ES-2108/ES-2108-G

Ethernet Switch

User's Guide

Version 3.60
10/2005
Edition 1

ZyXEL

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Interference Statements and Warnings

FCC 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.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Certifications

1 Go to www.zyxel.com

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

3 Select the certification you wish to view from this page.

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.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

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 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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character 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.

Customer Support

Please have the following information ready when you contact customer support.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE* / 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 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	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
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	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	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	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE* / FAX	WEB SITE / FTP SITE	REGULAR MAIL
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	+44-1344 303044 08707 555779 (UK only) +44-1344 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)

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ES-2108/ES-2108-G Ethernet Switch.

This preface introduces you to the ES-2108/ES-2108-G Ethernet Switch and discusses the conventions of this User's Guide. It also provides information on other related documentation.

Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

About This User's Guide

This manual is designed to guide you through the installation and configuration of your ES-2108/ES-2108G for its various applications.

Related Documentation

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one of the predefined choices.
- Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The ES-2108/ES-2108-G Ethernet Switch may be referred to as "the switch" unless otherwise specified in this User's Guide.

Graphics Icons Key

ES-2108/ES-2108-G 	Computer 	Server 
Computer 	DSLAM 	Gateway 
Central Office/ ISP 	Internet 	Hub/Switch 

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.

CHAPTER 1
Getting to Know Your Switch

This chapter introduces the main features and applications of the switch.

1.1 Introduction

The switch is a stand-alone layer-2 Ethernet switch with eight 10/100Mbps ports. The ES-2108-G also includes one Gigabit/Mini-GBIC port.

With its built-in web configurator, managing and configuring the switch is easy. In addition, the switch can also be managed via Telnet, SSH (Secure SHell), any terminal emulator program on the console port, or third-party SNMP management.

1.2 Software Features

This section describes the general software features of the switch.

DHCP Client

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. You can configure the switch as a DHCP client to obtain TCP/IP information (such as the IP address and subnet mask) from a DHCP server. If you disable the DHCP service, you must manually enter the TCP/IP information.

VLAN

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.

Differentiated Services (DiffServ)

With DiffServ, the switch 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.

Queuing

Queuing is used to help solve performance degradation when there is network congestion. Two scheduling services are supported: Strict Priority Queuing (SPQ) and Weighted Round Robin (WRR). This allows the switch to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

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 mirror port (the port you copy the traffic to) without interference.

Static Route

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

IGMP Snooping

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.

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.

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.

Port Authentication and Security

For security, the switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch.

Maintenance and Management Features

- Access Control

  You can specify the service(s) and computer IP address(es) to control access to the switch for management.

- Cluster Management

Cluster management (also known as iStacking) 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.

- Configuration and Firmware Maintenance

  You can backup or restore the switch configuration or upgrade the firmware on the switch.

1.3 Hardware Features

This section describes the ports on the switch.

Ethernet Ports

The ports allow the switch to connect to another Ethernet devices.

Gigabit Ethernet Port

Avaliable on the ES-2108-G, the port allows the switch to connect to another WAN switch.

Mini-GBIC Slot

Install SPF transceivers in this slot to connect to other Ethernet switches at longer distances than the Ethernet port.

Console Port

Use the console port for local management of the switch.

1.4 Applications

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

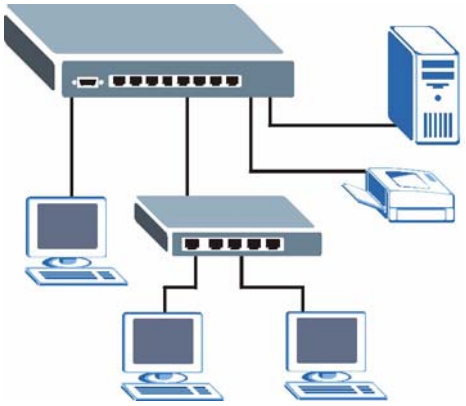
1.4.1 Backbone Application

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 port or connect other switches to the switch.

In this example, all computers can share high-speed applications on the server. To expand the network, simply add more networking devices such as switches, routers, computers, print servers etc.

Figure 1 Backbone Application



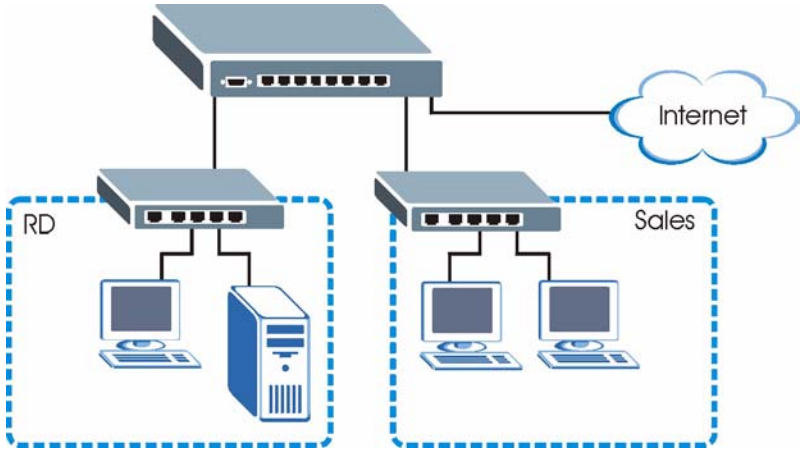
1.4.2 Bridging Example

In this example application the switch connects different company departments (**RD** and **Sales**) 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.

For ES-2108G, you can provide a super-fast uplink connection by using a Gigabit Ethernet/ mini-GBIC port on the switch.

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

Figure 2 Bridging Application

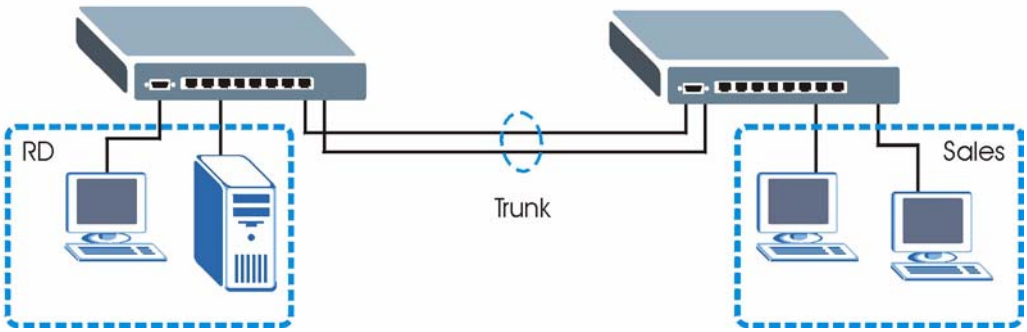


1.4.3 High Performance Switched Example

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

Switching to higher-speed LANs such as ATM (Asynchronous Transmission Mode) 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 switch can provide the same bandwidth as 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 3 High Performance Switched Application



1.4.4 IEEE 802.1Q VLAN Application Examples

This section shows a workgroup and a shared server example using 802.1Q tagged VLANs.

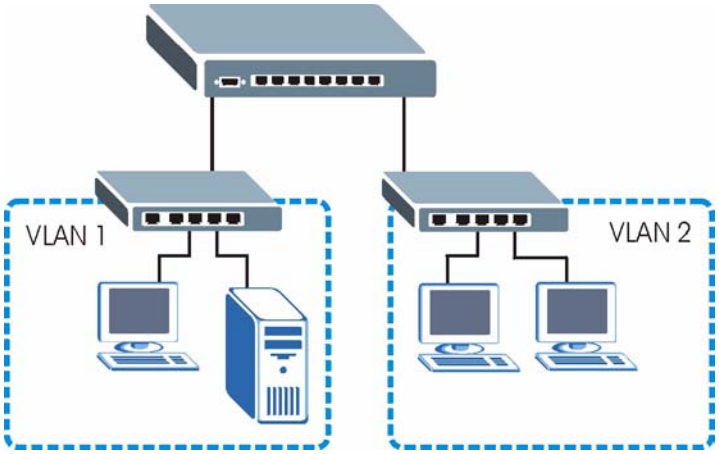
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

For more information on VLANs, refer to Chapter 8, "VLAN," on page 67.

1.4.4.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame 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.

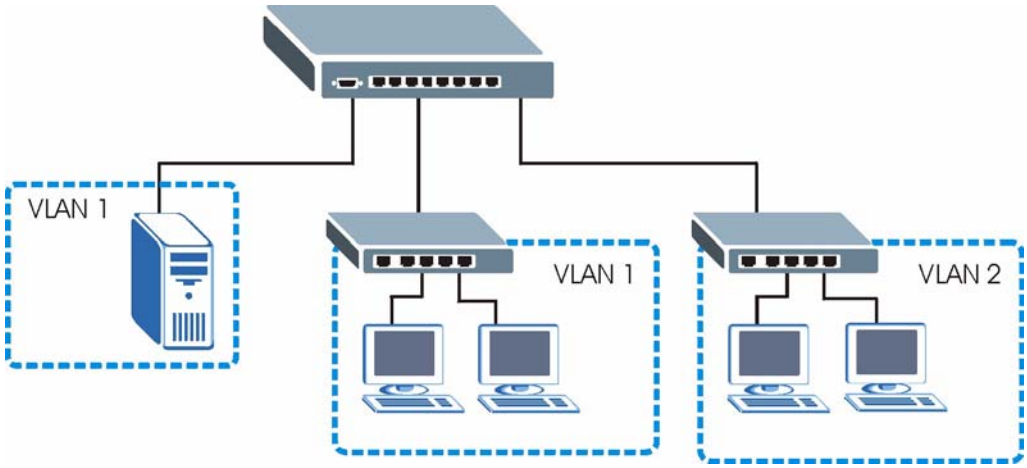
Figure 4 Tag-based VLAN Application



1.4.4.2 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. Ports can belong to other VLAN groups too.

Figure 5 Shared Server Using VLAN Example



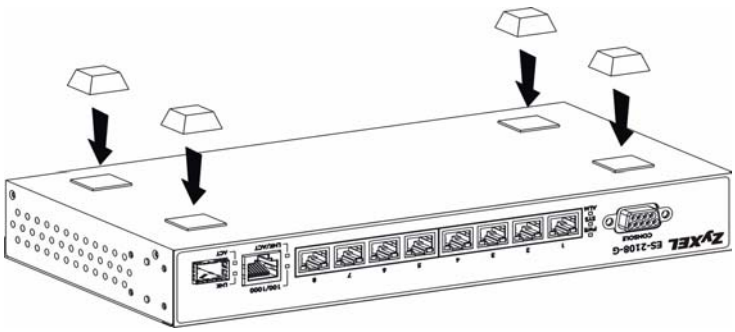
CHAPTER 2
Hardware Installation and Connection

This chapter shows you how to install and connect the switch.

2.1 Freestanding Installation

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 devices when stacking.

Figure 6 Attaching Rubber Feet



Note: Do NOT block the ventilation holes. Leave space between devices when stacking.

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.

2.2 Mounting the Switch on a Rack

This section lists the rack mounting requirements and precautions and describes the installation steps.

2.2.1 Rack-mounted Installation Requirements

- Two mounting brackets.
- Eight M3 flat head screws and a #2 Philips screwdriver.
- Four M5 flat head screws and a #2 Philips screwdriver.

Note: Failure to use the proper screws may damage the unit.

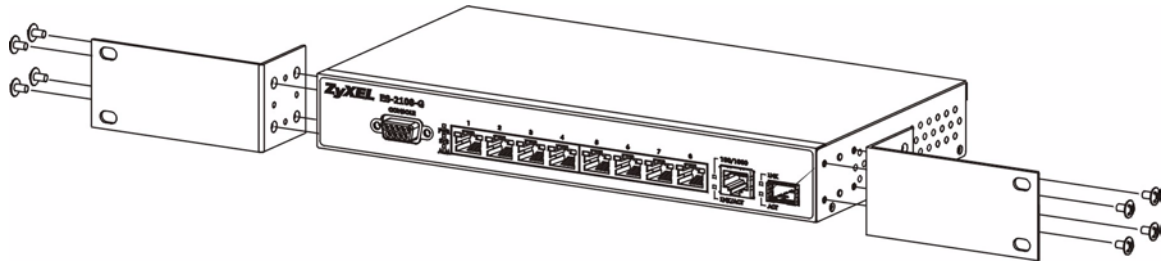
2.2.1.1 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains.
- Make sure the position of the switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.2.2 Attaching the Mounting Brackets to the Switch

1 Position a mounting bracket on one side of the switch, lining up the four screw holes on the bracket with the screw holes on the side of the switch.

Figure 7 Attaching the Mounting Brackets



2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the switch.

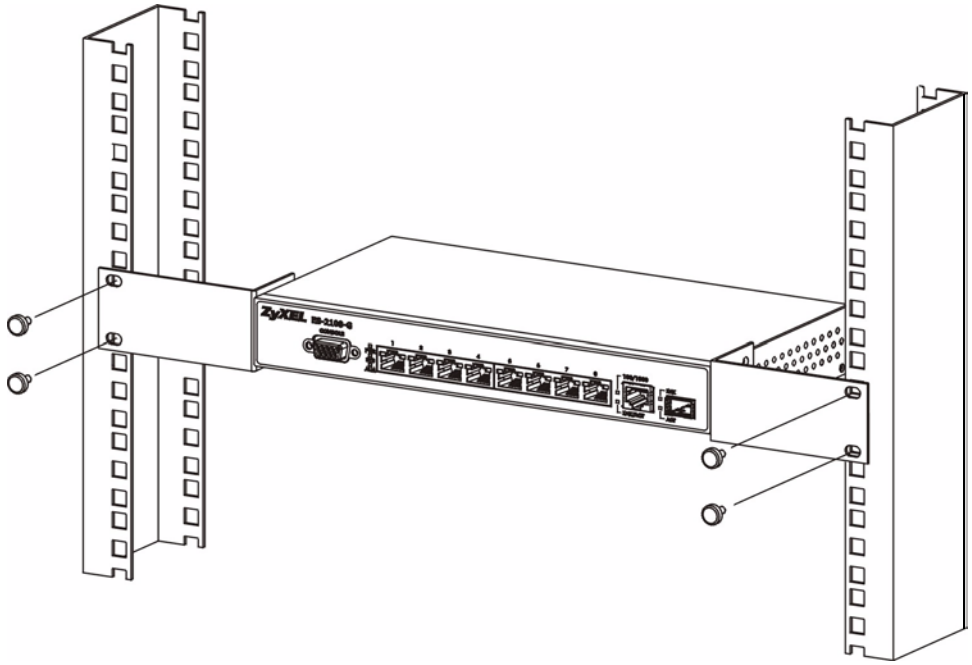
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the switch.

4 You may now mount the switch on a rack. Proceed to the next section.

2.2.3 Mounting the Switch on a Rack

1 Position a mounting bracket (that is already attached to the switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes on the side of the rack.

Figure 8 Mounting the Switch on a Rack



2 Using a #2 Philips screwdriver, install the M5 flat head screws through the mounting bracket holes into the rack.

3 Repeat steps 1 and 2 to attach the second mounting bracket on the other side of the rack.

CHAPTER 3
Hardware Overview

This chapter describes the front panel and rear panel of the switch and shows you how to make the hardware connections.

3.1 Front Panel Connection

The figure below shows the front panel of the switch.

Figure 9 Front Panel: ES-2108

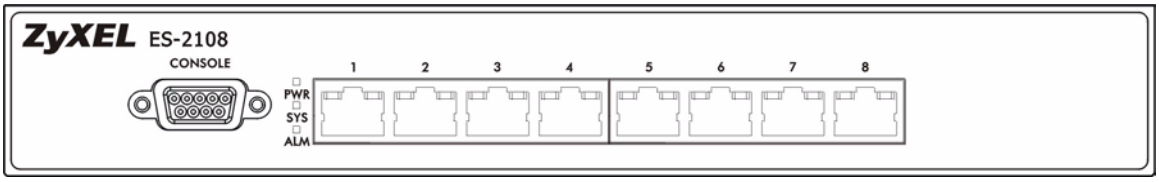
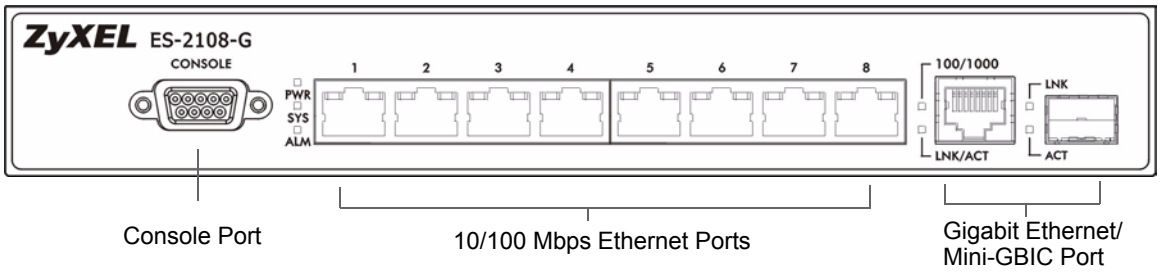


Figure 10 Front Panel: ES-2108-G



The following table describes the port labels on the front panel.

Table 1 Front Panel

PORT	DESCRIPTION
CONSOLE	Only connect this port if you want to configure the switch using the command line interface (CLI) via the console port.
Eight 10/100 Mbps RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
Gigabit Ethernet/ mini-GBIC port	This is not available on ES-2108. Connect this Gigabit Ethernet port to high-bandwidth backbone network Ethernet switches. Alternatively, use a mini-GBIC transceiver in this slot for fiber-optical connections to backbone Ethernet switches

3.1.1 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 of the switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.2 Ethernet Ports

The switch has Eight 10/100Mbps auto-negotiating, auto-crossover Ethernet ports. In 10/100Mbps Fast Ethernet, the speed can be 10Mbps or 100Mbps and the duplex mode can be half duplex or full duplex.

The ES-2108-G also comes with a Gigabit/Mini-GBIC port each. The mini-GBIC port has priority over the Gigabit port. This means that if the mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled. The speed of the Gigabit Ethernet/mini-GBIC port can be 100Mbps or 1000Mbps and the duplex mode can be half duplex (at 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100Mpbs) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

3.1.2.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the switch are:

- Speed: Auto
- Duplex: Auto
- Flow control: off

3.1.3 Mini-GBIC Slot

This is a slot 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 SFP Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

There is one Gigabit Ethernet and mini-GBIC port each. The mini-GBIC port has priority over the Gigabit port. This means that if the mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

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.

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

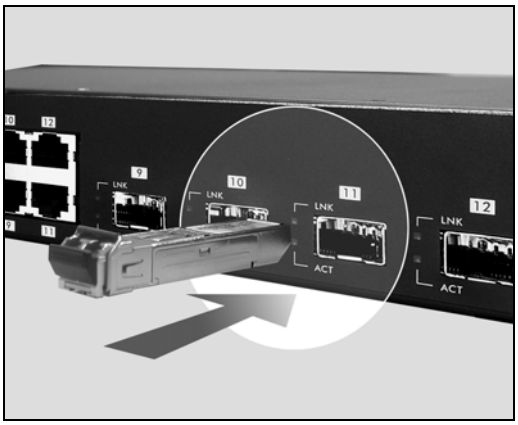
Note: To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

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

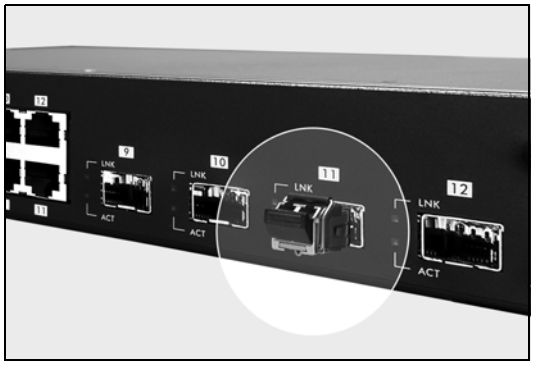
1. Insert the transceiver into the slot with the exposed section of PCB board facing down.

Figure 11 Transceiver Installation Example



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 12 Installed Transceiver

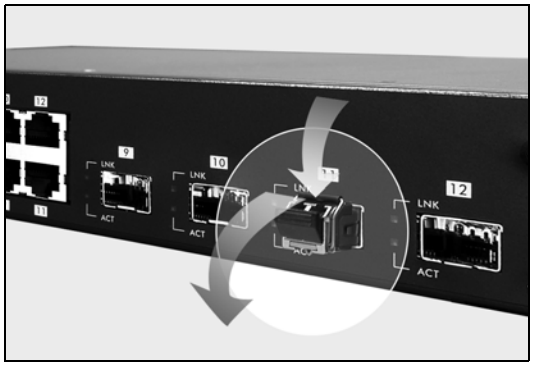


3.1.3.2 Transceiver Removal

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

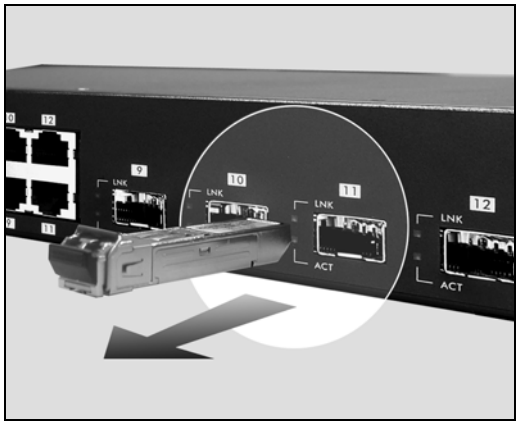
1 Open the transceiver's latch (latch styles vary).

Figure 13 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

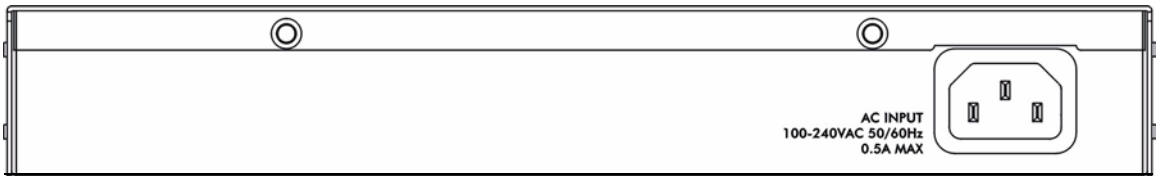
Figure 14 Transceiver Removal Example



3.2 Rear Panel

The following figure shows the rear panel of the switch. The power receptacle is on the rear panel.

Figure 15 Rear Panel



3.2.1 Power Connector

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

To connect the power to the switch, 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 the power source. Make sure that no objects obstruct the airflow of the fans.

3.3 Front Panel LEDs

The LEDs are located on the front panel. The following table describes the LEDs on the front panel.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
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.
ALM	Red	On	There is a hardware failure.
		Off	The system is functioning normally.
LNK/ACT (Ethernet ports)	Green	Blinking	The system is transmitting/receiving to/from a 10 Mbps Ethernet network.
		On	The link to a 10 Mbps Ethernet network is up.
	Amber	Blinking	The system is transmitting/receiving to/from a 100 Mbps Ethernet network.
		On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
100/1000	Green	On	The link to a 1000 Mbps Ethernet network is up.
	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
ACT	Green	Blinking	The port is receiving or transmitting data.
		On	The port has a connection to an Ethernet network but not receiving or transmitting data.
		Off	The link to an Ethernet network is down.
LNK (mini-GBIC Slot)	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.
ACT (mini GBIC Slot)	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data.

CHAPTER 4
The Web Configurator

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

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

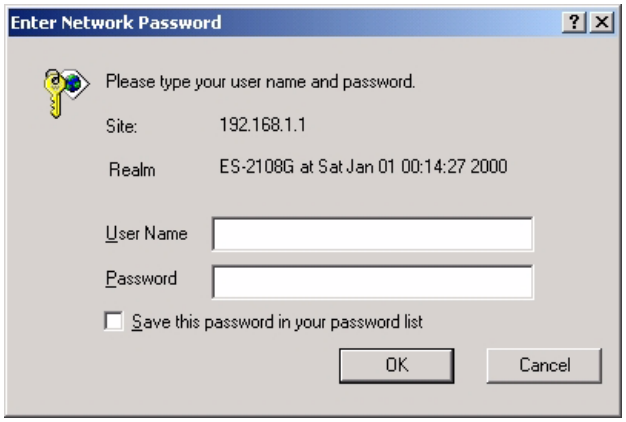
In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- Java Script (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

1. Start your web browser.
2. Type "http://" and the IP address of the switch (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].
3. The login screen appears. The default username is **admin** and 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 16 Web Configurator: Login



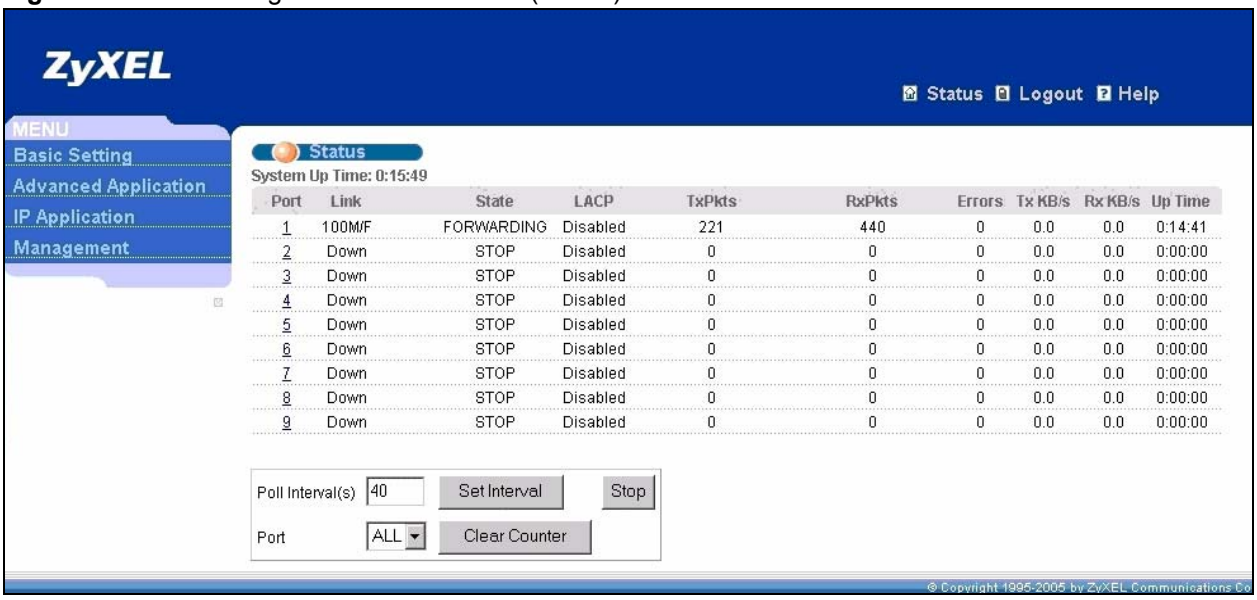
4 Click **OK** to view the first web configurator screen.

4.3 The Status Screen

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

Figure 17 Web Configurator Home Screen (Status)



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

Table 3 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
MENU Basic Setting Advanced Application IP Application Management System Info General Setup Switch Setup IP Setup Port Setup	MENU Basic Setting Advanced Application IP Application Management VLAN Static MAC Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Authentication Port Security Queuing Method	MENU Basic Setting Advanced Application IP Application Management Static Routing DiffServ	MENU Basic Setting Advanced Application IP Application Management Maintenance Access Control Diagnostic Cluster Management MAC Table ARP Table

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

Table 4 Web Configurator Screen Sub-links Details

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
System Info	VLAN	Static Routing	Maintenance
General Setup	VLAN Status	DiffServ	Firmware Upgrade
Switch Setup	VLAN Port Setting	DSCP Setting	Restore Configuration
IP Setup	Static VLAN		Backup Configuration
Port Setup	Static MAC Forwarding		Load Factory Default
	Filtering		Reboot System
	Spanning Tree Protocol		Diagnostic
	Status		Access Control
	Spanning Tree Protocol Configuration		SNMP
	Bandwidth Control		Logins
	Broadcast Storm Control		Service Access Control
	Mirroring		Remote Management
	Link Aggregation		Cluster Management Status
	Link Aggregation Control Protocol Status		Cluster Management Configuration
	Configuration		MAC Table
	Port Authentication		ARP Table
	RADIUS		
	802.1x		
	Port Security		
	Queuing Method		

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
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 management 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.

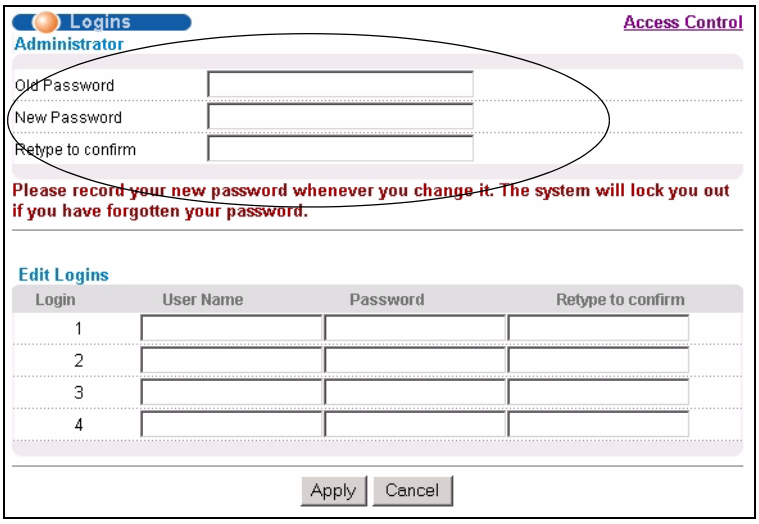
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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/RSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed from specified source(s) to specified destination(s).
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
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 aggregate 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 WFQ with associated queue weights for each port.
IP Application	
Static Route	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.
DiffServ	This link takes you to screens where you can enable DiffServ and set DSCP-to-IEEE802.1p mappings.
Advanced 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).
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.
Routing Table	This link takes you to a screen where you can view the routing table in the switch.

4.3.1 Change Your Password

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

Figure 18 Change Administrator Login Password



4.4 Switch Lockout

You could lock yourself (and all others) out from the switch by:

1. Deleting the management VLAN (default is VLAN 1).
2. Deleting all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the switch.
3. Filtering all traffic to the CPU port.
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.

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

4.5 Resetting the Switch

If you lock yourself (and others) from the switch or forget the switch password, you will need to reload the factory-default configuration file or reset the switch back to the factory defaults.

4.5.1 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 factory-default configuration file, do the following:

1. Connect to the console port using a computer with terminal emulation software. See Section 3.1.1 on page 34 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 the factory-default configuration file upload, type `atgo` to restart the switch.

Figure 19 Resetting the Switch: Via the Console Port

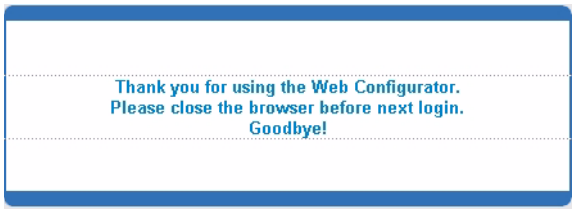
```
Bootbase Version: V1.0 | 04/25/2003 10:01:06
RAM: Size = 32768 Kbytes
FLASH: Intel 32M
ZyNOS Version: V3.50(DU.0)| 07/11/2003 18:00:29
Press any key to enter debug mode within 3 seconds.
.....................
Enter Debug Mode
ras> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total  262144 bytes received.
Erasing..
.............................................................
OK
ras> atgo
```

The switch is now re initialized with the factory-default configuration file including the default password of "1234".

4.6 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 20 Web Configurator: Logout Screen



4.7 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
Initial Setup Example

This chapter shows how to set up the switch for an example network.

5.1 Overview

The following lists the configuration steps for the initial setup:

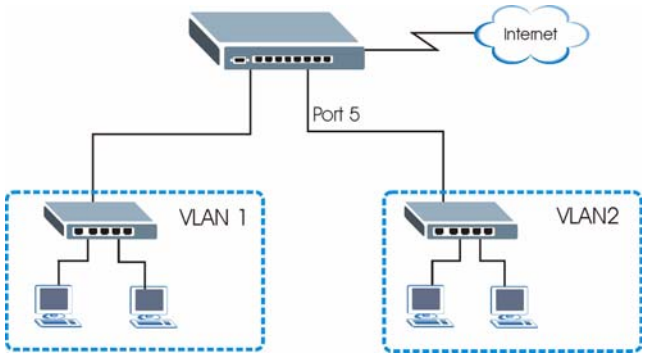
- Create a VLAN
- Set port VLAN ID
- Configure the switch IP management address

5.1.1 Creating a VLAN

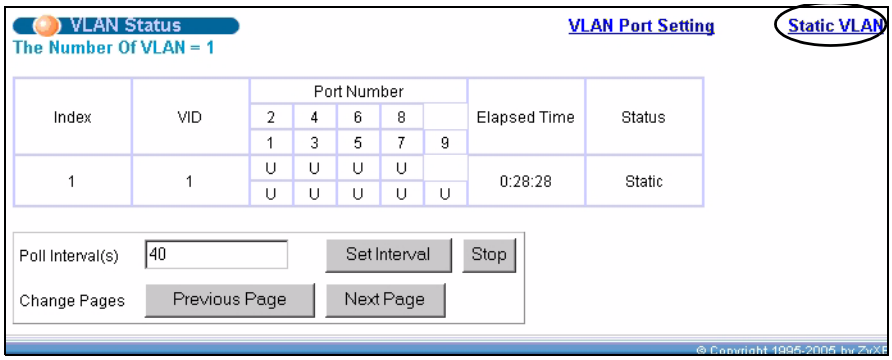
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 5 as a member of VLAN 2.

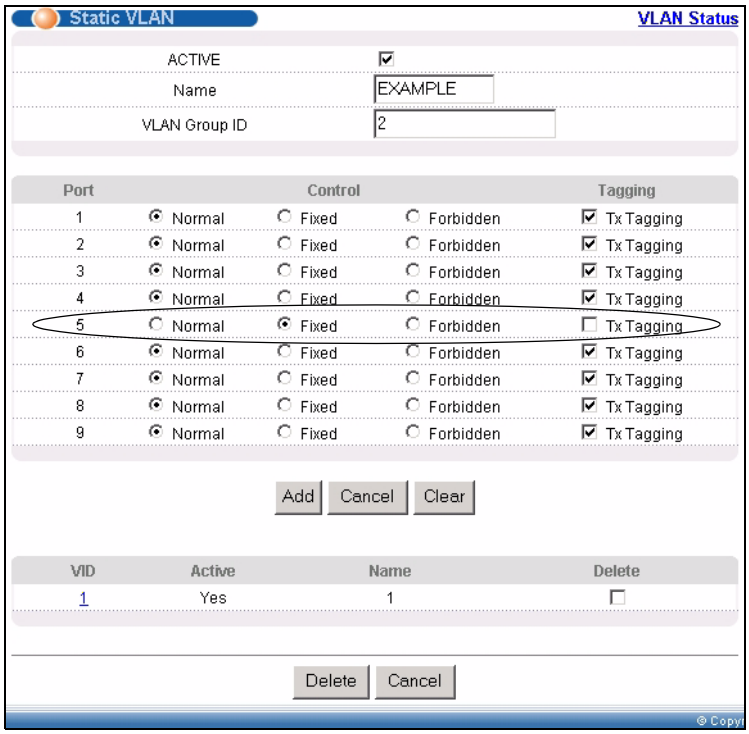
Figure 21 Initial Setup Network Example: VLAN



1 Click **Advanced Application** and **VLAN** in the navigation panel and click the **Static VLAN** link.



2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.



Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 5 on the switch, select **Fixed** to configure port 5 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the switch to remove VLAN tags before sending.

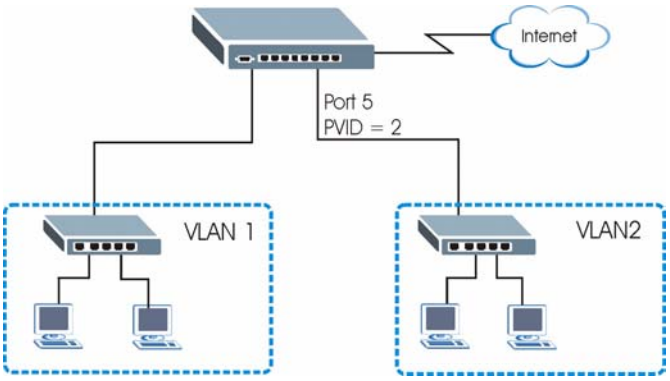
5 Click **Add** to save the settings.

5.1.2 Setting Port VID

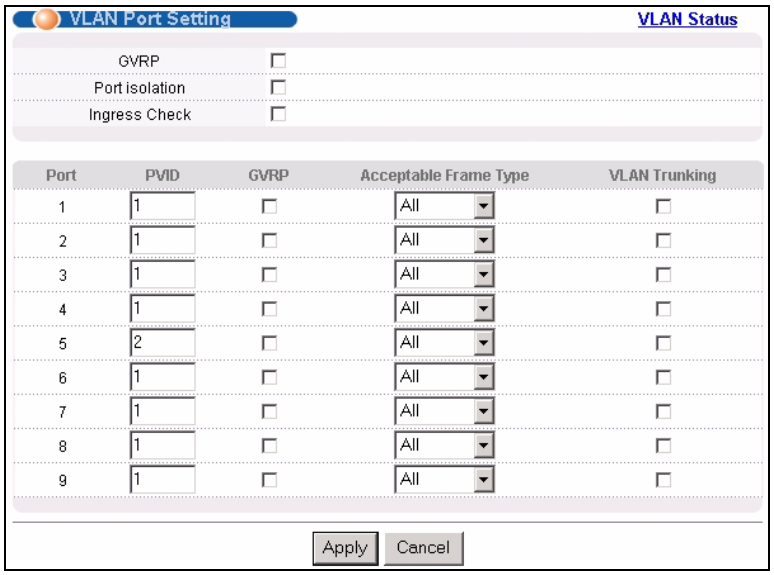
Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 2 as the port VID on port 5 so that any untagged frames received on that port get sent to VLAN 2.

Figure 22 Initial Setup Network Example: Port VID



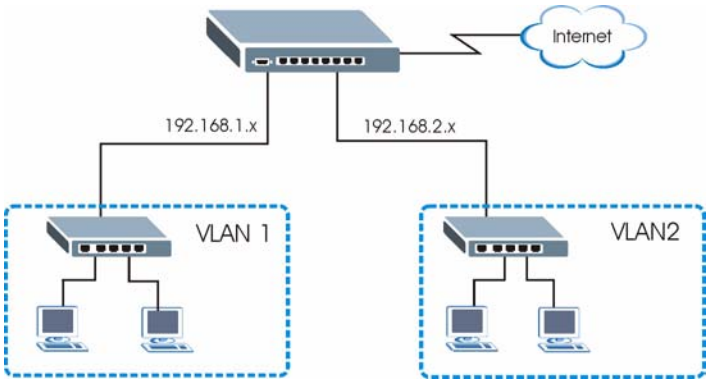
1. Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.
2. Enter 2 in the **PVID** field for port 5 and click **Apply** to save the settings.



5.1.3 Configuring Switch Management IP Address

The default management IP address of the switch is 192.168.1.1. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 23 Initial Setup Example: Management IP Address



1 Connect your computer to any Ethernet port on the switch. Make sure your computer is in the same subnet as the switch.

2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the web configurator. See Section 4.2 on page 39 for more information.

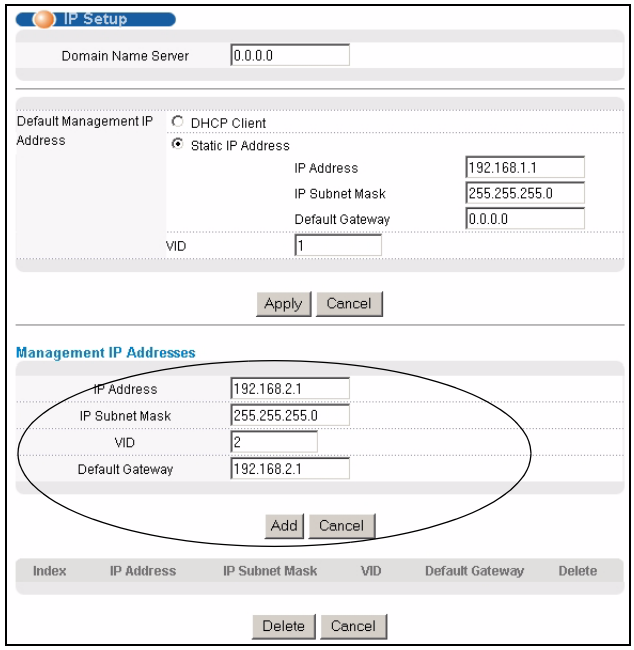
3 Click **Basic Setting** and **IP Setup** in the navigation panel.

4 Configure the related fields in the **IP Setup** screen.

For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.

5 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.

6 Click **Add**.



CHAPTER 6
System Status and Port Statistics

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

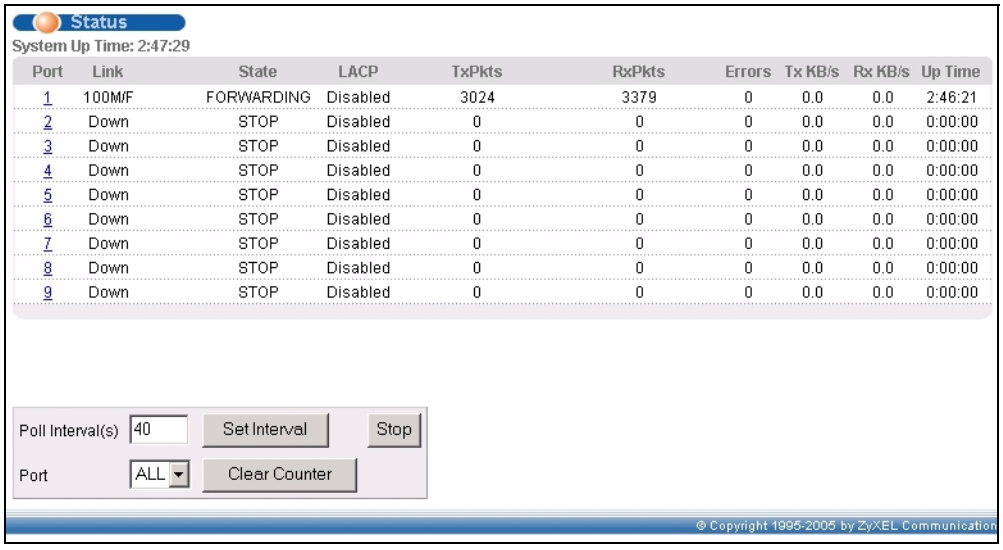
6.1 Overview

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

6.2 Port Status Summary

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

Figure 24 Status



The following table describes the labels in this screen.

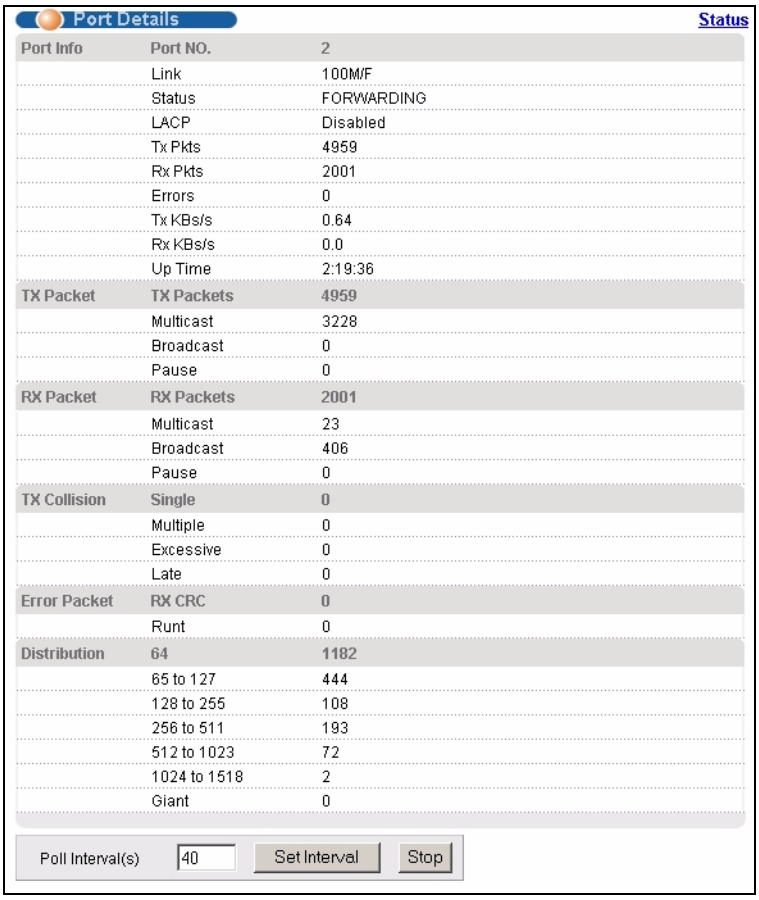
Table 6 Status

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 25 on page 53).
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or another value depending on the uplink module being used) and the duplex (**F** for full duplex or **H** for half duplex).
State	This field displays the STP (Spanning Tree Protocol) state of the port. See the chapter on STP for details on STP states.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) 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.

6.2.1 Status: 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 25 Status: Port Details



The following table describes the labels in this screen.

Table 7 Status: Port Details

LABEL	DESCRIPTION
Port Info	
Link	This field shows whether the Ethernet 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.
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 packets transmitted.	

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
TX Packet	This field shows the number of good packets (unicast, multicast and broadcast) transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Rx Packet The following fields display detailed information about packets received.	
RX Packet	This field shows the number of good packets (unicast, multicast and broadcast) received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
TX Collision	The following fields display information on collisions while transmitting.
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets 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 packets have already been transmitted.
Error Packet	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
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.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
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 7
Basic Setting

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

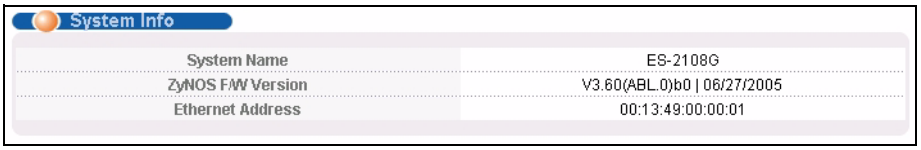
7.1 Overview

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(s) and DNS (domain name server) for management purposes.

7.2 System Information

In the navigation panel, click **Basic Setting** and **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 26 System Info



The following table describes the labels in this screen.

Table 8 System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the switch for identification purposes.
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.

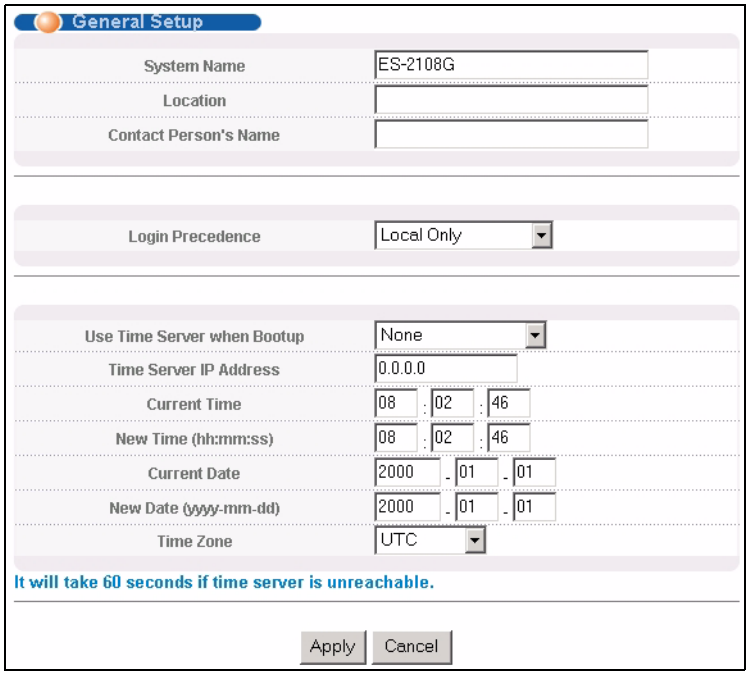
Table 8 System Info (continued)

LABEL	DESCRIPTION
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.

7.3 General Setup

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

Figure 27 General Setup



The following table describes the labels in this screen.

Table 9 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 9 General Setup (continued)

LABEL	DESCRIPTION
Login Precedence	Use this drop-down list box to select which database the switch should use (first) to authenticate an administrator (user for switch management). Configure the local user accounts in the **Access Control Logins** screen. The RADIUS is an external server. 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 administrator accounts configured in the **Access Control Logins** screen. Select **Local then RADIUS** to have the switch check the administrator 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 **Port Authentication Radius** 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 time servers 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 2000-1-1 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 reset the fields to your previous configuration.

7.4 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: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 8 on page 67 for information on port-based and 802.1Q tagged VLANs.

7.5 IGMP Snooping

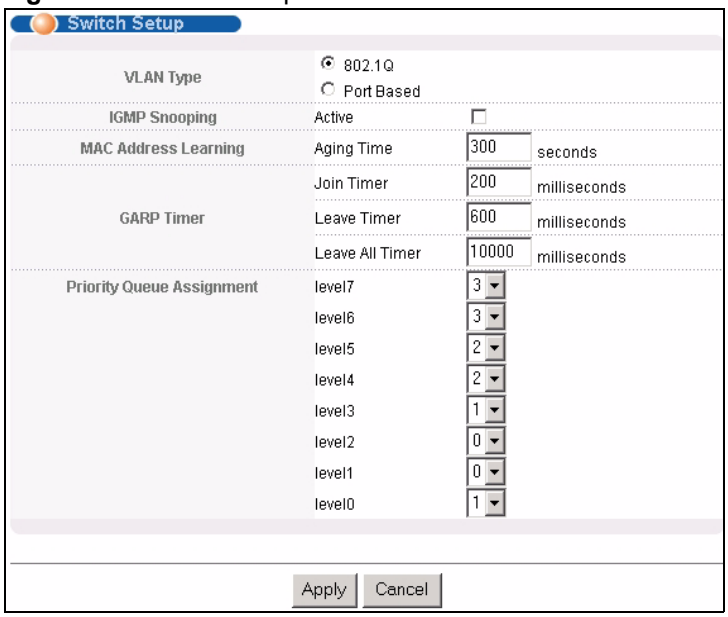
A switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures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

7.6 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel to 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 VLAN.

Figure 28 Switch Setup



The following table describes the labels in this screen.

Table 10 Switch Setup

LABEL	DESCRIPTION
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 Chapter 8 on page 67 for more information.
IGMP Snooping	Select **Active** to enable IGMP snooping have group multicast traffic only forwarded to ports that are members significantly reducing multicast traffic passing through your switch. See Section 7.5 on page 60 for more information on IGMP snooping.
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).
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.
Leave Timer	Leave Time 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.
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.

Table 10 Switch Setup (continued)

LABEL	DESCRIPTION
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 four physical queues that you can map to the 8 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.
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.
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 the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

7.7 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add switch IP address.

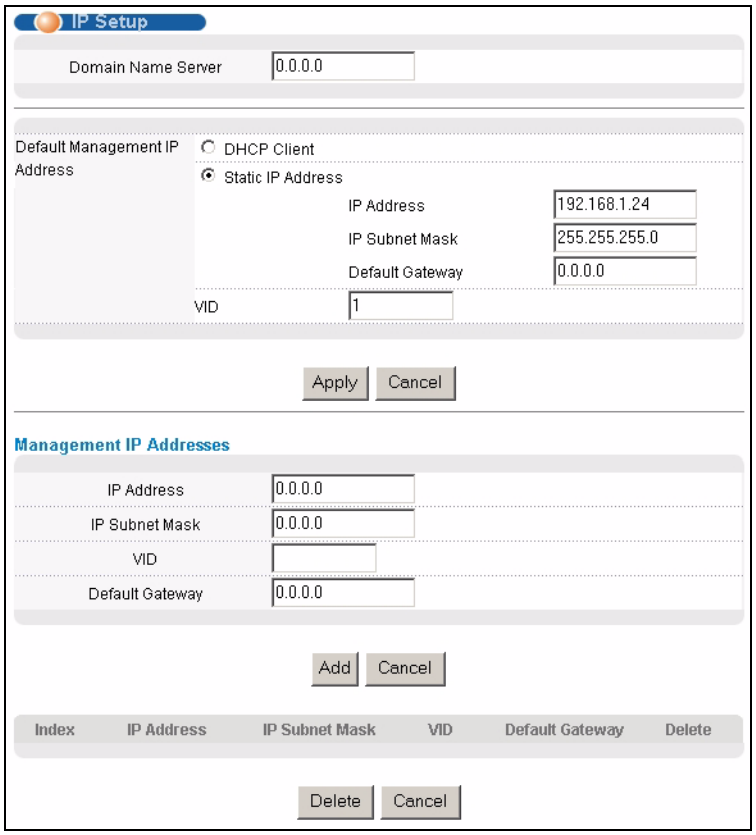
7.7.1 Management IP Addresses

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

You can configure up to 64 IP addresses which are used to access and manage the switch from the ports belonging to the pre-defined VLAN(s).

Note: You must configure a VLAN first.

Figure 29 IP Setup



The following table describes the labels in this screen.

Table 11 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.
Default Management IP Address	Configure the fields to set the default management IP address.
DHCP Client	Select this option if you have a DHCP server that can assign the switch an IP address and subnet mask, a default gateway IP address and a domain name server IP address.
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

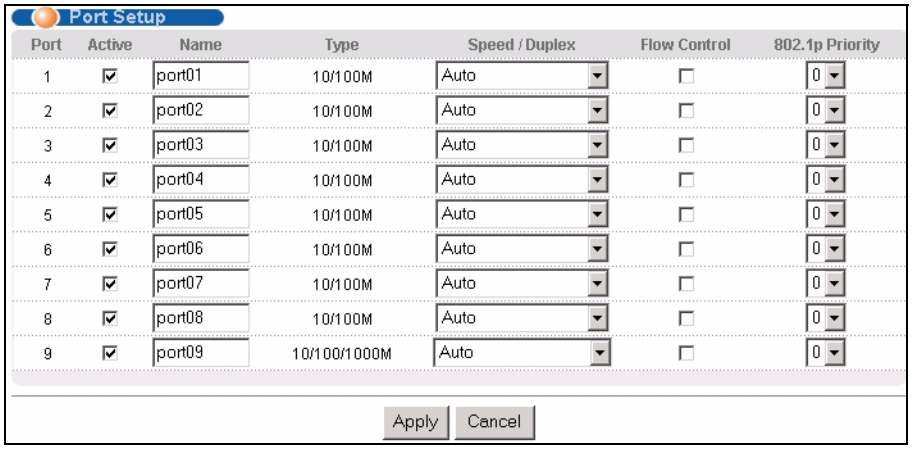
Table 11 IP Setup (continued)

LABEL	DESCRIPTION
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.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Management IP Addresses	Configure the fields to set additional management IP address.
IP Address	Enter the IP address for managing the switch by the members of the VLAN specified in the **VID** field below.
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation. For example, 255.255.255.0.
VID	Enter the VLAN 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.
Index	This field displays the index number of an entry.
IP Address	This field displays the management IP address of the switch.
Subnet Mask	This field displays the subnet mask of the switch.
VID	This field displays the VLAN identification number of the network.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.8 Port Setup

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

Figure 30 Port Setup



The following table describes the labels in this screen.

Table 12 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 **10/100M** for an Ethernet connection and **1000M** for the Gigabit Ethernet/ mini-GBIC ports.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. For Ethernet ports, select **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex** or **100M/Full Duplex**. For the Gigabit Ethernet/mini-GBIC port, select **Auto**, **100M/Full Duplex** or **1000M/ Full Duplex**. Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer 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 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 port are the same in order to connect.
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 back-pressure 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 **Flow Control** to enable it.

Table 12 Port Setup (continued)

LABEL	DESCRIPTION
802.1P Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 10 on page 61 for more information.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

CHAPTER 8
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.

8.1 Introduction to IEEE 802.1Q Tagged VLAN

A 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 VLAN configurations are 4,094.

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

8.1.1 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.

8.2 Automatic VLAN Registration

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

8.2.1 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.

8.2.1.1 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.

8.2.2 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 13 IEEE 802.1q 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.

Table 13 IEEE 802.1q Terminology (continued)

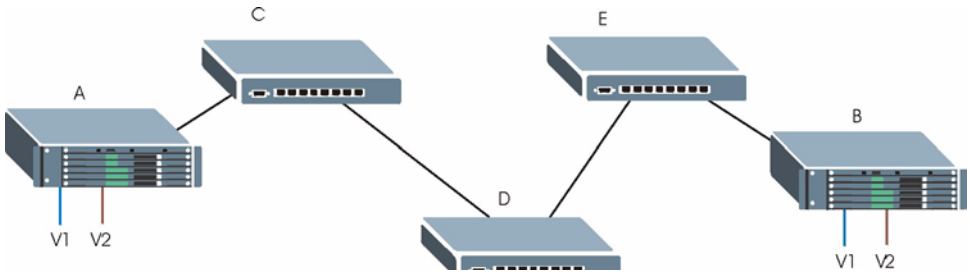
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards incoming frames for VLANs that do not have this port as a member

8.3 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).

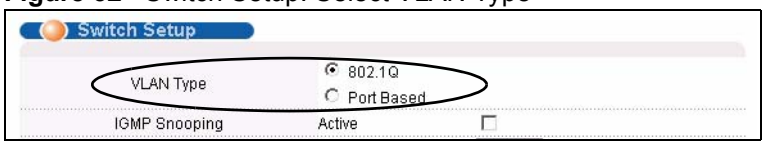
Figure 31 Port VLAN Trunking



8.4 Select the VLAN Type

1 Select a VLAN type in the **Switch Setup** screen.

Figure 32 Switch Setup: Select VLAN Type



8.5 Static VLAN

Use a static VLAN to decide whether an incoming frame on a port should be

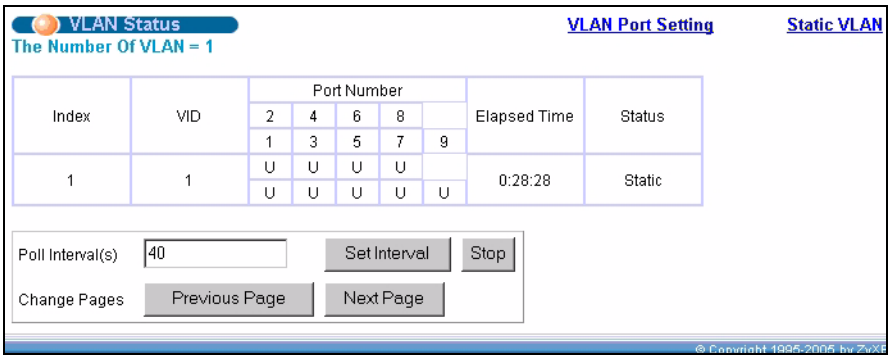
- sent to a VLAN group as normal depends on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

8.5.1 Static VLAN Status

Click **Advanced Application**, **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 33 VLAN: VLAN Status



The following table describes the labels in this screen.

Table 14 VLAN: 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	This is the VLAN identification number that was configured in the **VLAN Setup** screen.

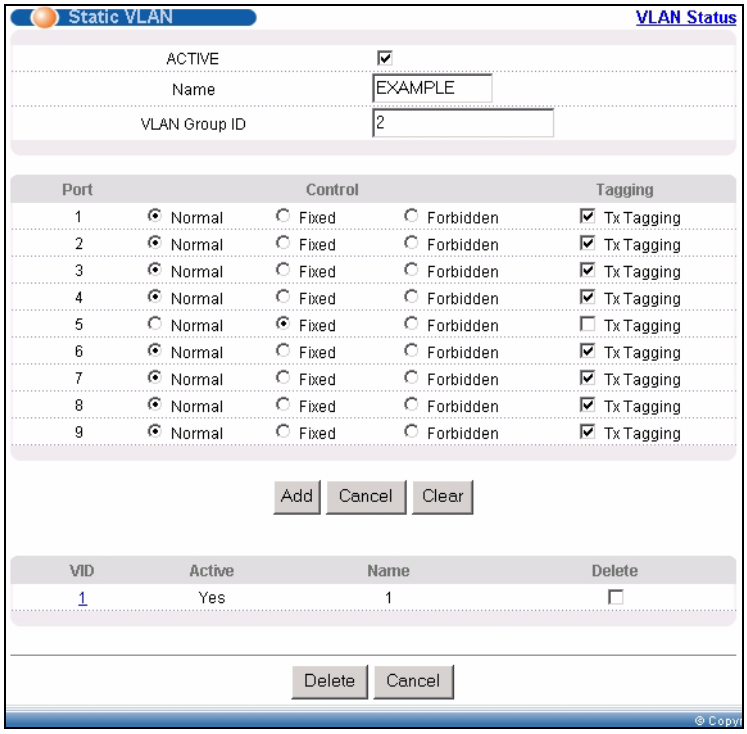
Table 14 VLAN: VLAN Status (continued)

LABEL	DESCRIPTION
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 are 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.
Change Pages	Click **Previous Page** or **Next Page** to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 Configure a Static VLAN

To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 34 VLAN: Static VLAN



The following table describes the related labels in this screen.

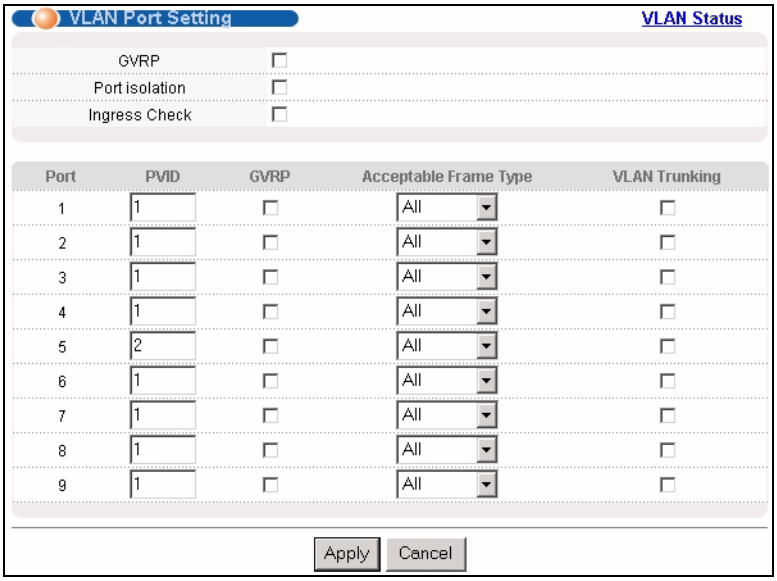
Table 15 VLAN: Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes.
VLAN Group ID	Enter the VLAN ID for this static 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 add the settings as a new entry in the summary table below.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to start configuring the screen again.
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	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

8.5.3 Configure VLAN Port Settings

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

Figure 35 VLAN: VLAN Port Setting



The following table describes the labels in this screen.

Table 16 VLAN: VLAN Port Setting

LABEL	DESCRIPTION
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. Select this check box to permit VLAN groups beyond the local switch.
Port Isolation	**Port Isolation** isolates ports on the same VLAN (802.1q). 'This option is the most limiting but also the most secure.
Ingress Check	Select this check box to activate ingress filtering on the switch. Clear this check box to disable ingress filtering the switch.
Port	This field displays the port number.
PVID	Enter a number between 1and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All** and **Tag Only**. Select **All** from the drop-down list box to accept all 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 will be 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.

Table 16 VLAN: VLAN Port Setting (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save the changes
Cancel	Click **Cancel** to start configuring the screen again.

8.6 Port-based VLAN Setup

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.

Note: When you activate port-based VLAN, the switch uses a default VLAN ID of 1. You cannot change it.

In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

8.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen (see Figure 32 on page 70) and then click **VLAN** from the navigation panel to display the next screen.

Figure 36 Port Based VLAN Setup (All Connected)

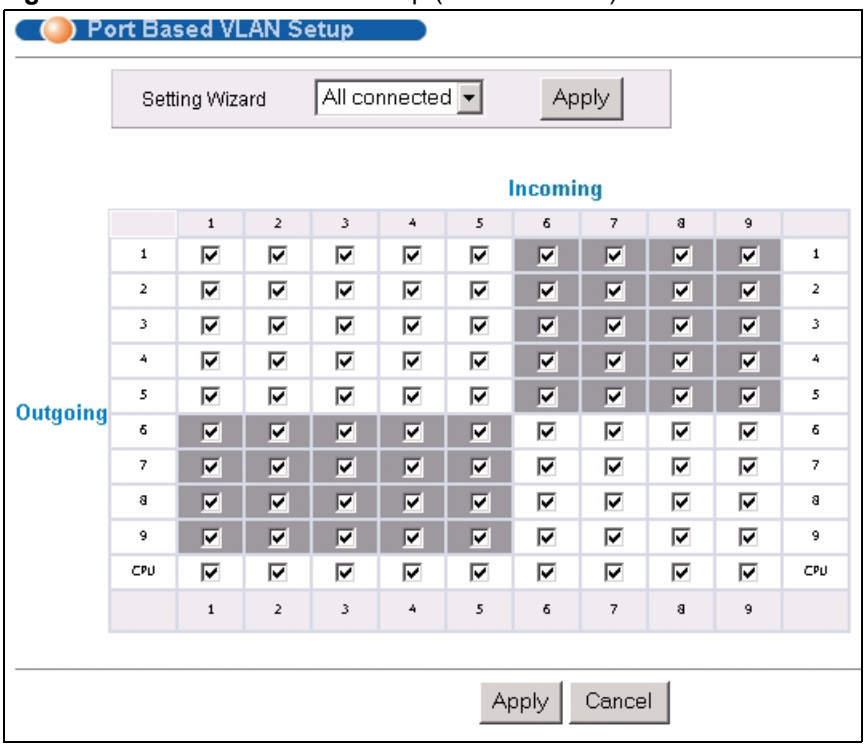
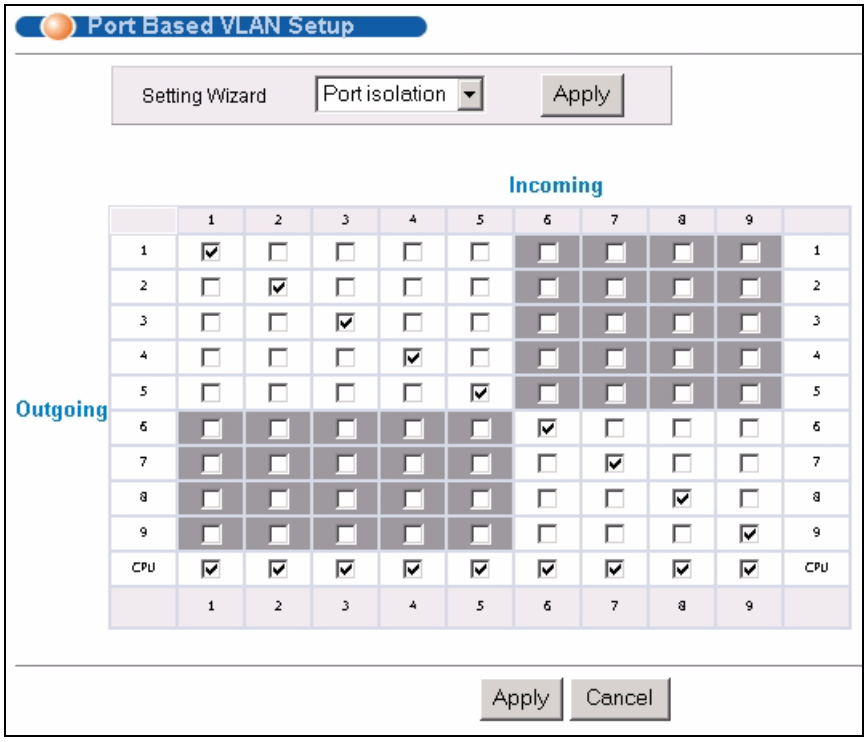


Figure 37 Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 17 Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose **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. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. 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 switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the switch cannot be managed from that port.
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 switch management port. By default it forms a VLAN with all Ethernet 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.
Cancel	Click **Cancel** to start configuring the screen again.

CHAPTER 9
Static MAC Forwarding

Use these screens to configure static MAC address forwarding.

9.1 Overview

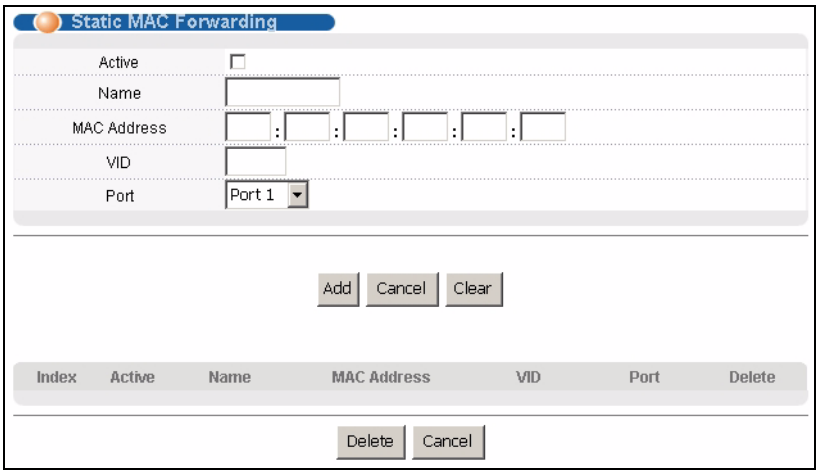
A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the switch. See Chapter 17 on page 101 for more information on port security.

9.2 Configuring Static MAC Forwarding

Click **Advanced Applications, Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 38 Static MAC Forwarding



The following table describes the labels in this screen.

Table 18 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. **Note:** Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Select a port where the MAC address entered in the previous field will be automatically forwarded.
Add	After you set the fields above, click **Add** to insert a new rule.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to begin configuring this screen afresh.
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 and 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.
VID	This field displays the VLAN identification number.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

CHAPTER 10
Filtering

This chapter discusses static IP and MAC address port filtering.

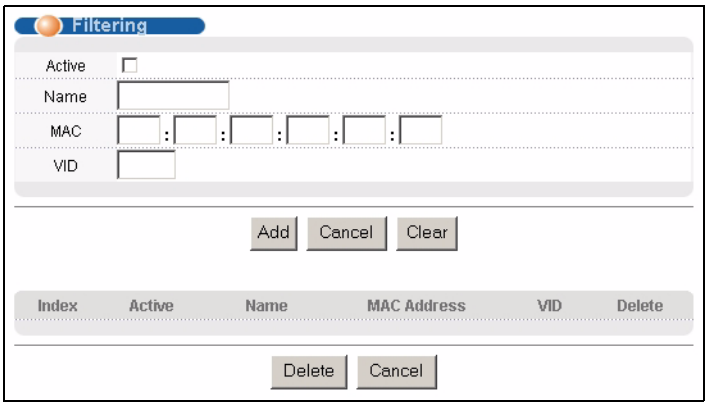
10.1 Overview

Port filtering means discarding (or dropping) packets based on the MAC addresses and VLAN group.

10.2 Configure a Filtering Rule

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

Figure 39 Filtering



The following table describes the related labels in this screen.

Table 19 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 (up to 32 printable ASCII characters) for this rule. This is for identification purpose only.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.

Table 19 FIltering (continued)

LABEL	DESCRIPTION
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.
Index	This field displays the index number of the rule. Click an index number to change the settings.
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.
VID	This field displays the VLAN identification number.
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 checkbox(es) in the **Delete** column.

CHAPTER 11
Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP).

11.1 Overview

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

11.1.1 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.

Table 20 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.

11.1.2 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.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

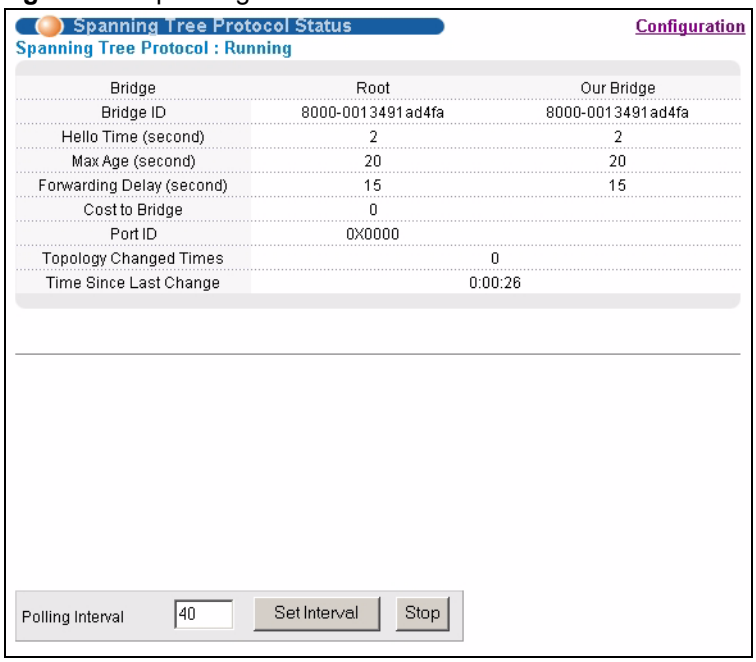
Table 21 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.2 STP Status

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

Figure 40 Spanning Tree Protocol: Status



The following table describes the labels in this screen.

Table 22 Spanning Tree Protocol: Status

LABEL	DESCRIPTION
Spanning Tree Protocol	This field displays **Running** if STP is activated. Otherwise, it displays **Down**.
Configuration	Click **Configuration** to configure STP settings. Refer to Section 11.3 on page 84.
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.
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.

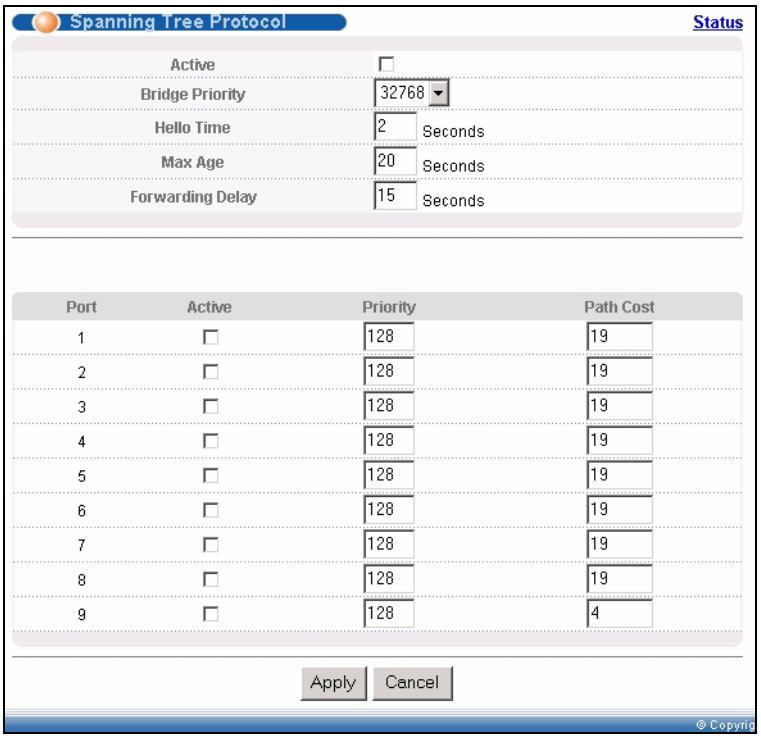
Table 22 Spanning Tree Protocol: Status (continued)

LABEL	DESCRIPTION
Polling Interval	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.

11.3 Configure STP

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

Figure 41 Spanning Tree Protocol: Configuration



The following table describes the labels in this screen.

Table 23 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Status	Click **Status** to display the **Spanning Tree Protocol Status** screen (see Figure 40 on page 83).
Active	Select this check box to activate STP. Clear this checkbox to disable STP.

Table 23 Spanning Tree Protocol: Configuration (continued)

LABEL	DESCRIPTION
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. Select a value from the drop-down list box. 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: **Note:** 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 the 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 20 on page 81 for more information.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 12
Bandwidth Control

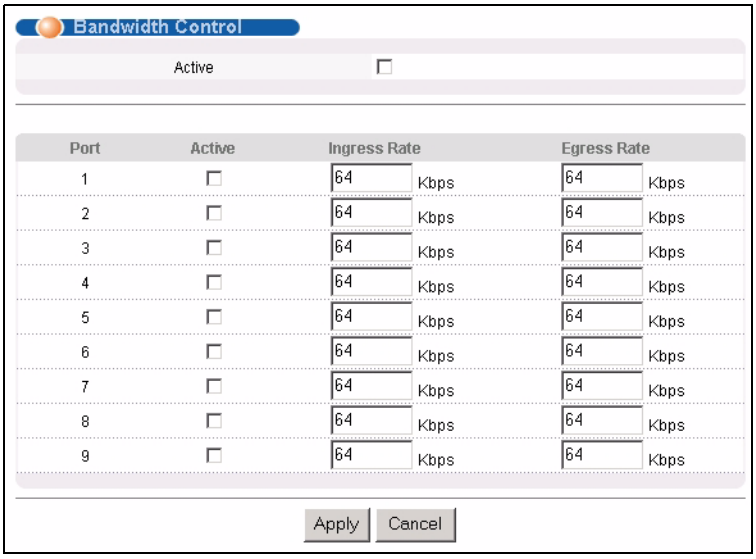
This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

12.1 Bandwidth Control Setup

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

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

Figure 42 Bandwidth Control



The following table describes the related labels in this screen.

Table 24 Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the switch.
Port	This field displays the port number.
Active	Make sure to select this check box to activate bandwidth control on a port.

Table 24 Bandwidth Control (continued)

LABEL	DESCRIPTION
Ingress Rate	Specify the maximum bandwidth allowed in Kilobits per second (Kbps) for the incoming traffic flow on a port. If you enter a number between 64 and 1728, the switch automatically rounds the number down to the nearest multiple of 64. If you enter a number between 1729 and 1999, the rate is fixed at 1792. If you enter a number between 2000 and 103999, the switch rounds the number down to the nearest multiple of 1000. On a Gigabit Ethernet/ Mini-GBIC port, the switch rounds a number down to the nearest multiple of 8000 for a number between 104000 and 1000000.
Egress Rate	Specify the maximum bandwidth allowed in Kilobits per second (Kbps) for the out-going traffic flow on a port. If you enter a number between 64 and 1728, the switch automatically rounds the number down to the nearest multiple of 64. If you enter a number between 1729 and 1999, the rate is fixed at 1792. If you enter a number between 2000 and 103999, the switch rounds the number down to the nearest multiple of 1000. On a Gigabit Ethernet/ Mini-GBIC port, the switch rounds a number down to the nearest multiple of 8000 for a number between 104000 and 1000000.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

CHAPTER 13
Broadcast Storm Control

This chapter introduces and shows you how to configure the broadcast storm control feature.

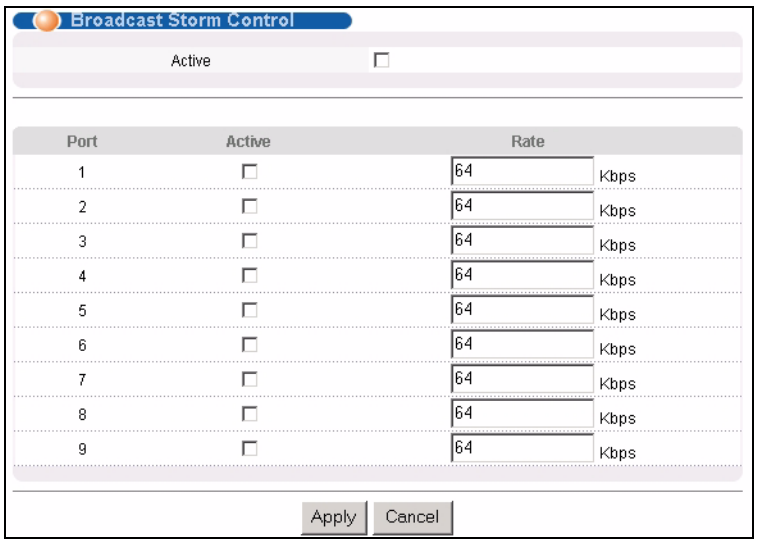
13.1 Overview

Broadcast storm control limits the number of broadcast frames that can be stored in the switch buffer or sent out from the switch. Broadcast frames that arrive when the buffer is full are discarded. Enable this feature to reduce broadcast traffic coming into your network.

13.2 Broadcast Storm Control Setup

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

Figure 43 Broadcast Storm Control



The following table describes the labels in this screen.

Table 25 Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable broadcast storm control on the switch. Clear this check box to disable the feature.
Port	This field displays a port number.
Active	Select this check box to enable broadcast storm control on the port. Clear this check box to disable the feature.
Rate	Specify the traffic a port receives in Kilobits per second (Kbps). If you enter a number between 64 and 1728, the switch automatically rounds the number down to the nearest multiple of 64. If you enter a number between 1729 and 1999, the rate is fixed at 1792. If you enter a number between 2000 and 103999, the switch rounds the number down to the nearest multiple of 1000. On a Gigabit Ethernet/ Mini-GBIC port, the switch rounds a number down to the nearest multiple of 8000 for a number between 104000 and 1000000.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 14
Mirroring

This chapter discusses the Mirror setup screens.

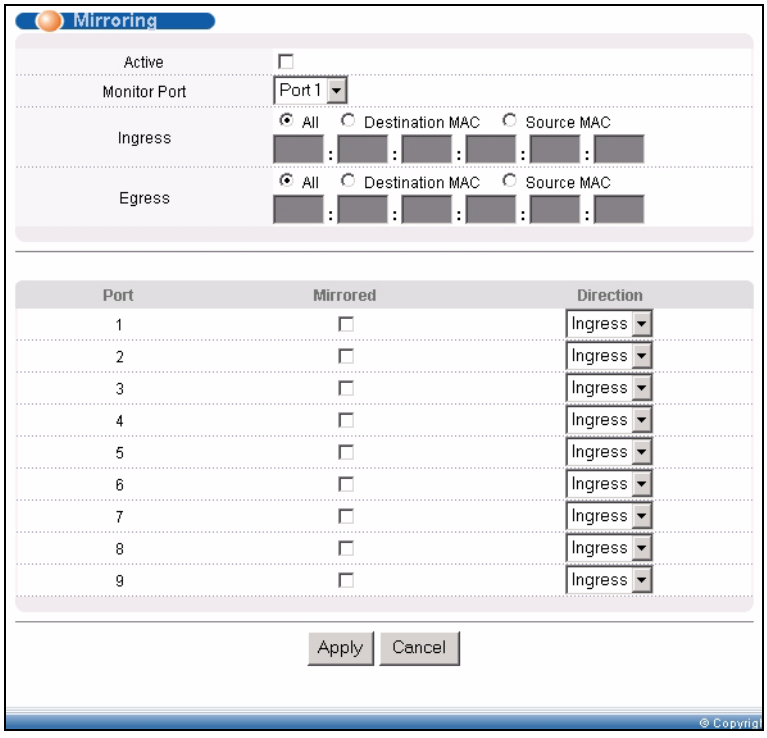
14.1 Overview

Port mirroring allows you to copy a traffic flow to a mirror port (the port you copy the traffic to) in order that you can examine the traffic from the mirror port without interference.

14.2 Port Mirroring Setup

Click **Advanced Application**, **Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a mirror port and specify the traffic flow to be copied to the mirror port.

Figure 44 Mirroring



The following table describes the labels in this screen.

Table 26 Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Mirror Port	The mirror 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.
Ingress	You can specify to copy all incoming traffic or traffic to/from a specified MAC address. Select **All** to copy all incoming traffic from the mirrored port(s). Select **Destination MAC** to copy incoming traffic to a specified MAC address on the mirrored port(s). Enter the destination MAC address in the fields provided. Select **Source MAC** to copy incoming traffic from a specified MAC address on the mirrored port(s). Enter the source MAC address in the fields provided.
Egress	You can specify to copy all outgoing traffic or traffic to/from a specified MAC address. Select **All** to copy all outgoing traffic from the mirrored port(s). Select **Destination MAC** to copy outgoing traffic to a specified MAC address on the mirrored port(s). Enter the destination MAC address in the fields provided. Select **Source MAC** to copy outgoing traffic from a specified MAC address on the mirrored port(s). Enter the source MAC address in the fields provided.
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 changes.
Cancel	Click **Cancel** to start configuring the screen again.

CHAPTER 15
Link Aggregation

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

15.1 Overview

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.

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

The beginning port of each trunk group must be physically connected to form a trunk group.

15.2 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 IEEE802.3ad 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. LACP also allows port redundancy, that is, if an operational port fails, then one of the "standby" ports become operational without user intervention. 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.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 27 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

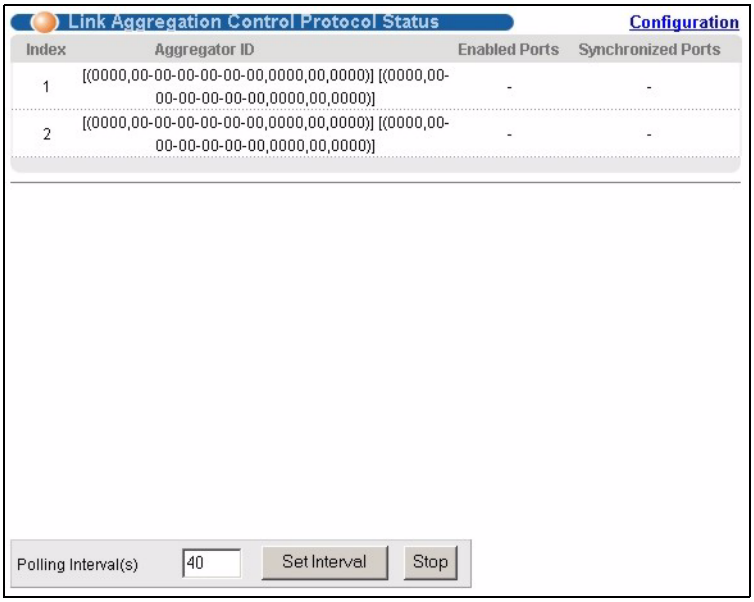
Table 28 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

15.3 Link Aggregation Status

Click **Advanced Application**, **Link Aggregation** in the navigation panel. The **Link Aggregation Control Protocol Status** screen displays by default.

Figure 45 Link Aggregation Control Protocol Status



The following table describes the labels in this screen.

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

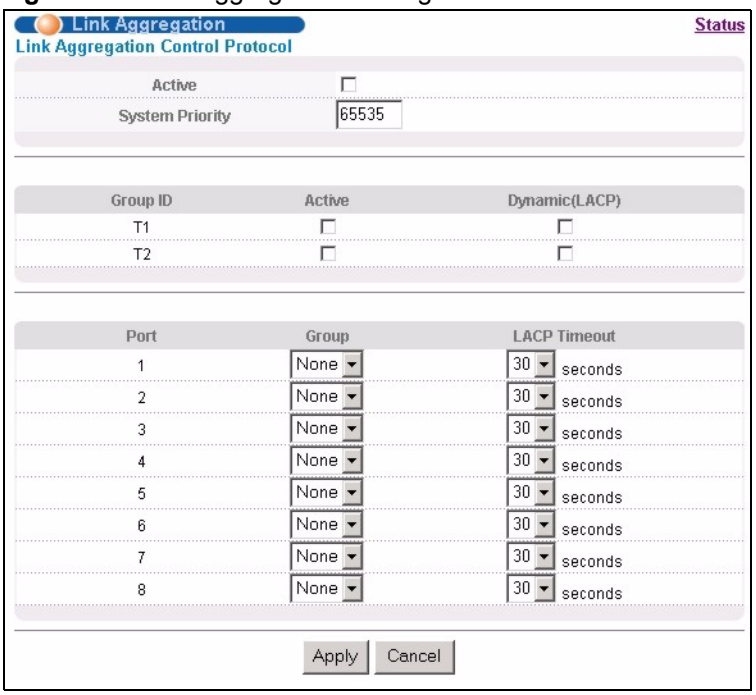
Table 29 Link Aggregation Control Protocol Status

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 Section 15.2.1 on page 94 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.

15.4 Link Aggregation Setup

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

Figure 46 Link Aggregation: Configuration



The following table describes the labels in this screen.

Table 30 Link Aggregation Control Protocol: 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.
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 16
Port Authentication

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

16.1 Overview

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 and accounting management on a network RADIUS server.

16.1.1 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 47 RADIUS Server

16.2 Port Authentication Configuration

To enable port authentication, first activate IEEE802.1x security (both on the switch and the port(s)) then configure the RADIUS server settings.

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

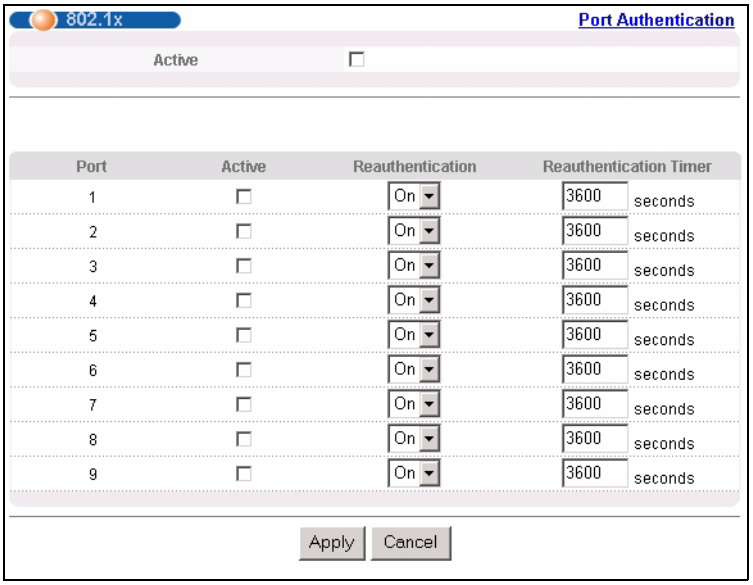
2. At the time of writing, only Windows XP of the Microsoft operating systems supports it. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install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

Figure 48 Port Authentication

16.2.1 Activate IEEE 802.1x Security

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

Figure 49 Port Authentication: 802.1x



The following table describes the labels in this screen.

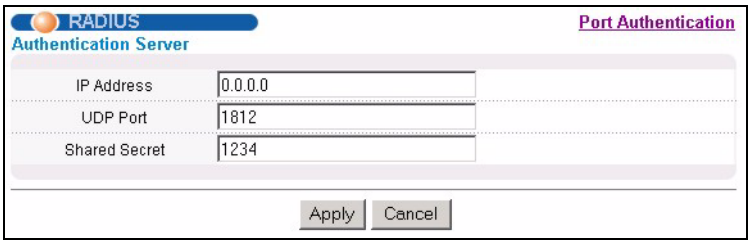
Table 31 Port Authentication: 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the switch. **Note:** You must first enable 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 802.1x authentication on this port. You must first allow 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.

16.2.2 Configuring RADIUS Server Settings

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

Figure 50 Port Authentication: RADIUS



The following table describes the labels in this screen.

Table 32 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 32 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.

CHAPTER 17
Port Security

This chapter shows you how to set up port security.

17.1 Overview

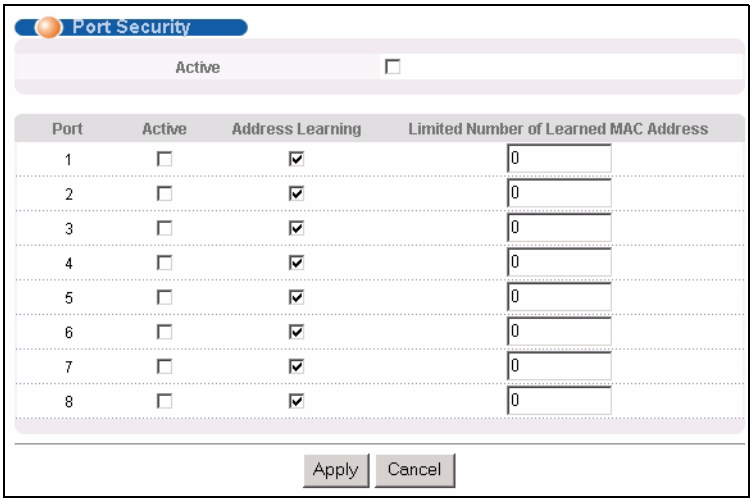
Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the switch.

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.

17.2 Port Security Setup

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

Figure 51 Port Security



The following table describes the labels in this screen.

Table 33 Port Security

LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on the switch.
Port	This field displays a port number.
Active	Select this check box to enable the port security feature on this port. The switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The switch forwards all packets 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 "254". "0" means this feature is disabled.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 18
Queuing Method

This chapter introduces the queuing methods supported.

18.1 Overview

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.

Table 34 Physical Queue Priority

QUEUE	PRIORITY
Q3	4 (highest)
Q2	3
Q1	2
Q0	1 (lowest)

18.1.1 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, Q3 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q2 is transmitted until Q2 empties, and then traffic is transmitted on Q1 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.

18.1.2 Weighted Round Robin Scheduling (WRR)

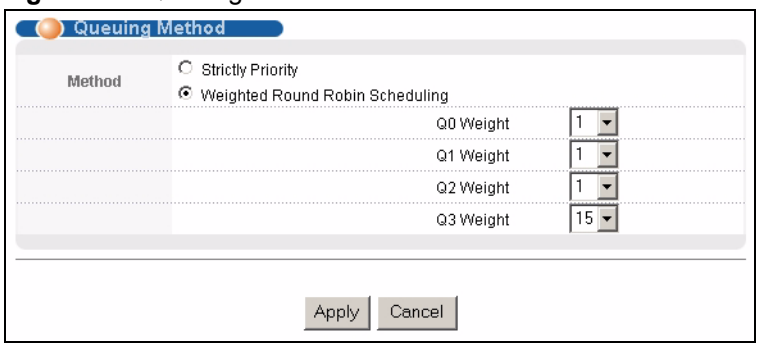
Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal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

18.2 Configuring Queuing Method

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

Figure 52 Queuing Method



The following table describes the labels in this screen.

Table 35 Queuing Method

LABEL	DESCRIPTION
Method	Select **Strictly Priority** or **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. Q3 has the highest priority and Q0 the lowest. The default queuing method is **Strictly Priority.** Weighted Round Robin Scheduling (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. **Note:** When you select **SPQ**, it applies to Q3 only (with priority over all other queues). Q0 ~ Q2 will use **Weighted Round Robin**.
Weight	When you select **Weighted Round Robin Scheduling**, use the drop-down list boxes to choose queue weights (1-15). Bandwidth is divided across the different traffic queues according to their weights.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 19
Static Route

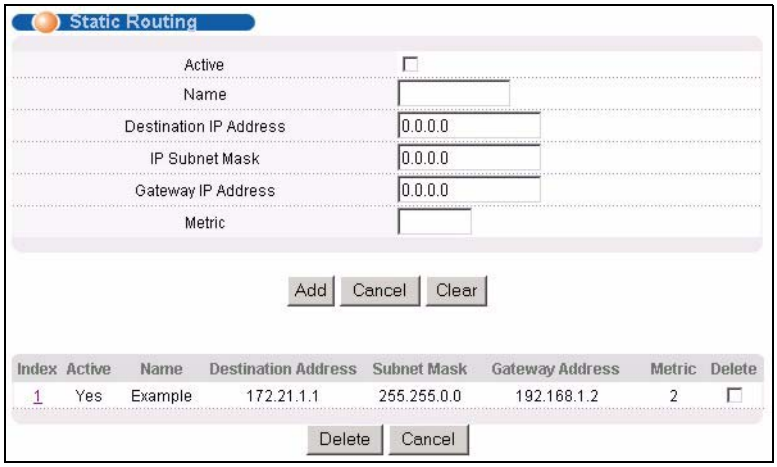
This chapter shows you how to configure static routes.

19.1 Configuring Static Route

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

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

Figure 53 Static Routing



The following table describes the labels in this screen.

Table 36 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
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 36 Static Routing (continued)

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 insert a new static route.
Cancel	Click **Cancel** to reset the above fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
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 it is 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	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

CHAPTER 20
Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the switch.

20.1 Overview

Quality of Service (QoS) mechanisms provide the best service on a per-flow guarantee. To fine-tune the levels of services on the priority of the traffic flow using QoS places a heavy burden on the network infrastructure.

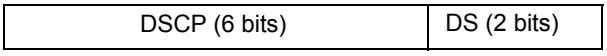
DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. 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.

20.1.1 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.

Figure 54 DiffServ: Differentiated Service Field

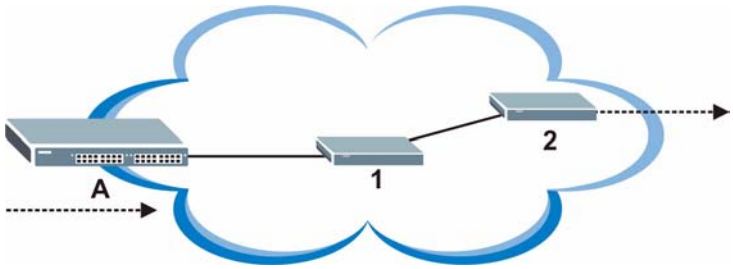


The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and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

20.1.2 DiffServ Network Example

The following figure depicts a simple DiffServ network consisting of a group of contiguous DiffServ-compliant network devices.

Figure 55 DiffServ Network Example



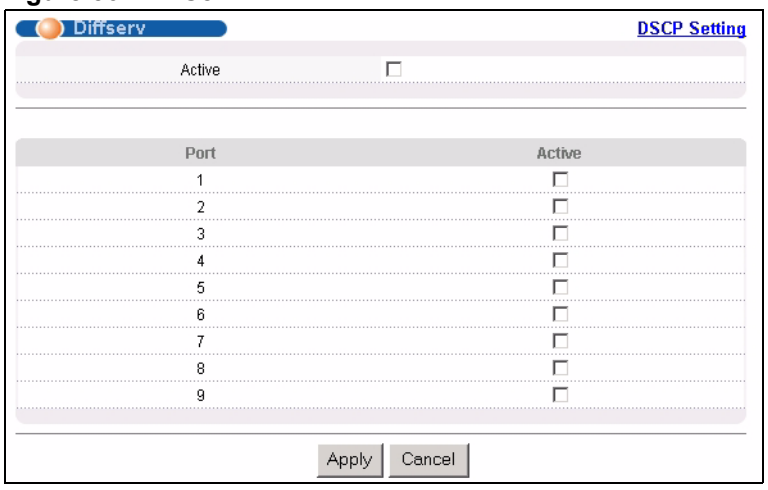
Switch **A** marks traffic flowing into the network based on the configured marking rules. Intermediary network devices **1** and **2** allocate network resources (such as bandwidth) by mapping the DSCP values and the associated policies.

20.2 Activating DiffServ

Activate DiffServ to allow the switch to enable DiffServ on the selected port(s).

Click **IP Application**, **DiffServ** in the navigation panel to display the screen as shown.

Figure 56 DiffServ



The following table describes the labels in this screen.

Table 37 DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the switch.
Port	This field displays the index number of a port on the switch.
Active	Select this option to enable DiffServ on the port.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to start configuring this screen again.

20.3 DSCP-to-IEEE802.1p Priority Mapping

You can configure the DSCP to IEEE802.1p mapping to allow the switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1P mapping.

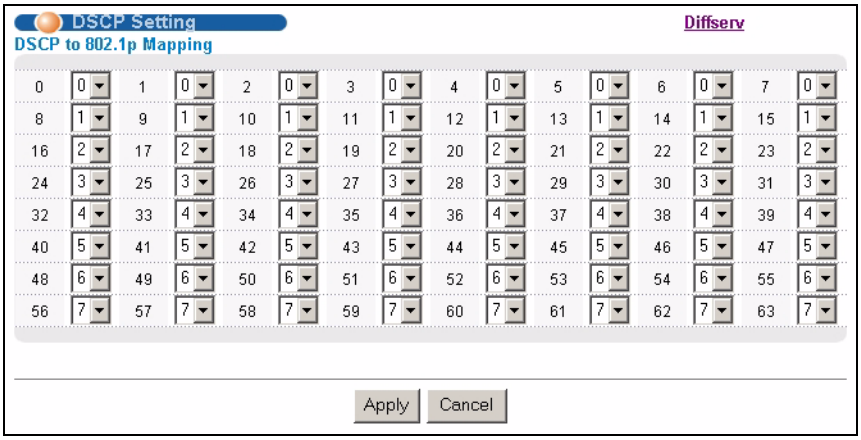
Table 38 Default DSCP-IEEE802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE802.1P	0	1	2	3	4	5	6	7

20.3.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 57 DiffServ: DSCP Setting



The following table describes the labels in this screen.

Table 39 DiffServ: DSCP Setting

LABEL	DESCRIPTION
0 … 63	This is the DSCP classification identification number. To set the IEEE802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and start configuring the screen again.

CHAPTER 21
Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

21.1 The Maintenance Screen

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

Figure 58 Maintenance

The following table describes the labels in this screen.

Table 40 Maintenance

LABEL	DESCRIPTION
Firmware Upgrade	Access this screen to upload a new firmware.
Restore Configuration	Access this screen to upload a previously saved configuration file to the switch.
Backup Configuration	Access this screen to back up the current switch configuration.
Load Factory Default	Click the button to clear all switch configuration information you configured and return to the factory defaults. **Note:** All custom configuration will be lost. This takes up to two minutes (or wait until the switch finishes rebooting). If you want 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).
Reboot System	Click the button to restart the switch without physically turning the power off. **Note:** This takes up to two minutes (or wait until the switch finishes rebooting). This does not affect the switch's configuration.

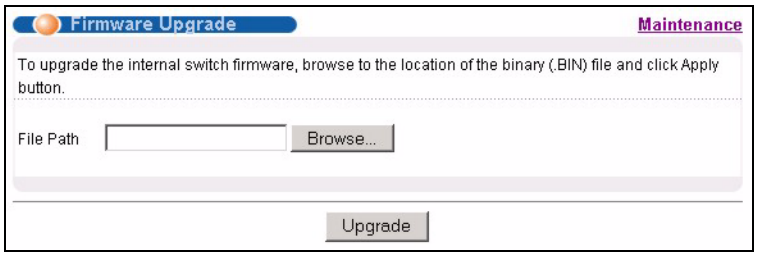
21.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Note: 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 59 Firmware Upgrade



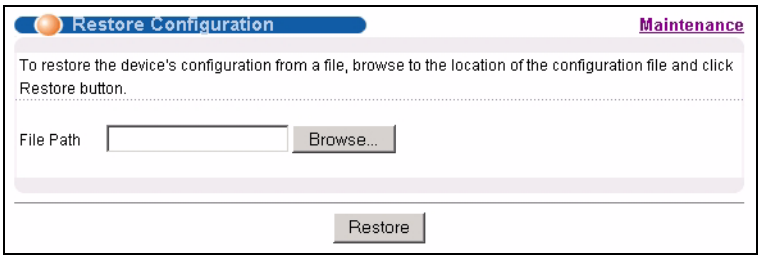
Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

21.3 Restore a Configuration File

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

Figure 60 Restore Configuration



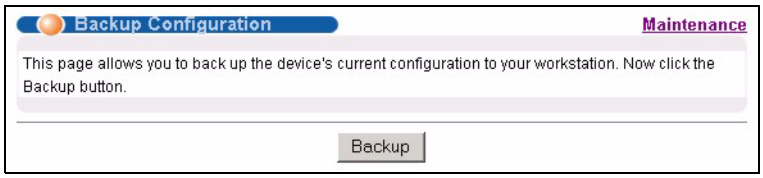
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file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

21.4 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 **Backup Configuration** screen.

Figure 61 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.

21.5 Load Factory Defaults

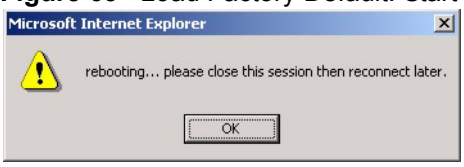
Follow the steps below to reset the switch back to the factory defaults.

1. In the **Maintenance** screen, click 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 62 Load Factory Default: Conformation

2. Click **OK** to display the screen shown next.

Figure 63 Load Factory Default: Start



3 Click **OK** to begin resetting all switch configurations to the factory defaults and then wait for the switch to restart. This takes up to two minutes. If you want 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).

21.6 Reboot System

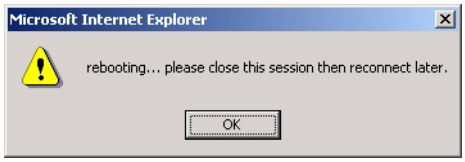
Reboot System allows you to restart the switch without physically turning the power off. Follow the steps below to reboot the switch.

1 In the **Maintenance** screen, click the **Click Here** button next to **Reboot System** to display the next screen.

Figure 64 Reboot System: Confirmation

2 Click **OK** to display the screen shown next.

Figure 65 Reboot System: Start



3 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.

21.7 FTP Command Line

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

21.7.1 Filename Conventions

The configuration file contains the settings in the screens such as password, switch setup, IP Setup, etc. Once you have customized the switch's settings, they can be saved (as a plain text file) back to your computer under a filename of your choosing.

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

Table 41 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, system-related data (including the default password), the error log and the trace log.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the switch.

21.7.1.1 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.

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

21.7.2 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 to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the switch to your computer and renames it to "config.cfg". See Table 41 on page 115 for more information on filename conventions.

7 Enter `quit` to exit the ftp prompt.

21.7.3 GUI-based FTP Clients

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

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).

21.7.4 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 22
Access Control

This chapter describes how to control access to the switch.

22.1 Overview

- 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.

Figure 66 Console Port Priority

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

- A console port or Telnet session can coexist with one FTP session, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions.

Table 42 Access Control Overview

	Console Port	SSH	Telnet	FTP	Web	SNMP
Number of concurrent sessions allowed	1 console port, SSH or Telnet. Console port has the highest priority and Telnet has the lowest priority.			1	5	No limit

22.2 The Access Control Main Screen

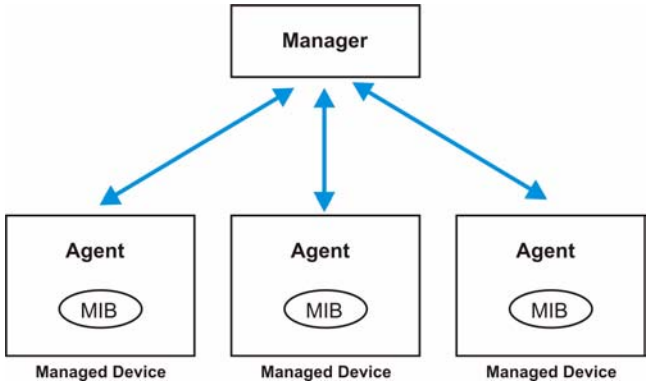
Click **Management**, **Access Control** in the navigation panel to display the main screen as shown.

Figure 67 Access Control

22.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). 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 68 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 switch). 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 43 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
Get Next	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 Get Next operations.

Table 43 SNMP Commands

COMMAND	DESCRIPTION
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.

22.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- Private MIBs

22.3.2 SNMP Traps

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

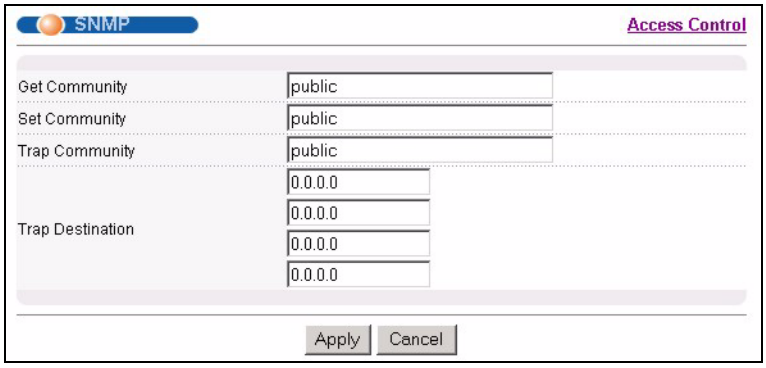
Table 44 SNMP Traps

GENERIC TRAP	SPECIFIC TRAP	DESCRIPTION
0 (Cold Start)	0	This trap is sent when the switch is turned on.
1 (Warm Start)	0	This trap is sent when the switch restarts.
2 (linkDown)	0	This trap is sent when the Ethernet link is down.
3 (linkUp)	0	This trap is sent when the Ethernet link is up.
4 (Authentication Failure)	0	This trap is sent when an SNMP request comes from non-authenticated hosts.

22.3.3 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 69 Access Control: SNMP



The following table describes the labels in this screen.

Table 45 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.

22.4 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.

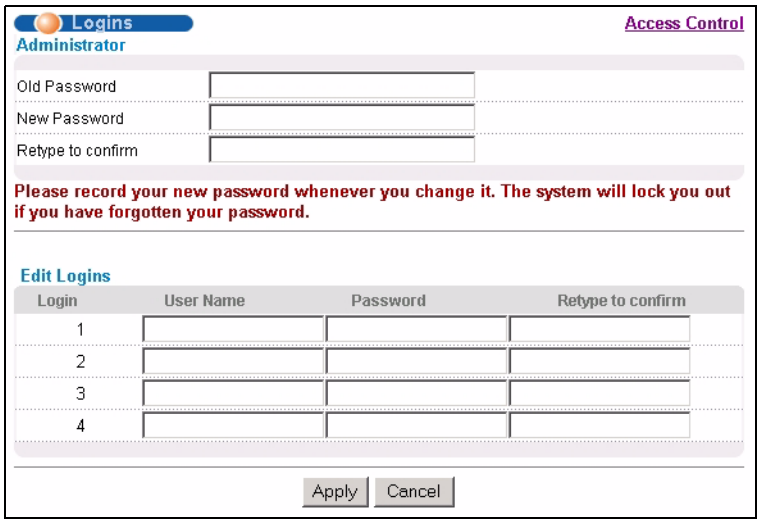
- An administrator is someone who can both view and configure switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

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

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

Figure 70 Access Control: Logins



The following table describes the labels in this screen.

Table 46 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 30 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.

22.5 SSH Overview

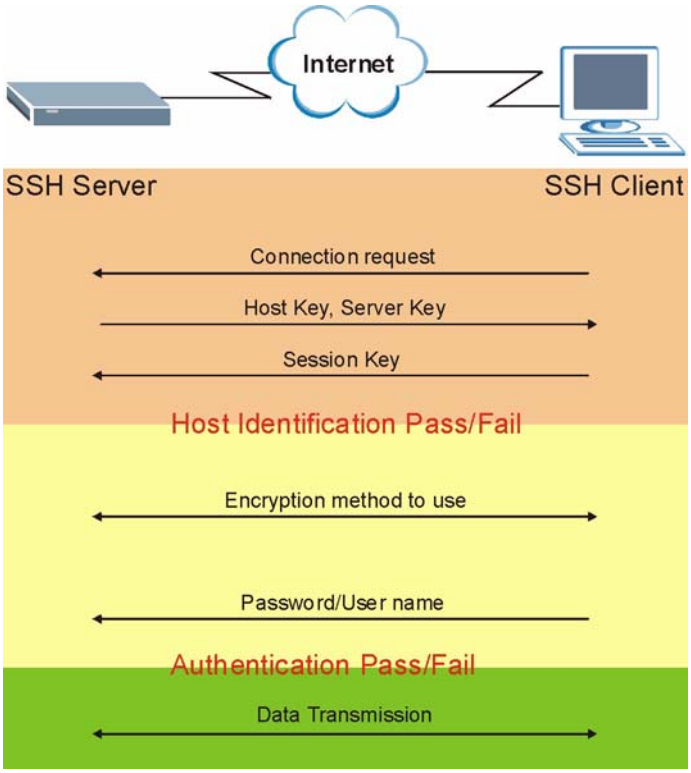
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 71 SSH Communication Example

22.6 How SSH works

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

Figure 72 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.

22.7 SSH Implementation on the Switch

Your switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

22.7.1 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.

22.7.2 SSH Login Example

You can use an SSH client program to access the switch. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Figure 73 SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: HOST IDENTIFICATION HAS CHANGED!         @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key to "C:/Documents and Settings/Administrator/Application
Data/SSH/hostkeys/key_22_192.168.1.1.pub" to get rid of this message.
Received server key's fingerprint: xigil-gidot-homug-duzab-tocyh-pamyb-
ronep-tisaf-hebip-gokeb-goxix You can get a public key's fingerprint by
running % ssh-keygen -F publickey.pub
on the keyfile. Agent forwarding is disabled to avoid attacks by corrupted
servers. X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)? yes

Do you want to change the host key on disk (yes/no)? yes

Agent forwarding re-enabled.
X11 forwarding re-enabled.
Host key saved to C:/Documents and Settings/Administrator/Application Data/
SSH/hostkeys/key_22_192.168.1.1.pub host key for 192.168.1.1, accepted by
Administrator Thu May 12 2005 09:52:21
admin's password:
Authentication successful.
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras>
```

22.8 Introduction to HTTPS

HTTPS (Hyper Text 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.

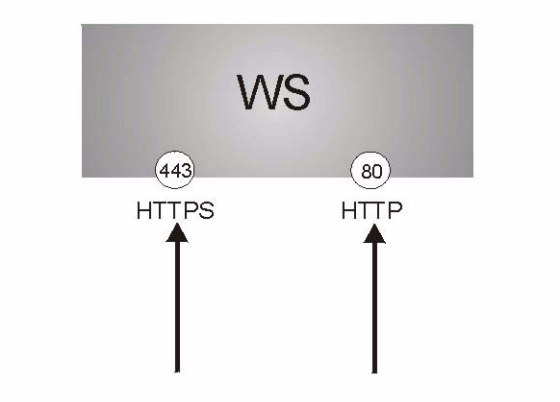
HTTPS on the switch is used so that you may securely access the switch using the web configurator. The SSL protocol specifies that the SSL server (the switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the switch a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the switch.

Please refer to the following figure.

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

2 HTTP connection requests from a web browser go to port 80 (by default) on the switch's WS (web server).

Figure 74 HTTPS Implementation



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

22.9 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.

22.9.1 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 75 Security Alert Dialog Box (Internet Explorer)

22.9.2 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 76 Security Certificate 1 (Netscape)

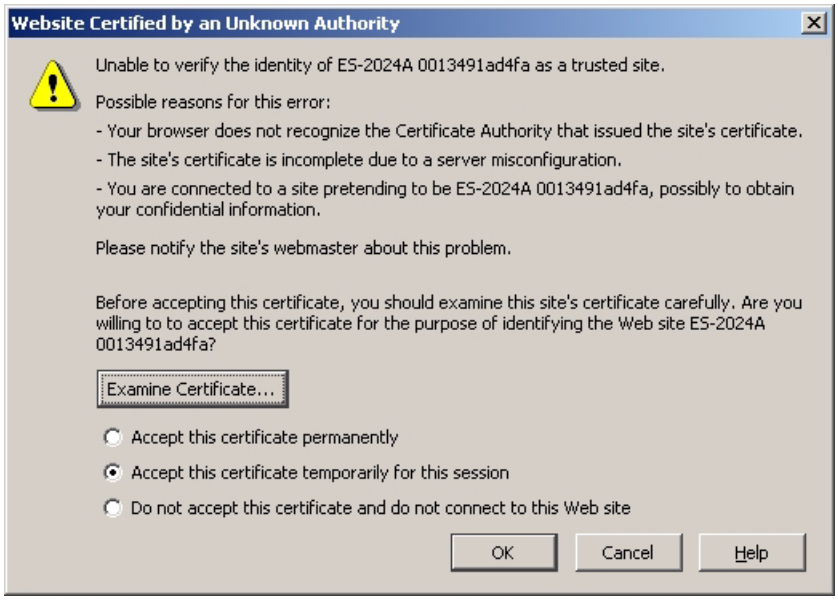
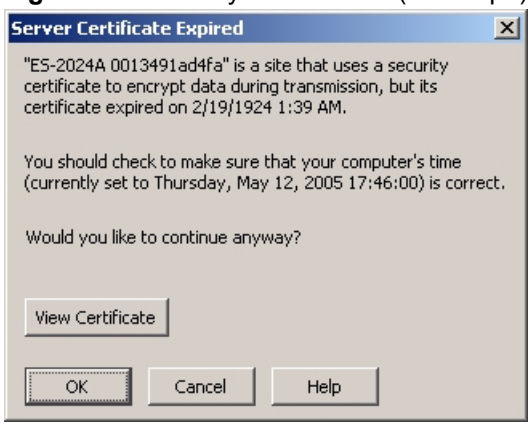


Figure 77 Security Certificate 2 (Netscape)



22.9.3 The Main Screen

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

Figure 78 Login Screen (Internet Explorer)

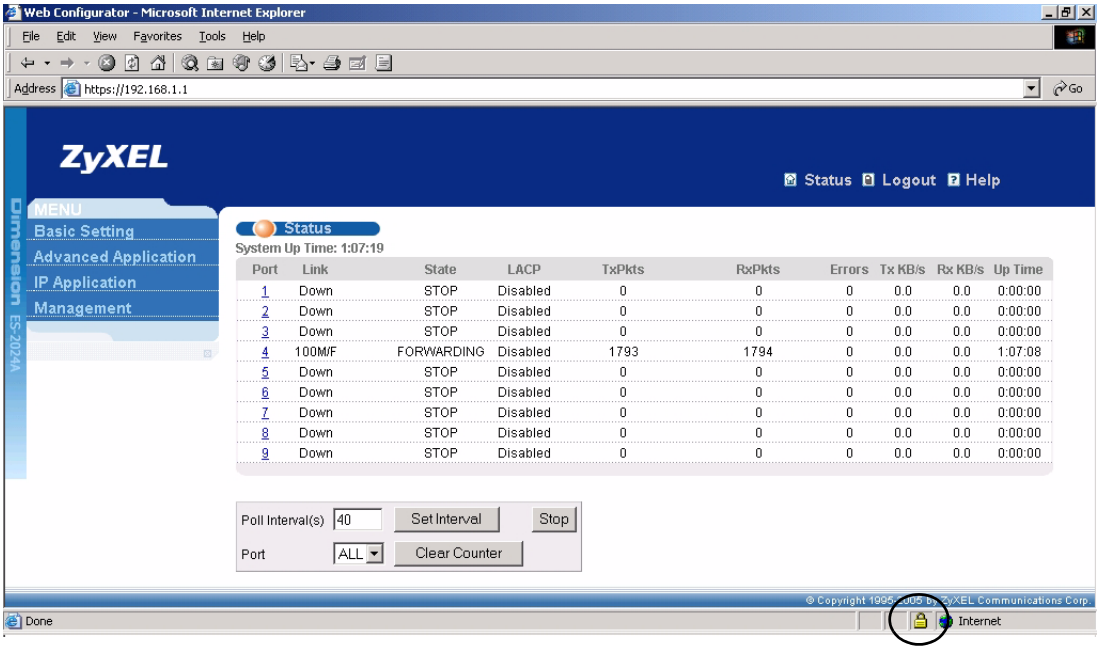
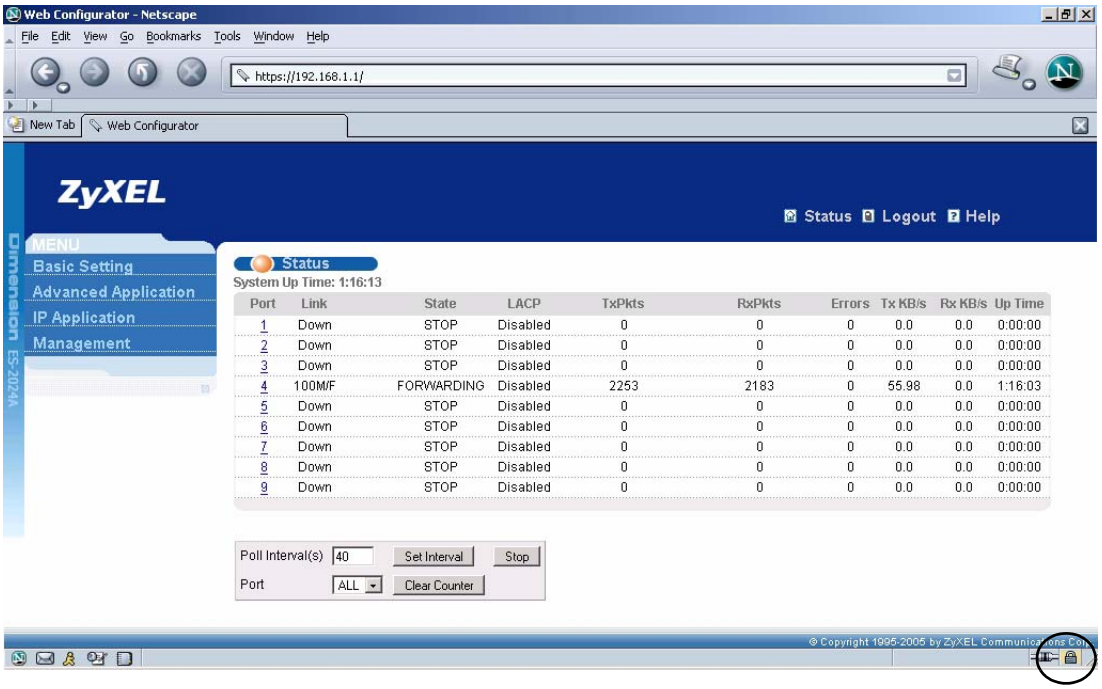


Figure 79 Login Screen (Netscape)

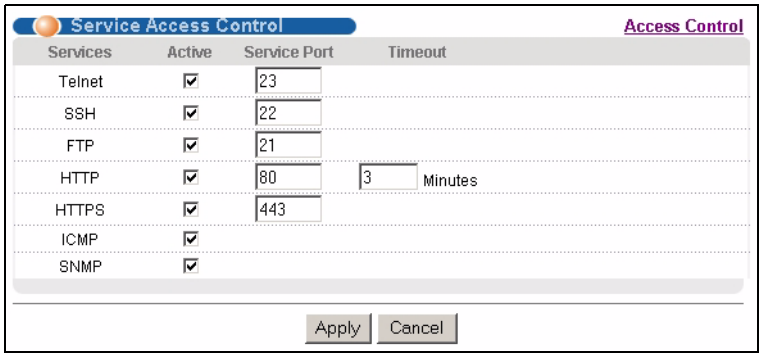


22.10 Service Port Access Control

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 main **Access Control** screen.

Figure 80 Access Control: Service Access Control



The following table describes the fields in this screen.

Table 47 Access Control: Service Access Control

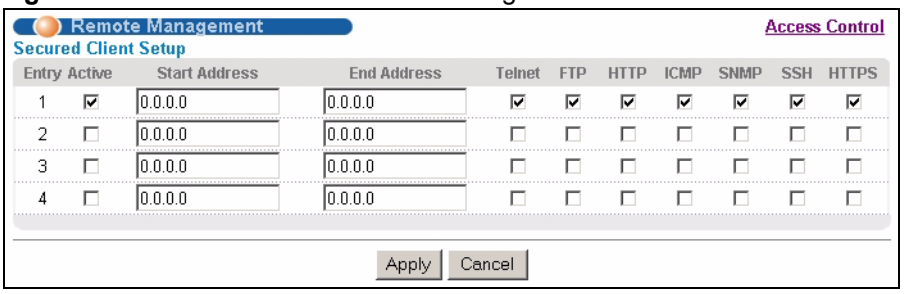
LABEL	DESCRIPTION
Services	Services you may use to access the switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Server 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 time-outs may have security risks.
Apply	Click **Apply** to save your changes back to the switch.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22.11 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 81 Access Control: Remote Management



The following table describes the labels in this screen.

Table 48 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 from 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/ Web/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.

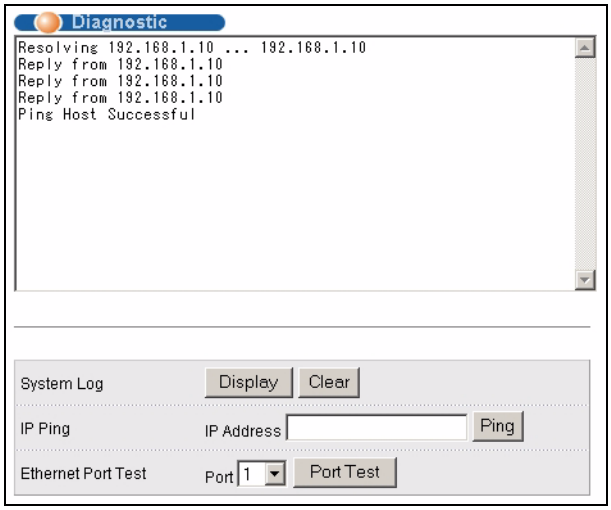
CHAPTER 23
Diagnostic

This chapter explains the **Diagnostic** screen.

23.1 Diagnostic

Click **Management**, **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, reset the system or ping IP addresses.

Figure 82 Diagnostic



The following table describes the labels in this screen.

Table 49 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 24
Cluster Management

This chapter introduces cluster management.

24.1 Overview

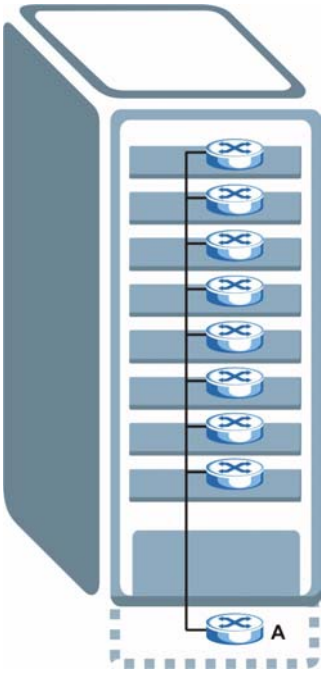
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 50 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 83 Clustering Application Example

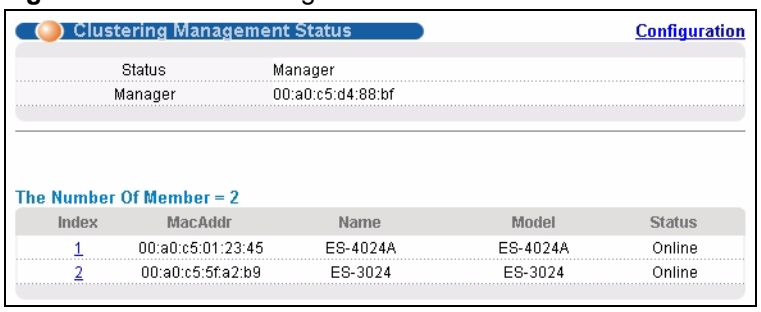


24.2 Cluster Management Status

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

Note: A cluster can only have one manager.

Figure 84 Cluster Management: Status



The following table describes the labels in this screen.

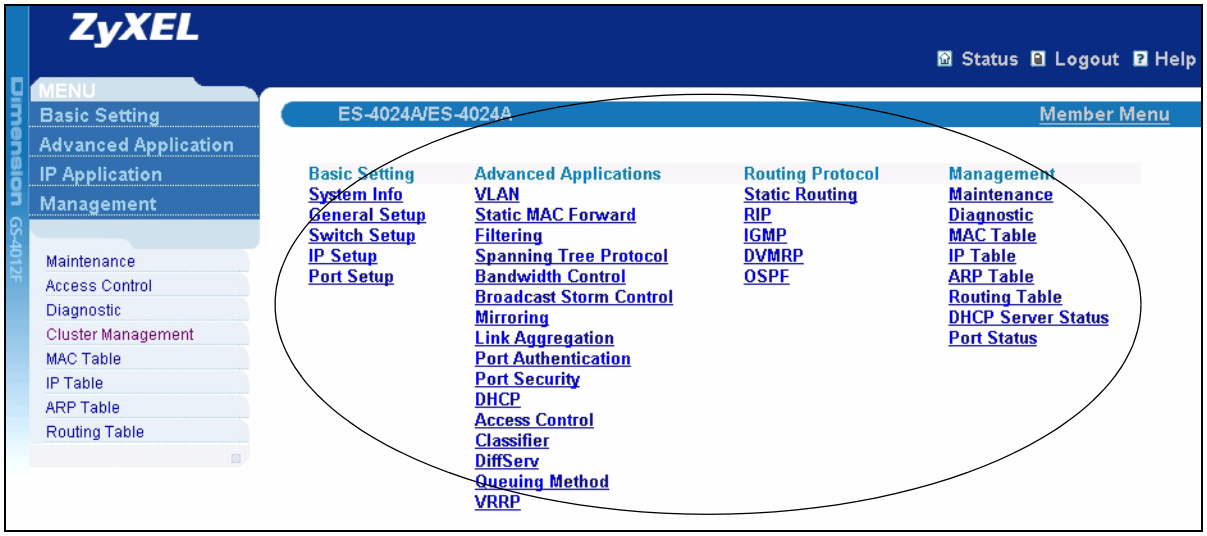
Table 51 Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **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 85 on page 135).
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.
Status	This field displays: **Online** (the cluster member switch is accessible) **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.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

24.2.1 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.

Figure 85 Cluster Management: Cluster Member Web Configurator Screen



24.2.1.1 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.

Figure 86 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220  FTP version 1.0 ready at Thu Jan  1 00:47:52 1970
User (192.168.1.1:(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         3209434 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-a0-c5-d4-88-bf
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-d4-88-bf
226 File sent OK
ftp: 463 bytes received in 0.00Seconds 463000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 350du1.bin fw-00-a0-c5-d4-88-bf
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-d4-88-bf
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

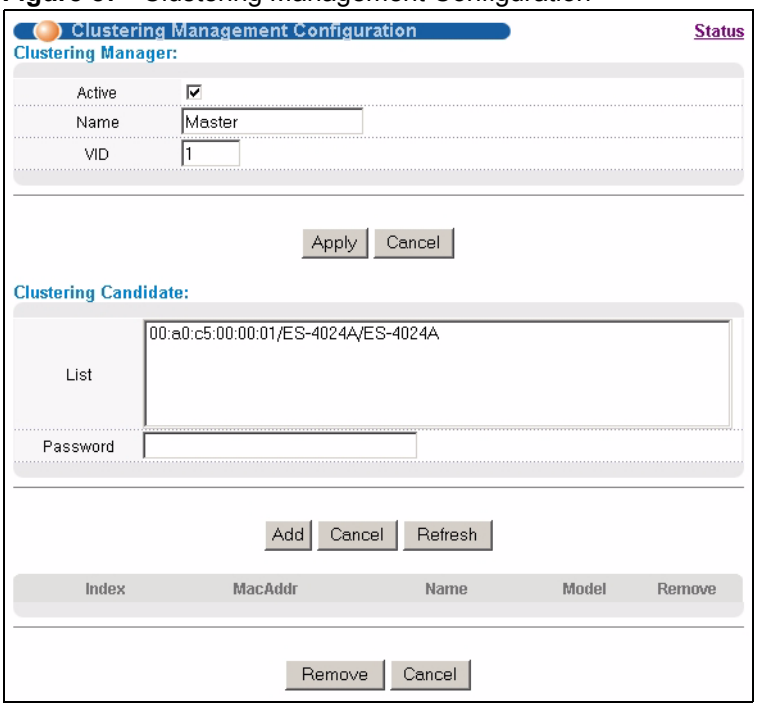
Table 52 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
`User`	Enter "admin".
`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.
`350du1.bin`	This is the name of the firmware file you want to upload to the cluster member switch.
`fw-00-a0-c5-d4-88-bf`	This is the cluster member switch's firmware name as seen in the cluster manager switch.
`config-00-a0-c5-d4-88-bf`	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

24.3 Configuring Cluster Management

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

Figure 87 Clustering Management Configuration



The following table describes the labels in this screen.

Table 53 Clustering Management Configuration

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 20 printable characters (no spaces are allowed).
VID	This is the VLAN ID and is only applicable if the switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same 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.
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.

Table 53 Clustering Management Configuration (continued)

LABEL	DESCRIPTION
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.
Add	Click **Add** to save this part of the screen 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 information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
HwAddr	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 25
MAC Table

This chapter introduces the **MAC Table** screen.

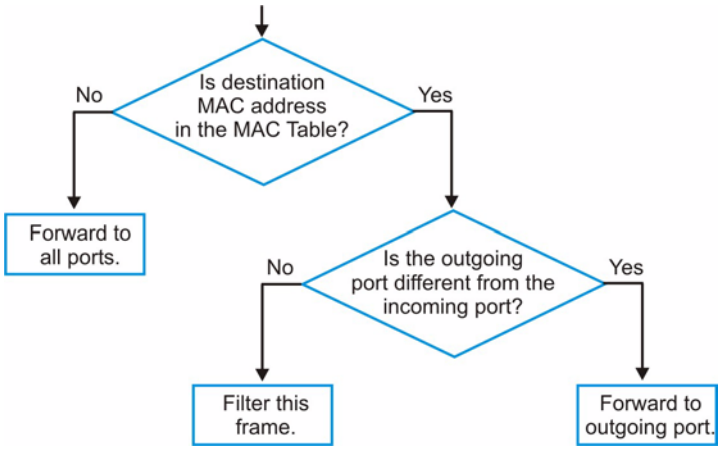
25.1 Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) 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 the **Static MAC Forwarding** screen).

The switch uses the MAC table 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 MAC table.
    - 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.

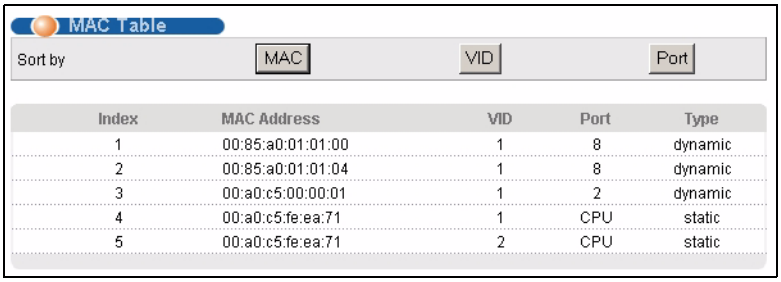
Figure 88 MAC Table Flowchart



25.2 Viewing the MAC Table

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

Figure 89 MAC Table



The following table describes the labels in this screen.

Table 54 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. This field displays Drop if you configure a filtering rule to drop the traffic from the MAC address.
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. This field displays **drop** if you configure a filter rule for the MAC address in the **Filtering** screen.
Type	This shows whether the MAC address is **dynamic** (learned by the switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

CHAPTER 26
ARP Table

This chapter introduces ARP Table.

26.1 Overview

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.

26.1.1 How ARP Works

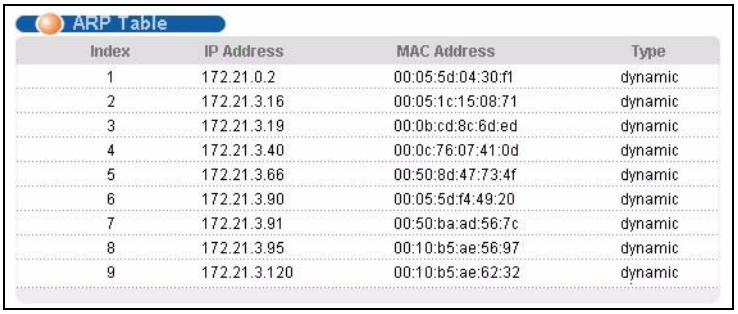
When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

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.

26.2 Viewing the ARP Table

Click **Management**, **ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s).

Figure 90 ARP Table


ARP Table

Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic

The following table describes the labels in this screen.

Table 55 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 the **Static MAC Forwarding** screen).

CHAPTER 27
Introducing the Commands

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

27.1 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.

Note: See the web configurator parts of this User's Guide for background information on features configurable by the web configurator.

27.1.1 Switch Configuration File

When you configure the switch using either the CLI (Command Line Interface) 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.

Note: 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.

27.2 Accessing the CLI

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

Note: 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.

27.2.1 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 CLI management session 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.

27.2.2 The Console Port

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

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

27.2.2.1 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 27.3 on page 145).

Figure 91 Initial Console Port Screen

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
initialize switch, ethernet address: 00:13:49:1a:d4:fa
ZyXEL ADM5120 10/100 Mbps Ethernet Controller 2002.9.27.0
Press ENTER to continue...
```

27.2.3 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 27.3 on page 145).

27.2.4 SSH

You can use an SSH client program to access the switch. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Figure 92 SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: HOST IDENTIFICATION HAS CHANGED!         @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the host key has just been changed.
Please contact your system administrator.
Add correct host key to "C:/Documents and Settings/Administrator/Application
Data/SSH/hostkeys/key_22_192.168.1.1.pub" to get rid of this message.
Received server key's fingerprint: xigil-gidot-homug-duzab-tocyh-pamyb-
ronep-tisaf-hebip-gokeb-goxix You can get a public key's fingerprint by
running % ssh-keygen -F publickey.pub
on the keyfile. Agent forwarding is disabled to avoid attacks by corrupted
servers. X11 forwarding is disabled to avoid attacks by corrupted servers.
Are you sure you want to continue connecting (yes/no)? yes

Do you want to change the host key on disk (yes/no)? yes

Agent forwarding re-enabled.
X11 forwarding re-enabled.
Host key saved to C:/Documents and Settings/Administrator/Application Data/
SSH/hostkeys/key_22_192.168.1.1.pub host key for 192.168.1.1, accepted by
Administrator Thu May 12 2005 09:52:21
admin's password:
Authentication successful.
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras>
```

27.3 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".

Figure 93 CLI Login

```
                Enter User Name : admin
                Enter Password : XXXX
```

27.4 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 "`configure`" 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.

27.5 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.

27.5.1 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.

Figure 94 CLI Help: List of Commands: Example 1

```
ras> help
  Commands available:

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

Figure 95 CLI Help: List of Commands: Example 2

```
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
    logout                    Exit from the EXEC
    ping                      Exec ping
    show                      Show system information
    ssh                       SSH client
    traceroute                Exec traceroute
ras>
```

27.5.2 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.

Figure 96 CLI Help: Detailed Command Information: Example 1

```
ras> ping help
  Commands available:
  ping <ip>
    <
      [ vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
ras>
```

Figure 97 CLI: Help: Detailed Command Information: Example 2

```
ras> ping ?
    <ip>                        destination ip address
    help                        Description of ping help
```

27.6 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 `configure` or `config`. The Configure mode command prompt consists of the word "`config`" and the pound sign (#). There are various sub configuration modes: interface, router and VLAN.

- To enter config-vlan mode, type `vlan` followed by a number (between 1 to 4094). For example, `vlan 10` to configure settings for VLAN 10.
- To enter config-interface mode and configure the ports, enter `interface port-channel` followed by a port number. For example, `interface port-channel 8`.

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

27.7 Using Command History

The switch keeps a list of up to 256 commands 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.

Figure 98 CLI: History Command Example

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

27.8 Saving Your Configuration

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

Figure 99 CLI: write memory

```
ras# write memory
```

Note: 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.

27.8.1 Logging Out

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

27.9 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.

27.9.1 User Mode

The following table describes the commands available for User mode.

Table 56 Command Summary: User Mode

COMMAND		DESCRIPTION
`enable`		Accesses Enable (or privileged) mode. See Section 27.9.2 on page 150.
`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.
`logout`		Exits from the CLI.
`ping`	`<IP|host-name>`	Sends Ping request to an Ethernet device.
	`<IP|host-name> [vlan <vlan-id>] [size <0-1472>] [-t]`	Sends Ping request to an Ethernet device in the specified VLAN(s) with the specified parameters.
	`help`	Displays command help information.
`show`	`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>`	Determines the path a packet takes to a device.
	`<ip|host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]`	Determines the path a packet takes to a device in a VLAN.
	`help`	Displays command help information.

27.9.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 57 Command Summary: Enable Mode

COMMAND			DESCRIPTION
`baudrate`	`<1|2|3|4|5>`		Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).
`boot`	`config`		Restarts the system.
`configure`			Accesses Configuration mode. See Section 27.9.3 on page 153.
`disable`			Exits Enable (or privileged) mode.

Table 57 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION
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.
logout			Exits Enable (or privileged) mode.
mac-flush			Clears the MAC address table.
	<port-num>		Removes all learned MAC address on the specified port(s).
no	arp		Clears the ARP table.
	interface		Clears interface statistics.
	logging		Disables syslog logging.
ping	<IP|host-name>		Sends Ping request to an Ethernet device.
		[vlan <vlan-id>][..]	Sends Ping request to an Ethernet device in the specified VLAN(s).
	help		Displays command help information.
reload	config		Restarts the system.
show	cluster		Displays cluster management status.
		candidates	Displays cluster candidate information.
		member	Displays the MAC address of the cluster member(s).
		member mac <mac-addr>	Displays the status of the cluster member(s).
		members config	Displays the configuration of the cluster member(s).
	diffserv		Displays general DiffServ settings.
	garp		Displays GARP information.
	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.
	interface <port-number>		Displays current interface status.
	interfaces config <port-list>		Displays current interface configuration.
		bandwidth-control	Displays bandwidth control settings.

Table 57 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION
		bstorm-control	Displays broadcast storm control settings.
		egress	Displays outgoing port information.
	ip		Displays IP related information.
		arp	Displays the ARP table.
		route	Displays IP routing information.
		route static	Displays IP static route information.
	lacp		Displays LACP (Link Aggregation Control Protocol) settings.
	logging		Displays system logs.
	loginPrecedence		Displays login precedence settings.
	logins		Displays login account information.
	mac	address-table <all [mac|vid|port]>	Displays MAC address table. You can sort by MAC address, VID or port.
		address-table static	Displays static MAC address table.
	mac-aging-time		Displays MAC learning aging time.
	multi-login		Displays multi-login information
	plt		DIsplays PLT (Port Loopback Test) 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.
		[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 internal SSH public and private key information.
		known-hosts	Displays known SSH hosts information.

Table 57 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION
		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.
	vlan-stacking		Displays VLAN stacking settings.
	vlan1q	gvrp	Displays GVRP settings.
		port-isolation	Displays port isolation settings.
ssh	<1|2> <[user@]dest-ip>		Connects to an SSH server with the specified SSH version.
		[command </>]	Connects to an SSH server with the specified SSH version and addition commands to be executed on the server.
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.
	help		Displays command help information.
write	memory		Saves current configuration to the configuration file the switch is currently using.
		<index>	Saves current configuration to the specified configuration file on the switch.

27.9.3 General Configuration Mode

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

Table 58 Command Summary: Configuration Mode

COMMAND			DESCRIPTION
admin-password	<pw-string> <confirm-string>		Changes the administrator password.
bandwidth-control			Enables bandwidth control.
diffserv			Enables DiffServ.
	dscp <0-63> priority <0-7>		Sets the DSCP-to-IEEE 802.1q mappings.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
exit			Exits from the CLI.
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.
help			Displays help information.
history			Displays a list of previous command(s) that you have executed.
hostname	<name_string>		Sets the switch's name for identification purposes.
https	cert-regeneration <rsa|dsa>		Re-generates a certificate.
	timeout <0-65535>		Sets the HTTPS timeout period.
igmp-snooping			Enables IGMP snooping.
interface	port-channel <port-list>		Enables a port or a list of ports for configuration. See Section 27.9.4 on page 160 for more details.
ip	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.
logout			Exits from the CLI.
mac-aging-time	<10-3000>		Sets learned MAC aging time.
mac-filter	name <name> mac <mac-addr> vlan <vlan-id>		Configures a static MAC address port filtering rule.
		inactive	Disables a static MAC address port filtering rule.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Configures a static MAC address forwarding rule.
		inactive	Disables a static MAC address forwarding rule.
mirror-filter	egress	mac <mac-addr>	Sets port mirroring for the MAC address on the outgoing traffic.
		type <all|dest|src>	Sets the direction of the outgoing traffic for port mirroring.
	ingress	mac <mac-addr>	Sets port mirroring for the MAC address on the incoming traffic.
		type <all|dest|src>	Sets the direction of the incoming traffic for port mirroring.
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.
no	bandwidth-control		Disable bandwidth control on the switch.
	cluster		Disables cluster management on the switch.
	cluster member	<mac-address>	Removes the cluster member.
	diffserv		Disables the DiffServ settings.
	https	timeout	Resets the session timeout to the default of 300 seconds.
	igmp-snooping		Disables IGMP snooping.
	ip		Sets the management IP address to the default value.
		route <ip> <mask>	Removes a specified IP static route.
		route <ip> <mask> inactive	Enables a specified IP static route.
	lacp		Disables the link aggregation control protocol (dynamic trunking) on the switch.
	logins		Disables login access to the specified name.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
	mac-filter	mac <mac-addr> vlan <vlan-id> drop <src/dst/ both> inactive	Enables the specified MAC-filter rule.
		mac <mac-addr> vlan <vlan-id> drop <src/dst/ both>	Disables the specified MAC filter rule.
	mac-forward	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).
		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).
	mirror-port		Disables port mirroring on the switch.
	multi-login		Disables another administrator from logging into Telnet or the CLI.
	port-access-authenticator		Disables port authentication on the switch.
		<port-list>	Disables authentication on the listed ports.
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).
	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).
	service-control	ftp	Disables FTP access to the switch.
		http	Disables web browser control to the switch.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
		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.
		known-hosts	Removes all remote hosts.
		known-hosts <host-ip>	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.
	timesync		Disables timeserver settings.
	trunk	<T1|T2>	Disables the specified trunk group.
		<T1|T2> interface <port-list>	Removes ports from the specified trunk group.
		<T1|T2> lacp	Disables LACP in the specified trunk group.
	vlan	<vlan-id>	Deletes the static VLAN entry.
	vlan1q	gvrp	Disables GVRP on the switch.
		ingress-check	Disables VLAN tag checking on incoming traffic.
		port-isolation	Disables port isolation.
password			Change the password for Enable mode.
port-access-authenticator			Enables 802.1x authentication on the switch.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
	<port-list>		Enables 802.1x authentication on the specified port(s).
		reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.
		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).
		learn inactive	Disables MAC address learning on the specified port(s).
		address-limit <number>	Limits the number of (dynamic) MAC addresses that may be learned on a port.
queue	level <0-7> priority <0-3>		Sets the priority level-to-physical queue mapping.
radius-server	host <ip> [acct-port <socket-number>] [key <key-string>]		Sets the IP address and/or the port number and key of the external RADIUS server.
remote-management	<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 for services such as Ping.
	snmp		Allows SNMP management.
	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.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
	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> path-cost <1-65535>		Sets the STP path cost for a specified port.
	<port-list> priority <0-255>		Sets the priority for a specified port.
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.
	help		Displays help information.
	priority <0-61440>		Sets the bridge priority of the switch.
spq			Sets the switch to use Strictly Priority Queuing (SPQ).
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.
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.
	help		Displays help information.
	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>		Activates a trunk group.
	<T1|T2>interface <port-list>		Adds a port(s) to the specified trunk group.

Table 58 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION
	<T1|T2>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 27.9.5 on page 162 for more information.
vlan-type	<802.1q|port-based>		Specifies the VLAN type.
vlan1q	gvrp		Enables GVRP.
	ingress-check		Enables VLAN tag checking on incoming traffic.
	port-isolation		Enables port-isolation.
wrr			Sets the switch to use Weighted Round Robin queuing (WRR).
		<wt1 .. wt4>	Sets the WRR weight. A weight value of one to eight is given to each variable from wt1 to wt4.

27.9.4 interface port-channel Commands

The following table lists the interface port-channel commands in configuration mode. Use these commands to configure the ports.

Table 59 interface port-channel Commands

COMMAND			DESCRIPTION
interface port-channel <port-list>			Enables a port or a list of ports for configuration.
	bandwidth-limit		Enables bandwidth control 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).
	bmstorm-limit		Enables broadcast storm control on the port.
		<Kbps>	Sets the limit of broadcast storm packets in kilobit per second (Kbps).
	diffserv		Enables DiffServ on the port(s).

Table 59 interface port-channel Commands (continued)

COMMAND			DESCRIPTION
	egress set <port-list>		Sets the outgoing traffic port list for a port-based VLAN.
	exit		Exits from the interface port-channel command mode.
	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 port-channel commands.
	inactive		Disables the specified port(s) on the switch.
	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.
	name <port-name-string>		Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).
	no	bandwidth-limit	Disables bandwidth limit on the port(s).
		bmstorm-limit	Disables broadcast storm control limit on the port(s).
		diffserv	Disables DiffServ on the port(s).
		egress set	Disables outgoing traffic on the port for port-based VLAN.
		flow-control	Disables flow control on the port(s).
		gvrp	Disables GVRP on the port(s).
		inactive	Enables the port(s) on the switch.
		mirror	Disables port mirroring on the port(s).
		vlan-trunking	Disables VLAN trunking on the port(s).

Table 59 interface port-channel Commands (continued)

COMMAND			DESCRIPTION
	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 or full) and speed (10, 100 or 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.
	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.

27.9.5 config-vlan Commands

The following table lists the vlan commands in configuration mode.

Table 60 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION
vlan <1-4094>			Creates a new VLAN group.
	exit		Leaves the VLAN configuration mode.
	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.
		<ip-address> <mask> [manageable]	Sets the management IP address and subnet mask of the switch in the specified VLAN.

Table 60 Command Summary: config-vlan Commands (continued)

COMMAND			DESCRIPTION
		`default-gateway <ip-address>`	Sets a default gateway IP address for this VLAN.
		`default-management dhcp-bootp`	Sets the dynamic in-band IP address
		`default-management <ip-address> <mask>`	Sets a static in-band IP address and subnet mask.
		`default-management dhcp-bootp release`	Releases the dynamic in-band IP address.
		`default-management 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.
		`ip address default-management 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>`	Enables VLAN tagging for outgoing traffic on the specified port(s).
	`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.

CHAPTER 28
Command Examples

This chapter describes some commands in more detail.

28.1 Overview

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

28.2 show Commands

These are the commonly used `show` commands.

28.2.1 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.

Figure 100 show system-information Command Example

```
ras> show system-information
System Name              : ES-2108
System Contact           :
System Location          :
Ethernet Address         : 00:13:49:1a:d4:fa
ZyNOS F/W Version        : V3.60(TX.0)| 04/22/2005
RomRasSize               : 1816320
System up Time           :     0:59:37 (5757d ticks)
Bootbase Version         : V1.07 | 04/20/2005
ras>
```

28.2.2 show ip

Syntax:

```
show ip
```

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

The following figure shows the default interface settings.

Figure 101 show ip Command Example

```
ras> show  ip
IP Interface
     IP[192.168.1.1], Netmask[255.255.255.0], VID[1]
ras>
```

28.2.3 show logging

Note: This command is not available in User mode.

Syntax:

```
show logging
```

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

Figure 102 show logging Command Example

```
ras# show logging
     0 Sat Jan 01 00:00:24 2000 PP0e -WARN  SNMP TRAP 26: Event On Trap
   1 Sat Jan 01 00:00:24 2000 PINI -WARN  SNMP TRAP 0: cold start
   2 Sat Jan 01 00:00:24 2000 PINI  INFO  main: init completed
   3 Sat Jan 01 00:07:54 2000 PP0e -WARN  SNMP TRAP 26: Event On Trap
   4 Sat Jan 01 00:07:54 2000 PINI -WARN  SNMP TRAP 1: warm start
   5 Sat Jan 01 00:07:54 2000 PINI  INFO  main: init completed
   6 Sat Jan 01 00:08:00 2000 PP0e -WARN  SNMP TRAP 26: Event On Trap
   7 Sat Jan 01 00:08:00 2000 PINI -WARN  SNMP TRAP 0: cold start
   8 Sat Jan 01 00:08:00 2000 PINI  INFO  main: init completed
   9 Sat Jan 01 00:08:06 2000 PP0e -WARN  SNMP TRAP 26: Event On Trap
  10 Sat Jan 01 00:08:06 2000 PINI -WARN  SNMP TRAP 0: cold start
  11 Sat Jan 01 00:08:06 2000 PINI  INFO  main: init completed
  12 Sat Jan 01 00:08:12 2000 PP0e -WARN  SNMP TRAP 26: Event On Trap
  13 Sat Jan 01 00:08:12 2000 PINI -WARN  SNMP TRAP 0: cold start
  14 Sat Jan 01 00:08:12 2000 PINI  INFO  main: init completed
  15 Sat Jan 01 00:08:18 2000 PP0e -WARN  SNMP TRAP 26: Event On Trap
  16 Sat Jan 01 00:08:18 2000 PINI -WARN  SNMP TRAP 0: cold start
  17 Sat Jan 01 00:08:18 2000 PINI  INFO  main: init completed
  18 Sat Jan 01 00:08:23 2000       INFO  adjtime task pause 1 day
Clear Error Log (y/n):
```

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

28.2.4 show interface

Syntax:

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

This command displays statistics of a port. The following example shows that port 2 is up and the related information.

Figure 103 show interface Command Example

```
ras# show interface 2
     Port Info     Port NO.                :2
                   Link                    :100M/F
                   Status                  :FORWARDING
                   LACP                    :Disabled
                   TxPkts                  :1744
                   RxPkts                  :12
                   Errors                  :0
                   Tx KBs/s                :0.64
                   Rx KBs/s                :0.0
                   Up Time                 :1:00:40
  TX Packet        Tx Packets              :1744
                   Multicast               :1744
                   Broadcast               :0
                   Pause                   :0
  RX Packet        Rx Packets              :12
                   Multicast               :12
                   Broadcast               :0
                   Pause                   :0
  TX Collision     Single                  :0
                   Multiple                :0
                   Excessive               :0
                   Late                    :0
  Error Packet     RX CRC                  :0
                   Runt                    :0
  Distribution     64                      :12
                   65 to 127               :0
                   128 to 255              :0
                   256 to 511              :0
                   512 to 1023             :0
                   1024 to 1518            :0
                   Giant                   :0
ras#
```

28.2.5 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 the MAC address table.

Figure 104 show mac address-table Command Example

```
ras# show mac address-table all
Port      VLAN ID        MAC Address         Type
2         1              00:85:a0:01:01:04   Dynamic
ras#
```

28.3 ping

Syntax:

```
ping <ip> < [vlan <vlan-id> ] [ size <0-8024> ] [ -t ]>
```

where

`<ip>`	=	The IP address of an Ethernet device.
`[vlan <vlan-id> ]`	=	Specifies the VLAN ID to which the Ethernet device belongs.
`[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`.

Figure 105 ping Command Example

```
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#
```

28.4 traceroute

Syntax:

```
traceroute <ip> [vlan <vlan-id>][ttl <1-255>] [wait <1-60>]
[queries <1-10>]
```

where

`<ip>`	=	The IP address of an Ethernet device.
`[vlan <vlan-id> ]`	=	Specifies 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.
`[quesries <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`.

Figure 106 traceroute Command Example

```
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:
```

28.5 Enabling RSTP

To enable RSTP on a port. Enter `spanning-tree` followed by the port number and press [ENTER].

The following example enables RSTP on port 10.

Figure 107 Enable RSTP Command Example

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

28.6 Configuration File Maintenance

The following sections shows how to manage the configuration files.

28.6.1 Restarting the Switch

There are two ways in which you can restart the switch: restart the switch (cold reboot) and restart the system (warm reboot).

Use the `boot config` command to restart the switch. The following figure shows an example.

Figure 108 CLI: boot config Command Example

```
ras# boot config
```

Use the `reload config` command to restart the system. The following figure shows an example.

Figure 109 CLI: reload config Command Example

```
ras# reload config
```

28.6.2 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 configuration file.

The following example resets the configuration file to the factory default settings.

Figure 110 CLI: Reset to the Factory Default Example

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

28.7 no Command Examples

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

28.7.1 no mirror-port

Syntax:

```
no mirror-port
```

Disables port mirroring on the switch.

An example is shown next.

Figure 111 no mirror-port Command Example

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

28.7.2 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.

Figure 112 no https timeout Command Example

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

28.7.3 no trunk

Syntax:

```
no trunk <T1|T2>
no trunk <T1|T2> lacp
no trunk <T1|T2> interface <port-list>
```

where

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

- An example is shown next.
- Disable trunk one (T1).
- Remove ports one, three, four and five from trunk two (T2).

Figure 113 no trunk Command Example

```
ras(config)# no trunk T1
ras(config)# no trunk T2 interface 1,3-5
```

28.7.4 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.

Figure 114 no port-access-authenticator Command Example

```
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
```

28.7.5 no ssh

Syntax:

```
no ssh key <rsa1|rsa|dsa>
no ssh known-hosts <host-ip>
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.

Figure 115 no ssh Command Example

```
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
```

28.8 spq

Syntax:

```
spq
```

Activates Strict Priority Queuing (SPQ). An example is shown next.

Figure 116 spq Command Example

```
ras(config)# spq
```

28.9 wrr

Syntax:

```
wrr <wt1> <wt2> <wt3><wt4>
```

where

	Enables WRR (Weighted Round Robin) queuing method on the switch.
`<wt1> .. <wt4>`	Sets the interface to use WRR queuing. A weight value of one to eight is given to each variable from `wt1` to `wt4`.

The following example sets the switch to use WRR queuing and sets the queue weights for Q0 to Q3.

Figure 117 wrr Command Example

```
ras# configure
ras(config)# wrr
ras(config)# wrr 4 3 2 1
```

28.10 interface Commands

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

28.10.1 interface port-channel

Syntax:

```
interface port-channel <port-list>
```

Use this command to enable the specified ports for configuration. 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 mode.
- Enable ports one, three, four and five for configuration.
- Begin configuring for those ports.

Figure 118 interface Command Example

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

28.10.2 bmstorm-limit

Syntax:

```
bmstorm-limit
bmstorm-limit <Kbps>
```

where

	Enables broadcast storm control limit on the switch.
`<Kbps>`	Limits broadcast packet traffic the interface receives per second.

An example is shown next.

- Enable port one for configuration.
- Enable broadcast control.
- Set the broadband packet traffic the interface receives per second.

Figure 119 broadcast-limit Command Example

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

28.10.3 bandwidth-limit

Syntax:

```
bandwidth-limit
bandwidth-limit egress <Kbps>
bandwidth-limit ingress <Kbps>
```

where

	Enables bandwidth control on the switch.
`<Mbps>`	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 70Kbps.
- Set the incoming traffic bandwidth limit to 90Kbps.

Figure 120 bandwidth-limit Command Example

```
ras(config)# interface port-channel 1
ras(config-interface)# bandwidth-limit
ras(config-interface)# bandwidth-limit egress 70
ras(config-interface)# bandwidth-limit ingress 90
```

28.10.4 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 ports.
- 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).

Figure 121 mirror Command Example

```
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
```

28.10.5 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.

Figure 122 gvrp Command Example

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

28.10.6 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 tagged frame-types on the interface.

Figure 123 frame-type Command Example

```
ras(config-vlan1q)# ingress-check
ras(config)# interface port-channel 1,3-5
ras(config-interface)# frame-type tagged
```

28.10.7 egress set

Syntax:

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

where

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

An example is shown next.

- Enable port-based VLAN tagging on the switch.
- Enable ports one, three, four and five for configuration.
- Set the outgoing traffic ports as the CPU (0), seven (7), eight (8) and nine (9).

Figure 124 egress set Command Example

```
ras(config)# vlan-type port-based
ras(config)# interface port-channel 1,3-5
ras(config-interface)# egress set 0,7-9
```

28.10.8 qos priority

Syntax:

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

where

`<0 .. 7>` Sets the quality of service priority for a port.

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).

Figure 125 qos priority Command Example

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

28.10.9 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 ports.

Figure 126 name Command Example

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

28.10.10 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 or full) and speed (10, 100 or 1000 Mbps) of the connection on the port. 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.

Figure 127 speed-duplex Command Example

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

CHAPTER 29
IEEE 802.1Q Tagged VLAN Commands

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

29.1 IEEE 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.

29.2 VLAN 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).

29.2.1 Static Entries (SVLAN Table)

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

29.2.2 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.

29.3 Configuring 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.

- Use the `vlan <vlan-id>` command to configure or create a VLAN on the switch. The switch automatically enters the config-vlan mode.Use the `inactive` command to deactivate the VLAN(s).
- Use the `interface port-channel <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.
- Use the `exit` command when you are finished configuring the VLAN.

Example:

Figure 128 Tagged VLAN Configuration and Activation Example

```
ras (config)# vlan 2000
ras (config-vlan)# name up1
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
```

2 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:

Figure 129 CPU VLAN Configuration and Activation Example

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

29.4 Global VLAN1Q Tagged VLAN Configuration Commands

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

29.4.1 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.

Figure 130 GARP STATUS Command Example

```
ras # show garp
GARP Timer
------------------------
Join Timer = 200
Leave Timer = 600
Leave All Timer = 10000
ras#
```

29.4.2 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.

Figure 131 GARP Timer Command Example

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

29.4.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

Figure 132 GVRP Status Command Example

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

29.4.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

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

29.4.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

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

29.4.6 Enable Ingress Checking

Syntax:

```
ingress-check
```

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

The following example activates ingress checking on the switch.

Figure 133 ingress-check Command Example

```
ras(config)# vlan1q ingress-check
```

29.5 Port VLAN Commands

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

29.5.1 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.

Figure 134 vlan1q port default vid Command Example

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

29.5.2 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.

Figure 135 frame type Command Example

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

29.5.3 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.

Figure 136 no gvrp Command Example

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

29.5.4 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.

29.5.4.1 Modify a Static VLAN Table Example

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

Figure 137 Modifying Static VLAN Example

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

29.5.4.2 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.

29.5.5 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.

Figure 138 no vlan Command Example

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

29.6 Enable VLAN

Syntax:

```
vlan <vlan-id>
```

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

29.7 Disable VLAN

Syntax:

```
vlan <vlan-id>
inactive
```

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

29.8 Show VLAN Setting

Syntax:

```
show vlan
```

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

An example is shown next.

- For the `AdCtl` section of the last column, "-" is a port set to normal, "x" is a forbidden port and "F" is a fixed port.
- For the `TagCtl` section of the last column, "T" is a tagged port, "U" is an untagged port.

Figure 139 show vlan Command Example

```
ras# show vlan
  802.1Q VLAN Static Entry:
  idx. Name         VID  Active   AdCtl / TagCtl
  ---- ------------ ---- -------- ------------------------
     0            1    1  active  FFFFFFFFFFFFFFFFFFFFFFFF
                                   UUUUUUUUUUUUUUUUUUUUUUUU
     1                 2  active  ------------------------
                                   TTTTTTTTTTTTTTTTTTTTTTTT
ras#
```

CHAPTER 30
Troubleshooting

This chapter covers potential problems and possible remedies.

30.1 Problems Starting Up the Switch

Table 61 Troubleshooting the Start-Up of Your Switch

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the switch.	Check the power connection and make sure the power source is turned on.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

30.2 Problems Accessing the Switch

Table 62 Troubleshooting Accessing the Switch

PROBLEM	CORRECTIVE ACTION
I cannot access the switch using Telnet.	Make sure the ports are properly connected. You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later. Check that you have enabled Telnet service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
I cannot access the web configurator.	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details. Your computer's and the switch's IP addresses must be on the same subnet. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

30.2.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

30.2.1.1 Internet Explorer Pop-up Blockers

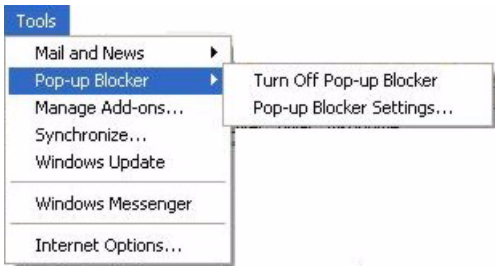
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

30.2.1.1.1 Disable pop-up Blockers

1. In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

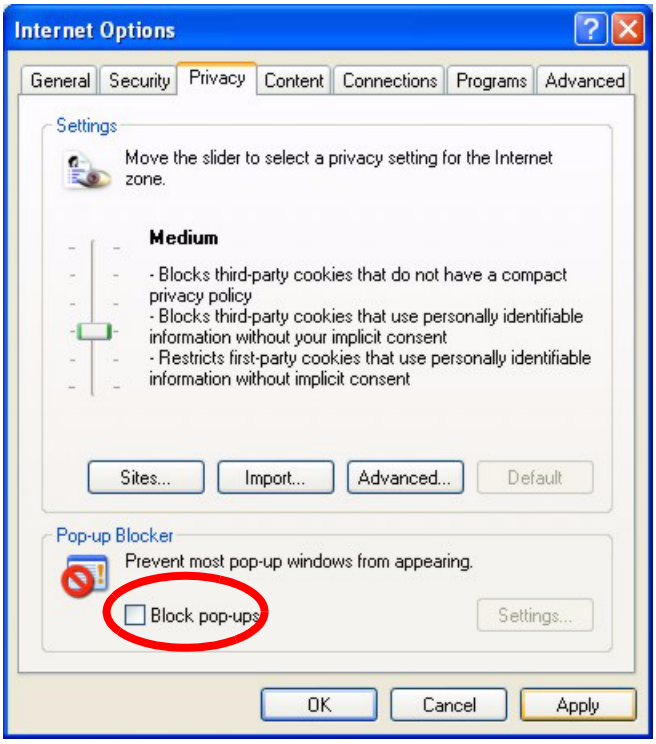
Figure 140 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1. In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.
2. Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 141 Internet Options



3 Click **Apply** to save this setting.

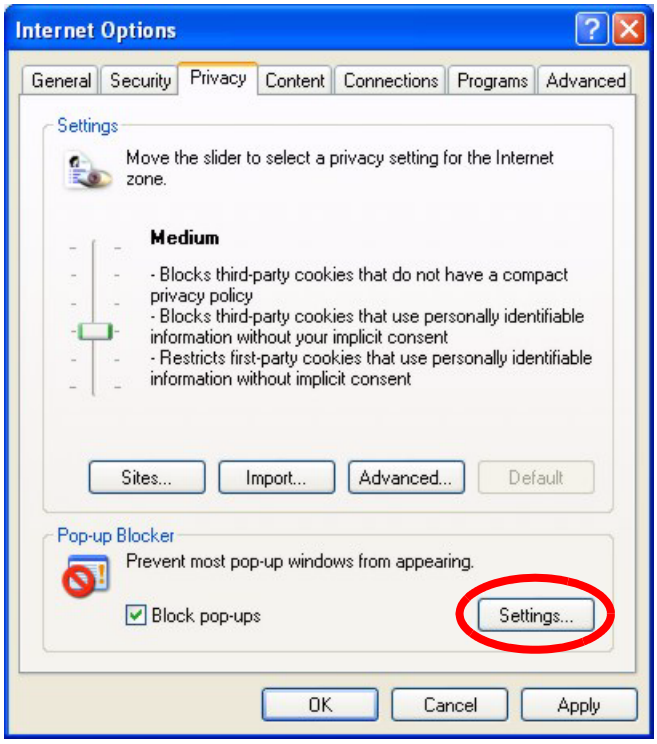
30.2.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

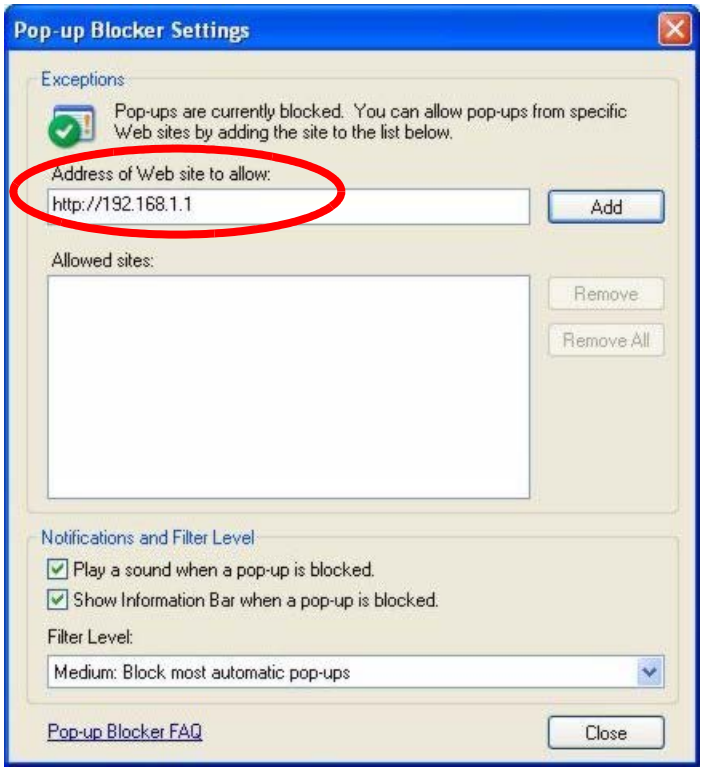
Figure 142 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 143 Pop-up Blocker Settings



5 Click **Close** to return to the **Privacy** screen.

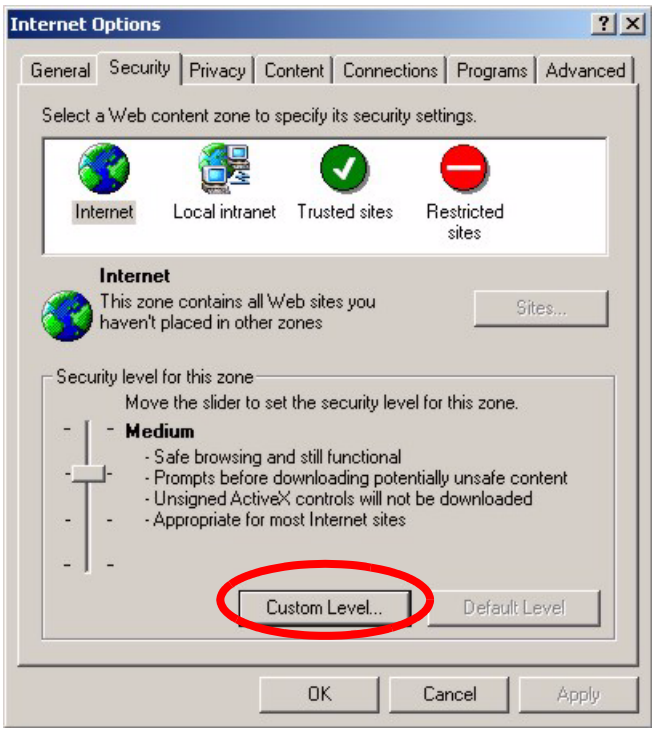
6 Click **Apply** to save this setting.

30.2.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 144 Internet Options



2 Click the **Custom Level...** button.

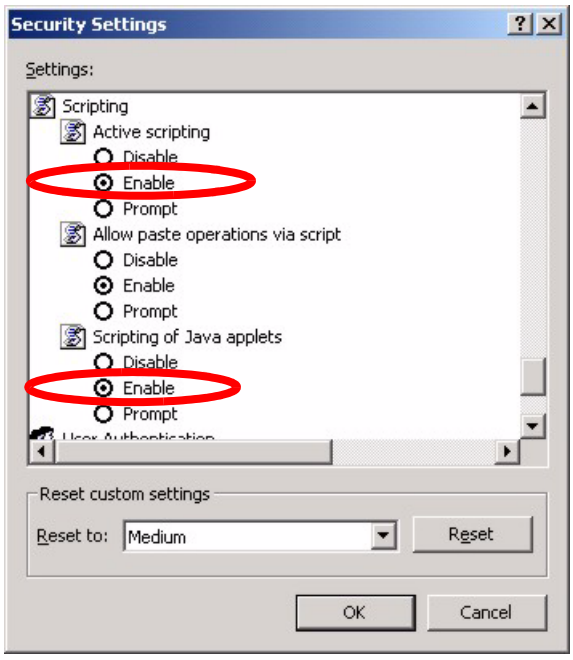
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

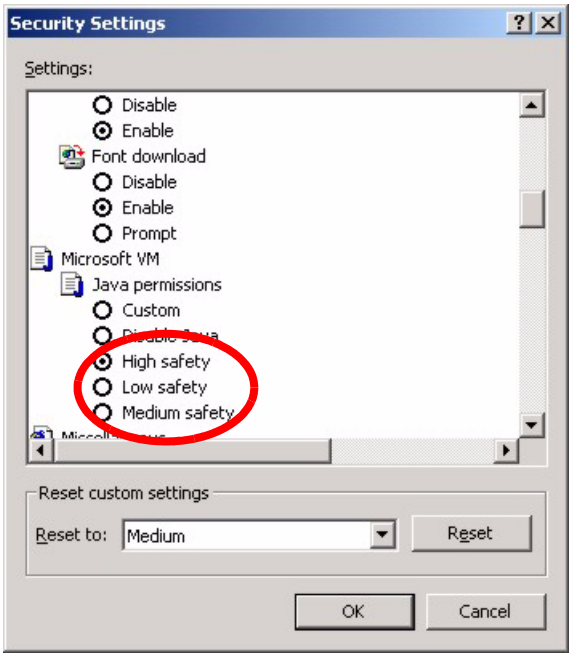
Figure 145 Security Settings - Java Scripting



30.2.1.3 Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

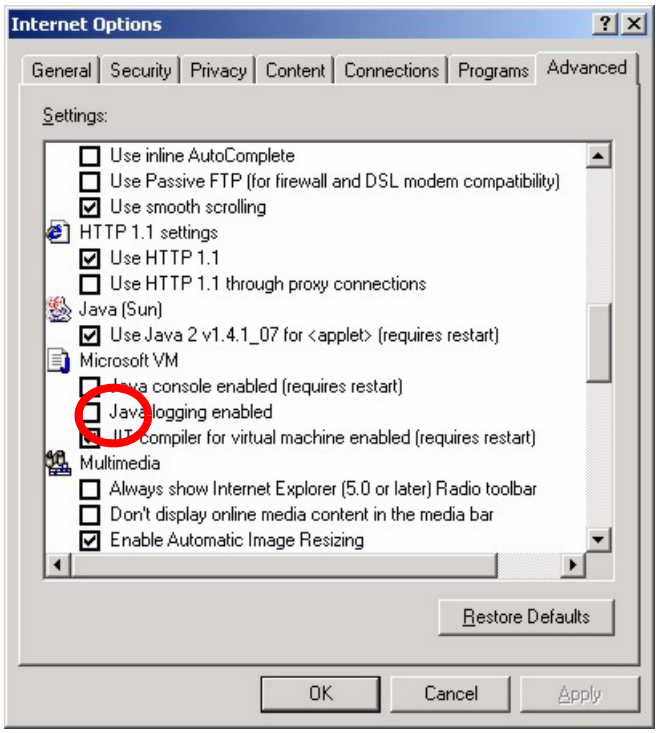
Figure 146 Security Settings - Java



30.2.1.3.1 JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

Figure 147 Java (Sun)



30.3 Problems with the Password

Table 63 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the switch.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	The administrator username is "admin". The default administrator password is "1234". The username and password are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.

APPENDIX A
Product Specifications

These are the switch product specifications.

Table 64 General Product Specifications

Fast Ethernet Interface	Eight 10/100 Base-TX interfaces Auto-negotiation Auto-MDI/MDIX Compliant with IEEE 802.3/802.3u Back pressure flow control for half duplex mode Flow control for full duplex (IEEE 802.3x) RJ-45 Ethernet cable connector Rate limiting at 64Kbps steps
Gigabit Interface	One Gigabit Ethernet and one mini-GBIC port (ES-2108-G only) Compliant with 802.3z/802.3ab/802.3u Copper/fiber interface auto-selection by signal detection (Fiber first)
Bridging	8K MAC addresses Static MAC address filtering (256 entries) Static MAC address forwarding (256 entries) Broadcast storm control
Switching	Switching fabric: 5.6 Gbps non-blocking (only 3.6 Gbps is used) Max. Frame size: 1522 bytes including tag/CRC Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Corrupted packet forwarding prevention
STP	IEEE 802.1d spanning tree protocol IEEE 802.1w, rapid reconfiguration to recover network failure
QoS	IEEE 802.1p Four priority queues with SP/WRR by switch Supports RFC 2475 DiffServ, DSCP to IEEE 802.1p priority mapping
Security	IEEE 802.1x port-based authentication Static MAC Address Forwarding Static MAC Address Filtering Blocks unresolved address forwarding/Port Security
VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K (256 static VLANs) Supports GVRP VLAN ingress filtering
Link aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking 2 groups, 4 ports per group maximum
Port mirroring	Port based mirroring to a monitor port
IGMP	Supports IGMP snooping

Table 65 Management Specifications

System Management	Alarm/Status surveillance LED indication for alarm and system status Performance monitoring Line speed Four RMON groups 1,2,3,9 (history, statistics, alarms, and events) Throughput monitoring CMP packet transmission Port mirroring and aggregation Spanning Tree Protocol IGMP snooping Firmware upgrade and download through FTP/web/console Configuration by console/telnet/web Configuration backup and restore by FTP/web/console Login authorization and security levels (read-only and read/write) Self diagnostics FLASH memory
Network Management	CLI through console port and Telnet Web-based management Up to 64 management IP address in different VLAN Clustering: up to 24 switches can be managed by one IP SNMP RMON groups (history, statistics, alarms and events)
MIB	RFC1213 MIB II RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 Four groups of RMON RFC 1155 SMI RFC2674 Bridge MIB extension (for IEEE 802.1Q) ZyXEL Private MIBs for ES-2108 series

Table 66 Physical and Environmental Specifications

LEDs	Per switch: PWR (Green), SYS (Green), ALM (Red) Per Ethernet port: LNK/ACT (Amber/Green) 1000Base-T RJ45: SPD (Amber/Green), LNK/ACT (Green) SFP: LNK (Green), ACT (Green)
Dimensions	250mm (W) x 135mm (D) x 35mm (H) Standard 19" rack mountable
Weight	1.2 Kg
Temperature	Operating: 0º C ~ 45º C (32º F ~ 113º F) Storage: -25º C ~ 70º C (13º F ~ 158º F)
Humidity	10 ~ 90% (non-condensing)

Table 66 Physical and Environmental Specifications (continued)

Power Supply	Overload protection 100-240VAC, 50/60Hz, 0.5A Max.
Safety Standards	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

APPENDIX B
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Table 67 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.

A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Table 68 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 69 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Table 70 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 71 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 72 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 73 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 74 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 75 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 76 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 77 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 78 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class "C" subnet planning.

Table 79 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 67 on page 205) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 80 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z