is disabled, so the switch will learn MAC addresses up to the global limit of 16K.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 17 Queuing Method

This chapter introduces SPQ and WFQ.

17.1 Introduction to Queuing

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

The switch has eight physical queues, Q0 to Q7. Q7 has the highest priority and Q0 has the lowest.

Table 17-1 Physical Queue Priority

QUEUE	PRIORITY
Q7	8 (highest)
Q6	7
Q5	6
Q4	5
Q3	4
Q2	3
Q1	2
Q0	1 (lowest)

17.1.1 Strict Priority Queuing (SPQ)

Strict Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SPQ does not automatically adapt to changing network requirements.

17.1.2 Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the

end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the **Weight** field – see *Figure 17-1*) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

17.2 Configuring Queuing

Click **Queuing Method** under **Advanced Application** in the navigation panel.

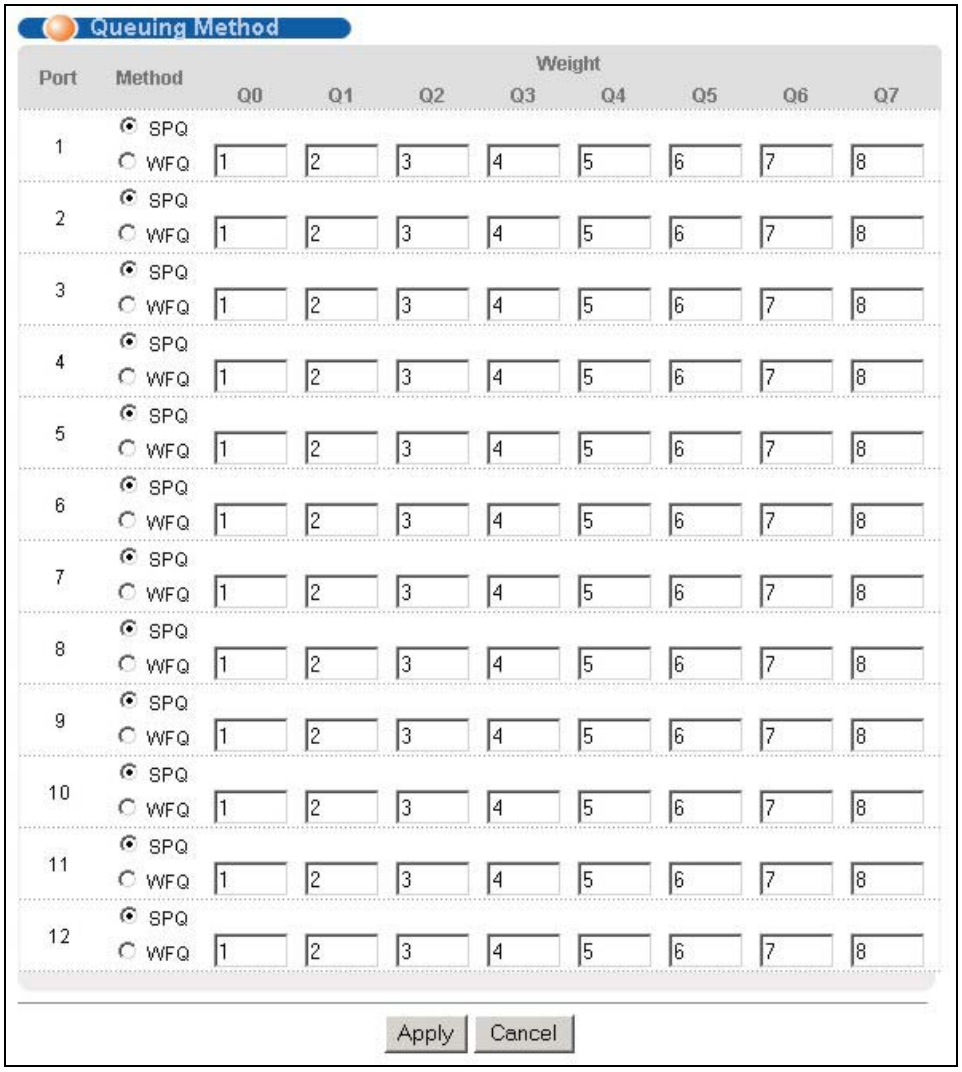


Figure 17-1 Queuing Method

The following table describes the labels in this screen.

Table 17-2 Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
Method	Select **SPQ** (Strict Priority Queuing) or **WRR** (Weighted Round Robin Scheduling). Strict Priority Queuing (SPQ) services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. WRR services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select **WRR**, enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights. Queues with larger weights get more service than queues with smaller weights.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 18 Classifier

This chapter introduces and shows you how to configure the packet classifier on the switch.

18.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

1. Configure classifiers to sort traffic into different flows.
2. Configure policy rules to define actions to be performed for a classified traffic flow (refer to *Chapter 19* to configure policy rules).

18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that match the rules. To configure policy rules, refer to *Chapter 19* .

Click **Advanced Application** and **Classifier** in the navigation panel to display the configuration screen as shown.

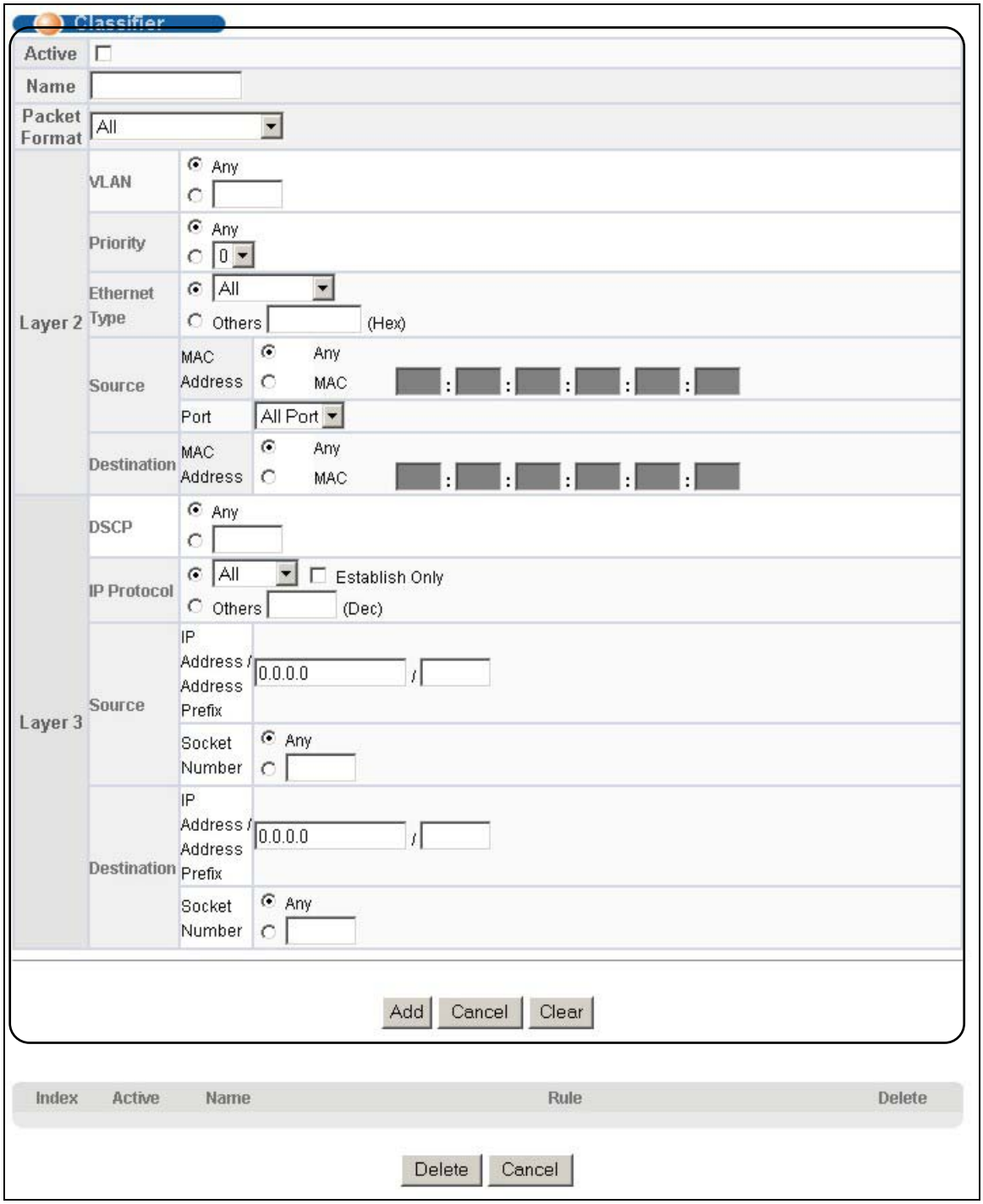


Figure 18-1 Classifier

The following table describes the labels in this screen.

Table 18-1 Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.

Table 18-1 Classifier

LABEL	DESCRIPTION
Packet Format	Specify the format of the packet. Choices are **All**, **802.3 tagged**, **802.3 untagged**, **Ethernet II tagged** and **Ethernet II untagged**. A value of **802.3** indicates that the packets are formatted according to the IEEE 802.3 standards. A value of **Ethernet II** indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Layer 2 Specify the fields below to configure a layer 2 classifier.	
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value. Refer to *Table 18-3* for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Select the port to which the rule should be applied. You may choose one port only or all ports (**All Ports**).
Destination	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer 3 classifier.	
DSCP	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select **Other** and enter the protocol number in decimal value. Refer to *Table 18-4* for more information. You may select **Establish Only** for **TCP** protocol type. This means that the switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.

Table 18-1 Classifier

LABEL	DESCRIPTION
Socket Number	**You *must* select either** UDP **or** TCP **in the** IP Protocol **field before you configure the socket numbers.** Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	**You *must* select either** UDP **or** TCP **in the** IP Protocol **field before you configure the socket numbers.** Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click **Add** to insert the entry in the summary table below.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

When two rules conflict with each other, a higher layer rule has priority over lower layer rule.

Figure 18-2 Classifier: Summary Table

The following table describes the labels in this screen.

Table 18-2 Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click **Delete** to remove the selected entry from the summary table.

Table 18-2 Classifier: Summary Table

LABEL	DESCRIPTION
Cancel	Click **Cancel** to clear the **Delete** check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 18-3 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

Table 18-4 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Classifier Example

The following figure shows an example where you configure a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

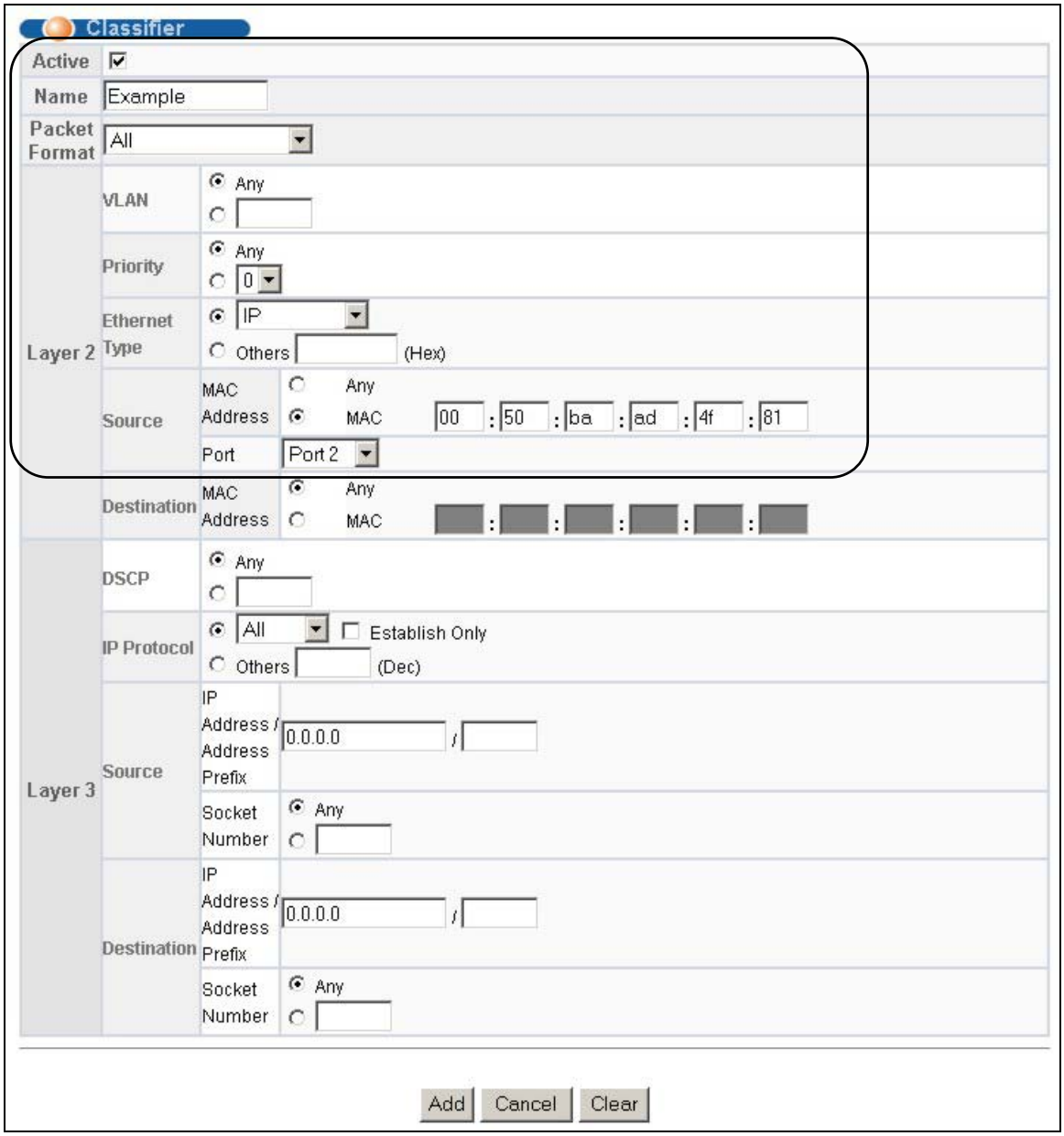


Figure 18-3 Classifier: Example

Chapter 19 Policy Rule

This chapter shows you how to configure policy rules.

19.1 About Policy Rules

A classifier distinguishes traffic into flows based on the configured criteria (refer to *Chapter 18* for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

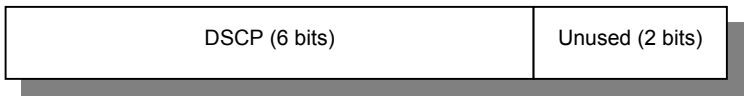
19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring Policy Rules

You must first configure a classifier in the Classifier **screen. Refer to *Chapter 18* for more information.**

Click **Advanced Applications** and then **Policy Rule** in the navigation panel to display the screen as shown.

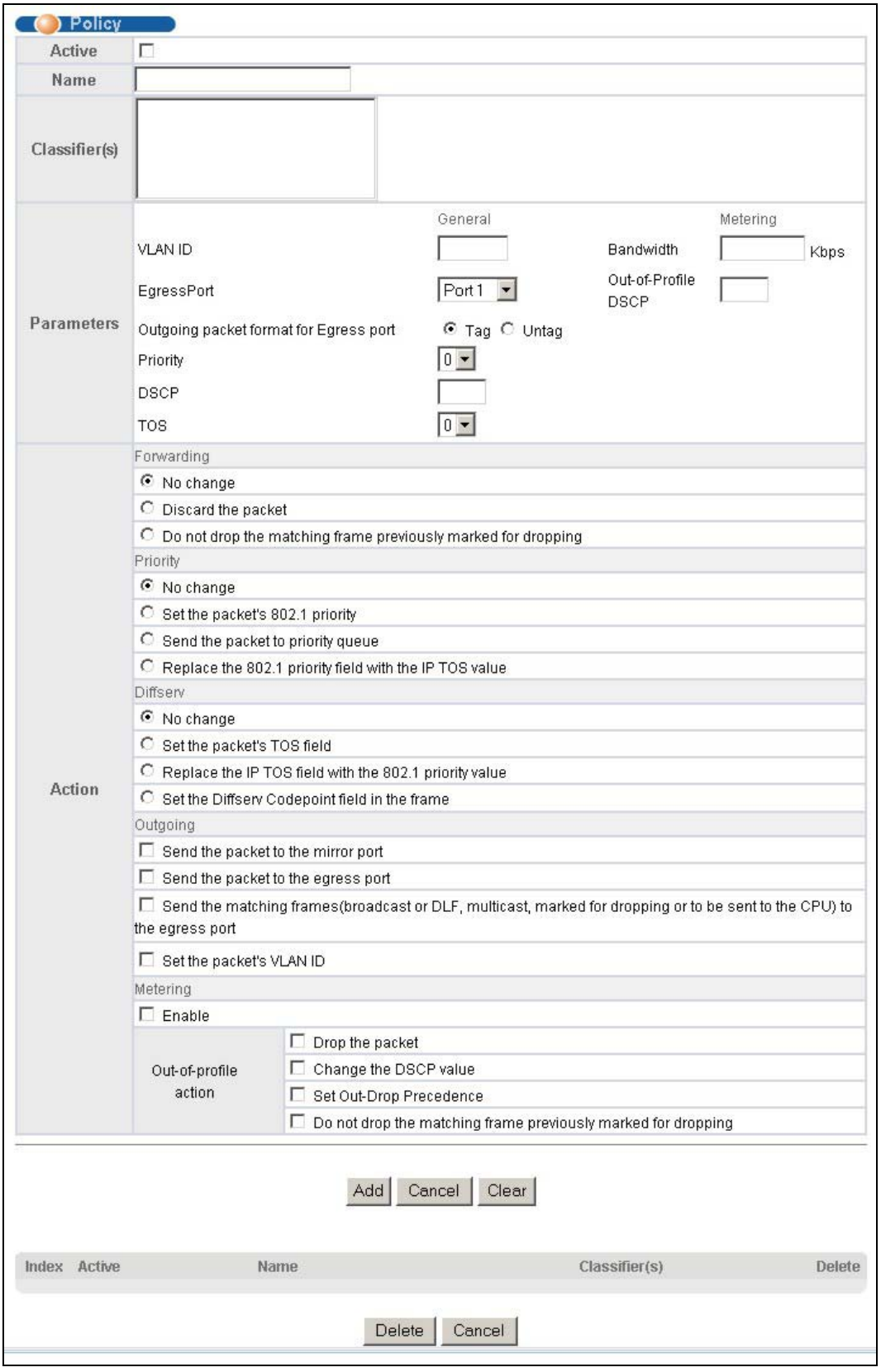


Figure 19-1 Policy

The following table describes the labels in this screen.

Table 19-1 Policy

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the **Classifier** screen (refer to *Chapter 18*). Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the **Action** field.	
General	
VLAN ID	Specify a VLAN ID number.
Egress Port	Select an outgoing port.
Outgoing packet format for Egress Port	Select **Tag** to add the specified VID to packets on the specified outgoing port. Otherwise, select **Untag**.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobits per second (Kbps).
Out of Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the switch takes on the associated classified traffic flow.	
Forwarding	Select **No change** to forward the packets. Select **Discard packet** to drop the packets. Select **Do not drop the matching frame previously marked for dropping** to retain the frames that were marked to be dropped before.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1 priority** to replace the 802.1 priority field with the value you set in the **Priority** field. Select **Send the packet to priority queue** to put the packets in the designated queue. Select **Replace the 802.1 priority field with IP TOS value** to replace the 802.1 priority field with the value you set in the **TOS** field.

Table 19-1 Policy

LABEL	DESCRIPTION
DiffServ	Select **No change** to keep the TOS and/or DSCP fields in the packets. Select **Set the packet's TOS field** to set the TOS field with the value you configure in the **TOS** field. Select **Replace the IP TOS with the 802.1 priority value** to replace the TOS field with the value you configure in the **Priority** field. Select **Set the Diffserv Codepoint field in the frame** to set the DSCP field with the value you configure in the **DSCP** field.
Outgoing	Select **Send the packet to the mirror port** to sent the packet to the mirror port. Select **Send the packet to the egress port** to send the packet to the egress port. Select **Send the matching frames (broadcast or DLF, multicast, marked for dropping or to be sent to the CPU) to the egress port** to send the broadcast, multicast, DLF, marked-to-drop or CPU frames to the egress port. Select **Set the packet's VLANID** to set the VLAN ID of the packet with the value you configure in the **VLANID** field.
Metering	Select **Enable** to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select **Drop the packet** to discard the out-of-profile traffic. Select **Change the DSCP Value** to replace the DSCP field with the value specified in the **Out of profile DSCP** field. **Set Out-Drop Precedence** is related to the metering bandwidth setting. The switch marks traffic that is higher than the metering bandwidth setting as drop precedence. Select **Set Out-Drop Precedence** to drop packets that are marked drop-precedence first when there is traffic congestion. Select **Do not drop the matching frame previously marked for dropping** to queue the frames that are marked to be dropped.
Add	Click **Add** to inset the entry to the summary table below.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.

19.3 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

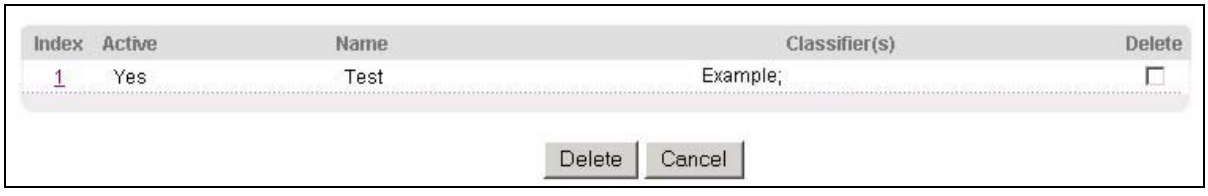


Figure 19-2 Policy: Summary Table

The following table describes the labels in this screen.

Table 19-2 Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this policy. This is for identification purposes only.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-band traffic on a traffic flow classified using the **Example** classifier (refer to *Section 18.4*).

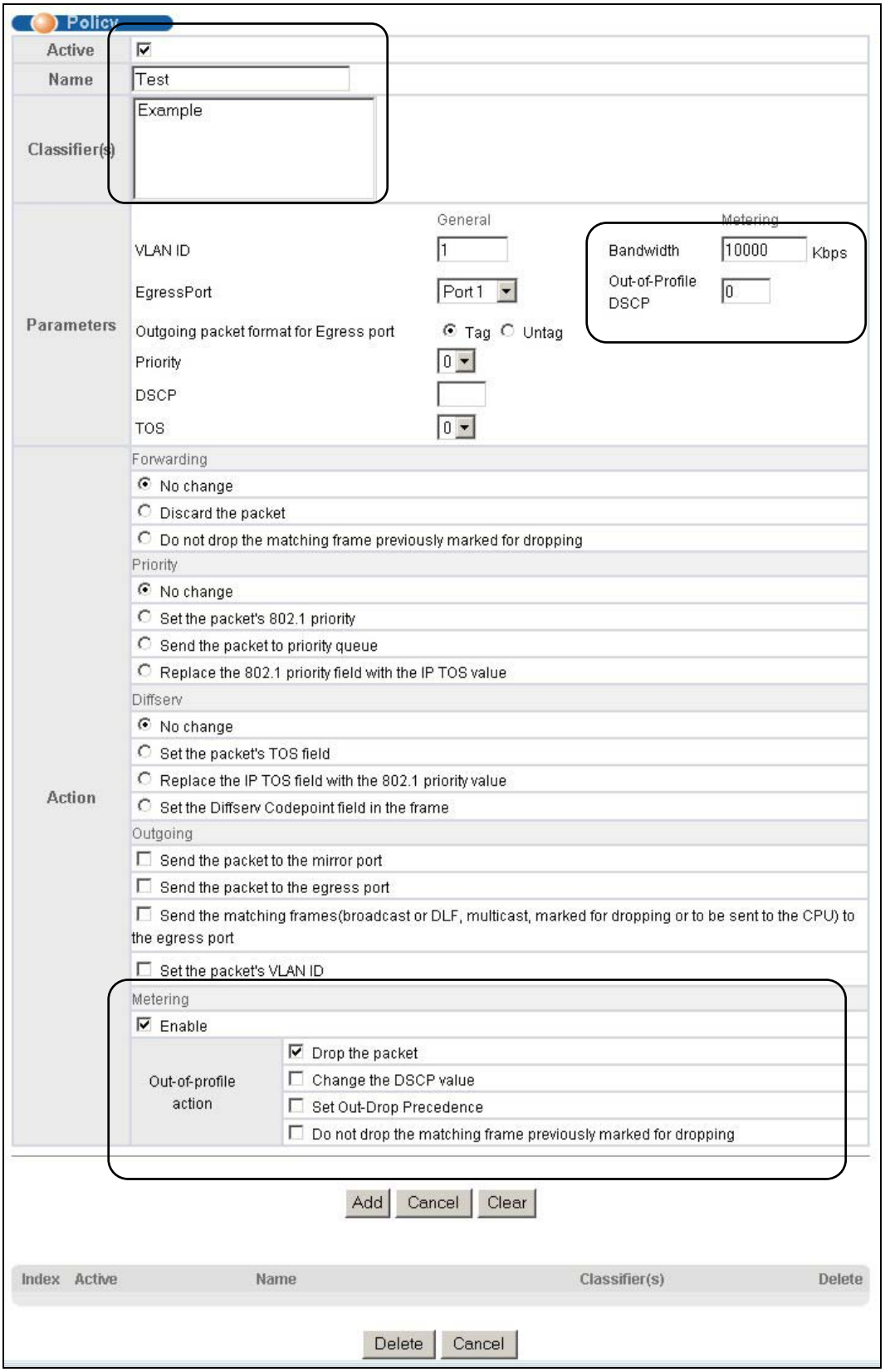


Figure 19-3 Policy Example

Chapter 20 Multicast

This chapter shows you how to configure various multicast features.

20.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.

20.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

20.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

20.1.3 IGMP Snooping

IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to *RFC 1112* and *RFC 2236* for information on IGMP versions 1 and 2 respectively.

A switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP

packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the switch to learn multicast groups without you having to manually configure them.

The switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. The switch discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

20.2 Multicast Status

Click Advanced Applications and Multicast to display the screen as shown. This screen shows the multicast group information.

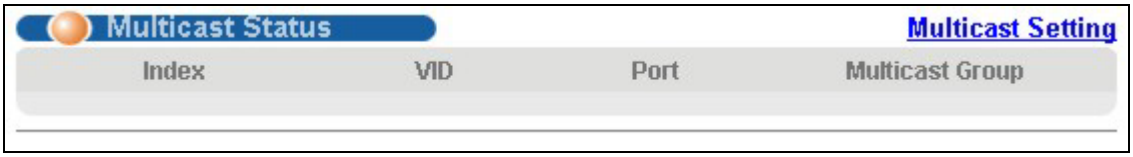


Figure 20-1 Multicast Status

The following table describes the labels in this screen.

Table 20-1 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

20.3 Multicast Setup

Click **Advanced Applications**, **Multicast** and the **Multicast Setting** link to display the screen as shown.

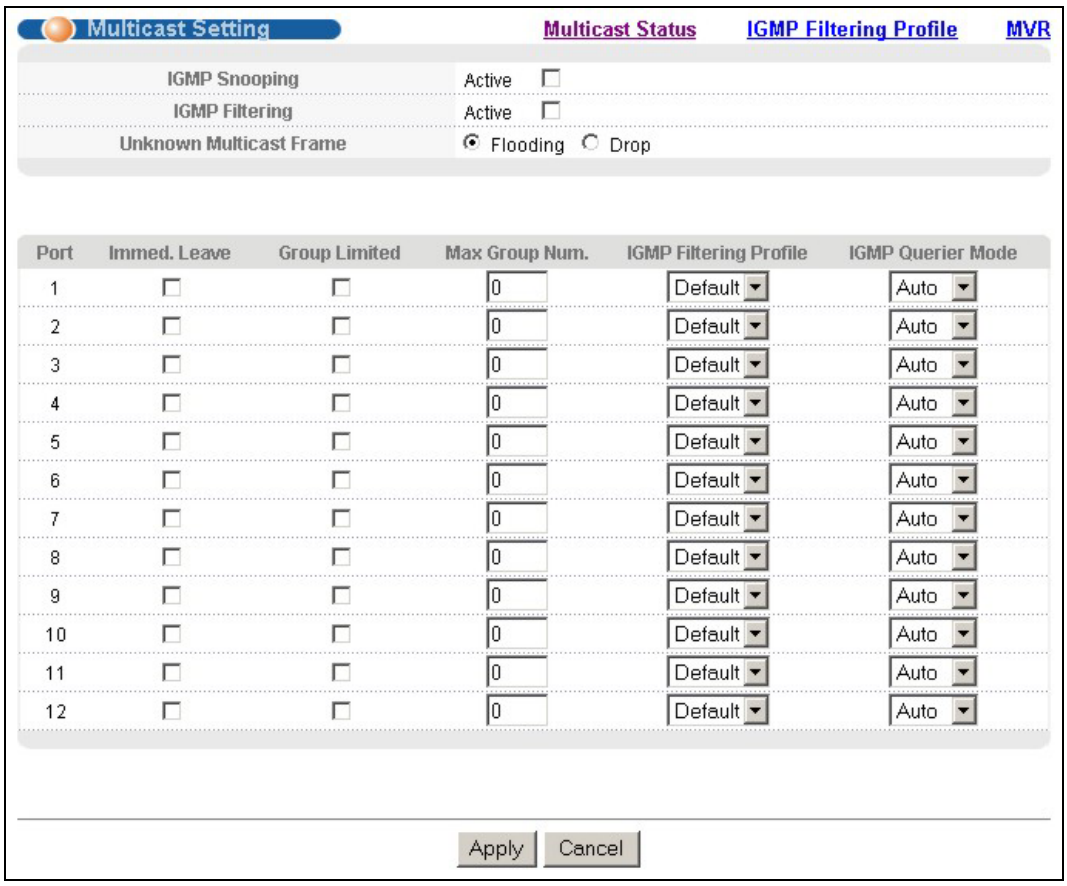


Figure 20-2 Multicast Setting

The following table describes the labels in this screen.

Table 20-2 Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Select **Active** to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.
Unknown Multicast Frame	Specify the action to perform when the switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.
Immed. Leave	Select this option to set the switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group.

Table 20-2 Multicast Setting

LABEL	DESCRIPTION
IGMP Querier Mode	The switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the switch from using the port as an IGMP query port. The switch will not keep any record of an IGMP router being connected to this port. The switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

20.4 IGMP Filtering Profile

IGMP filter profiles allow you to control access to IGMP multicast groups. This allows you to have a service available to a specific IGMP multicast group. You can configure an IGMP filter profile for an IGMP multicast group that has access to a service (like a SIP server for example). Within a profile, configure an IGMP filter to specify the multicast IP address ranges. Then assign the IGMP filter profile to the ports (in the **Multicast Setting** screen) that are allowed to use the service.

Click **Advanced Applications** and **Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Filtering Profile** link to display the screen as shown.

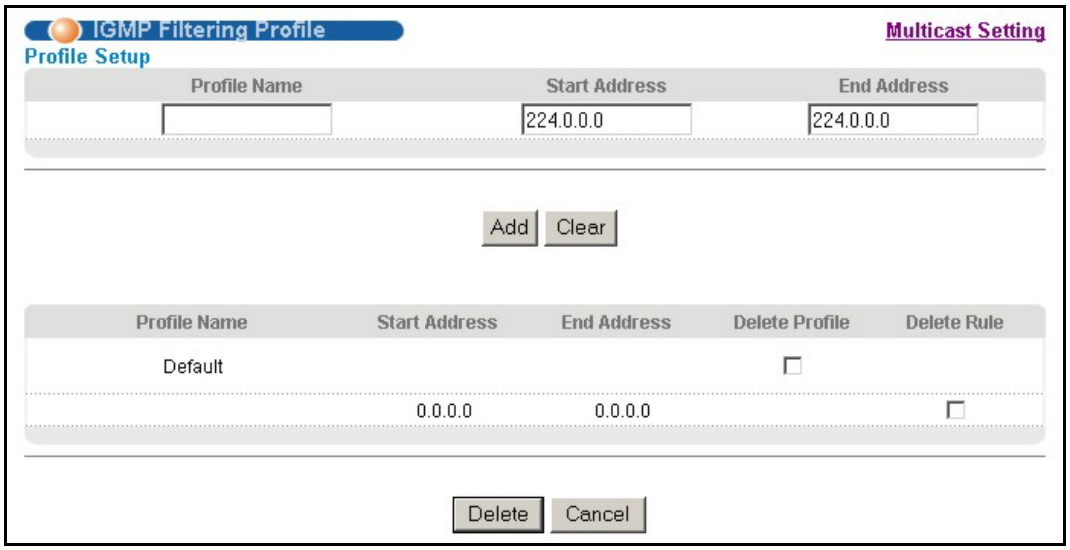


Figure 20-3 Multicast: IGMP Filtering Profile

The following table describes the labels in this screen.

Table 20-3 Multicast: IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click **Add** to save the settings to the switch.
Clear	Click **Clear** to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

20.5MVR Overview

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscriber to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

You must enable IGMP snooping to use MVR. However, MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the switch and **S**.

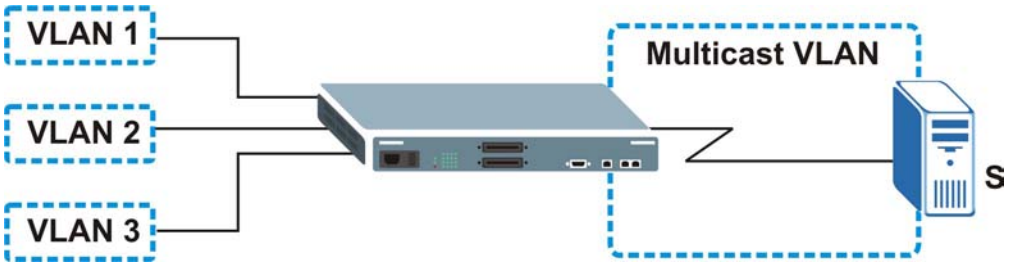


Figure 20-4 MVR Network Example

20.5.1 Types of MVR Ports

In MVR, a source port is a port on the switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast data. Once configured, the switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

20.5.2 MVR Modes

You can set your switch to operate in either dynamic or compatible mode.

In dynamic mode, the switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

20.5.3 How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the switch. Multiple subscriber devices can connect through a port configured as the receiver on the switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the switch, an entry is created in the forwarding table on the switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the switch to leave the multicast group. The switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port

will still be on the list of forwarding destination for the multicast traffic. Otherwise, the switch removes the receiver port from the forwarding table.

Figure 20-5 MVR Multicast Television Example

20.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications** and **Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **MVR** link to display the screen as shown next.

You can create up to three multicast VLANs and up to 256 multicast rules on the switch.

Your switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

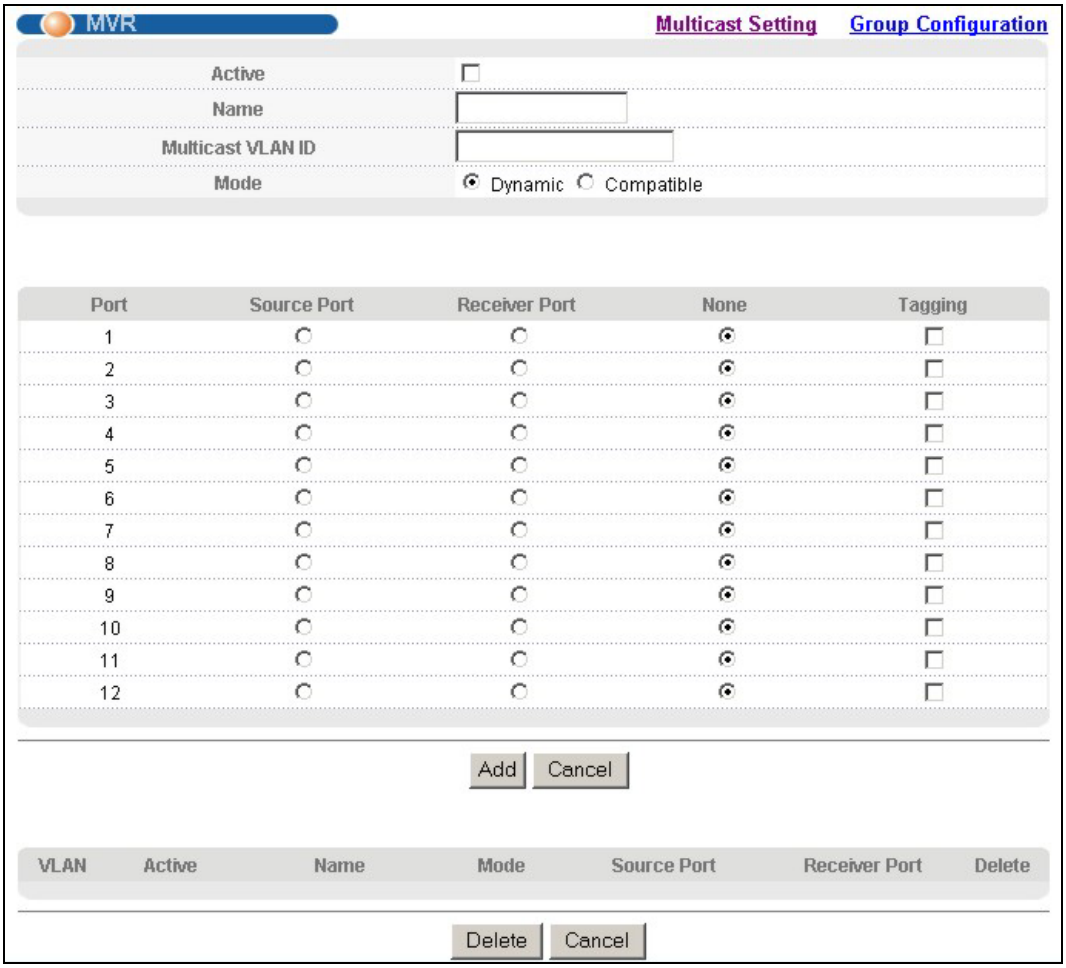


Figure 20-6 MVR

The following table describes the related labels in this screen.

Table 20-4 MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
Mode	Specify the MVR mode on the switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the switch not to send IGMP reports.
Port	This field displays the port number on the switch.
Source Port	This field is applicable for **Ethernet** ports. Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic. A receiver port cannot belong to a multicast VLAN.

Table 20-4 MVR

LABEL	DESCRIPTION
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click **Add** to save the settings.
Cancel	Click **Cancel** to discard all changes.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

20.7 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

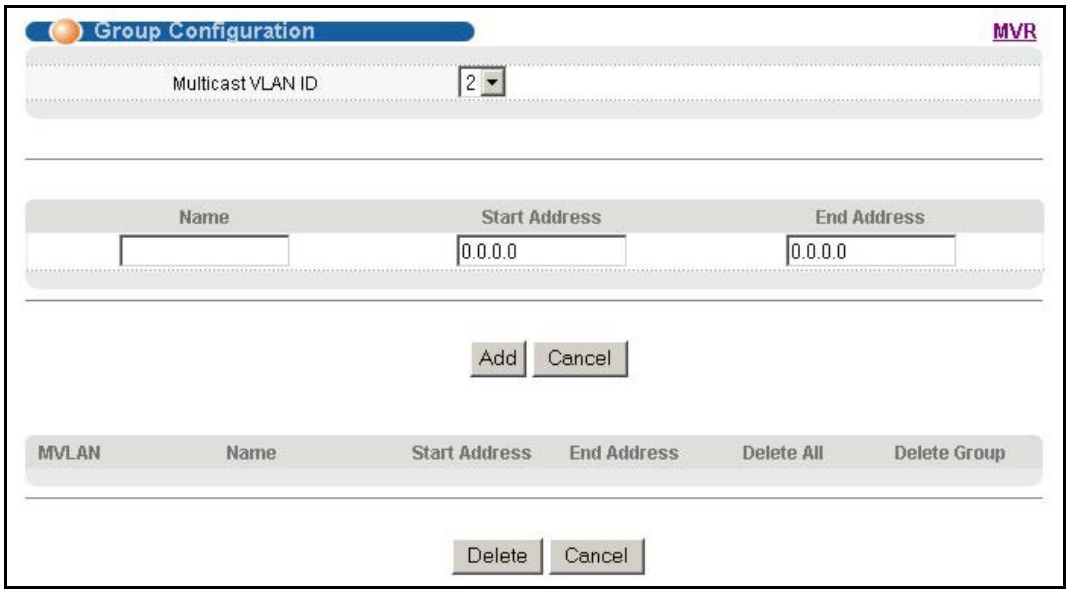


Figure 20-7 MVR Group Configuration

The following table describes the labels in this screen.

Table 20-5 MVR Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to *Section 20.1.1* for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to *Section 20.1.1* for more information on IP multicast addresses.
Add Cancel	Click **Add** to save the settings. Click **Cancel** to discard all changes.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select **Delete All** and click **Delete** to remove all entries from the table. Select **Delete Group** and click **Delete** to remove the selected entry(ies) from the table.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

20.7.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers **A**, **B** and **C** in VLAN are able to receive the traffic.

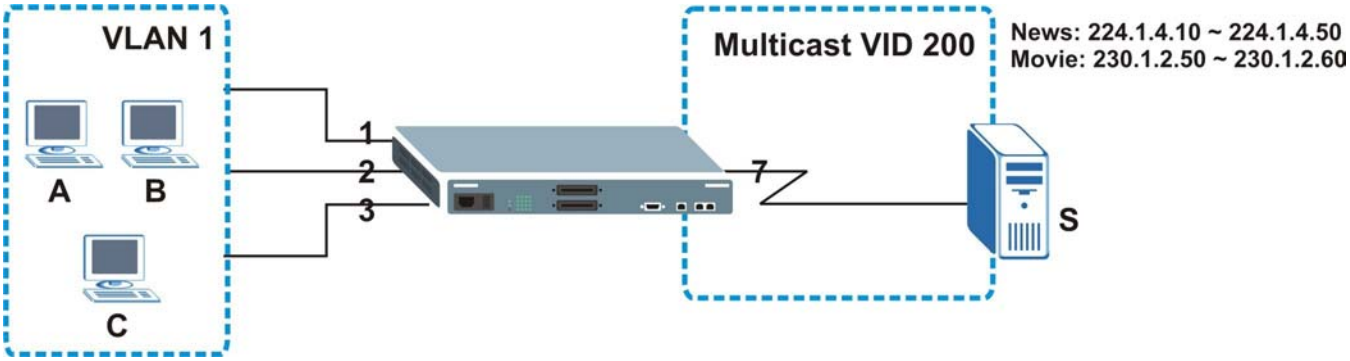


Figure 20-8 MVR Configuration Example

To configure the MVR settings on the switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

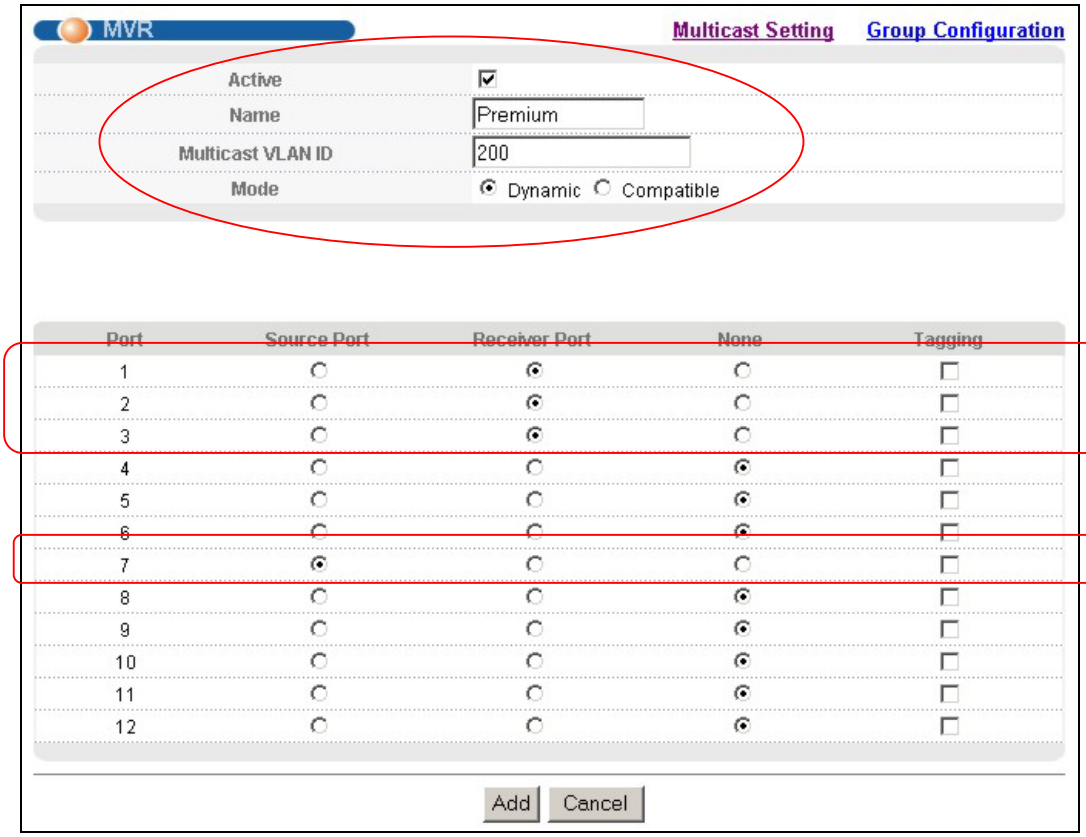


Figure 20-9 MVR Configuration Example

To set the switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

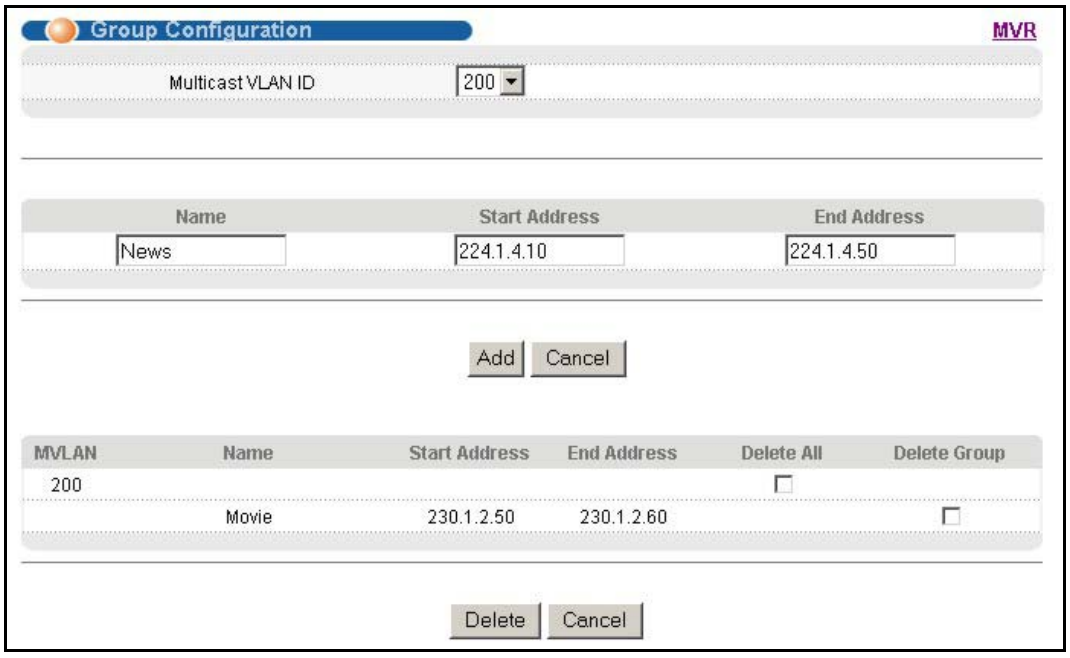


Figure 20-10 MVR Configuration Example

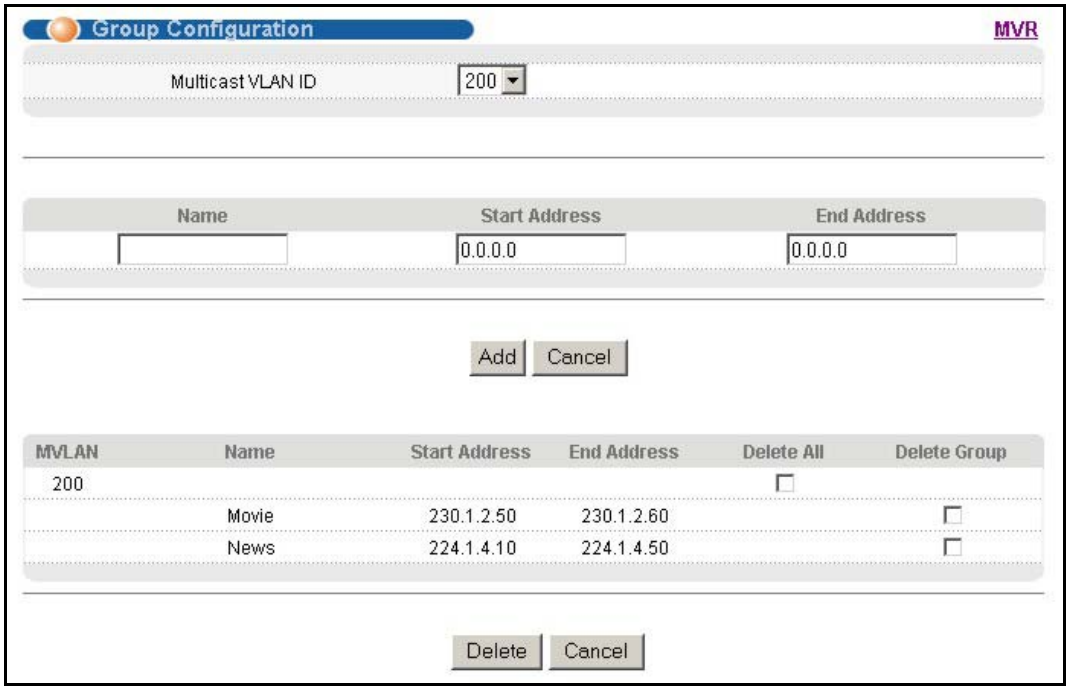


Figure 20-11 MVR Configuration Example

Part VI

IP Application and Management

This part describes the IP Application and Management screens.

Chapter 21
Routing Protocol

This chapter shows you how to configure the routing functions.

21.1 Static Route

Static routes tell the switch how to forward IP traffic when you configure the TCP/IP parameters manually.

Click **IP Application** in the navigation panel and then **Static Routing** to display the screen as shown.

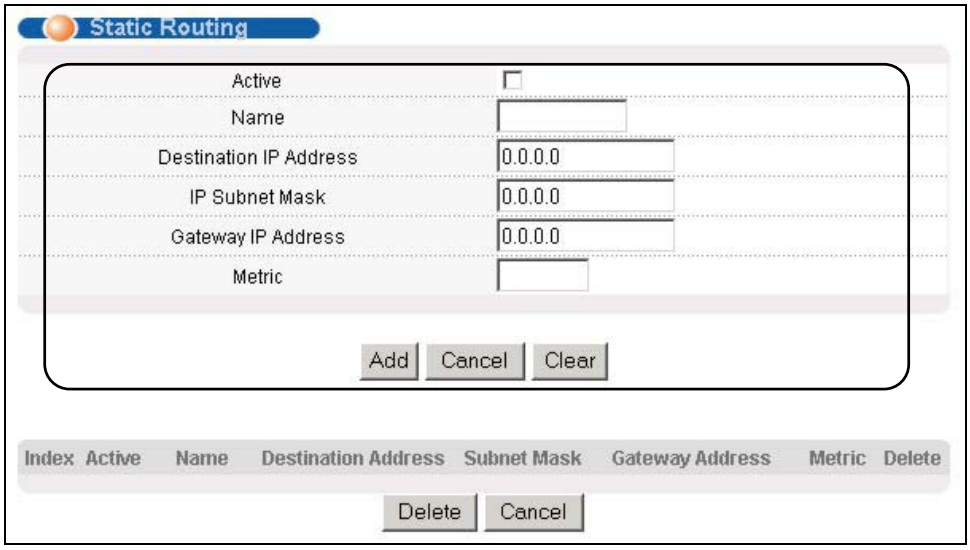


Figure 21-1 Static Routing

The following table describes the related labels you use to create a static route.

Table 21-1 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name for this route. This is for identification purpose only.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination. The gateway must be a router on the same segment as your switch.

Table 21-1 Static Routing

LABEL	DESCRIPTION
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to save the new rule to the switch. It then displays in the summary table at the bottom of the screen.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to clear the fields to the factory defaults.

View the current static routes on the switch in the summary table at the bottom of the screen.

Figure 21-2 Static Routing: Summary Table

The following table describes the labels in the summary table.

Table 21-2 Static Routing: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when is it deactivated.
Name	This field displays the descriptive name for this route. This is for identification purpose only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Check the rule(s) that you want to remove in the **Delete** column, and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkboxes in the **Delete** column.

Chapter 22 DHCP Relay

This chapter describes the DHCP relay and shows you how to configure the **DHCP Relay** screen.

22.1 DHCP Relay Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a DHCP server. You can configure the switch to relay client DHCP requests to a DHCP server and the server's responses back to the clients.

22.1.1 DHCP "Relay Agent Information Option"

The switch can add information to client DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the switch to add to the client DHCP requests that it relays to the DHCP server. Please refer to RFC 3046 for more details.

22.1.2 DHCP Relay Agent Circuit ID Sub-option Format

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of client DHCP request frames that the switch relays to a DHCP server. The Agent Information field that the switch adds contains an "Agent Circuit-ID sub-option" that includes the following information about where the DHCP request was received.

- Slot ID (1 byte, this is 0 with this model)
- Port ID (1 byte)
- VLAN ID (2 bytes)
- System name (up to 32 bytes, this is optional)

22.2 DHCP Relay Configuration

To configure DHCP relay information and specify the DHCP server(s), click **IP Application** and **DHCP Relay** to display the screen as shown next.

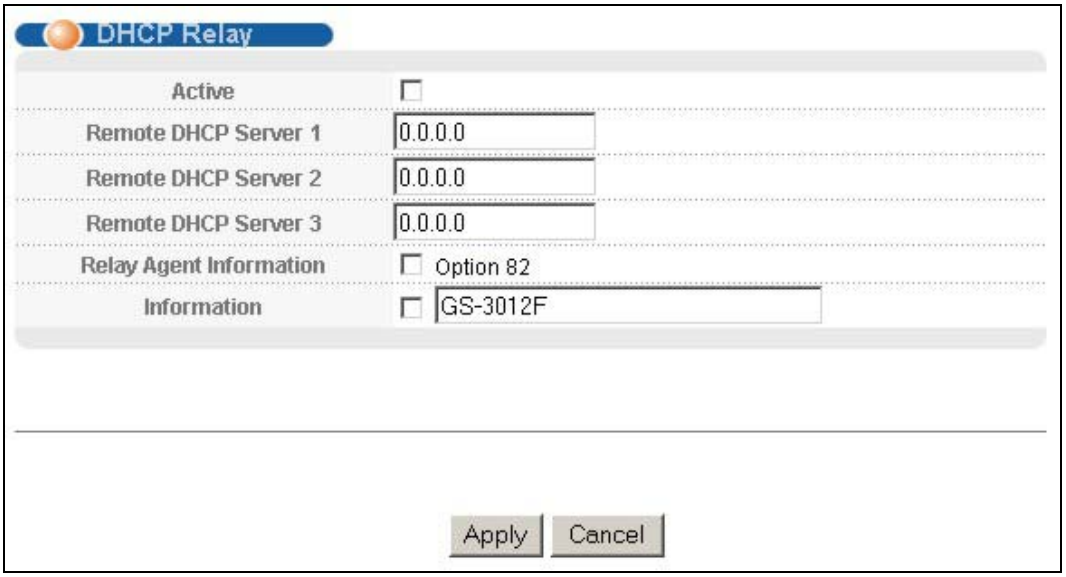


Figure 22-1 DHCP Relay

The following table describes the labels in this screen.

Table 22-1 DHCP Relay

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the switch add information (slot number, port number and VLAN ID) to client TCP/IP configuration requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box to add the switch name to the DHCP client requests that the switch relays to a DHCP server.
Add	Click **Add** to inset the entry to the summary table below.
Cancel	Click **Cancel** to reset the fields back to your previous configuration.

Chapter 23 Maintenance

This chapter explains how to configure the maintenance screens. The links on the upper right of the Maintenance screen lead to different screens that let you maintain the firmware and configuration files.

23.1 Maintenance

Click **Management** and then **Maintenance** in the navigation panel to open the following screen.

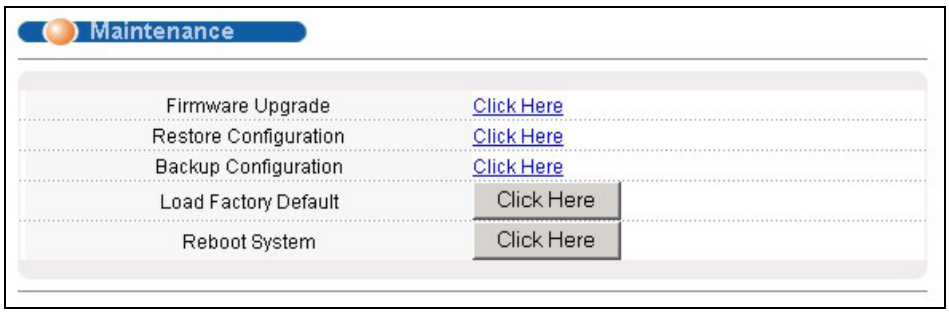


Figure 23-1 Maintenance

23.2 Firmware Upgrade

Click **Firmware Upgrade** in the **Maintenance** screen if you want to upgrade your switch firmware. See the **System Info** screen to verify your current firmware version number. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

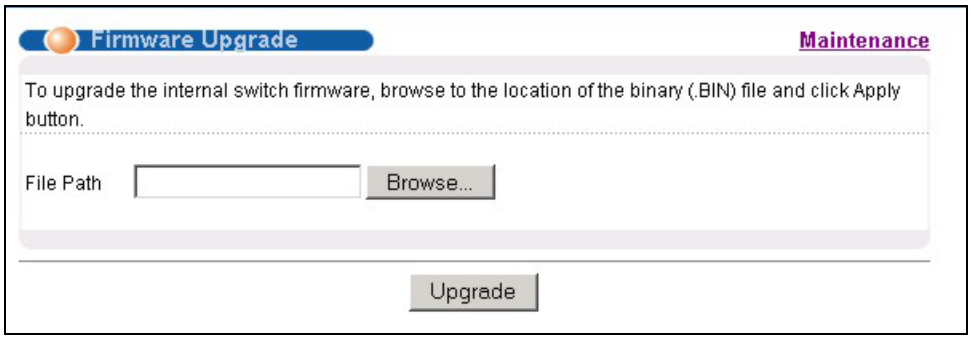


Figure 23-2 Firmware Upgrade

Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

23.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the switch using the **Restore Configuration** screen.

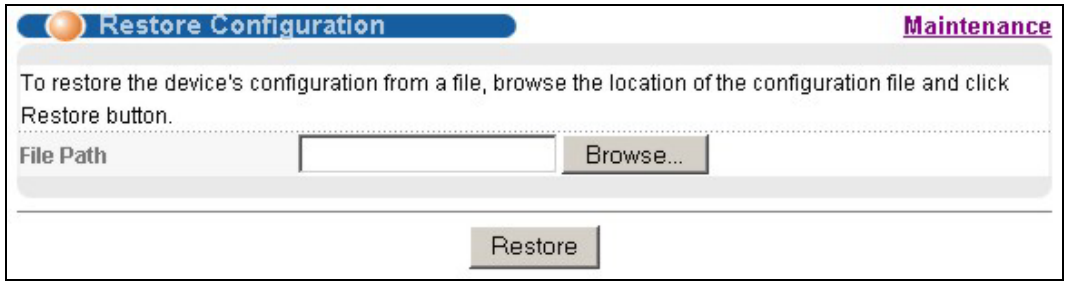


Figure 23-3 Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display a **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the switch, so your backup configuration file is automatically renamed when you restore using this screen.

23.4 Backing Up a Configuration File

Backing up your switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current switch configuration to a computer using the **Configuration Backup** screen.

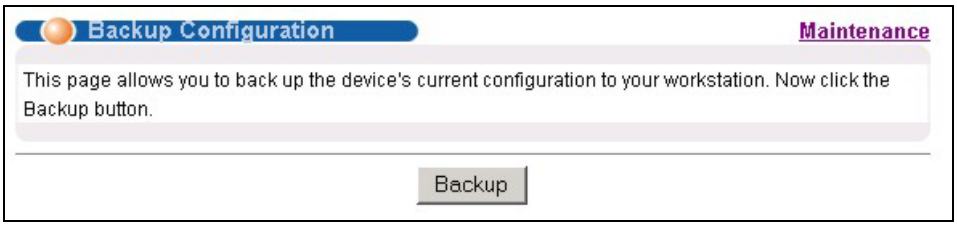


Figure 23-4 Backup Configuration

Follow the steps below to back up the current switch configuration to your computer in this screen.

1. Click **Backup**.
2. Click **Save** to display the **Save As** screen.
3. Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

23.5 Load Factory Defaults

Press the **Click Here** button next to **Load Factory Defaults** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 23-5 Confirm Load factory Defaults

Click **OK** to go to the next screen.

Figure 23-6 Close Browser After Load Factory Defaults

Click **Yes** to close this window. Open a new browser window to access the switch web configurator again. You may need to change the IP address of your computer to be in the same subnet as that of the default switch IP address (192.168.1.1).

23.6 Reboot System

Reboot System allows you to restart the switch without physically turning the power off. Press the **Click Here** button next to **Reboot System** to display the next screen.

Figure 23-7 Confirm Restarting of the Switch

Click **OK** to see the screen as shown in *Figure 23-6*. Click **OK** again and then wait for the switch to restart. This takes up to two minutes. This does not affect the switch's configuration.

23.7 Command Line FTP

This section shows some examples of uploading to or downloading files from the switch using FTP commands. First, understand the filename conventions.

23.7.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the screens such as password, switch setup, IP setup, etc. Once you have customized the switch's settings, they can be saved back to your computer under a filename of your choosing.

A configuration file that you save from your switch to your computer does not include the password, the error log or the trace log.

When you restore a backup configuration file from your computer to your switch, does not change the password, the error log or the trace log.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 23-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config		This is the configuration filename on the switch. Uploading the config file replaces the specified configuration file system, including your switch configurations and system-related data.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the switch .

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

23.7.2 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter "open", followed by a space and the IP address of your switch.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "bin" to set transfer mode to binary.
6. Use "put" to transfer files from the computer to the switch, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the switch and renames it "ras". Similarly, "put config.cfg config" transfers the configuration file on your computer (config.cfg) to the switch and renames it "config". Likewise "get config config.cfg" transfers the configuration file on the switch to your computer and renames it "config.cfg." See earlier in this chapter for more information on filename conventions.
7. Enter "quit" to exit the ftp prompt.

23.7.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 23-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

23.7.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Access Control** screen.
- The IP address(es) in the **Secured Client Set** in the **Remote Management** screen does not match the client IP address. If it does not match, the switch will disconnect the Telnet session immediately.

Chapter 24 Access Control

This chapter describes how to control access to the switch.

24.1 About Access Control

Click **Maintenance**, **Access Control** from the navigation panel to display the screen as shown. From this screen you can configure SNMP, up to four web configurator administrators, enable/disable remote service access and configure trusted computers for remote access.

Figure 24-1 Access Control

24.2 Access Control Overview

The following table describes how many concurrent management sessions are permitted when the multiple login feature is either enabled or disabled.

Table 24-1 Access Control Overview

Multiple Login	Console port	SSH	Telnet	FTP	Web	SNMP
Enabled	One console port session	SSH and Telnet share four sessions.		One session	Up to five accounts	No limit
Disabled	The console port, SSH and Telnet share one session. The console port has the highest priority and Telnet has the lowest priority.			One session	Up to five accounts	No limit

With the multiple login feature disabled, a console port access control session and Telnet access control session cannot coexist. The console port has higher priority. If you telnet to the switch and someone is already logged in from the console port, then you will see the following message.

```
"Local administrator is configuring this device now!!!
Connection to host lost."
```

Figure 24-2 Console Port Priority

24.3 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network switches. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the switch through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

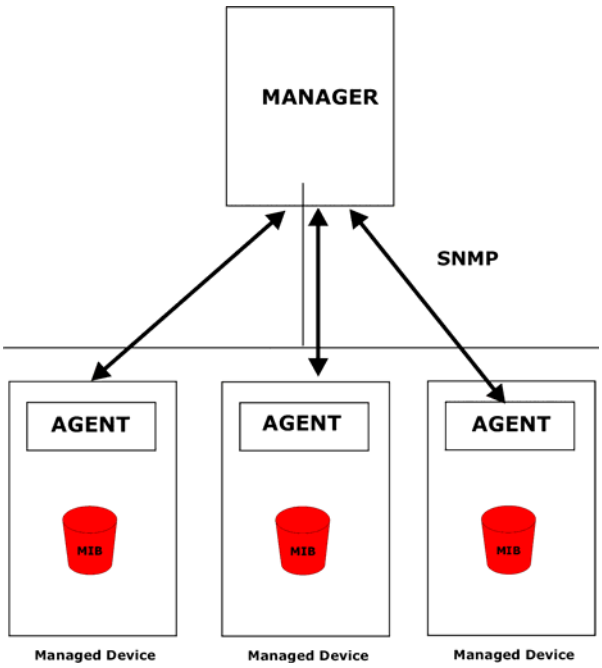


Figure 24-3 SNMP Management Model

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch (the GS). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 24-2 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

24.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1493 Bridge MIBs
- RFC 1155 SMI
- RFC 2863 if-mib
- RFC 2925 Ping and trace route
- RFC 1157 SNMP v1
- RFC 1643 Ethernet MIBs
- SNMPv2, SNMPv2c
- Bridge extension MIBs RFC 2674

24.3.2 SNMP Traps

The switch sends traps to an SNMP manager when an event occurs. SNMP traps supported are outlined in the following table.

Table 24-3 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Traps		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the ES-3124 is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the ES-3124 restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
topology change	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.

24.3.3 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

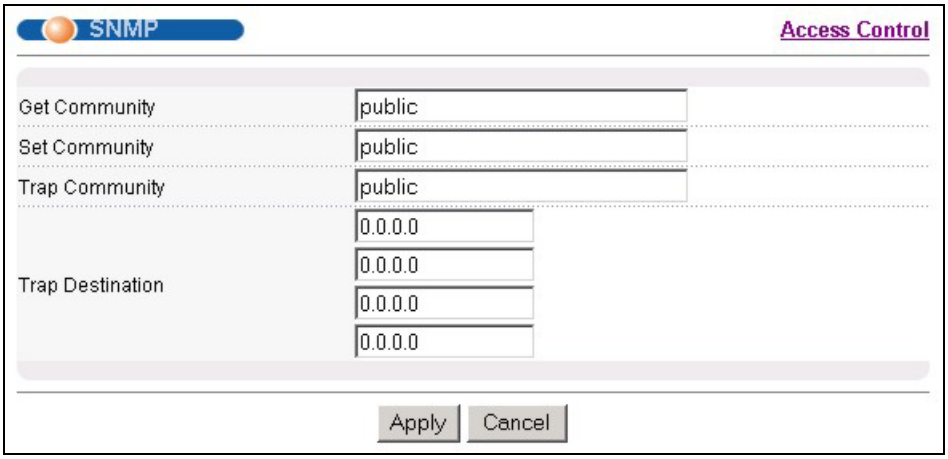


Figure 24-4 Access Control: SNMP

The following table describes the labels in this screen.

Table 24-4 Access Control: SNMP

LABEL	DESCRIPTION
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination	Enter the IP addresses of up to four stations to send your SNMP traps to.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.3.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the switch via web configurator at any one time.

1. An administrator is someone who can both view and configure switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

It is highly recommended that you change the default administrator password ("1234").

2. A non-administrator (username is something other than **admin**) is someone who can view but not configure switch changes.

Click **Access Control** from the navigation panel and then click Logins from this screen.

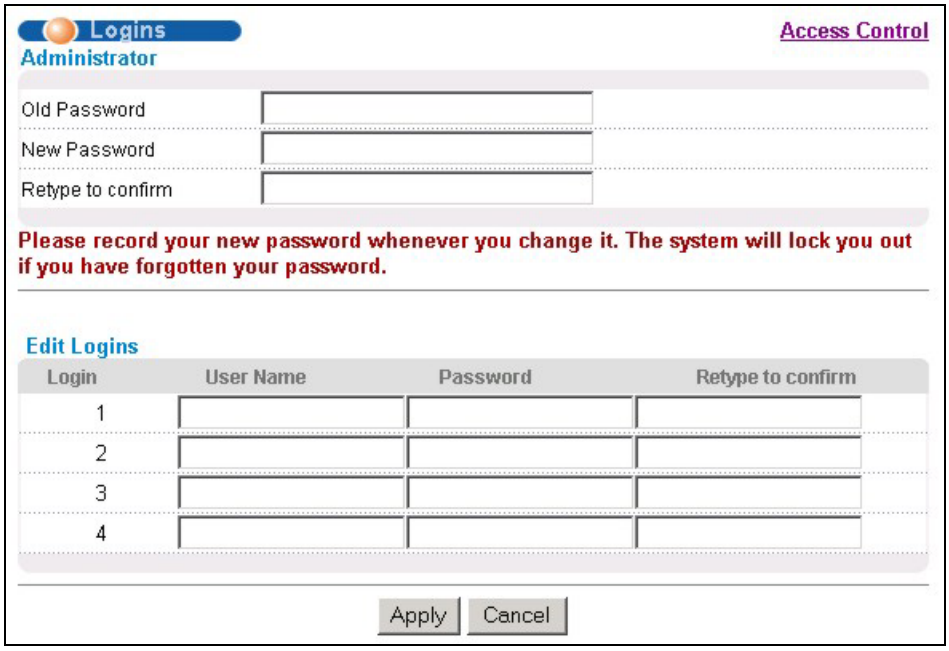


Figure 24-5 Access Control: Logins

The following table describes the labels in this screen.

Table 24-5 Access Control: Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the "admin" user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password ("1234" is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These people have read-only access.	
User Name	Set a user name (up to 32 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.4 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 24-6 SSH Communication Example

24.5 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

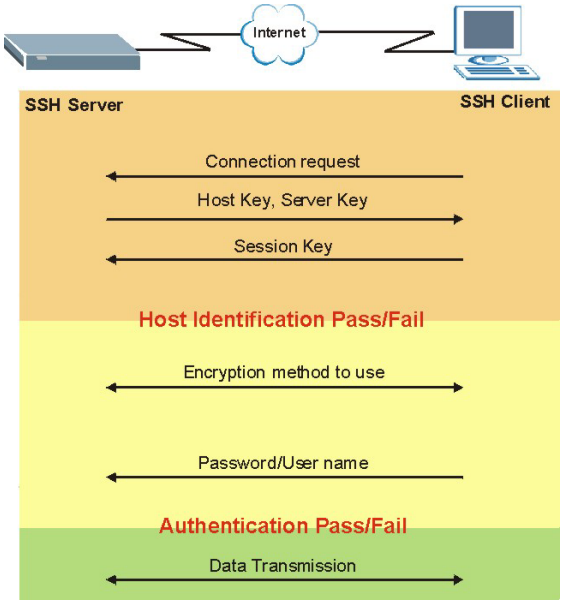


Figure 24-7 How SSH Works

1. Host Identification The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server. The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.
2. Encryption Method Once the identification is verified, both the client and server must agree on the type of encryption method to use.
3. Authentication and Data Transmission After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

24.6 SSH Implementation

Your switch supports SSH versions 1 and 2 using RSA and DSA authentication and five encryption methods (AES, 3DES, RC4, Blowfish and CAST). The SSH server is implemented on the switch for remote SMT management and file transfer on port 22 (by default). Up to four SSH connections are allowed at a time.

24.6.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the switch over SSH.

24.7 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

HTTPS on the switch is used so that you may securely access the switch using the web configurator. The SSL protocol specifies that the SSL server must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so.

Please refer to the following figure.

8. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the switch's WS (web server).
9. HTTP connection requests from a web browser go to port 80 (by default) on the switch's WS.

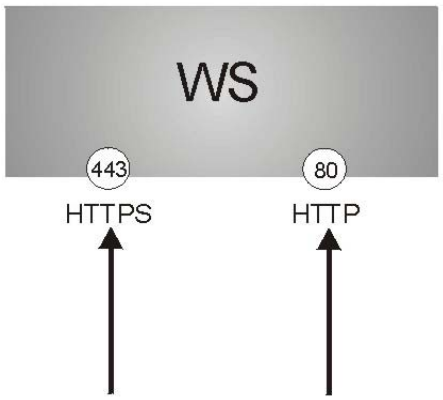


Figure 24-8 HTTPS Implementation

If you disable HTTP **in the** Service Access Control **screen, then the switch blocks all HTTP connection attempts.**

24.7.1 HTTPS Example

If you haven't changed the default HTTPS port on the switch, then in your browser enter "https:// switch IP Address/" as the web site address where "switch IP Address" is the IP address or domain name of the switch you wish to access.

The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the switch, for example 8443, then you must notify people who need to access the switch web configurator to use "https:// switch IP Address:**8443**" as the URL.

24.7.2 Internet Explorer Warning Messages

When you attempt to access the switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the switch.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 24-9 Security Alert Dialog Box (Internet Explorer)

24.7.3 Netscape Navigator Warning Messages

When you attempt to access the switch HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the switch.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the switch's certificate into the SSL client.

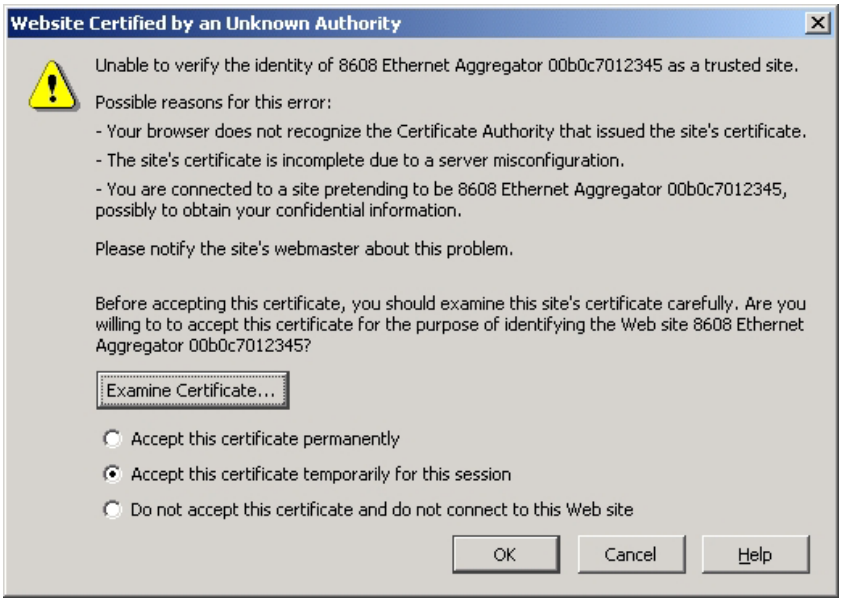


Figure 24-10 Security Certificate 1 (Netscape)

Figure 24-11 Security Certificate 2 (Netscape)

24.7.4 Login Screen

After you accept the certificate and login in, the switch main screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

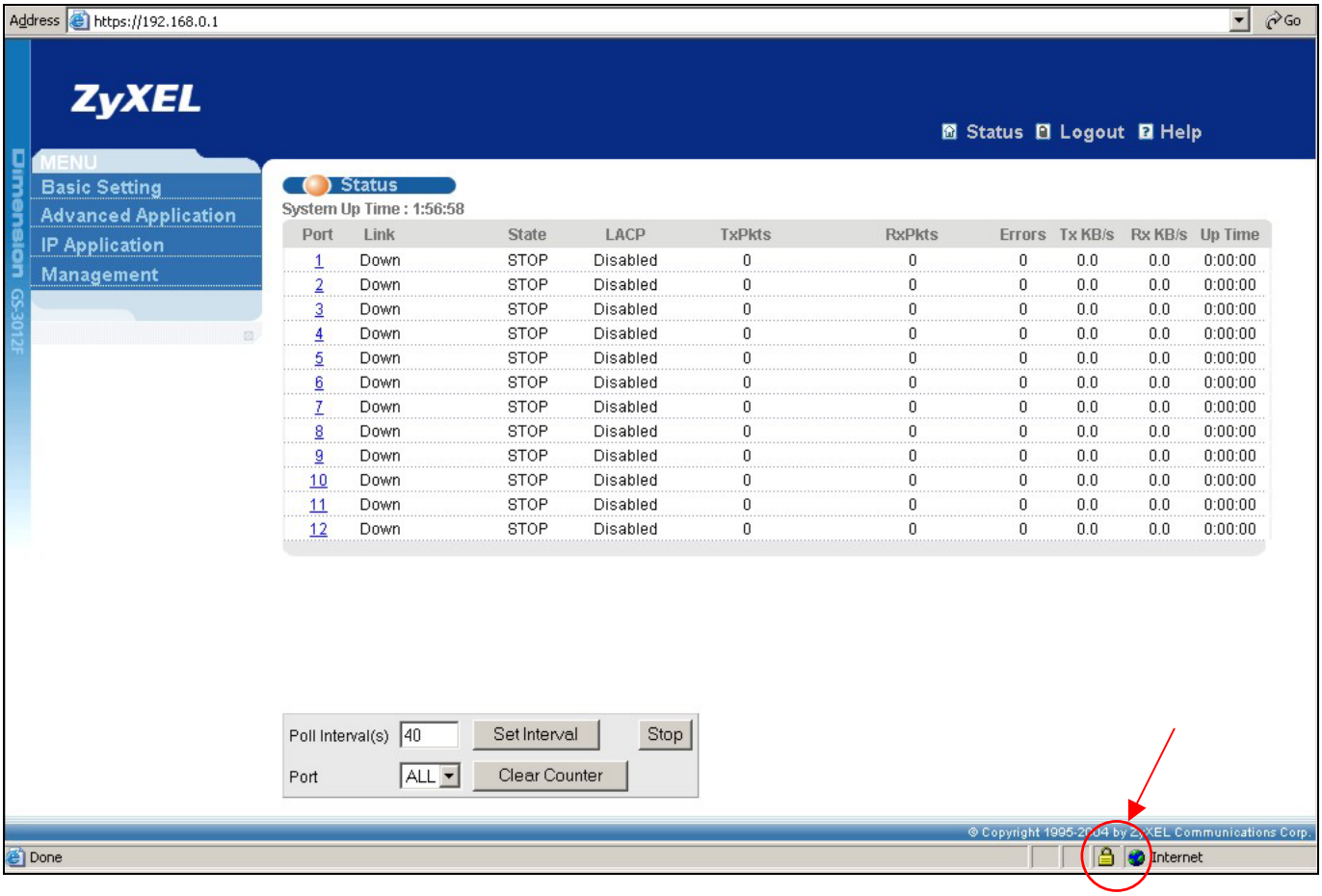


Figure 24-12 Status Screen (Internet Explorer)

Figure 24-13 Status Screen (Netscape)

24.8 Service Access Control

Service Access Control allows you to decide what services you may use to access the switch. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the **Access Control** screen.

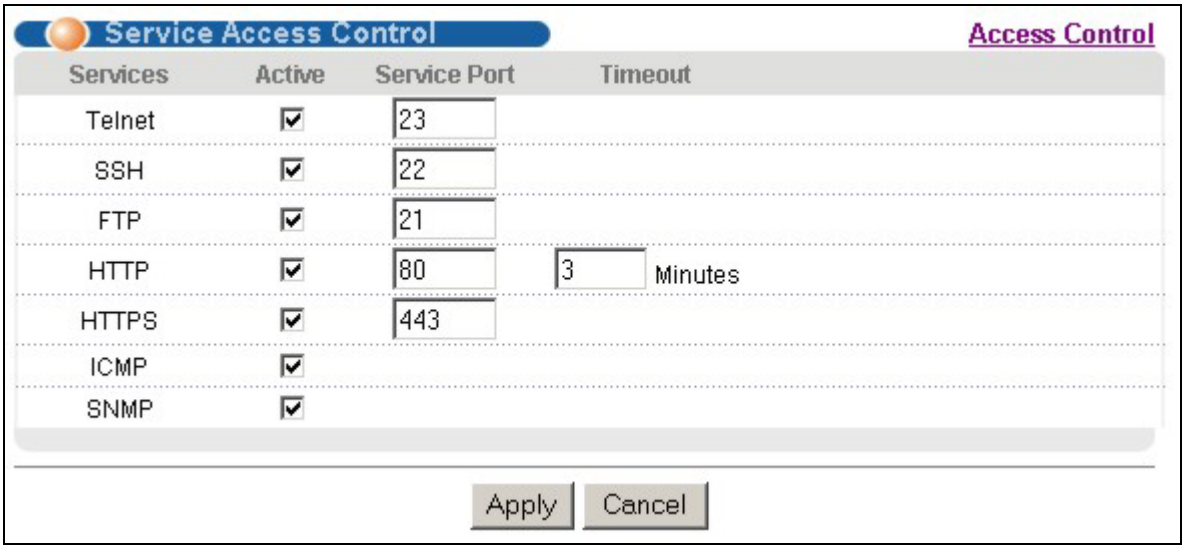


Figure 24-14 Access Control: Service Access Control

The following table describes the fields in this screen.

Table 24-6 Access Control: Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Service Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value greater than "0" must be entered.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24.9 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the switch. Click **Access Control** to return to the **Access Control** screen.

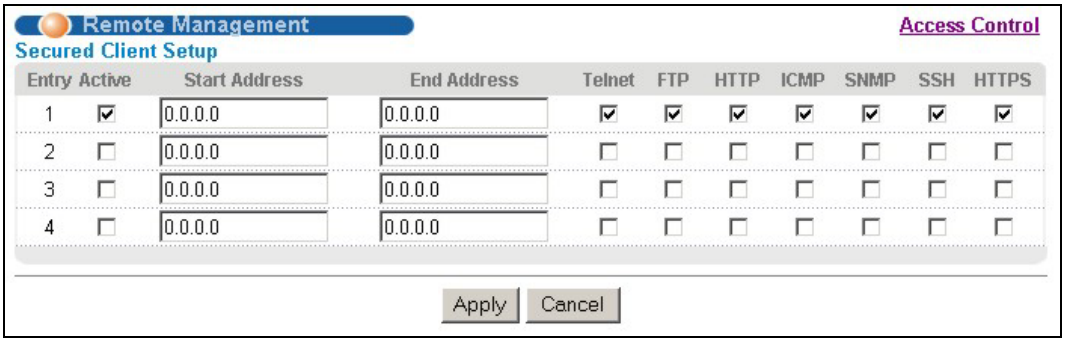


Figure 24-15 Access Control: Remote Management

The following table describes the labels in this screen.

Table 24-7 Access Control: Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers fro which you can manage this switch. The switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The switch immediately disconnects the session if it does not match.
Telnet/FTP/HTTP/ICMP /SNMP/SSH/HTTPS	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 25 Diagnostic

This chapter explains the Diagnostic screens.

25.1 Diagnostic

Click **Management** and then **Diagnostic** in the navigation panel to display this screen. Use this screen to check system logs, ping IP addresses or perform loopback tests on a port.

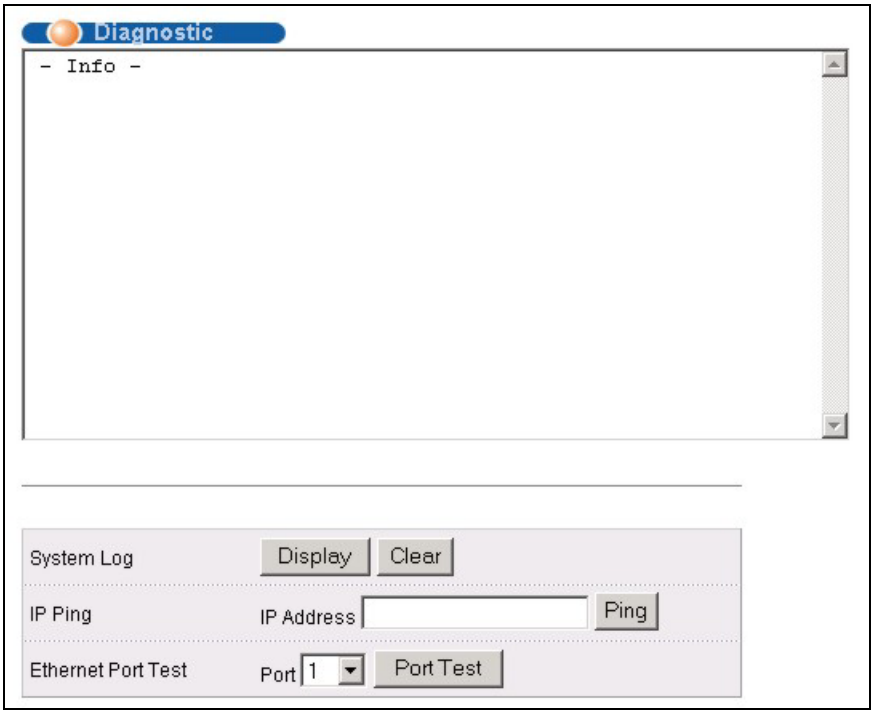


Figure 25-1 Diagnostic

The following table describes the labels in this screen.

Table 25-1 Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the switch ping the IP address (in the field to the left).
Ethernet Port Test	From the **Port** drop-down list box, select a port number and click **Port Test** to perform internal loopback test.

Chapter 26 Syslog

This chapter explains the syslog screens.

26.1 Syslog

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 26-1 Syslog Severity Levels

NUMERICAL CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

26.2 Syslog Setup

Click **Management** and then **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

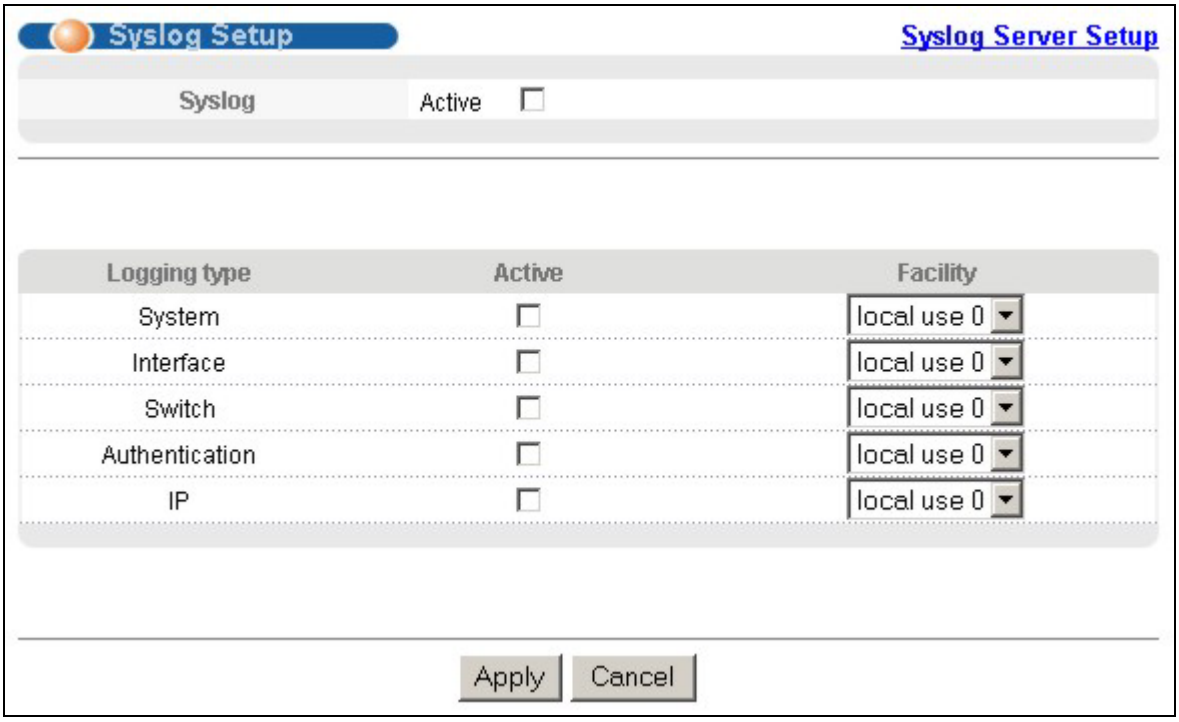


Figure 26-1 Syslog Setup

The following table describes the labels in this screen.

Table 26-2 Syslog Setup

LABEL	DESCRIPTION
Syslog	Select this check box to turn on syslog (system logging) and then configure the syslog settings.
Logging type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes back to the device.
Cancel	Click **Cancel** to begin configuring this screen afresh.

26.3 Syslog Server Setup

Click **Management** and then **Syslog** in the navigation panel to display the **Syslog Setup** screen. Click the **Syslog Server Setup** link to open the following screen. Use this screen to configure a list of external syslog servers.

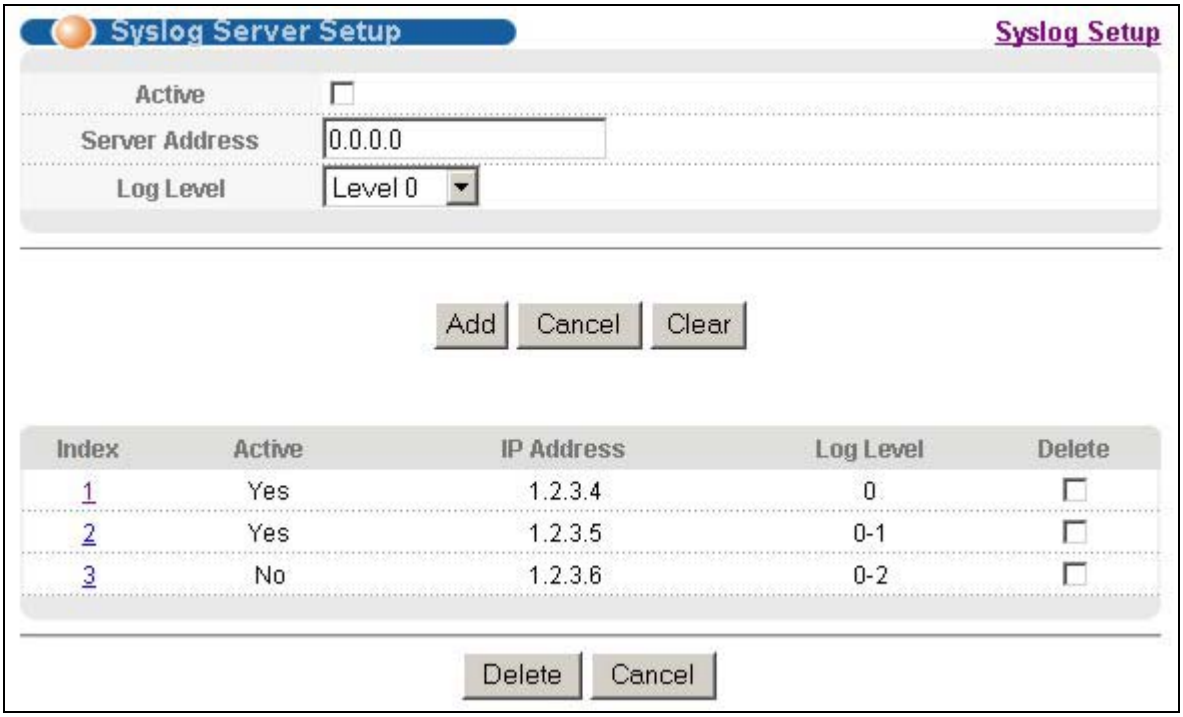


Figure 26-2 Syslog Server Setup

The following table describes the labels in this screen.

Table 26-3 Syslog Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes back to the device. The entry displays in the table below.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.

Table 26-3 Syslog Server Setup

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.

Chapter 27
Cluster Management

This chapter introduces cluster management.

27.1 Introduction to Cluster Management

Cluster Management[1] allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 27-1 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager switch.

In the following example, switch A in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

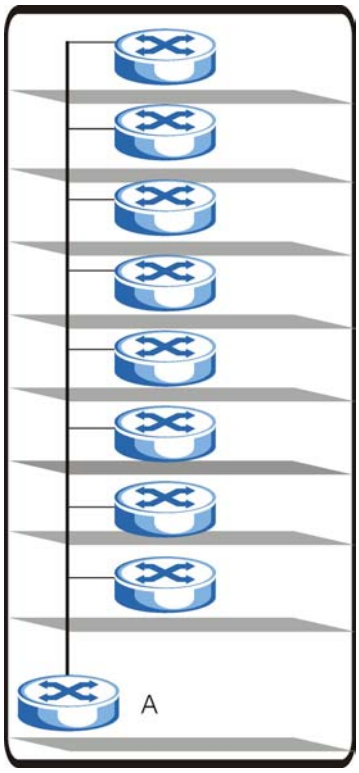


Figure 27-1 Clustering Application Example

[1] Cluster management may also be referred to as "iStacking" in other ZyXEL documentation.

27.2 Cluster Management Status

Click **Management** in the navigation panel and then **Cluster Management** to display the following screen.

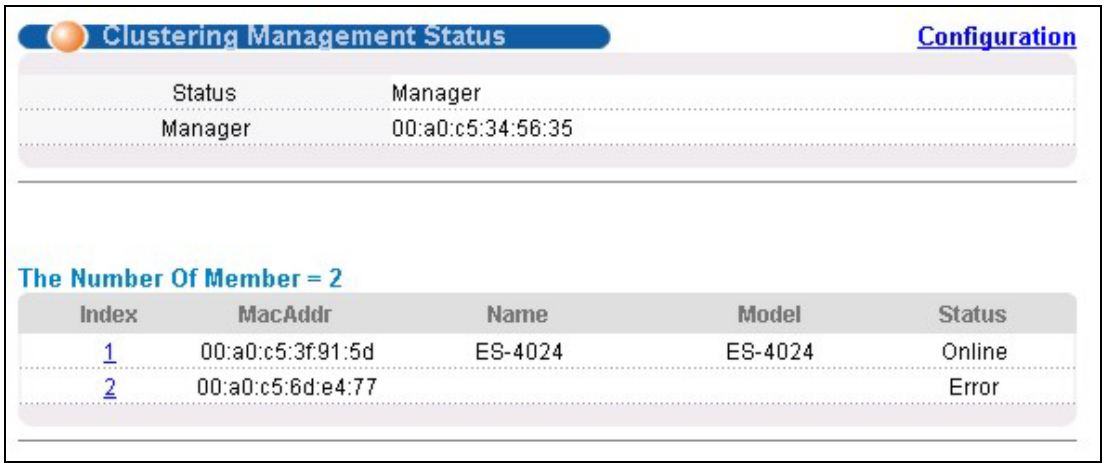


Figure 27-2 Cluster Management Status

The following table describes the labels in this screen.

Table 27-2 Cluster Management Status

LABEL	DESCRIPTION
A cluster can only have one manager.	
Status	This field displays the role of this switch within the cluster. o **Manager** o **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) o **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC Address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see *Figure 27-3*).
MacAddr	This is the cluster member switch's hardware MAC Address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.

Table 27-2 Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays: o **Online** (the cluster member switch is accessible) o **Error** (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) o **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down).

27.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different (see *Figure 27-3*).

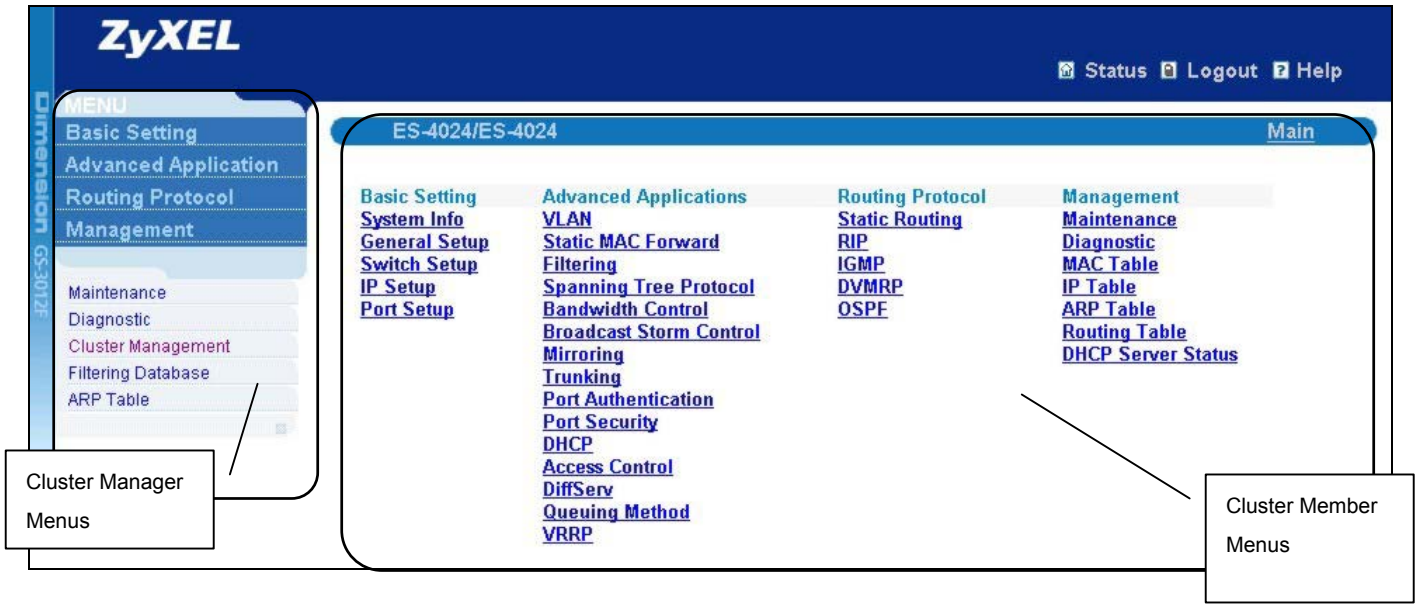


Figure 27-3 Cluster Member Web Configuration Screen

Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

```
C:\> ftp <Cluster Manager IP address>
Connected to 192.168.0.1.
220 GS-3012F FTP version 1.0 ready at Thu Jan  1 00:31:12 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3075006 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-13-49-00-00-02
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-13-49-00-00-02
226 File sent OK
ftp: 296 bytes received in 0.01Seconds 19.73Kbytes/sec.
ftp> put 360ABM0.bin fw-00-13-49-00-00-02
ftp> bye
```

Figure 27-4 Example: Uploading Firmware to a Cluster Member Switch

The following table explains some of the FTP parameters.

Table 27-3 FTP Upload to Cluster member Example

FTP PARAMETER	DESCRIPTION
User name	Press [ENTER]
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
fw-00-13-49-00-00-02	The cluster member switch's firmware name as seen in the cluster manager switch.
config-00-13-49-00-00-02	The cluster member switch's configuration file name as seen in the cluster manager switch.
360ABM0.bin	The name of the firmware file you want to upload to the cluster member switch.

27.3 Configuring Cluster Management

Click **Configuration** from the **Cluster Management** screen to display the next screen.

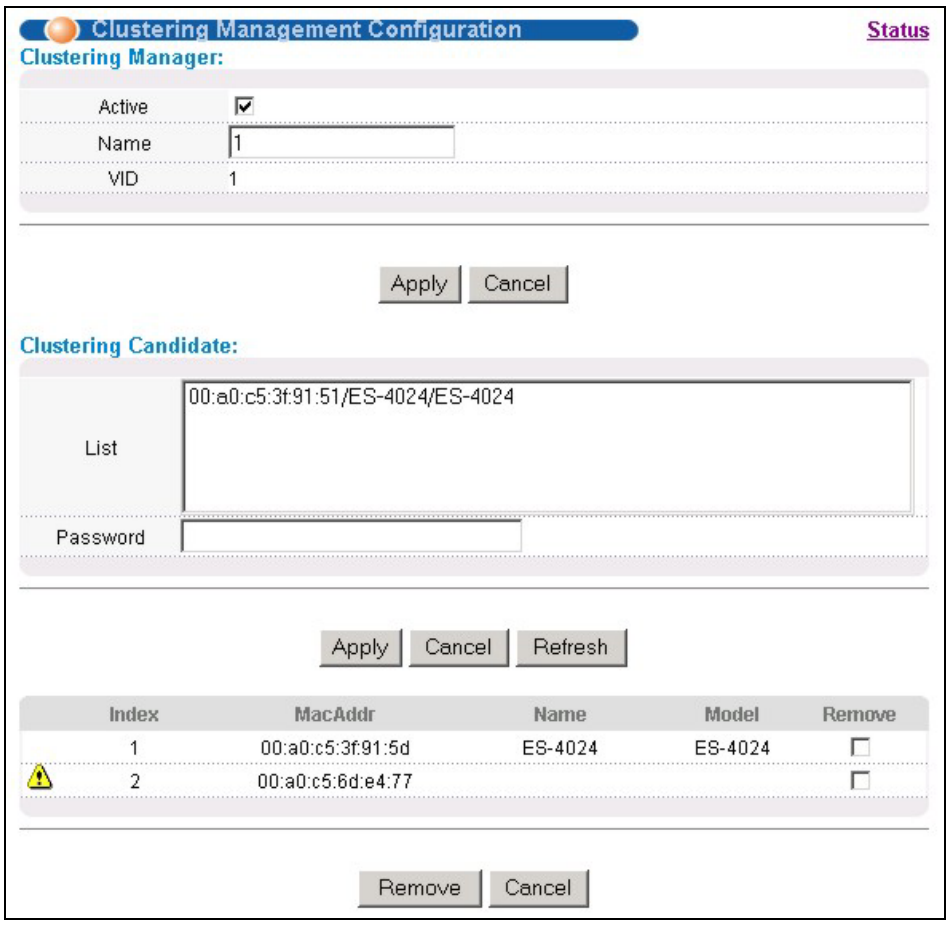


Figure 27-5 Configuring Cluster Management

The following table describes the labels in this screen.

Table 27-4 Configuring Cluster Management

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager.** You may use up to 32 printable characters (no spaces are allowed).
VID	This is the Management VLAN ID and is only applicable if the switch is set to **802.1Q** VLAN. All switches must be in the same management VLAN group to belong to the same cluster. Switches that are not in the same management VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save these changes to the switch.

Table 27-4 Configuring Cluster Management

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon ( ) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Apply	Click **Apply** to save these changes to the switch.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the devices selected for clustering.	
Index	This is the index number of a cluster member switch.
MAC Address	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.

Chapter 28 MAC Table

This chapter introduces MAC Table.

28.1 Introduction to MAC Table

The MAC table shows how frames are forwarded or filtered across the switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

The switch uses the Filtering Database to determine how to forward frames. See the following figure.

1. The switch examines a received frame and learns the port on which this source MAC address came.
2. The switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the Filtering Database.
   - If the switch has already learned the port for this MAC address, then it forwards the frame to that port.
   - If the switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
   - If the switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

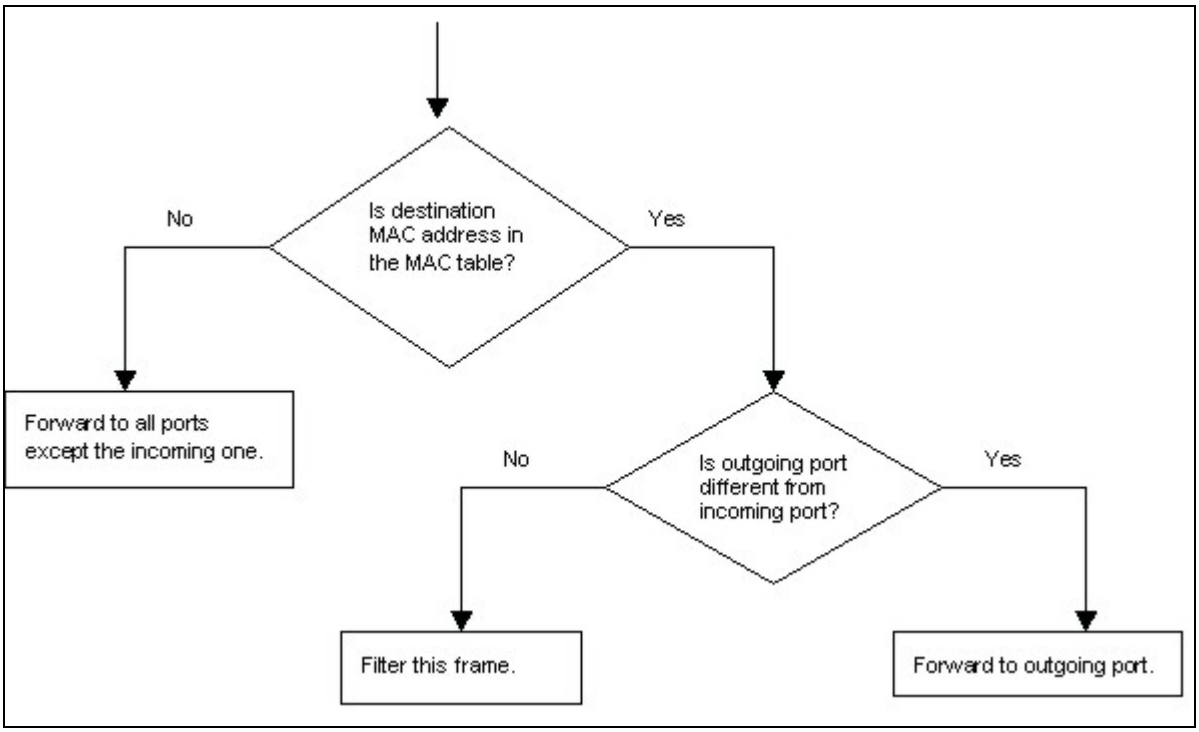


Figure 28-1 MAC Table Flowchart

28.2 Viewing MAC Table

Click **Management** in the navigation panel and then **MAC Table** to display the following screen.

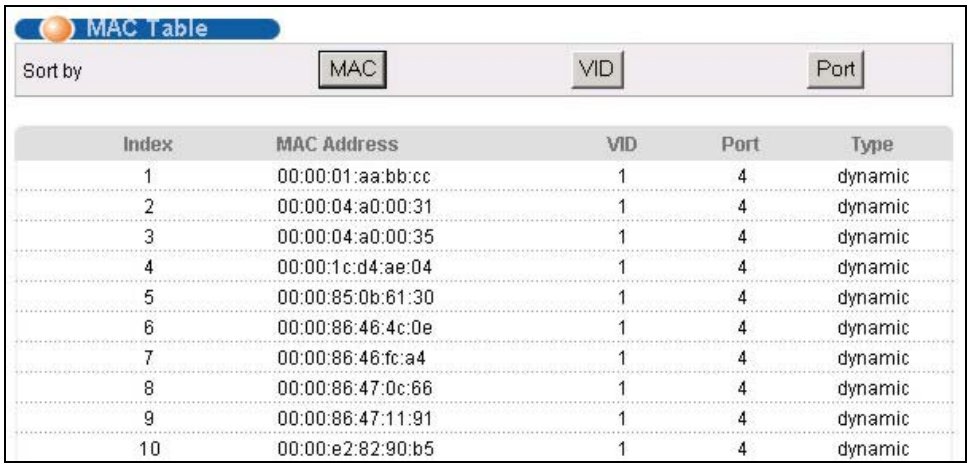


Figure 28-2 MAC Table

The following table describes the labels in this screen.

Table 28-1 MAC Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

Chapter 29 ARP Table

This chapter introduces ARP Table.

29.1 Introduction to ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

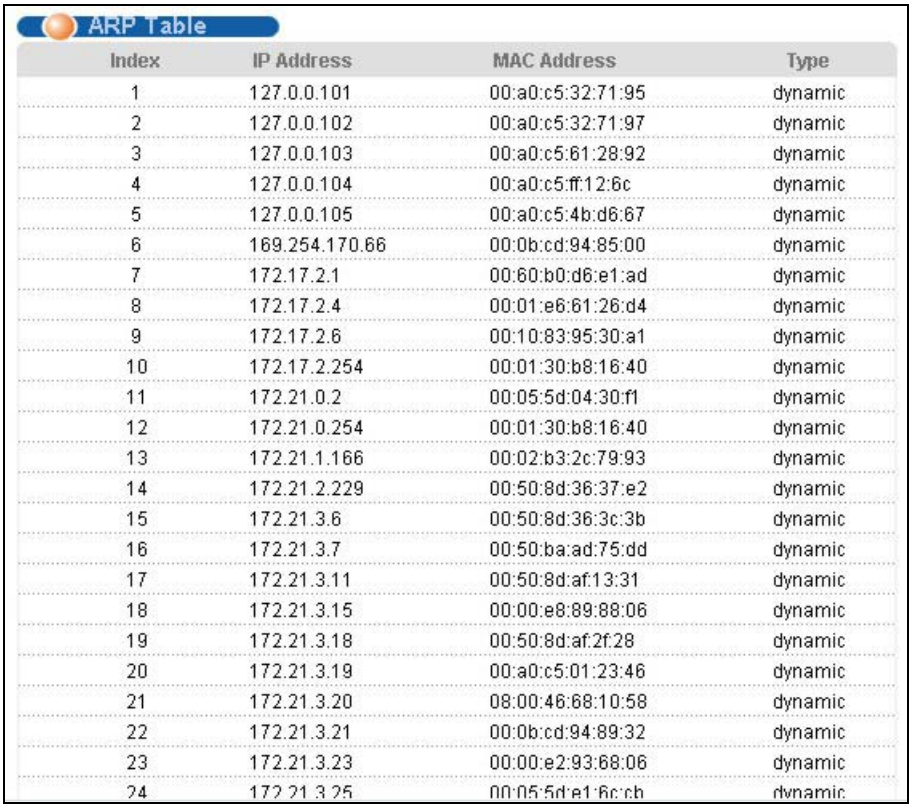
29.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

29.2 Viewing ARP Table

Click **Management** in the navigation panel and then **ARP Table** to open the following screen. The ARP table can hold up to 500 entries.



ARP Table

Index	IP Address	MAC Address	Type
1	127.0.0.101	00:a0:c5:32:71:95	dynamic
2	127.0.0.102	00:a0:c5:32:71:97	dynamic
3	127.0.0.103	00:a0:c5:61:28:92	dynamic
4	127.0.0.104	00:a0:c5:ff:12:6c	dynamic
5	127.0.0.105	00:a0:c5:4b:d6:67	dynamic
6	169.254.170.66	00:0b:cd:94:85:00	dynamic
7	172.17.2.1	00:60:b0:d6:e1:ad	dynamic
8	172.17.2.4	00:01:e6:61:26:d4	dynamic
9	172.17.2.6	00:10:83:95:30:a1	dynamic
10	172.17.2.254	00:01:30:b8:16:40	dynamic
11	172.21.0.2	00:05:5d:04:30:f1	dynamic
12	172.21.0.254	00:01:30:b8:16:40	dynamic
13	172.21.1.166	00:02:b3:2c:79:93	dynamic
14	172.21.2.229	00:50:8d:36:37:e2	dynamic
15	172.21.3.6	00:50:8d:36:3c:3b	dynamic
16	172.21.3.7	00:50:ba:ad:75:dd	dynamic
17	172.21.3.11	00:50:8d:af:13:31	dynamic
18	172.21.3.15	00:00:e8:89:88:06	dynamic
19	172.21.3.18	00:50:8d:af:2f:28	dynamic
20	172.21.3.19	00:a0:c5:01:23:46	dynamic
21	172.21.3.20	08:00:46:68:10:58	dynamic
22	172.21.3.21	00:0b:cd:94:89:32	dynamic
23	172.21.3.23	00:00:e2:93:68:06	dynamic
24	172.21.3.25	00:05:5d:e1:6c:cb	dynamic

Figure 29-1 ARP Table

The following table describes the labels in this screen.

Table 29-1 ARP Table

LABEL	DESCRIPTION
Index	This is the ARP Table entry number.
IP Address	This is the learned IP address of a device connected to a switch port with corresponding MAC address below.
MAC Address	This is the MAC address of the device with corresponding IP address above.
Type	This shows whether the MAC address is dynamic (learned by the switch) or static (manually entered in **Static MAC Forwarding**).

Part VII

Commands

This part gives information on the Command Line Interface (CLI).

Chapter 30 Introducing the Commands

This chapter introduces the commands and gives a summary of commands available.

30.1 Overview

In addition to the web configurator, you can use line commands to configure the switch. Use line commands for advanced switch diagnosis and troubleshooting. If you have problems with your switch, customer support may request that you issue some of these commands to assist them in troubleshooting.

30.1.1 Switch Configuration File

When you configure the switch using either the CLI or web configurator, the settings are saved as a series of commands in a configuration file on the switch. You can perform the following with a configuration file:

- Back up switch configuration once the switch is set up to work in your network.
- Restore switch configuration.
- Use the same configuration file to set all switches (of the same model) in your network to the same settings.

You may also edit a configuration file using a text editor.

Make sure you use valid commands. The switch rejects configuration files with invalid or incomplete commands.

30.2 Accessing the CLI

You can use a direct console connection or Telnet to access the CLI on the switch.

The switch automatically logs you out of the management interface after five minutes of inactivity. If this happens to you, simply log back in again.

30.2.1 Access Priority

- You can only access the CLI with the administrator account (the default username is **admin** and password is **1234**).
- By default, only one concurrent access to the CLI is allowed via either the console port or Telnet. Console port access has higher priority.
- Use the `configure multi-login` command in the configuration mode to allow multiple concurrent logins. However, no more than five concurrent login sessions are allowed.

30.2.2 The Console Port

Connect to the switch's console port using terminal emulation software configured to the following settings:

- VT100 terminal emulation
- 9600 bps
- No parity
- 8 data bits
- 1 stop bit
- No flow control

Initial Screen

When you turn on your switch, it performs several internal tests as well as line initialization. You can view the initialization information using the console port. After the initialization, the login screen displays (refer to *Section 30.3*).

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
initialize mgmt, ethernet address: 00:13:49:00:00:01
initialize switch, ethernet address: 00:13:49:00:00:02
Initializing switch unit 0...
Press ENTER to continue...
```

Figure 30-1 Initial Console Port Screen

30.2.3 Telnet

Use the following steps to telnet into your switch.

1. For local management, connect your computer to the RJ-45 management port (labeled **MGMT**) on the switch.
2. Make sure your computer IP address and the switch IP address are on the same subnet. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type `telnet 192.168.1.1` (the default management IP address) and click **OK**.
3. A login screen displays (refer to Section 30.3).

30.3 The Login Screen

After you have successfully established a connection to the switch using a direct console connection or Telnet, a login screen displays as shown below. For your first login, enter the default administrator login username "admin" and password "1234".

```
Enter User Name : admin

Enter Password : XXXX
```

Figure 30-2 CLI: Login Screen

30.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in `courier new` font.
- The required fields in a command are enclosed in angle brackets <>, for instance, `ping <ip>` means that you must specify an IP number for this command.
- The optional fields in a command are enclosed in square brackets `[]`; for instance, `configure snmp-server [contact <system contact>] [location <system location>]` means that the `contact` and `location` fields are optional.
- "Command" refers to a command used in the command line interface (CI command).
- The `|` symbol means "or".
- The entry `<cr>` in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up (▲) or down (▼) arrow key to scroll through the command history list.
- The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the switch automatically display the full command. For example, if you enter `config` and press [TAB], the full command of `configuration` automatically displays.
- Each interface refers to an Ethernet port on the switch. Commands configured after the interface command correspond to those ports.
- Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

30.5 Getting Help

The system includes a help facility to provide you with the following information about the commands:

- List of available commands under a command group.
- Detailed descriptions of the commands.

30.5.1 List of Available Commands

Enter `help` to display a list of available commands and the corresponding sub commands.
Enter `?` to display a list of commands you can use.

```
ras> help
  Commands available:

  help
  exit
  history
  enable
  show ip <cr>
  show hardware-monitor <C|F>
  show system-information
  ping help
  ping <ip> [vlan <vlan-id>][..]
  ping <ip> <cr>
  traceroute help
  traceroute <ip> [vlan <vlan-id>][..]
  traceroute <ip> <cr>
  ssh <1|2> <[user@]dest-ip> [command </>]
  ssh <1|2> <[user@]dest-ip> <cr>
ras>
```

Figure 30-3 CLI Help: List of Commands: Example 1

```
ras> ?
    enable                  Turn on privileged commands
    exit                    Exit from the EXEC
    help                    Description of the interactive help system
    history                 Show a list of previously run commands
    ping                    Exec ping
    show                    Show system information
    ssh                     SSH client
    traceroute              Exec traceroute
ras>
```

Figure 30-4 CLI Help: List of Commands: Example 2

30.5.2 Detailed Command Information

Enter `<command> help` to display detailed sub command and parameters.
Enter `<command> ?` to display detailed help information about the sub commands and parameters.

```
ras> ping help
  Commands available:

  ping <ip|host-name>
    <
      [ in-band|out-of-band|vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
ras>
```

Figure 30-5 CLI Help: Detailed Command Information: Example 1

```
ras> ping ?
    <ip|host-name>          destination ip address
    help                    Description of ping help
```

Figure 30-6 CLI: Help: Detailed Command Information: Example 2

30.6 Command Modes

There are three CLI command modes: User, Enable and Configure.

When you first log into the CLI, the initial command mode is the User mode. The User mode commands are a subset of the Enable mode commands. The User mode command prompt ends with an angle bracket (>).

To enter Enable (or privileged) mode, type `enable` and enter a password when prompted (the default is 1234). When you enter the Enable mode, the command prompt changes to the pound sign (#).

To enter the configuration mode, type `configuration` or `config`. The Configure mode command prompt consists of the word `config` and the pound sign (#). There are two sub configuration modes: VLAN and interface. To enter config-vlan mode, type `vlan` followed by a number (between 1 to 4094). For example, `vlan 10`. To enter config-interface mode, enter `interface port-channel` followed by a port number. For example, `interface port-channel 10`.

Enter `exit` to quit from the current mode or log out from the CLI.

30.7 Using Command History

The switch keeps a list of up to 256 commands(s) you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER]. Use the history command to display the list of commands.

```
ras> history
  enable
  exit
  show ip
  history
ras>
```

Figure 30-7 CLI: History Command Example

30.8 Saving Your Configuration

After you set the switch settings with the configuration commands, use the `write memory` command to save the changes permanently.

```
ras# write memory
```

Figure 30-8 CLI: write memory

The `write memory` command is not available in User mode.

You must save your changes after each CLI session. All unsaved configuration changes are lost once you restart the switch.

30.8.1 Logging Out

In User mode, enter the `exit` command to log out of the CLI.

30.9 Command Summary

The following sections summarize the commands available in the switch together with a brief description of each command. Commands listed in the tables are in the same order as they are displayed in the CLI. See the related section in the User's Guide for more background information.

30.9.1 User Mode

The following table describes the commands available for User mode.

Table 30-1 Command Summary: User Mode

COMMAND			DESCRIPTION
`enable`			Accesses Enable (or privileged) mode.
`exit`			Logs out from the CLI.
`help`			Displays help information.
`history`			Displays a list of previously command(s) that you have executed. The switch stores up to 256 commands in history.

`ping`	`<IP|host-name>`
	`[<in-band|out-of-band|vlan <vlan-id>]`
	`[size <0-1472>]`
	`[-t]`
			Sends a Ping request to an Ethernet device.

`show`	`hardware-monitor <C|F>`		Displays current hardware monitor information with the specified temperature unit (Celsius **C** or Fahrenheit **F**).
	`ip`		Displays IP related information.
	`system-information`		Displays general system information.
`ssh`	`<1|2> <[user@]dest-ip>`		Connects to an SSH server with the specified SSH version.

`traceroute`	`<ip|host-name>`
	`[in-band|out-of-band|vlan <vlan-id>]`
	`[ttl <1-255>]`
	`[wait <1-60>]`
	`[queries <1-10>]`
			Determines the path a packet takes to a device.

30.9.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 30-2 Command Summary: Enable Mode

COMMAND			DESCRIPTION
baudrate	<1|2|3|4|5>		Changes the console port speed. Choices are 1 (38400), 2 (19200), 3(9600), 4 (57600) and 5 (115200).
boot	config <index>		Restarts the system with the specified configuration file (1 or 2).
configure			Accesses Configuration mode.
copy	running-config tftp <ip> <remote-file>		Backs up running configuration to the specified TFTP server with the specified file name.
	tftp	config <index> <ip> <remote-file>	Restores configuration with the specified filename from the specified TFTP server.
		flash <ip> <remote-file>	Restores firmware via TFTP.
disable			Exits Enable (or privileged) mode.
enable			Accesses Enable (or privileged) mode.
erase	running-config		Resets to the factory default settings.
exit			Exits Enable (or privileged) mode.
help			Displays help information.
history			Displays a list of command(s) that you have previously executed.
igmp-flush			Removes all IGMP information.
kick tcp	<Session ID>		Drops a TCP session.
mac-flush			Clears the MAC address table.
	<port-num>		Removes all learned MAC address on the specified port(s).
no	arp		Flushes the ARP (Address Resolution Protocol) table.
	interface <port-number>		Clears the interface status of the specified port(s).
	logging		Clears the system log.
ping	<ip|host-name> [<in-band|out-of-band|vlan <vlan-id>] [size <0-1472>] [-t]		Sends a Ping request to an Ethernet device.
reload	config <index>		Restarts the system with the specified configuration file.
show			

Table 30-2 Command Summary: Enable Mode

COMMAND			DESCRIPTION
	classifier		Displays all classifier related information.
		<name>	Displays the specified classifier related information.
	cluster		Displays cluster management status.
		candidates	Displays cluster candidate information.
		member	Displays the status of the cluster member(s).
		member config	Displays the configuration of the cluster member(s).
		member mac <mac-addr>	Displays the MAC address of the cluster member(s).
	garp		Displays GARP information.
	hardware-monitor <C|F>		Displays current hardware monitor information with the specified temperature unit (Celsius **C** or Fahrenheit **F**).
	https		Displays the HTTPS information.
		certificate	Displays the HTTPS certificates.
		key <rsa|dsa>	Displays the HTTPS key.
		session	Displays current HTTPS session(s).
		timeout	Displays the HTTPS session timeout.
	igmp-filtering profile		Displays IGMP filter profile settings.
	igmp-snooping		Displays IGMP snooping settings.
	interface <port-number>		Displays current interface status.
	interfaces config <port-list>		Displays current interface configuration.
		bandwidth-control	Displays bandwidth control settings.
		bstorm-control	Displays broadcast storm control settings.
		egress	Displays outgoing port information.
		igmp-immediate-leave	Displays IGMP immediate leave settings.
		igmp-filtering	Displays IGMP filter profile settings.
		igmp-group-limited	Displays IGMP group settings.

Table 30-2 Command Summary: Enable Mode

COMMAND			DESCRIPTION
		igmp-query-mode	Displays IGMP query mode settings on the port(s).
	ip		Displays IP related information.
		TCP	Displays the switch's current TCP sessions.
		UDP	Displays the switch's current UDP sessions.
	ip arp		Displays the ARP table.
	ip route		Displays IP routing information.
	ip route static		Displays IP static route information.
	lacp		Link Aggregation Control Protocol.
	logging		Displays system logs.
	loginPrecedence		Displays login precedence settings.
	logins		Displays login account information.
	mac	address-table static	Displays static MAC address table. You can sort by MAC address, VID or port.
		address-table <all> <mac|vid|port>	Displays MAC address table. You can sort by MAC address, VID or port.
		address-table count	Displays the total number of MAC addresses in the MAC address table.
	mac-aging-time		Displays MAC learning aging time.
	multi-login		Displays multi-login information
	multicast		Displays multicast settings.
	mvr		Displays all MVR (Multicast VLAN Registration) settings.
		<vlan-id>	Displays specified MVR information.
	plt		Displays Packet Loop Test (PLT).
	policy		Displays all policy related information.
		<name>	Displays the specified policy related information.
	port-access-authenticator		Displays all port authentication settings.
		<port-list>	Displays port authentication settings on the specified port(s).
	port-security		Displays all port security settings.

Table 30-2 Command Summary: Enable Mode

COMMAND			DESCRIPTION
		<port-list>	Displays port security settings on the specified port(s).
	radius-server		Displays RADIUS server settings.
	remote-management		Displays all secured client information.
		<index>	Displays the specified secured client information.
	running-config		Displays current operating configuration.
	service-control		Displays service control settings.
	snmp-server		Displays SNMP settings.
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.
	ssh		Displays general SSH settings.
		key <rsa1|rsa|dsa>	Displays the SSH public and private keys
		known-hosts	Displays known SSH hosts information.
		session	Displays current SSH session(s).
	system-information		Displays general system information.
	time		Displays current system time and date.
	timesync		Displays time server information.
	trunk		Displays link aggregation information.
	vlan		Displays the status of all VLANs.
		<vlan-id>	Displays the status of the specified VLAN.
	vlan1q	gvrp	Displays GVRP setting.
		port-isolation	Displays port isolation setting.
ssh	<1|2> <[user@]dest-ip>		Connects to an SSH server with the specified SSH version.
traceroute	<ip|host-name> [in-band|out-of-band|vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]		Determines the path a packet takes to a device.
write	memory		Saves the configuration to the configuration file the switch is currently using.
		<index>	Saves the configuration to the specified configuration file on the switch.

30.9.3 Configure Mode

The following table lists the commands in Configuration (or Config) mode.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
admin-password	<pw-string> <confirm-string>		Changes the administrator password.
bandwidth-control			Enables bandwidth control.
bcp-transparency			Enables Bridge Control Protocol Transparency.
classifier	<name> <[packet-format <802.3untag|802.3tag| EtherIIuntag|EtherIItag>] [priority <0-7>] [vlan <vlan-id>] [ethernet-type <ether-num|ip|ipx| arp|rarp| appletalk|decnet| sna|netbios|dlc>] [source-mac <src-mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [dscp <0-63>] [ip-protocol <protocol-num|tcp|udp|icmp|egp|ospf|rsvp|igmp| igp|pim|ipsec> [establish-only]] [source-ip <src-ip-addr> [mask-bits <mask-bits>]] [source-socket <socket-num>] [destination-ip <dest-ip-addr> [mask-bits <mask-bits>]] [destination-socket <socket-num>] [inactive]>		Configures a classifier. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
cluster	<vlan-id>		Sets the cluster management VLAN ID.
	member <mac-address> password <password-str>		Sets the cluster member switch's hardware MAC address and password.
	name <cluster name>		Configures a name to identify the cluster manager
	rcommand <mac-address>		Logs into a cluster member switch.
default-management	<in-band|out-of-band>		Specifies through which traffic flow the switch is to send packets.
dhcp-relay			Enables DHCP relay.
	helper-address <svr_ip> [svr2_ip] [svr3_ip]		Sets the IP addresses of up to 3 DHCP servers.
	information		Allows the switch to add system name to agent information.
	option		Allows the switch to add DHCP relay agent information.
exit			Returns you to User mode.
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.
help			Displays help information.
history			Displays a list of previously command(s) that you have executed.
hostname	<name_string>		Sets the switch's name for identification purposes. **Spaces are allowed in the CLI only when the system name is in "quotation marks".** **Eg:** <config># hostname "GS-3012 a"
https	cert-regeneration <rsa|dsa>		Re-generates a certificate.
	timeout <0-65535>		Sets the HTTPS timeout period.
igmp-filtering			Enables IGMP filtering on the switch.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
	profile <name> start-address <ip> end-address <ip>		Sets the range of multicast address(es) in a profile.
igmp-snooping			Enables IGMP snooping.
	unknown-multicast-frame <drop|flooding>		Sets how to treat traffic from unknown multicast group.
interface	port-channel <port-list>		Enables a port or a list of ports for configuration. See *Section 30.9.5* for more details.
ip	address	<ip> <mask>	Sets the IP address and subnet mask of the out-of-band management port.
	address default-gateway	<ip>	Sets the default gateway's IP address for the out-of-band management port.
	name-server	<ip>	Sets the IP address of a domain name server.
	route	<ip> <mask> <next-hop-ip>	Creates a static route.
		<ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]	Sets the metric of a static route or deactivates a static route.
lacp			Enables Link Aggregation Control Protocol (LACP).
	system-priority	<1-65535>	Sets the priority of an active port using LACP.
loginPrecedence	<LocalOnly | LocalRADIUS | RADIUSOnly>		Select which database the switch should use (first) to authenticate a user.
logins	username <name> password <pwd>		Configures up to four read-only login accounts.
mac-aging-time	<10-3000>		Sets learned MAC aging time.
mac-filter	name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both>		Configures a static MAC address port filtering rule.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
	name <name> mac <mac-addr> vlan <vlan-id> drop <src/dst/both> inactive		Disables a static MAC address port filtering rule.
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Configures a static MAC address forwarding rule.
	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive		Disables a static MAC address forwarding rule.
mirror-port			Enables port mirroring.
	<port-num>		Enables port mirroring on a specified port.
mode	zynos		Changes the CLI mode to the ZyNOS format.
multi-login			Enables multi-login.
mvr <vlan-id>			Enters the MVR (Multicast VLAN Registration) configuration mode. See *Section 30.9.6* for more information.
no			
	bandwidth-control		Disables bandwidth control.
	bcp-transparency		Disables bridging control protocols such as STP.
	classifier	<name>	Disables the classifier. Each classifier has one rule. If you disable a classifier you cannot use policy rule related information.
		<name> inactive	Enables a classifier.
	cluster		Disables cluster management on the switch.
		member <mac-address>	Removes the cluster member.
	dhcp-relay		Disables DHCP relay.
		information	System name is not appended to option 82 information field.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
		option	Disables the relay agent information option 82.
	https	timeout	Resets the session timeout to the default of 300 seconds.
	igmp-filtering		Clears the IGMP filtering settings on the switch.
		profile <name>	Deletes the IGMP filtering profile.
		profile <name> start-address <ip> end-address <ip>	Deletes a rule in the IGMP filtering profile.
	igmp-snooping		Disables IGMP snooping.
	ip		Sets the management IP address to the default value.
		route <ip> <mask> inactive	Enables a specified IP static route.
		route <ip> <mask>	Removes a specified IP static route.
	lacp		Disables the link aggregation control protocol (dynamic trunking) on the switch.
	logins	<name>	Disables login access to the specified name.
	mac-filter	mac <mac-addr> vlan <vlan-id> inactive	Enables the specified MAC-filter rule.
		mac <mac-addr> vlan <vlan-id>	Disables the specified MAC filter rule.
	mac-forward	mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive	Enables the specified MAC address, belonging to a VLAN group (if any) forwarded through an interface(s).
		mac <mac-addr> vlan <vlan-id> interface <interface-id>	Removes the specified MAC forwarding entry, belonging to a VLAN group (if any) forwarded through an interface(s).
	mirror-port		Disables port mirroring on the switch.
	multi-login		Disables another administrator from logging into Telnet or the CLI.
	mvr	<vlan-id>	Disables MVR on the switch.
	policy	<name>	Deletes the policy. A policy sets actions for classifier traffic.
		<name> inactive	Enables a policy.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
	port-access-authenticator		Disables port authentication on the switch.
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).
		<port-list>	Disables authentication on the listed ports.
	port-security		Disables port security on the switch.
		<port-list>	Disables port security on the specified ports.
		<port-list> learn inactive	Enables MAC address learning on the specified ports.
	radius-server		Disables the use of authentication from the RADIUS server.
	remote-management	<index>	Clears a secure client set entry from the list of secure clients.
		<index> service < [telnet][ftp][http] [icmp][snmp][ssh][https]>	Disables a secure client set entry number from using the selected remote management service(s).
		<name> inactive	Enables a policy.
	service-control	ftp	Disables FTP access to the switch.
		http	Disables web browser control to the switch.
		https	Disables secure web browser access to the switch.
		icmp	Disables ICMP access to the switch such as pinging and tracerouting.
		snmp	Disables SNMP management.
		ssh	Disables SSH (Secure Shell) server access to the switch.
		telnet	Disables telnet access to the switch.
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.
	spanning-tree		Disables STP.
		<port-list>	Disables STP on listed ports.
	ssh	key <rsa1|rsa|dsa>	Disables the secure shell server encryption key. Your switch supports SSH versions 1 and 2 using RSA and DSA authentication.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
		known-hosts	Removes all remote hosts.
		known-hosts <host-ip> <cr>	Removes the specified remote hosts from the list of all known hosts.
		known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).
	storm-control		Disables broadcast storm control.
	syslog		Disables syslog.
		server <ip>	Disables a syslog server entry.
		server <ip> inactive	Enables a syslog server entry.
		type <system, interface, switch, authentication, ip>	Sets the device to not generate a category of logs.
	timesync		Disables the time setting on the timeserver.
	trunk	<T1|T2|T3|T4|T5|T6> lacp	Disables LACP in the specified trunk group.
		<T1|T2|T3|T4|T5|T6> interface <port-list>	Removes ports from the specified trunk group.
		<T1|T2|T3|T4|T5|T6> <cr>	Disables the specified trunk group.
	vlan	<vlan-id>	Deletes the static VLAN entry.
	vlan1q	gvrp	Disables GVRP on the switch.
		port-isolation	Disables port isolation.
	wfq fe-spq		Sets the switch to use WFQ to service all queues for the 10/100Mbps Ethernet port.
password			Change the password for Enable mode.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
policy	<name> classifier <classifier-list> < [vlan<vlan-id>] [egress-port <port-num>] [priority <0-7>] [dscp <0-63>] [tos <0-7>] [bandwidth <bandwidth>] [egress-mask <port-list>] [outgoing-packet-format <tagged|untagged>] [out-of-profile-dscp <0-63>] [forward-action <drop|forward|egressmask>] [queue-action <prio-set|prio-queue|prio-replace-tos>] [diffserv-action <diff-set-tos|diff-replace-priority|diff-set-dscp>] [outgoing-mirror] [outgoing-eport] [outgoing-non-unicast-eport] [outgoing-set-vlan] [metering] [out-of-profile-action <[change-dscp][drop][forward] [set-drop-prec]>] [inactive]>		Configures a policy. A classifier distinguishes traffic into flows based on the configured criteria. A policy rule ensures that a traffic flow gets the requested treatment in the network.
port-access-authenticator			Enables 802.1x authentication on the switch.
	<port-list>		Enables 802.1x authentication on the specified port(s).
	<port-list> reauthenticate		Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
	<port-list> reauth-period <reauth-period>		Specifies how often a client has to re-enter the username and password to stay connected to the specified port(s).
port-security			Enables port security on the switch.
	<port-list>		Enables the port security feature on the specified port(s).
	<port-list> learn inactive		Disables MAC address learning on the specified port(s).
	<port-list> address-limit <number>		Limits the number of (dynamic) MAC addresses that may be learned on a port.
	<port-list> MAC-freeze		Disables MAC address learning and enables port security. **All previously learned dynamic MAC addresses are saved to the static MAC address table.**
queue	level <0-7> priority <0-7>		Sets the priority level-to-physical queue mapping.
radius-server	host <ip> [acct-port <socket-number>] [key <key-string>]		Sets the IP address of the external RADIUS server, UDP port and shared key.
remote-management	<index>		Enables a specified secured client set.
	<index> start-addr <ip> end-addr <ip> service <[telnet] [ftp][http][icmp] [snmp][ssh][https]>		Specifies a group of trusted computer(s) from which an administrator may use a service to manage the switch.
service-control	ftp <socket-number>		Allows FTP access on the specified service port.
	http <socket-number> <timeout>		Allows HTTP access on the specified service port and defines the timeout period.
	https <socket-number>		Allows HTTPS access on the specified service port.
	icmp		Allows ICMP access to the switch such as pinging and tracerouting.
	snmp		Allows SNMP management.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
	ssh <socket-number>		Allows SSH access on the specified service port.
	telnet <socket-number>		Allows Telnet access on the specified service port.
snmp-server	[contact <system contact>] [location <system location>]		Sets the geographic location and the name of the person in charge of this switch.
	get-community <property>		Sets the get community.
	set-community <property>		Sets the set community.
	trap-community <property>		Sets the trap community.
	trap-destination <ip>		Sets the IP addresses of up to four stations to send your SNMP traps to.
spanning-tree			Enables STP on the switch.
	<port-list>		Enables STP on a specified port.
	<port-list> priority <0-255>		Sets the priority for a specified port.
	<port-list> path-cost <1-65535>		Sets the STP path cost for a specified port.
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.
	priority <0-61440>		Sets the bridge priority of the switch.
spq			Sets the queuing method to SPQ (Strictly Priority Queuing).
ssh	known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa> <key>		Adds a remote host to which the switch can access using SSH service.
storm-control			Enables broadcast storm control on the switch.
syslog	<cr>		Enables syslog.
	server <ip>	inactive	Disables a syslog server entry.
		level <0-7>	Sets which severity level(s) of logs are sent to this syslog server. A lower number is more critical.

Table 30-3 Command Summary: Configure Mode

COMMAND			DESCRIPTION
	type <system, interface, switch, authentication, ip>		Sets the device to generate a category of logs.
	type <system, interface, switch, authentication, ip>	facility <0-7>	Sets the facility (file) on the syslog server to which the switch sends a category of logs.
time	<Hour:Min:Sec>		Sets the time in hour, minute and second format.
	date <month/day/year>		Sets the date in year, month and day format.
	timezone <-1200|...|1200>		Selects the time difference between UTC (formerly known as GMT) and your time zone.
timesync	<daytime|time|ntp>		Sets the time server protocol.
	server <ip>		Sets the IP address of your time server.
trunk	<T1|T2|T3|T4|T5|T6>		Activates a trunk group.
	<T1|T2|T3|T4|T5|T6> interface <port-list>		Adds a port(s) to the specified trunk group.
	<T1|T2|T3|T4|T5|T6> lacp		Enables LACP for a trunk group.
	interface <port-list> timeout <lacp-timeout>		Defines the port number and LACP timeout period.
vlan <1-4094>			Enters the VLAN configuration mode. See *Section 30.9.4* for more information.
vlan-type	<802.1q|port-based>		Specifies the VLAN type.
vlan1q	gvrp		Allows VLAN groups beyond the local switch.
	port-isolation		Enables port isolation.

30.9.4 config-vlan Commands

The following table lists the config-vlan commands in configuration mode.

Table 30-4 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION
vlan <1-4094>			Creates a new VLAN group.
	exit		Leaves config-vlan mode.

Table 30-4 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION
	fixed <port-list>		Specifies the port(s) to be a permanent member of this VLAN group.
	forbidden <port-list>		Specifies the port(s) you want to prohibit from joining this VLAN group.
	help		Displays a list of available VLAN commands.
	inactive		Disables the specified VLAN.
	ip address		
		<ip-address> <mask>	Sets the IP address and subnet mask of the switch in the specified VLAN for packet loopback test.
		<ip-address> <mask> manageable	Allows the switch to be managed using this specified IP address.
		default-gateway <ip-address>	Sets a default gateway IP address for this VLAN.
		inband-default <ip-address> <mask>	Sets a static in-band IP address and subnet mask.
		inband-default dhcp-bootp	Sets the dynamic in-band IP address.
		inband-default dhcp-bootp release	Releases the dynamic in-band IP address.
		inband-default dhcp-bootp renew	Updates the dynamic in-band IP address.
	name <name-str>		Specifies a name for identification purposes.
	no	fixed <port-list>	Sets fixed port(s) to normal port(s).
		forbidden <port-list>	Sets forbidden port(s) to normal port(s).
		inactive	Enables the specified VLAN.
		ip address <ip-address> <mask>	Deletes the IP address and subnet mask from this VLAN.
		ip address default-gateway	Deletes the default gateway from this VLAN.

Table 30-4 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION
		`ip address inband-default dhcp-bootp`	Sets the default in-band interface to use a static IP address in this VLAN. The switch will use the default IP address of 0.0.0.0 if you do not configure a static IP address.
		`untagged <port-list>`	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.
	`normal <port-list>`		Specifies the port(s) to dynamically join this VLAN group using GVRP
	`untagged <port-list>`		Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.

30.9.5 interface Commands

The following commands are listed in configuration mode as "interface" switch commands; all are preceded with the command `interface`.

Table 30-5 Command Summary: Interface

COMMAND			DESCRIPTION
`interface port-channel <port-list>`			Enables a port or a list of ports for configuration.
	`bandwidth-limit`		Enables bandwidth limit on the switch.
		`cir <Kbps>`	Sets the guaranteed bandwidth allowed for incoming traffic on the port(s).
		`egress <Kbps>`	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).
		`ingress <Kbps>`	Sets the maximum bandwidth allowed for incoming traffic on the port(s).
		`pir <Kbps>`	Sets the maximum bandwidth allowed for incoming traffic on the port(s).
	`broadcast-limit`		Enables broadcast storm control limit on the switch.
		`<pkt/s>`	Sets how many broadcast packets the interface receives per second.

Table 30-5 Command Summary: Interface

COMMAND			DESCRIPTION
	bpdu-control	<peer|tunnel|discard|network>	Sets how Bridge Protocol Data Units (BPDUs) are used in STP port states.
	cable_diagnostics		Displays whether a cable is connected to the port (**good**) or not (**open**).
	dlf-limit		Enables the Destination Lookup Failure (DLF) limit.
		<pkt/s>	Sets the interface DLF limit in packets per second (pps).
	egress set	<port-list>	Sets the outgoing traffic port list for a port-based VLAN.
	exit		Exits from the interface configuration command set.
	flow-control		Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.
	frame-type	<all|tagged>	Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	gvrp		Enables this function to permit VLAN groups beyond the local switch.
	help		Displays a description of the interface commands.
	igmp-filtering profile <name>		Sets the IGMP filtering profile for this port.
	igmp-group-limited		Limits the number of multicast groups.
	igmp-group-limited number <number>		Sets the number of multicast groups this port is allowed to join.
	igmp-immediate-leave		Enables IGMP immediate leave on the port.
	igmp-querier-mode <auto|fixed|edge>		Sets the IGMP querier mode of a port. `auto` uses the port as an IGMP query port after it receives IGMP query packets. `fixed` always uses the port as an IGMP query port. `edge` stops the switch from using the port as an IGMP query port.
	inactive		Disables the specified interface on the switch

Table 30-5 Command Summary: Interface

COMMAND			DESCRIPTION
	ingress-check		Enables the device to discard incoming frames for VLANs that are not included in a port member set.
	intrusion-lock		Enables intrusion lock on a port and a port cannot be connected again after you disconnected the cable.
	mirror		Enables port mirroring in the interface.
		dir <ingress|egress|both>	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one or all ports to another or all ports for external analysis.
	multicast-limit		Enables the interface multicast limit.
		<pkt/s>	Sets how many multicast packets the interface receives per second.
	name	<port-name-string>	Sets a name for your interface. Enter a descriptive name (up to nine printable ASCII characters).
	no		
		bandwidth-limit	Disables bandwidth limit on the switch.
		broadcast-limit	Disables broadcast storm control limit on the switch.
		dlf-limit	Disables destination lookup failure (DLF) on the switch.
		egress set <port-list>	Disables the outgoing traffic port list for a port-based VLAN.
		flow-control	Disables flow control on the switch.
		gvrp	Disables GVRP on the switch.
		igmp-filtering profile	Disables IGMP filtering on the port.
		igmp-group-limited	Disables IGMP group limitation.
		igmp-immediate-leave	Disables IGMP immediate leave on the port.
		inactive	Enables the specified interface on the switch.

Table 30-5 Command Summary: Interface

COMMAND			DESCRIPTION
		ingress-check	Incoming traffic is not checked for VLAN tags.
		intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.
		mirror	Disables port mirroring on the switch.
		multicast-limit	Disables multicast limit on the switch.
		vlan-trunking	Disables VLAN trunking on the switch.
	pvid	<1-4094>	The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.
	qos priority	<0 .. 7>	Sets the quality of service priority for an interface.
	speed-duplex	<auto|10-half|10-full|100-half|100-full|1000-full>	Sets the duplex mode (half, full) and speed (10/100/1000 Mbps) of the connection on the interface. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.
	spq		Sets the interface to use Strict Priority Queuing.
	test		Performs an interface loopback test.
	vlan-trunking		Enables VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.
	wrr		Sets the interface to use Weighted Round Robin queuing (WRR).

30.9.6 mvr Commands

The following table lists the mvr commands in configuration mode.

Table 30-6 Command Summary: mvr Commands

COMMAND			DESCRIPTION
`mvr <1-4094>`			Enters the MVR (Multicast VLAN Registration) configuration mode.
	`exit`		Exist from the MVR configuration mode.
	`group <name-str> start-address <ip> end-address <ip>`		Sets the multicast group range for the MVR.
	`inactive`		Disables MVR settings.
	`mode <dynamic|compatible>`		Sets the MVR mode (dynamic or compatible).
	`name <name-str>`		Sets the MVR name for identification purposes.
	`no group`		Disables all MVR group settings.
	`no group <name-str>`		Disables the specified MVR group setting.
	`no inactive`		Enables MVR.
	`no receiver-port <port-list>`		Disables the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.
	`no source-port <port-list>`		Disables the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.
	`no tagged <port-list>`		Sets the port(s) to untag VLAN tags.
	`receiver-port <port-list>`		Sets the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.
	`source-port <port-list>`		Sets the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.
	`tagged <port-list>`		Sets the port(s) to tag VLAN tags.

Chapter 31 Command Examples

This chapter describes some commands in more detail.

31.1 Overview

These are commands that you may use frequently in maintaining your switch.

31.2 show Commands

These are the commonly used `show` commands.

31.2.1 show system-information

Syntax:

```
show system-information
```

This command shows the general system information (such as the firmware version and system up time).

An example is shown next.

```
ras> show system-information

System Name             : GS-3012
System Contact          :
System Location         :
Ethernet Address        : 00:13:49:00:00:02
ZyNOS F/W Version       : V3.60(LR.1)b0 | 11/11/2005
RomRasSize              : 3027468
System up Time          :     4:44:50 (1a13da ticks)
Bootbase Version        : V3.00 | 01/14/2005
ZyNOS CODE              : RAS Sep 27 2005 17:59:19
Product Model           : GS-3012
```

Figure 31-1 show system-information Command Example

31.2.2 show hardware-monitor

Syntax:

```
show hardware-monitor [c|f]
```

This command displays the current hardware status (such as temperature and voltage levels).

```
ras> show hardware-monitor c

Temperature Unit : (c)
Temperature(%c)  Current    Max    Min  Threshold  Status
-------------------------------------------------------------
            MAC     40.0   40.0   30.5       85.0  Normal
            CPU     35.0   36.0   29.0       85.0  Normal
            PHY     33.0   33.0   29.5       85.0  Normal

FAN Speed(RPM)  Current   Max   Min  Threshold  Status
-----------------------------------------------------
          FAN1     5625  5716  5493       2750  Normal
          FAN2     5958  6114  5859       2750  Normal
          FAN3     6061  6114  5810       2750  Normal

Voltage(V)  Current     Max     Min  Threshold  Status
-----------------------------------------------------
    VCOREA    2.528   2.544   2.528      +-10%  Normal
     VINRO    1.232   1.232   1.232      +-10%  Normal
    3.3VIN    3.344   3.344   3.344       +-8%  Normal
     12VIN   11.977  11.977  11.977      +-11%  Normal
    1.3VIN    1.312   1.312   1.312      +-10%  Normal
   1.25VIN    1.232   1.248   1.232       +-8%  Normal
    1.8VIN    1.824   1.840   1.824      +-10%  Normal
 BPS_12VIN       --      --      --         --  Absent
ras>
```

Figure 31-2 show hardware-monitor Command Example

31.2.3 show ip

Syntax:

```
show ip
```

This command displays the IP related information (such as IP address and subnet mask) on all switch interfaces.

```
ras> show ip
Out-of-band Management IP Address = 192.168.0.1
Management IP Address
     IP[192.168.0.1], Netmask[255.255.255.0], VID[0]
IP Interface
     IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
ras>
```

Figure 31-3 show ip Command Example

31.2.4 show logging

This command is not available in User mode.

Syntax:

```
show logging
```

This command displays the system logs. The following figure shows an example.

```
ras# show logging
  57 Thu Jan  1 00:00:05 1970 PINI  INFO  main: init completed
  58 Thu Jan  1 00:00:02 1970 PP0c -WARN  SNMP TRAP 3: link up
  59 Thu Jan  1 00:00:05 1970 PINI -WARN  SNMP TRAP 0: cold start
  60 Thu Jan  1 00:00:05 1970 PINI -WARN  SNMP TRAP 3: link up
  61 Thu Jan  1 00:00:05 1970 PINI  INFO  main: init completed
  62 Thu Jan  1 00:00:10 1970 PP24  INFO  adjtime task pause 1 day
  63 Thu Jan  1 00:14:36 1970 PP0c -WARN  SNMP TRAP 2: link down
Clear Error Log (y/n):
```

Figure 31-4 show logging Command Example

If you clear a log (by entering `y` at the `Clear Error Log (y/n):` prompt), you cannot view it again.

31.2.5 show interface

Syntax:

```
show interface [port-number]
```

This command displays statistics of a port. The following example shows that port 10 is up and the related information.

```
ras# show interface 10
  Port Info     Port NO.              :10
                Link                  :100M/F
                Statuss               :FORWARDING
                LACP                  :Disabled
                TxPkts                :69
                RxPkts                :4
                Errors                :0
                Tx KBs/s              :1.684
                Rx KBs/s              :1.684
                Up Time               :    0:02:12
  TX Packet     Tx Packets            :69
                Multicast             :0
                Broadcast             :0
                Pause                 :0
                Tagged                :0
  RX Packet     Rx Packets            :4
                Multicast             :0
                Broadcast             :4
                Pause                 :0
                Control               :0
  TX Collison   Single                :0
                Multiple              :0
                Excessive             :0
                Late                  :0
  Error Packet  RX CRC                :0
                Length                :0
                Runt                  :0
  Distribution  64                    :4
                65 to 127             :74
                128 to 255            :18
                256 to 511            :0
                512 to 1023           :0
                1024 to 1518          :44
                Giant                 :0
ras#
```

Figure 31-5 show interface Command Example

31.2.6 show mac address-table

Syntax:

```
show mac address-table <all <sort>|static>
```

Where

<sort> = Specifies the sorting criteria (MAC, VID or port).

This command displays the MAC address(es) stored in the switch. The following example shows a static MAC address table.

```
ras# show mac address-table static
Port      VLAN ID        MAC Address         Type
CPU       1              00:a0:c5:01:23:46   Static
ras#
```

Figure 31-6 show mac address-table Command Example

31.3ping

Syntax:

```
ping <ip> < [in-band|out-of-band|vlan <vlan-id> ] [ size <0-8024> ] [ -
t ]>
```

where

<ip>	=	The IP address of an Ethernet device.
[in-band|out-of-band|vlan <vlan-id>]	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs. out-of-band refers the management port while in-band means the other ports on the switch.
[size <0-8024>]	=	Specifies the packet size to send.
[-t]	=	Sends Ping packets to the Ethernet device indefinitely. Click [CTRL]+C to terminate the Ping process.

This command sends Ping packets to an Ethernet device. The following example sends Ping requests to and displays the replies from an Ethernet device with an IP address of 192.168.1.100.

```
ras# ping 192.168.1.100
 sent  rcvd  rate    rtt     avg    mdev     max     min  reply from
    1     1  100       0       0       0       0       0  192.168.1.100
    2     2  100       0       0       0       0       0  192.168.1.100
    3     3  100       0       0       0       0       0  192.168.1.100
ras#
```

Figure 31-7 ping Command Example

31.4 traceroute

Syntax:

```
traceroute <ip> [in-band|out-of-band|vlan <vlan-id>][ttl <1-255>] [wait
<1-60>] [queries <1-10>]
```

where

`<ip>`	=	The IP address of an Ethernet device.
`[in-band|out-of-band|vlan <vlan-id> ]`	=	Specifies the network interface or the VLAN ID to which the Ethernet device belongs.
`[ttl <1-255>]`	=	Specifies the Time To Live (TTL) period.
`[wait <1-60>]`	=	Specifies the time period to wait.
`[queries <1-10>]`	=	Specifies how many tries the switch performs the traceroute function.

This command displays information about the route to an Ethernet device. The following example displays route information to an Ethernet device with an IP address of 192.168.1.100.

```
ras> traceroute 192.168.1.100
traceroute to 192.168.1.100, 30 hops max, 40 byte packet
  1:192.168.1.100 (10 ms) (10 ms) (0 ms)
traceroute done:
```

Figure 31-8 traceroute Command Example

31.5 Enabling RSTP

To enable RSTP on a port, enter `spanning-tree` followed by the port number. You also need to use `spanning-tree` to enable RSTP on the switch. The following example enables RSTP on port 10.

```
ras(config)# spanning-tree 10
ras(config)# spanning-tree
```

Figure 31-9 Enable RSTP Command Example

31.6 Configuration File Maintenance

This section shows you how to backup or restore the configuration file on the switch using TFTP.

31.6.1 Backing up Configuration

Syntax:

```
copy running-config tftp <ip> <remote-file>
```

where

<ip>	=	The IP address of a TFTP server on which you want to store the backup configuration file.
<remote-file>	=	Specifies the name of the configuration file.

This command backs up the current configuration file on a TFTP server. The following example backs up the current configuration to a file (test.cfg) on the TFTP server (172.23.19.96).

```
ras# copy running-config tftp 172.23.19.96 test.cfg

Backuping
.  (599)Bytes Done!

ras#
```

Figure 31-10 CLI: Backup Configuration Example

31.6.2 Restoring Configuration

Syntax:

```
copy tftp config <index> <ip> <remote-file>
```

where

<index>	=	Specifies to restore which configuration file (1 or 2) on the switch.
<ip>	=	The IP address of a TFTP server from which you want to get the backup configuration file.
<remote-file>	=	Specified the name of the configuration file.

This command restores a configuration file on the switch. The following example uploads the configuration file (test.cfg) from the TFTP server (172.23.19.96) to the switch.

```
ras# copy tftp config 1 172.23.19.96 test.cfg

Restoring
.  (599)Bytes Done!

ras#
```

Figure 31-11 CLI: Restore Configuration Example

31.6.3 Using a Different Configuration File

You can store up to two configuration files on the switch. Only one configuration file is used at a time. By default the switch uses the first configuration file (with an index number of 1). You can set the switch to use a different configuration file. There are two ways in which you can set the switch to use a different configuration file: restart the switch (cold reboot) and restart the system (warm reboot).

Use the boot config command to restart the switch and use a different configuration file (if specified). The following example reboots the switch to use the second configuration file.

```
ras# boot config 2
```

Figure 31-12 CLI: boot config Command Example

Use the reload config command to restart the system and use a different configuration file (if specified). The following example restarts the system to use the second configuration file.

```
ras# reload config 2
```

Figure 31-13 CLI: reload config Command Example

When you use the `write memory` command without specifying a configuration file index number, the switch saves the changes to the configuration file the switch is currently using.

31.6.4 Resetting to the Factory Default

Follow the steps below to reset the switch back to the factory defaults.

1. Enter `erase running config` to reset the current running configuration.
2. Enter `write memory` to save the changes to the current configuration file. If you want to reset the second configuration file, use the `write memory` command again with the specified index number.

The following example resets both configuration files to the factory default settings.

```
ras# erase running-config
ras# write memory
ras# write memory 2
```

Figure 31-14 CLI: Reset to the Factory Default Example

31.7 Example no Commands

These are the commonly used command examples that belong to the `no` group of commands.

31.7.1 no mirror-port

Syntax:

```
no mirror-port
```

Disables port mirroring on the switch.

An example is shown next.

```
ras(config)# no mirror-port
```

Figure 31-15 no mirror-port Command Example

31.7.2 no https timeout

Syntax:

```
no https timeout
```

Resets the https session timeout to default.

An example is shown next. The session timeout is reset to 300 seconds.

```
ras(config)# no https timeout
  Cache timeout 300
```

Figure 31-16 no https timeout Command Example

31.7.3 no trunk

Syntax:

```
no trunk <T1|T2|T3|T4|T5|T6>
no trunk <T1|T2|T3|T4|T5|T6> lacp
no trunk <T1|T2|T3|T4|T5|T6> interface <port-list>
```

where

`<T1|T2|T3|T4|T5|T6>`	Disables the trunk group.
`<T1|T2|T3|T4|T5|T6> lacp`	Disables LACP in the trunk group.
`<T1|T2|T3|T4|T5|T6> interface <port-list>`	Removes ports from the trunk group.

An example is shown next.

Disable trunk one (T1).

Disable LAPC on trunk three (T3).

Remove ports one, three, four and five from trunk five (T5).

```
ras(config)# no trunk T1
ras(config)# no trunk T3 lacp
ras(config)# no trunk T5 interface 1,3-5
```

Figure 31-17 no trunk Command Example

31.7.4 no port-access-authenticator

Syntax:

```
no port-access-authenticator
no port-access-authenticator <port-list> reauthenticate
no port-access-authenticator  <port-list>
```

where

	Disables port authentication on the switch.
`<port-list> reauthenticate`	Disables the re-authentication mechanism on the listed port(s).
`<port-list>`	Disables authentication on the listed ports.

An example is shown next.

Disable authentication on the switch.

Disable re-authentication on ports one, three, four and five.

Disable authentication on ports one, six and seven.

```
ras(config)# no port-access-authenticator
ras(config)# no port-access-authenticator 1,3-5 reauthenticate
ras(config)# no port-access-authenticator 1,6-7
```

Figure 31-18 no port-access-authenticator Command Example

31.7.5 no ssh

Syntax:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <host-ip> <cr>
no ssh known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]
```

where

`key <rsa1|rsa|dsa>`	Disables the secure shell server encryption key. Your switch supports SSH versions 1 and 2 using RSA and DSA authentication.
`known-hosts <host-ip>`	Remove specific remote hosts from the list of all known hosts.
`known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]`	Remove remote known hosts with a specified public key (1024-bit RSA1, RSA or DSA).

An example is shown next.

Disable the secure shell RSA1 encryption key.

Remove the remote host with IP address 172.165.1.8 from the list of known hosts.

Remove the remote host with IP address 172.165.1.9 and with an SSH-RSA encryption key from the list of known hosts.

```
ras(config)# no ssh key rsa1
ras(config)# no ssh known-hosts 172.165.1.8
ras(config)# no ssh known-hosts 172.165.1.9 ssh-rsa
```

Figure 31-19 no ssh Command Example

31.8 interface Commands

These are some commonly used commands that belong to the interface group of commands.

31.8.1 interface

Syntax:

```
interface
```

Each interface refers to an Ethernet port on the switch. Commands configured after the interface command correspond to those ports. Type multiple ports or port ranges separated by a comma. Ranges of port numbers are typed separated by a dash.

An example is shown next.

Enter the configuration command set.

Enable ports one, three, four and five for configuration.

Begin configuring for those ports.

```
ras# config
ras(config)# interface port-channel 1,3-5
ras(config-interface)#
```

Figure 31-20 interface Command Example

31.8.2 bpdu-control

Syntax:

```
bpdu-control <peer|tunnel|discard|network>
```

where

`<peer|tunnel|discard|network>=`	Type `peer` to process any BPDUs received on these ports. Type `tunnel` to forward BPDUs received on these ports. Type `discard` to drop any BPDUs received on these ports. Type `network` to process a BPDU with no VLAN tag and forward a tagged BPDU.

An example is shown next.

Enable ports one, three, four and five for configuration.

Set the BPDU control to tunnel, to forward BPDUs received on ports one, three, four and five.

```
ras(config)# interface 1,3-5
ras(config-interface)# bpdu-control tunnel
ras(config-interface)#
```

Figure 31-21 interface bpdu-control Command Example

31.8.3 broadcast-limit

Syntax:

```
broadcast-limit
broadcast-limit <pkt/s>
```

where

	Enables broadcast storm control limit on the switch.
`<pkt/s>`	Sets how many broadcast packets the interface receives per second.

An example is shown next.

Enable port one for configuration.

Enable broadcast control.

Set the number of broadband packets the interface receives per second

```
ras(config)# interface port-channel 1
ras(config-interface)# broadcast-limit
ras(config-interface)# broadcast-limit 21
```

Figure 31-22 broadcast-limit Command Example

31.8.4 bandwidth-limit

Syntax:

```
bandwidth-limit
bandwidth-limit pir <Kbps>
bandwidth-limit cir <Kbps>
bandwidth-limit egress <Kbps>
```

where

	Enables bandwidth control on the switch.
`<Kbps>`	Sets the maximum bandwidth allowed for outgoing traffic (`egress`) or incoming traffic (`ingress`) on the switch.

An example is shown next.

Enable port one for configuration.

Enable bandwidth control.

Set the outgoing traffic bandwidth limit to 5000Kbps.

Set the guaranteed bandwidth allowed for incoming traffic to 4000Kbps.

Set the maximum bandwidth allowed for incoming traffic to 8000Kbps.

```
ras(config)# interface port-channel 1
ras(config-interface)# bandwidth-limit
ras(config-interface)# bandwidth-limit egress 5000
ras(config-interface)# bandwidth-limit cir 4000
ras(config-interface)# bandwidth-limit pir 8000
```

Figure 31-23 bandwidth-limit Command Example

31.8.5 mirror

Syntax:

```
mirror
mirror dir <ingress|egress|both>
```

where

	Enables port mirroring on the interface.
`<ingress|egress|both>`	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one or all ports to another or all ports for external analysis.

An example is shown next.

Enable port mirroring.

Enable the monitor port three.

Enable ports one, four, five and six for configuration.

Enable port mirroring on the interface.

Enable port mirroring for outgoing traffic. Traffic is copied from ports one, four, five and six to port three in order to examine it in more detail without interfering with the traffic flow on the original port(s).

```
ras(config)# mirror-port
ras(config)# mirror-port 3
ras(config)# interface port-channel 1,4-6
ras(config-interface)# mirror
ras(config-interface)# mirror dir egress
```

Figure 31-24 mirror Command Example

31.8.6 gvrp

Syntax:

```
gvrp
```

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLANs groups beyond the local switch.

An example is shown next.

Enable the IEEE 802.1Q tagged VLAN command to configure tagged VLAN for the switch.

Enable ports one, three, four and five for configuration.

Enable GVRP on the interface.

```
ras(config)# vlan1q gvrp
ras(config)# interface port-channel 1,3-5
ras(config-interface)# gvrp
```

Figure 31-25 gvrp Command Example

31.8.7 ingress-check

Syntax:

```
ingress-check
```

Enables the device to discard incoming frames for VLANs that are not included in a port member set.

An example is shown next.

Enable ports one, three, four and five for configuration.

Enable ingress checking on the interface.

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# ingress-check
```

Figure 31-26 ingress-check Command Example

31.8.8 frame-type

Syntax:

```
frame-type <all|tagged>
```

where

`<all|tagged>`	Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.

An example is shown next.

Enable ports one, three, four and five for configuration.

Enable ingress checking on the interface.

Enable tagged frame-types on the interface.

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# ingress-check
ras(config-interface)# frame-type tagged
```

Figure 31-27 frame-type Command Example

31.8.9 vlan-trunking

Syntax:

```
vlan-trunking
```

Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the switch.

An example is shown next.

Enable ports one, three, four and five for configuration.

Enable VLAN Trunking on the interface.

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# vlan-trunking
```

Figure 31-28 vlan-trunking Command Example

31.8.10 weight

Syntax:

```
weight <wt1> <wt2> ... <wt8>
```

where

`<wt1> <wt2> ... <wt8>`	Sets the interface WFQ weighting. A weight value of one to eight is given to each variable from `wt1` to `wt8`.

An example is shown next.

Enable port two and ports six to twelve for configuration.

Set the queue weights from Q0 to Q7.

```
ras# configure
ras(config)# interface port-channel 2,6-12
ras(config-interface)# weight 8 7 6 5 4 3 2 1
```

Figure 31-29 weight Command Example

31.8.11 egress set

Syntax:

```
egress set <port-list>
```

where

`<port-list>`	Sets the outgoing traffic port list for a port-based VLAN.

This command adds a port into the port-based VLAN. When you use the port-based VLAN, all of the ports are members by default. You must use the `no egress set` command to remove ports if you do not want all ports to be members. An example is shown next.

Enable port-based VLAN tagging on the switch.

Enable ports one, three, four and five for configuration.

Remove all ports (one through 12) from the VLAN.

Add ports 0, 6 and 7~9 as outgoing ports for the VLAN.

```
ras(config)# vlan-type port-based
ras(config)# interface port-channel 1,3-5
ras(config-interface)# no egress set 0-12
ras(config-interface)# egress set 0,6,7-9
```

Figure 31-30 egress set Command Example

31.8.12 qos priority

Syntax:

```
qos priority <0 .. 7>
```

where

`<0 .. 7>`	Sets the quality of service priority for an interface(s).

An example is shown next.

Enable ports one, three, four and five for configuration.

Set the IEEE 802.1p quality of service priority as four (4).

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# qos priority 4
```

Figure 31-31 qos priority Command Example

31.8.13 name

Syntax:

```
name <port-name-string>
```

where

`<port-name-string>`	Sets a name for your port interface(s).

An example is shown next.

Enable ports one, three, four and five for configuration.

Set a name for the interfaces.

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# name Test
```

Figure 31-32 name Command Example

31.8.14 speed-duplex

Syntax:

```
speed-duplex <auto|10-half|10-full|100-half|100-full|1000-full>
```

where

`<auto|10-half|10-full|100-half|100-full|1000-full>`	Sets the duplex mode (half, full) and speed (10/100/1000 Mbps) of the connection on the interface. Selecting auto (auto-negotiation) makes one port able to negotiate with a peer automatically to obtain the connection speed and duplex mode that both ends support.

An example is shown next.

Enable ports one, three, four and five for configuration.

Set the speed to 10 Mbps in half duplex mode.

```
ras(config)# interface port-channel 1,3-5
ras(config-interface)# speed-duplex 10-half
```

Figure 31-33 speed-duplex Command Example

Chapter 32
IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN and associated commands.

32.1IEEE 802.1Q Tagged VLAN Overview

See the *VLAN* chapter for more information on VLANs. There are two kinds of tagging:

1. Explicit Tagging

A VLAN identifier is added to the frame header that identifies the source VLAN.

2. Implicit Tagging

The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-LAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

32.2VLAN Databases

A VLAN database stores and organizes VLAN registration information useful for switching frames to and from a switch. A VLAN database consists of a static entries (Static VLAN or SVLAN table) and dynamic entries (Dynamic VLAN or DVLAN table).

32.2.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

32.2.2 Dynamic Entries (DVLAN Table)

Dynamic entries are learned by the switch and cannot be created or updated by administrators. The switch learns this information by observing what port, source address and VLAN ID (or VID) is associated with a frame. Entries are added and deleted using GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol.

32.3Configuring Tagged VLAN

The following procedure shows you how to configure tagged VLAN.

1. Use the IEEE 802.1Q tagged VLAN commands to configure tagged VLAN for the switch.
2. Use the `vlan <vlan-id>` command to configure or create a VLAN on the switch. The switch automatically enters the config-vlan mode.
3. Use the `exit` command when you are finished configuring the VLAN.
4. Use the `interface <port-list> command` to enter the config-interface mode to set the VLAN settings on a port, then use the `pvid <vlan-id>` command to set the VLAN ID you created for the port-list to that specific port in the PVID table.
5. Use the `inactive` command to deactivate the VLAN(s).

Example:

```
ras(config)# vlan 2000
ras(config-vlan)# name upl
ras(config-vlan)# fixed 10-12
ras(config-vlan)# no untagged 10-12
ras(config-vlan)# exit
ras(config)# interface port-channel 10-12
ras(config-interface)# pvid 2000
ras(config-interface)# exit
ras(config)#
```

Figure 32-1 Tagged VLAN Configuration and Activation Example

6. Configure your management VLAN.

   Use the `vlan <vlan-id>` command to create a VLAN (VID 3 in this example) for managing the switch, and the switch will activate the new management VLAN.

   Use the `inactive` command to disable the new management VLAN.

Example:

```
ras(config)# vlan 3
ras(config-vlan)# inactive
ras(config-vlan)#
```

Figure 32-2 CPU VLAN Configuration and Activation Example

32.4 Global VLAN1Q Tagged VLAN Configuration Commands

This section shows you how to configure and monitor the IEEE 802.1Q Tagged VLAN.

32.4.1 GARP Status

Syntax:

```
show garp
```

This command shows the switch's GARP timer settings, including the join, leave and leave all timers.

An example is shown next.

```
ras# show garp

GARP Timer
------------------------
Join  Timer      :200
Leave Timer      :600
Leave All Timer  :10000
ras#
```

Figure 32-3 garp status Command Example

32.4.2 GARP Timer

Syntax:

```
garp join <msec> leave <msec> leaveall <msec>
```

where

`join <msec>` =	This sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 32767 milliseconds; the default is 200 milliseconds.
`leave <msec>` =	This sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.
`leaveall <msec>` =	This sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer; the default is 10000 milliseconds.

This command sets the switch's GARP timer settings, including the join, leave and leave all timers.

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

The following example sets the Join Timer to 300 milliseconds, the Leave Timer to 800 milliseconds and the Leave All Timer to 11000 milliseconds.

```
ras(config)# garp join 300 leave 800 leaveall 11000
```

32.4.3 Show GVRP

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

```
ras# show vlan1q gvrp
GVRP Support
---------------------
gvrpEnable = YES
```

Figure 32-4 show gvrp Command Example

32.4.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

This command turns on GVRP in order to propagate VLAN information beyond the switch.

32.4.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

This command turns off GVRP so that the switch does not propagate VLAN information to other switches.

32.5 Port VLAN Commands

You must configure the switch port VLAN settings in config-interface mode.

32.5.1 Set Port VID

Syntax:

```
pvid <VID>
```

where

`<VID>` = Specifies the VLAN number between 1 and 4094

This command sets the default VLAN ID on the port(s).

The following example sets the default VID to 200 on ports 1 to 5.

```
ras(config)# interface port-channel 1-5
ras(config-interface)# pvid 200
```

Figure 32-5 port default vid Command Example

32.5.2 Set Acceptable Frame Type

Syntax:

```
frame-type <all|tagged>
```

where

`<all|tagged>` =	Specifies all Ethernet frames (tagged and untagged) or only tagged Ethernet frames.

This command sets the specified port to accept all Ethernet frames or only those with an IEEE 802.1Q VLAN tag.

The following example sets ports 1 to 5 to accept only tagged frames.

```
ras(config)# interface port-channel 1-5
ras(config-interface)# frame-type tagged
```

Figure 32-6 frame type Command Example

32.5.3 Enable or Disable Port GVRP

Use the `gvrp` command to enable GVRP on the port(s). Use the `no gvrp` command to disable GVRP.

The following example turns off GVRP for ports 1 to 5.

```
ras(config)# interface port-channel 1-5
ras(config-interface)# no gvrp
```

Figure 32-7 no gvrp Command Example

32.5.4 Modify Static VLAN

Use the following commands in the config-vlan mode to configure the static VLAN table.

Syntax:

```
vlan <vlan-id>
fixed <port-list>
forbidden <port-list>
name <name-str>
normal <port-list>
untagged <port-list>
no fixed <port-list>
no forbidden <port-list>
no untagged <port-list>
```

where

`<vlan-id>`	=	The VLAN ID [1 – 4094].
`<name-str>`	=	A name to identify the SVLAN entry.
`<port-list>`	=	This is the switch port list.

- Enter `fixed` to register the `<port-list>` to the static VLAN table with `<vlan-id>`.
- Enter `normal` to confirm registration of the `<port-list>` to the static VLAN table with `<vlan-id>`.
- Enter `forbidden` to block a `<port-list>` from joining the static VLAN table with `<vlan-id>`.
- Enter `no fixed` or `no forbidden` to change `<port-list>` to normal status.
- Enter `untagged` to send outgoing frames without a tag.
- Enter `no untagged` to tag outgoing frames.

Modify a Static VLAN Table Example

The following example configures ports 1 to 5 as fixed and untagged ports in VLAN 2000.

```
ras(config)# vlan 2000
ras(config-vlan)# fixed 1-5
ras(config-vlan)# untagged 1-5
```

Figure 32-8 Modifying Static VLAN Example

Forwarding Process Example

Tagged Frames

1. First the switch checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames.
2. The switch then checks the VID in a frame's tag against the SVLAN table.
3. The switch notes what the SVLAN table says (that is, the SVLAN tells the switch whether or not to forward a frame and if the forwarded frames should have tags).
4. Then the switch applies the port filter to finish the forwarding decision. This means that frames may be dropped even if the SVLAN says to forward them. Frames might also be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

Untagged Frames

1. An untagged frame comes in from the LAN.
2. The switch checks the PVID table and assigns a temporary VID of 1.
3. The switch ignores the port from which the frame came, because the switch does not send a frame to the port from which it came. The switch also does not forward frames to "forbidden" ports.
4. If after looking at the SVLAN, the switch does not have any ports to which it will send the frame, it won't check the port filter.

32.5.5 Delete VLAN ID

Syntax:

```
no vlan <vlan-id>
```

where

`<vlan-id>` The VLAN ID [1 – 4094].
=

This command deletes the specified VLAN ID entry from the static VLAN table. The following example deletes entry 2 in the static VLAN table.

```
ras(config)# no vlan 2
```

Figure 32-9 no vlan Command Example

32.6 Enable VLAN

Syntax:

`vlan <vlan-id>`

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

32.7 Disable VLAN

Syntax:

`vlan <vlan-id>`

`inactive`

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

32.8 Show VLAN Setting

Syntax:

`show vlan`

This command shows the IEEE 802.1Q Tagged SVLAN (Static VLAN) table.

An example is shown next.

```
ras# show vlan

  The Number of VLAN :     2
  idx.  VID   Status     Elap-Time    TagCtl
  ----  ----  ---------  -----------  ----------------------------------------

     1     1     Static      0:14:39  Untagged :1-12
                                      Tagged :

     2  2000     Static      0:02:36  Untagged :
                                      Tagged :  10-12

ras#
```

Figure 32-10 show vlan Command Example

Part VIII

Appendices and Index

This part contains an appendix and an index.

A Product Specifications

These are the GS-3012 and GS-3012F product specifications.

Chart 1 General Product Specifications

Standards	IEEE802.3 10BASE-T Ethernet (twisted-pair copper) IEEE802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) ANSI/IEEE802.3 Auto-negotiation IEEE802.3x Flow Control IEEE802.1p Priority Queues IEEE802.1q VLAN IEEE802.1d Spanning Tree IEEE 802.1x Authentication IEEE 802.3 ad Link Aggregation IEEE 802.1w Rapid reconfiguration
Protocol	CSMA/CD
Interfaces (GS-3012)	Eight 10/100/1000BASE-T RJ-45 Gigabit ports (with four paired Gigabit/mini GBIC ports) Four Gigabit interfaces consisting of a 10/100/1000BASE-T RJ-45 Gigabit port paired with a mini GBIC slot One console port One RJ-45 management port
Interfaces (GS-3012F)	Eight mini GBIC slots for uplinking Four Gigabit interfaces consisting of a 10/100/1000BASE-T RJ-45 Gigabit port paired with a mini GBIC slot One console port One RJ-45 management port
Data Transfer Rate	Ethernet (GS-3012): 10Mbps (half duplex), 20Mbps (full duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps(full duplex) Gigabit: 1000Mbps (half duplex), 2000Mbps (full duplex) Uplink rates depend on the uplink module used (see your module manual).
Network Cables	10BASE-T: 2-pair Unshielded Twisted Pair (UTP) Cat.3, 4, 5 (100 meters) EIA/TIA-586 100-ohm Shielded Twisted Pair (STP) (100 meters) 100BASE-TX, 1000BASE-T: UTP Cat.5 (100 m max.) EIA/TIA-568 100-ohm STP (100 m max.) Uplink cables depend on the uplink module used (see your module manual).
Full/Half Duplex	Full/half duplex for 100 Mbps speeds Full duplex 1000 Mbps speed

Chart 1 General Product Specifications

Media Interface Exchange	All ports are auto-crossover (auto-MDI-X) and auto-negotiating.

Chart 2 Performance and Management Specifications

Back plane	12.8 Gbps
Packet Forwarding Rate	148800 PPS for 100BASE-TX 1488000PPS for 1000Base-X Uplink packet forwarding rate depends on the uplink module used (see your module manual)
Switching Method	Store-and-forward
MAC Address Table	16 K entries
Data Buffer	1MB (excluding optional modules) Uplink data buffers depend on the uplink module used (see your module manual)
VLAN	IEEE 802.1Q tag-based VLAN, 4094 Max
IEEE 802.1p Priority Queues	Eight CoS queues
Port Link Aggregation	Static port trunking IEEE802.3ad dynamic port trunking
Port Security	Static MAC address filtering MAC address learning limit
Multicasting	Support IGMP snooping
Broadcast Storm	Support broadcast storm control
Port Mirroring	All Gigabit and uplink ports support port mirroring
Management	Web-based management Console Telnet SNMP Syslog
Management Security	User ID/Password for console, Telnet and Web-based management authentication Up to four administrators allowed

Chart 2 Performance and Management Specifications

MIBs	SNMP MIB II (RFC 1213) RFC 1157 SNMP v1 SNMPv2 or SNMPv2c RFC 1643 Ethernet MIBs RFC 1493 Bridge MIBs RFC 1155 SMI RFC 1757 RMON Bridge extension MIBs RFC 2674 RFC 2863 Interface MIB RFC 2925 Ping and Trace Route

Chart 3 Physical and Environmental Specifications

Weight	GS-3012 Main switch: 4Kg GS-3012F Main switch: 3Kg
LED	Main switch: BPS, PWR, SYS, ALM Per Port: LNK/ACT, FDX (GS-3012) Per Port: 1000, 100 (GS-3012F) Per GBIC Slot: LNK, ACT Per Management Port: 10, 100
Dimensions	Main switch: GS-3012: 438(W) x 300(D) x 45(H) mm GS-3012F: 438(W) x 225(D) x 45(H) mm 19-inch rack-mount width, 1 U height
Power Supply (AC Unit)	100 - 240VAC 50/60Hz 1.5A maximum internal universal power supply
Power Supply (DC Unit)	DC input of -48VDC－-60VDC 1.88A maximum for the GS-3012F 1.2A maximum for the GS-3012F
Power Consumption	GS-3012 AC unit: 50W maximum GS-3012 DC unit: 40W maximum GS-3012F AC unit: 36W maximum GS-3012F DC unit: 30W maximum

Chart 3 Physical and Environmental Specifications

Fuse Rating	T2A250VAC Caution: For continued protection against risk of fire, replace only with the same type and fuse rating.
Operating Temperature	0ºC ~45ºC (32ºF to 113ºF)
Storage Temperature	-25ºC ~70ºC (-13ºF to 158ºF)
Operational Humidity	10% to 90% (Non-condensing)
Safety	UL 60950-1 CSA 60950-1 EN60950-1 IEC60950 -1
EMC	FCC Part15 (Class A) CE EMC (Class A)

B Index

H

I

J

L

Q

R

S

T

U

V

W