ES-2024 Series

Ethernet Switch

User's Guide

Version 3.70
7/2006
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.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device 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 device 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 device 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.

Notices

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.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Certifications

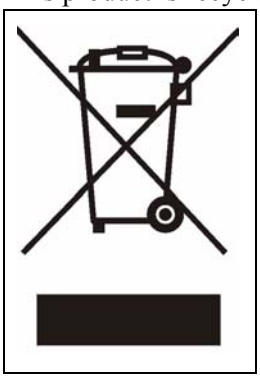
1. Go to www.zyxel.com
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

Safety Warnings

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

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- 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 should service or disassemble this device. Please contact your vendor for further information. For devices that use any external cables or cords.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

This product is recyclable. Dispose of it properly.



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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

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

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

Registration

Register your product online 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.

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 sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
COSTA RICA	soporte@zyxel.co.cr sales@zyxel.co.cr	+506-2017878 +506-2015098	www.zyxel.co.cr ftp.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
CZECH REPUBLIC	info@cz.zyxel.com info@cz.zyxel.com	+420-241-091-350 +420-241-091-359	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
DENMARK	support@zyxel.dk sales@zyxel.dk	+45-39-55-07-00 +45-39-55-07-07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
FRANCE	info@zyxel.fr	+33-4-72-52-97-97 +33-4-72-52-19-20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
HUNGARY	support@zyxel.hu info@zyxel.hu	+36-1-3361649 +36-1-3259100	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
KAZAKHSTAN	http://zyxel.kz/support sales@zyxel.kz	+7-3272-590-698 +7-3272-590-689	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave.,Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE / FAX	WEB SITE / FTP SITE	REGULAR MAIL
NORWAY	support@zyxel.no sales@zyxel.no	+47-22-80-61-80 +47-22-80-61-81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
POLAND	info@pl.zyxel.com	+48 (22) 333 8250 +48 (22) 333 8251	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 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 Arte, 21 5ª planta 28033 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)

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ES-2024 Series Ethernet Switch.

This preface introduces you to the ES-2024 Series 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-2024 seriesfor 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-2024 Series Ethernet Switch may be referred to as "the switch" or "the device" in this User's Guide.

Graphics Icons Key

ES-2024 Series 	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 24 10/100Mbps ports and two Gigabit Ethernet/mini-GBIC ports. The ES-2024PWR comes with the Power-over-Ethernet (PoE) feature.

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.

DiffServ Code Point (DSCP)

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 port to another port 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.

Multicast VLAN Registration (MVR)

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network.

This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

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.

Bandwidth Control

- The switch supports rate limiting in 64 Kbps increments allowing you to create different service plans.

- The switch supports IGMP snooping enabling group multicast traffic to be only forwarded to ports that are members of that group; thus allowing you to significantly reduce multicast traffic passing through your switch.
- Broadcast storm control

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 Ports

The ports allow the switch to connect to another WAN switch or daisy-chain to other switches.

Mini-GBIC Slots

Install SPF transceivers in these slots 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.

Power over Ethernet (PoE)

The ES-2024PWR can provide power to a device (that supports PoE) such as an access point or a switch through a 10/100Mbps Ethernet port.

1.4 Applications

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

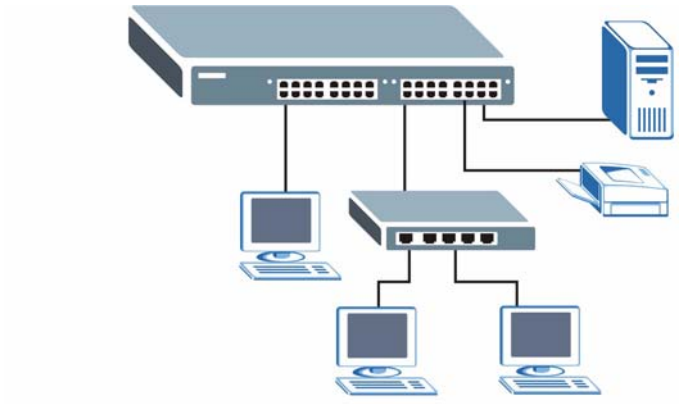
1.4.1 Backbone Application

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

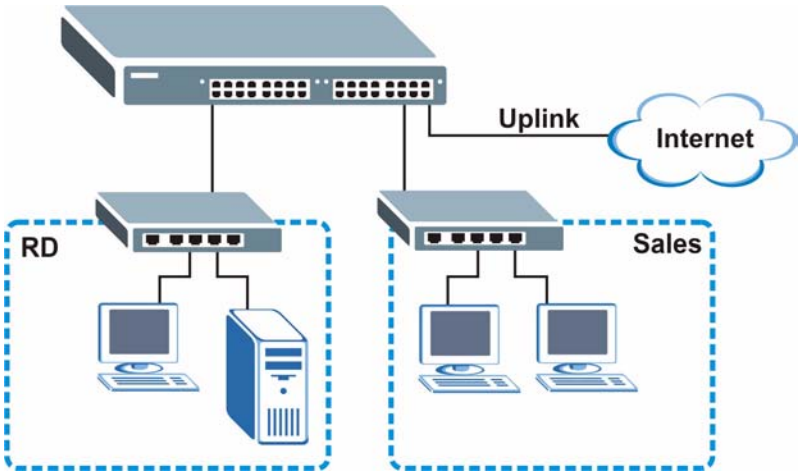


1.4.2 Bridging Example

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. 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

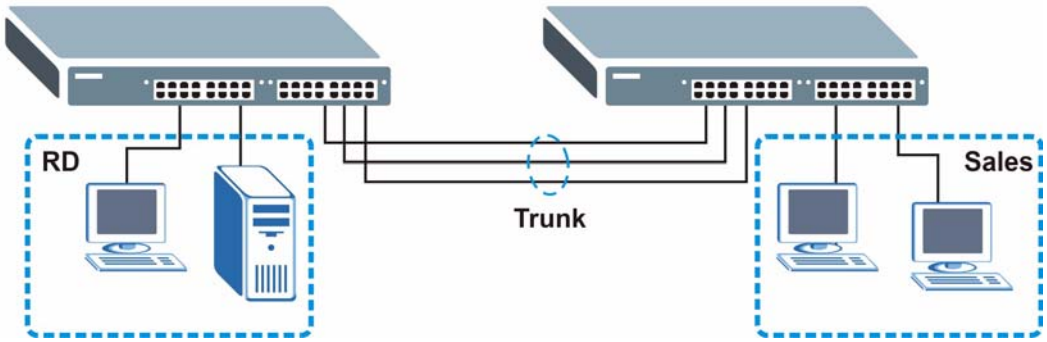


1.4.3 High Performance Switched Example

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.

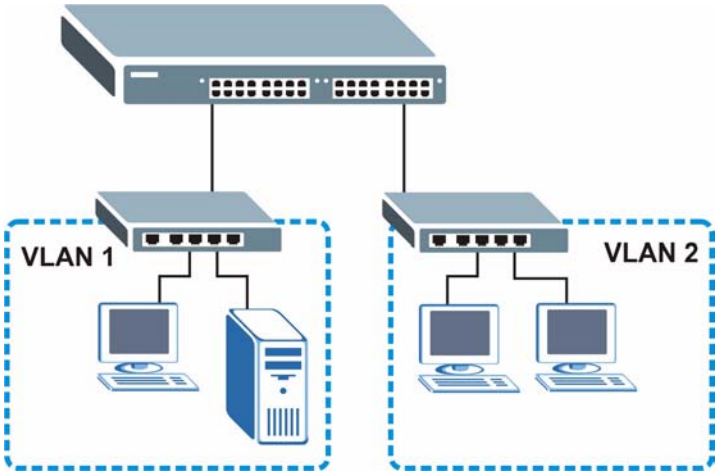
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s)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

For more information on VLANs, refer to Chapter 8, "VLAN," on page 78.

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.

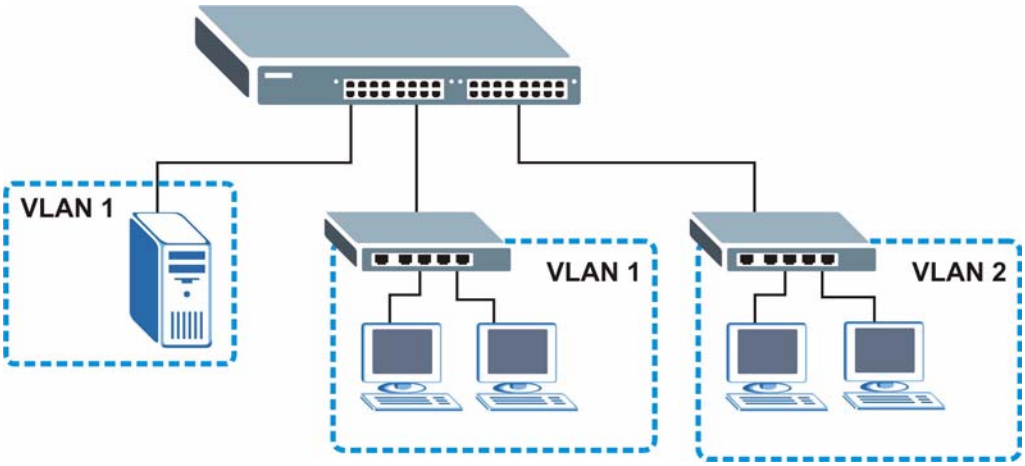
Figure 4 Tag-based VLAN Application



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



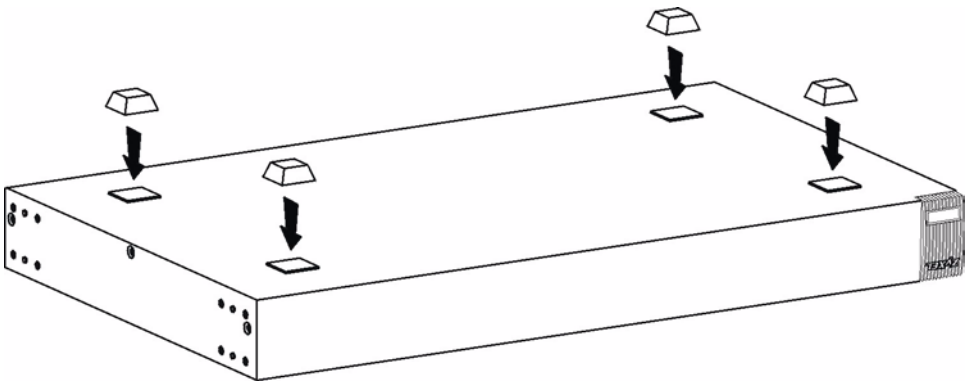
CHAPTER 2
Hardware Installation and Connection

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.

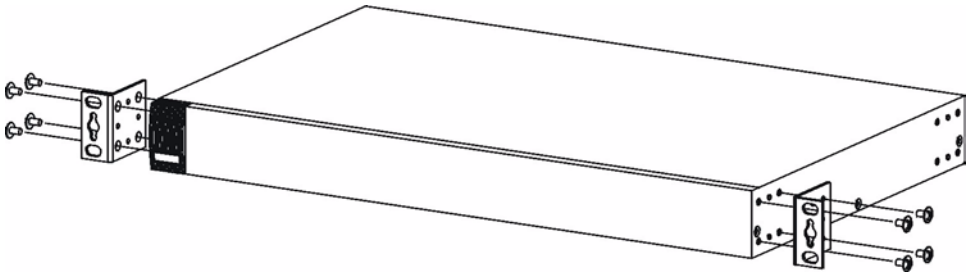
2.2.1.1 Precautions

- 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

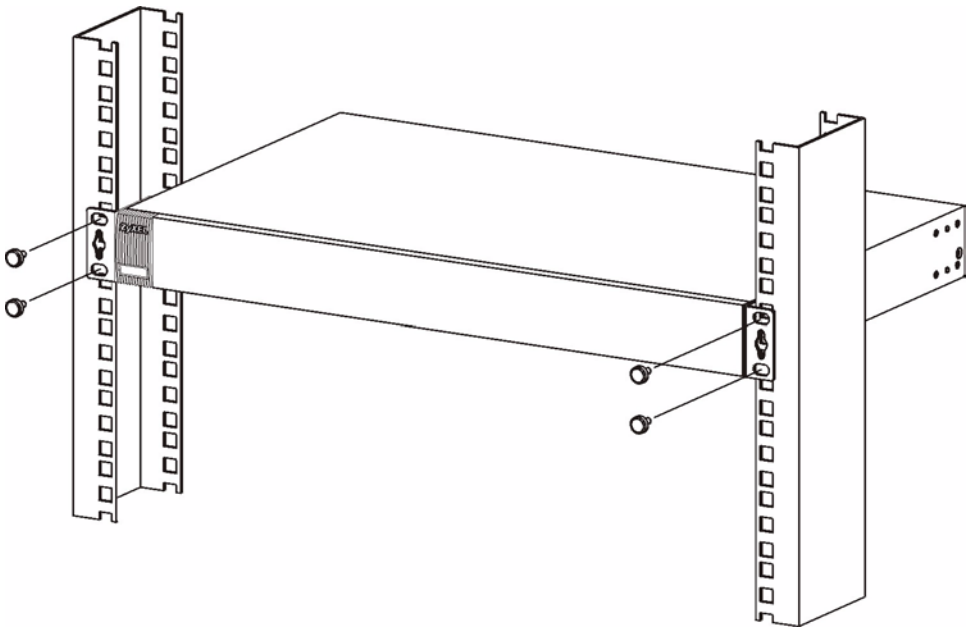


2. Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the switch.
3. Repeat steps 1 and 2 to install the second mounting bracket on the other side of the switch.
4. You may now mount the switch on a rack. Proceed to the next section.

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-2024A

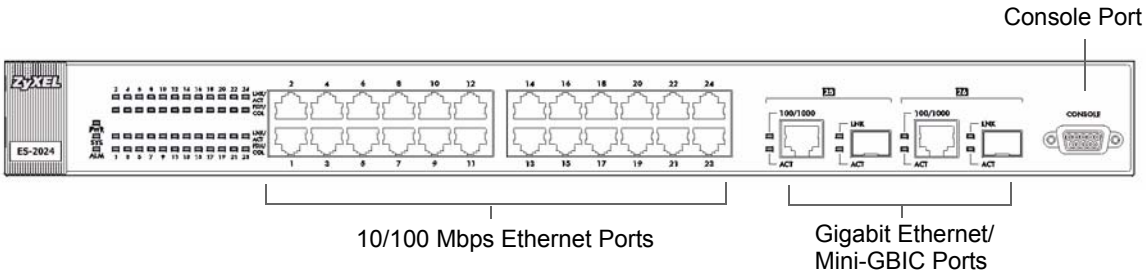
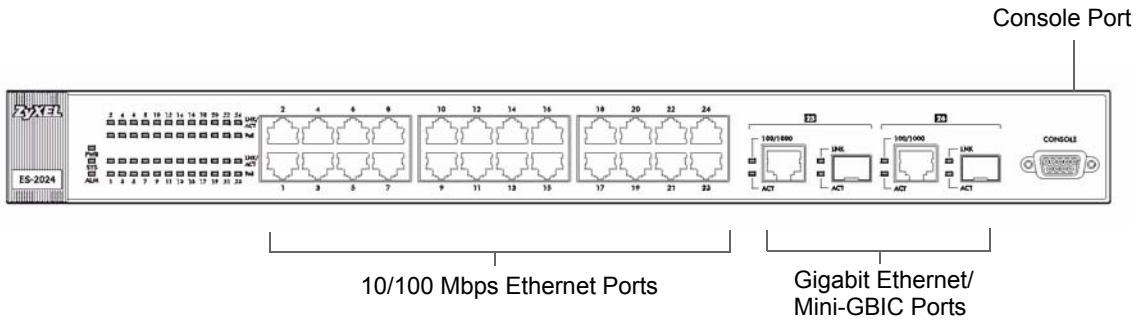


Figure 10 Front Panel: ES-2024PWR



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

Table 1 Front Panel

LABEL	DESCRIPTION
CONSOLE	Only connect this port if you want to configure the switch using the command line interface (CLI) via the console port.

Table 1 Front Panel (continued)

LABEL	DESCRIPTION
24 10/100 Mbps RJ-45 Ethernet Ports	Connect these ports to a computer, a hub, an Ethernet switch or router.
Gigabit Ethernet/ mini GBIC ports	Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches or use them to daisy-chain other switches. Alternatively, use mini-GBIC transceivers in these slots 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 24 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.

There are two pairs of Gigabit Ethernet/mini-GBIC ports. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled. The speed of the Gigabit Ethernet/mini-GBIC ports 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 Slots

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

There are two pairs of Gigabit Ethernet/mini-GBIC ports. The mini-GBIC ports have priority over the Gigabit ports. This means that if a mini-GBIC port and the corresponding Gigabit port are connected at the same time, the Gigabit port will be disabled.

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)

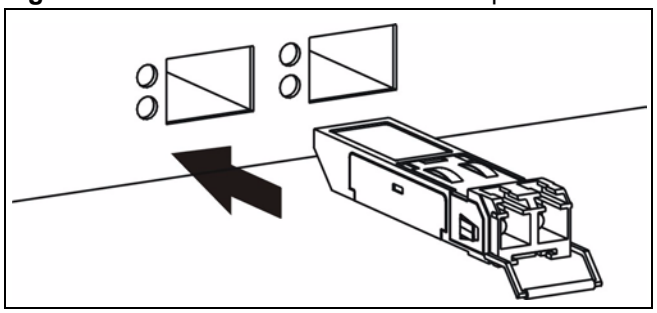
Note: To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.3.1 Transceiver Installation

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

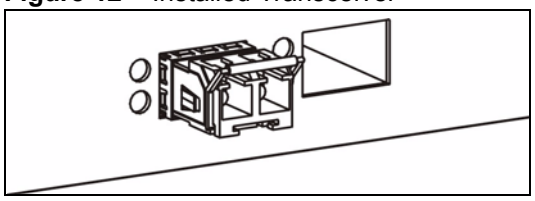
1. Insert the transceiver into the slot with the exposed section of PCB board facing down.

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

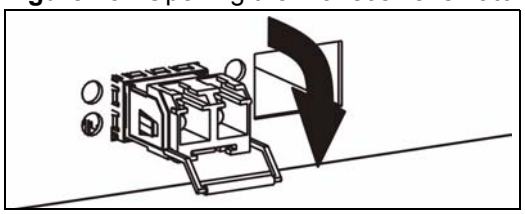


3.1.3.2 Transceiver Removal

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

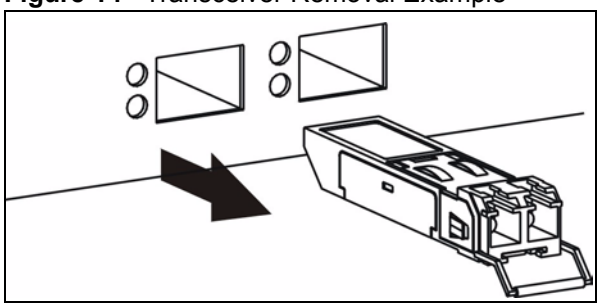
1 Open the transceiver's latch (latch styles vary).

Figure 13 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

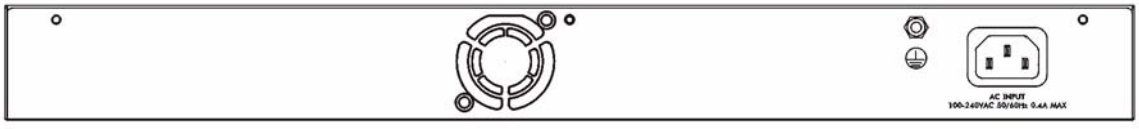
Figure 14 Transceiver Removal Example



3.2 Rear Panel

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

3.3 LEDs

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

Table 2 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.
Ethernet Ports			
LNK/ACT	Amber	Blinking	The system is transmitting/receiving to/from a 10/100 Mbps Ethernet network.
		On	The link to a 10/100 Mbps Ethernet network is up.
		Off	The link to an Ethernet network is down.
FDX/COL (ES-2024A)	Amber	Blinking	The Ethernet port is negotiating in half-duplex mode and collisions are occurring; the more collisions that occur the faster the LED blinks.
		On	The Ethernet port is negotiating in full-duplex mode.
		Off	The Ethernet port is negotiating in half-duplex mode and no collisions are occurring.
POE (ES-2024PWR)	Amber	On	Power is supplied to the port.
		Off	Power is not supplied to the port.
Gigabit Ports			
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.
Mini-GBIC Ports			
LNK	Green	On	The port has a successful connection.
		Off	No Ethernet device is connected to this port.

Table 2 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
ACT	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.

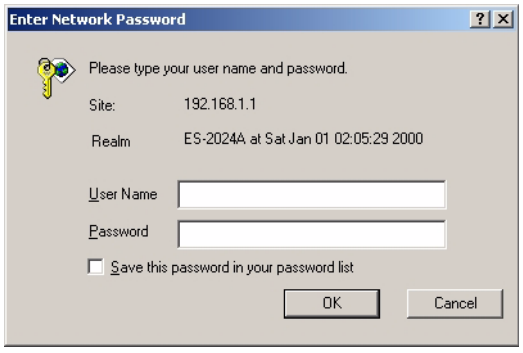
In order to use the web configurator you need to allow:

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



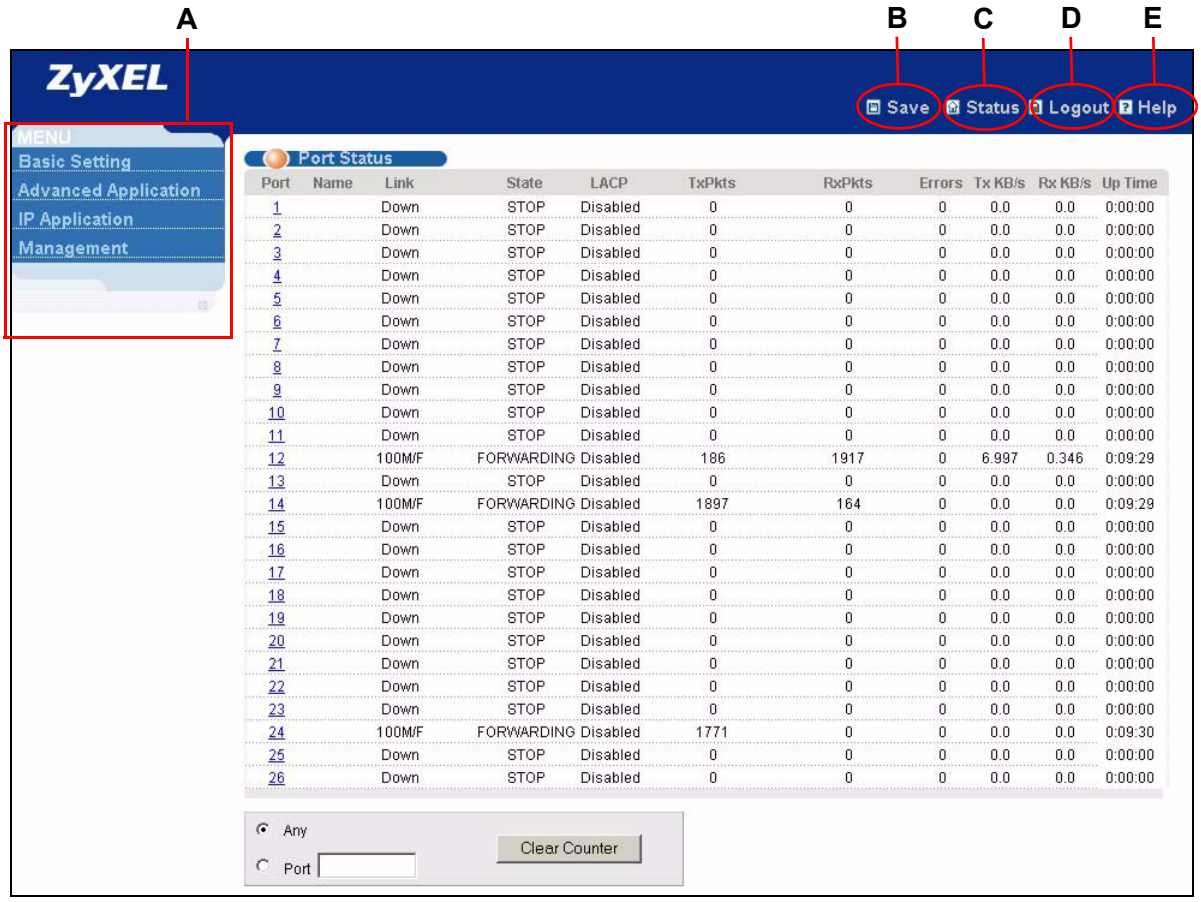
4. Click **OK** to view the first web configurator screen.

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)



The following describes the components in the web configurator screen.

A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, **C**, **D**, **E** - These are the common links for all web configurator screens.

B - Click this link to save your configuration into the switch's nonvolatile memory. Once saved, the configuration of your switch stays the same even if the switch's power is turned off.

C - Click this link to display the **Status** screen (or the home screen).

D - Click this link to logout of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

4.3.1 Menu Overview

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
			

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		Save Configuration
	Spanning Tree Protocol		Reboot System
	Status		Access Control
	Spanning Tree Protocol Configuration		SNMP
	Bandwidth Control		Logins
	Broadcast Storm Control		Service Access Control
	Mirroring		Remote Management
	Link Aggregation		Diagnostic
	Link Aggregation Protocol Status		Syslog
	Configuration		Syslog Setup
	Port Authentication		Syslog Server Setup
	RADIUS		Cluster Management
	802.1x		Cluster Management Status
	Port Security		Cluster Management Configuration
	Queuing Method		MAC Table
	Multicast		ARP Table
	Status		Configure Clone
	Multicast Setting		
	IGMP Filtering Profile		
	MVR		
	Group Configuration		

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 information. On the ES-2024PWR, you can also view the hardware monitoring and PoE 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, GARP and priority queues.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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.
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.
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
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).
Syslog	This link takes you to screens where you can setup system logs and a system log server.

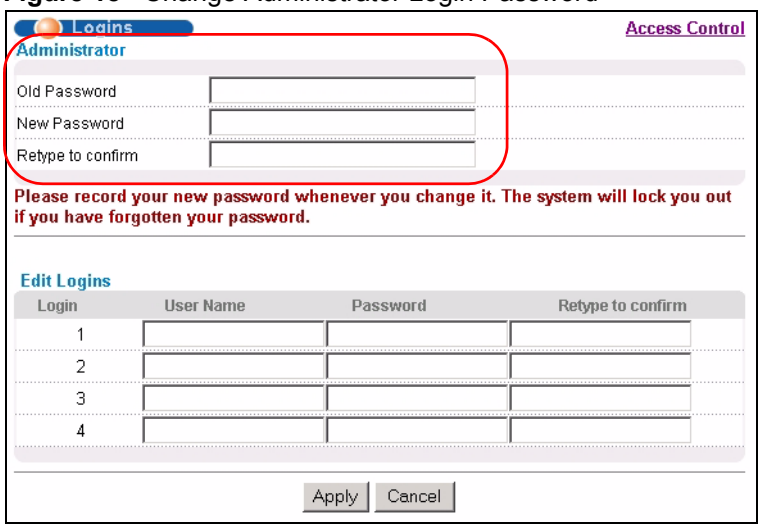
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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.
Configure Clone	This link takes you to a screen where you can clone port attributes of a port and transfer them to other port(s).

4.3.2 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 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the switch's storage that remains even if the switch's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from accessing the switch through the web configurator if you do one of the following:

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. Misconfiguring the text configuration file.
6. Forgetting the password and/or IP address.
7. Preventing all services from accessing the switch.
8. Changing a service port number but forgetting it.

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

4.6 Resetting the Switch

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

4.6.1 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 43 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: V1.07 | 04/20/2005 13:38:02
RAM: Size = 32768 Kbytes
FLASH: AMD 32M *1

ZyNOS Version: V3.70(TX.0)| 07/11/2006 19:59:04
Press any key to enter debug mode within 3 seconds.
.....................
Enter Debug Mode
ES-2024A> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total  262144 bytes received.
Erasing..
.............................................................
OK
ES-2024A> atgo
```

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

4.7 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

4.8 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:

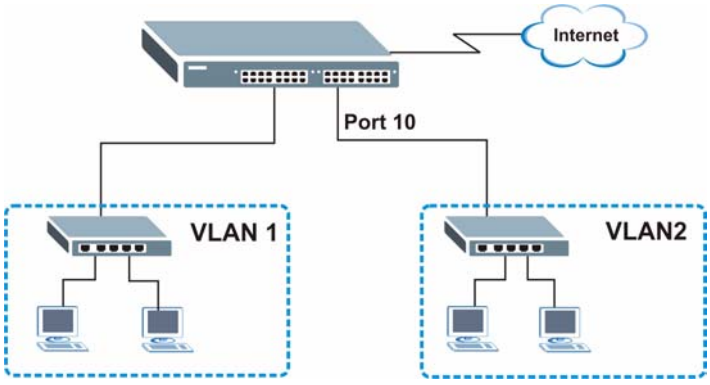
- Create a VLAN
- Set port VLAN ID
- Configure the switch IP management address

5.1.1 Creating a VLAN

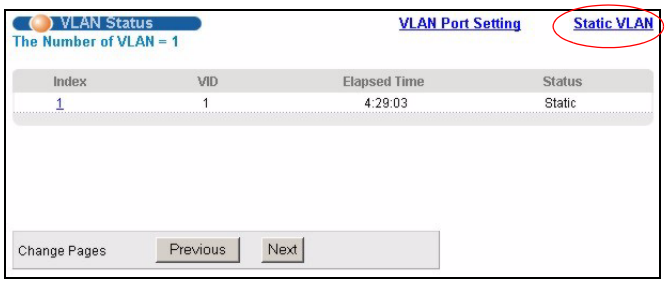
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 10 as a member of VLAN 2.

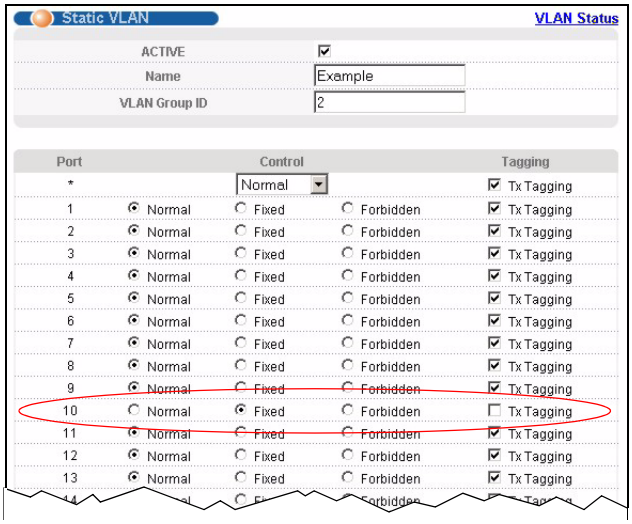
Figure 21 Initial Setup Network Example: VLAN



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 10 on the switch, select **Fixed** to configure port 10 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.

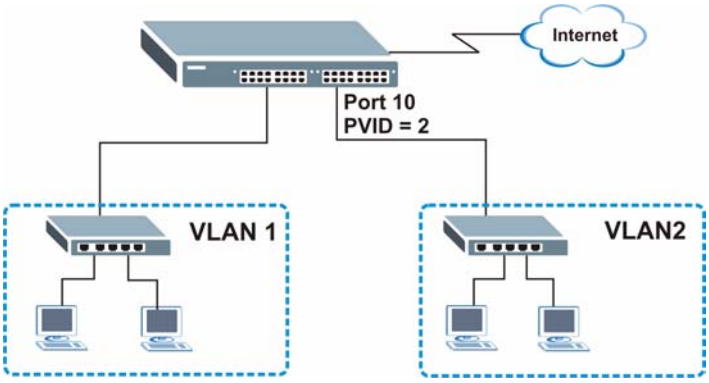
5 Click **Add** to create the static VLAN and click the **Save** button to save the settings.

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.

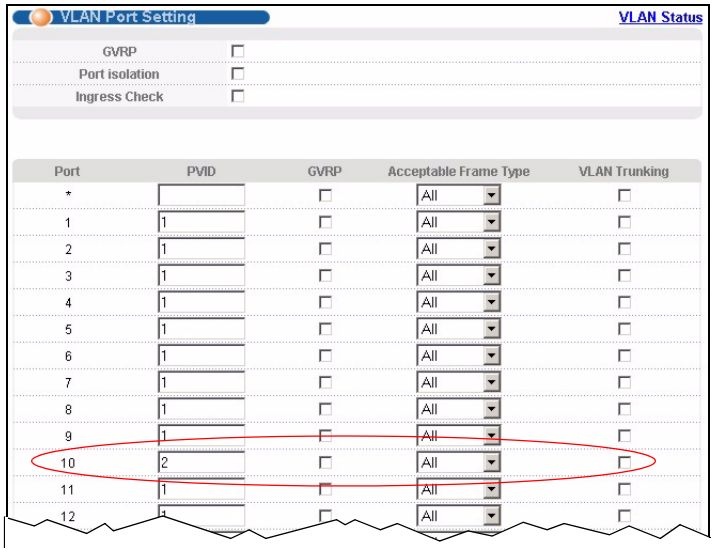
In the example network, configure 2 as the port VID on port 10 so that any untagged frames received on that port get sent to VLAN 2.

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.

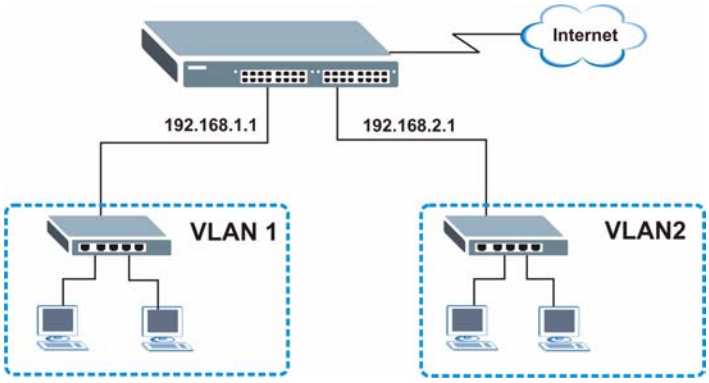
2 Enter 2 in the **PVID** field for port 10 and click **Apply** to set the VLAN port setting and click the **Save** button to save the settings.



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 48 for more information.

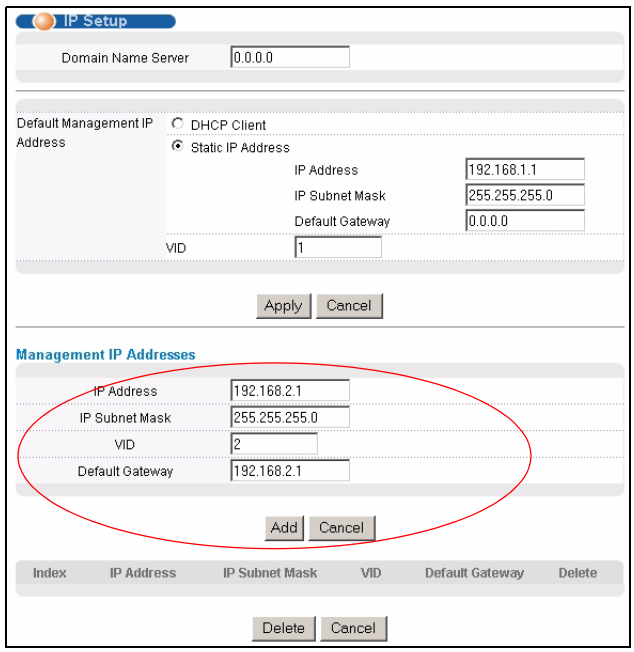
3 Click **Basic Setting** and **IP Setup** in the navigation panel.

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

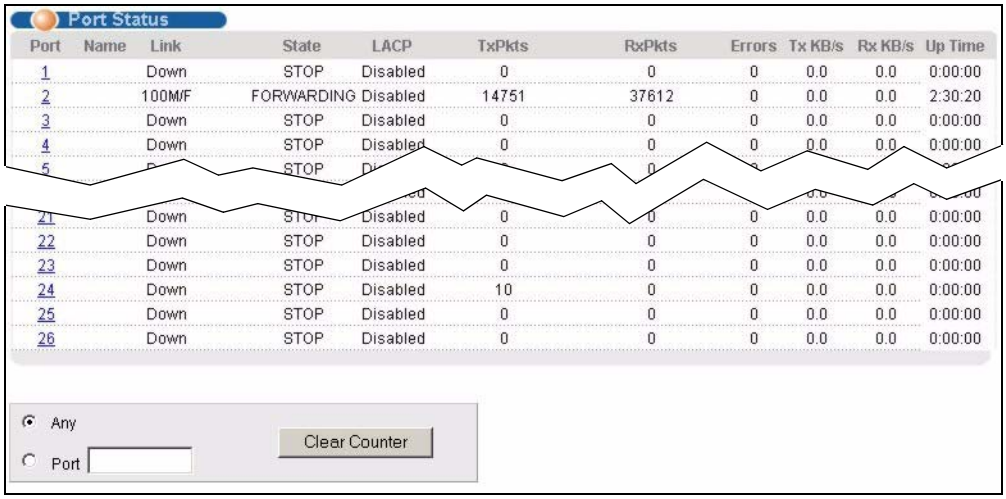
This chapter describes the system status (web configurator home page) and port details screens.

6.1 Port Status Summary

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

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
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 25 on page 62).
Name	This field displays the descriptive port name for identification purposes. This field displays the first eight characters of the port name.

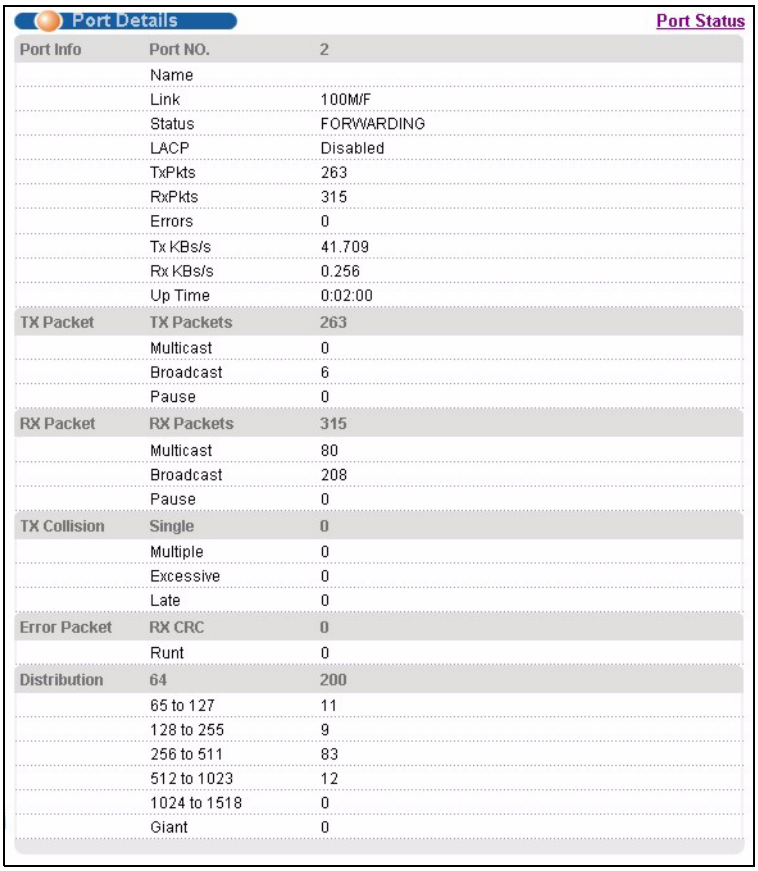
Table 6 Status (continued)

LABEL	DESCRIPTION
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	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.2 on page 95 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
PD	This field is available on ES-2024PWR. This fields displays whether PoE (Power over Ethernet) is enabled (**On**) or disabled (**Off**) on this port.
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.
Clear Counter	To erase statistical information of a port, select and enter the port number in the **Port** field and click **Clear Counter**. To erase statistical information of all ports, select **Any** and click **Clear Counter**.

6.1.1 Status: Port Details

Click a number in the **Port** column **i**n 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	
Port NO.	This field displays the port index number.
Name	This field displays the descriptive port name for identification purposes.
Link	This field shows whether the Ethernet connection is down, and the speed/duplex mode.
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.2 on page 95 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
PD PowerConsumption (mW)	This field is available on ES-2024PWR. This field shows the power consumption of the powered device connected to the port.
PD MaxCurrent (mA)	This field is available on ES-2024PWR. This field shows the maximum current a powered device can get from the switch.
PD MaxPower (mW)	This field is available on ES-2024PWR. This field shows the maximum power the switch can provide through this port.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
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.	
TX Packets	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 Packets	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 frames for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frame have already been transmitted.
Error Packet	
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.

Table 7 Status: Port Details (continued)

LABEL	DESCRIPTION
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.

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. 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 also check the firmware version number in this screen.

Figure 26 System Info (ES-2024)

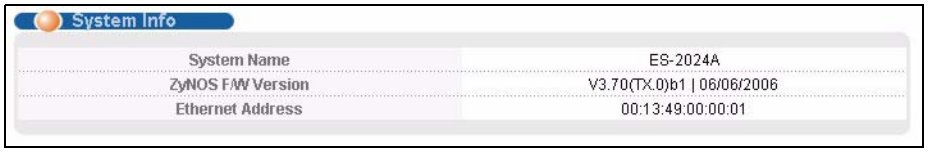
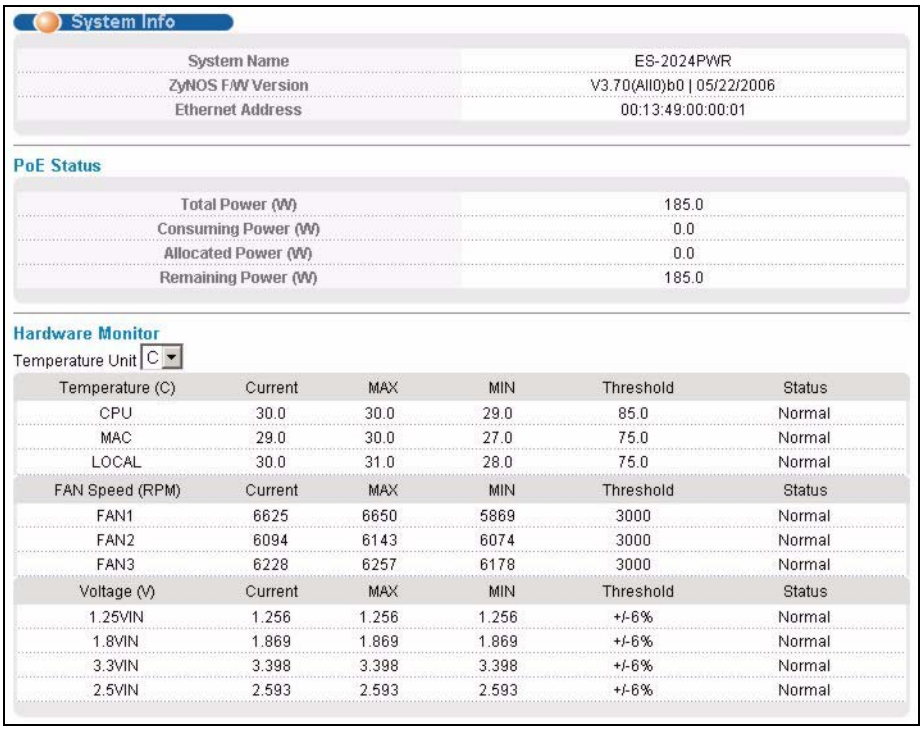


Figure 27 System Info (ES-2024PWR)



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.
PoE Status	
Total Power (W)	This field displays the total power the switch can provide to the connected PoE-enabled devices on the PoE ports.
Consuming Power (W)	This field displays the amount of power the switch is currently supplying to the connected PoE-enabled devices.
Allocated Power (W)	This field displays the total amount of power the switch has reserved for PoE after negotiating with the connected PoE device(s).

Table 8 System Info (continued)

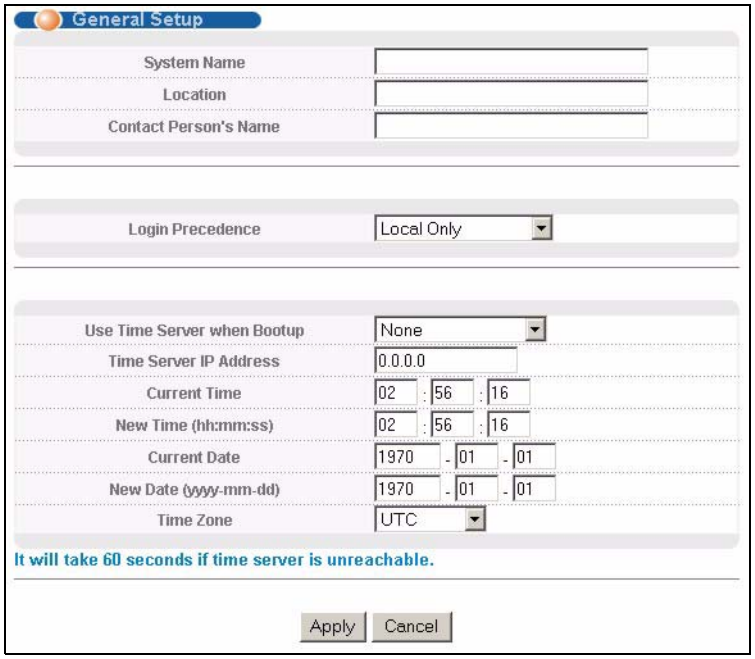
LABEL	DESCRIPTION
Remaining Power (W)	This field displays the amount of power the switch can still provide for PoE. **Note:** The switch must have at least 16W of remaining power in order to supply power to a PoE device; even if the PoE device requested for a lower power supply than 16W.
Hardware Monitor	
Temperature Unit	The switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**CPU**, **MAC** and **LOCAL** refer to the location of the temperature sensors on the circuit board.
Current	This shows the current temperature in degrees centigrade at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above. If **Error** displays, check that the fans are working and make sure that you do not block ventilation holes on the switch.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed. If **Error** displays, it is recommended that the fan(s) on the switch be replaced by a qualified technician.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the switch still works.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed. If **Error** displays, an electronic component might be defective. Have the switch serviced by a qualified technician.

7.3 General Setup

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

Use this screen to configure general settings such as the system name and time.

Figure 28 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 64 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.
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, password and the access privilege.

Table 9 General Setup (continued)

LABEL	DESCRIPTION
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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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.

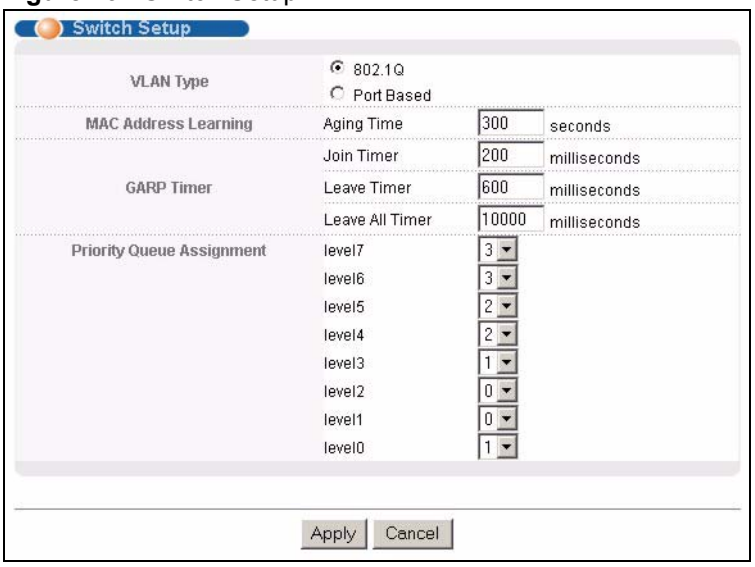
Note: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 8 on page 78 for information on port-based and 802.1Q tagged VLANs.

7.5 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 29 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 78 for more information.
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. See the chapter on VLAN setup for more background information.

Table 10 Switch Setup (continued)

LABEL	DESCRIPTION
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**.
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.
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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

7.6 IP Setup

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

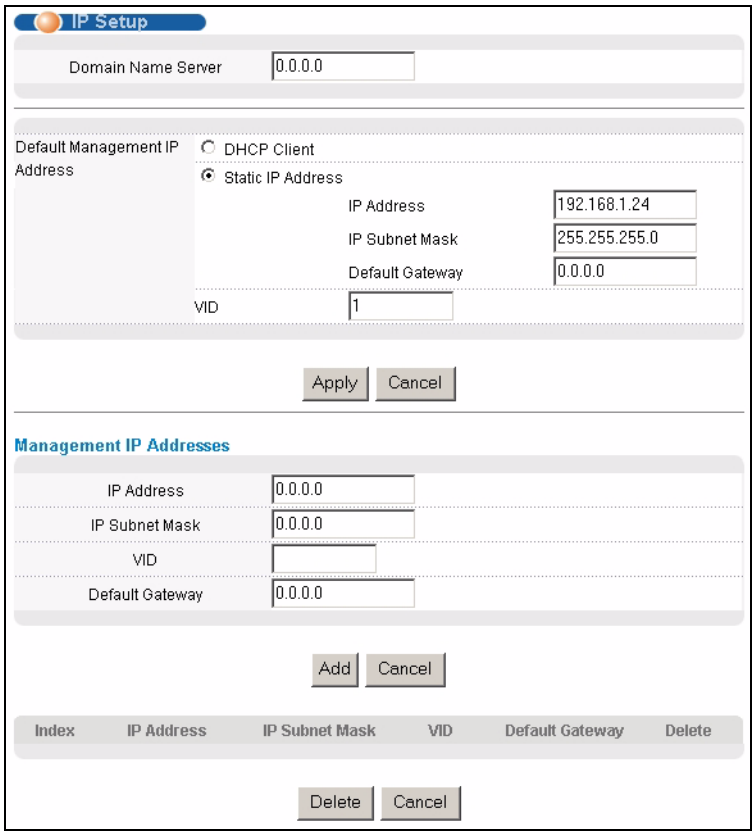
7.6.1 Management IP Addresses

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 30 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.

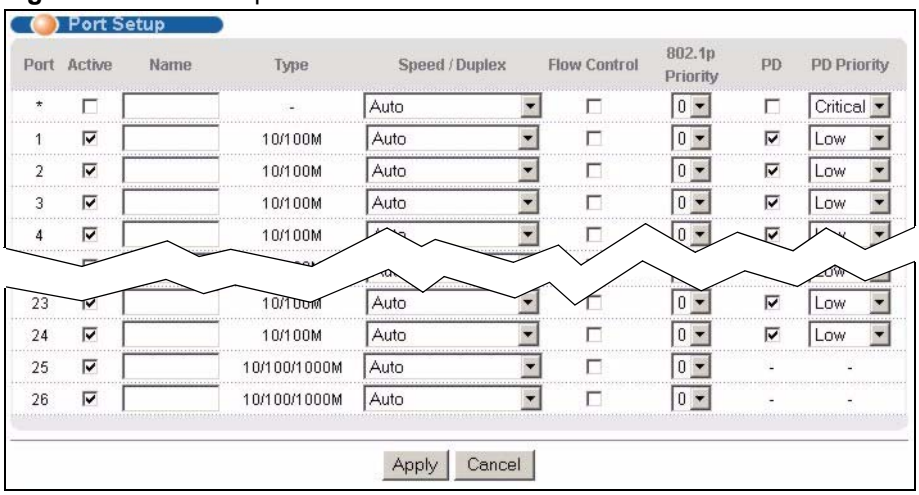
Table 11 IP Setup (continued)

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254
VID	Enter the VLAN identification number associated with the switch IP address. This is the VLAN ID of the CPU and is used for management only. The default is "1". All ports, by default, are fixed members of this "management VLAN" in order to manage the device from any port. If a port is not a member of this VLAN, then users on that port cannot access the device. To access the switch make sure the port that you are connected to is a member of Management VLAN.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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.
IP Subnet Mask	This field displays the subnet mask for the corresponding IP address.
VID	This field displays the VLAN identification number of the network.
Default Gateway	This field displays the IP address of default gateway.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.7 Port Setup

Click **Basic Setting** and then **Port Setup** in the navigation panel to display the configuration screen. Use this screen to configure switch port settings.

Figure 31 Port Setup



The following table describes the labels in this screen.

Table 12 Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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. You can enter up to 64 alpha-numerical characters. **Note:** Due to space limitation, the port name may be truncated in some web configurator screens.
Type	This field displays **10/100M** for an Ethernet connection and **10/100/1000M** 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 ports, select **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/Half Duplex**, **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.

Table 12 Port Setup (continued)

LABEL	DESCRIPTION
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x 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.
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 71 for more information.
PD	This field is only available on the ES-2024PWR but not available for the Gigabit or mini-GBIC ports. A powered device (PD) is a device such as an access point or a switch, that supports PoE (Power over Ethernet) so that it can receive power from another device through a 10/100Mbps Ethernet port. Select the check box to allow a powered device (connected to the port) to receive power from the switch.
PD Priority	This field is only available on the ES-2024PWR but not available for the Gigabit or mini-GBIC ports. When the total power requested by the PDs exceeds the total PoE power budget on the switch, you can set the PD priority to allow the switch to provide power to ports with higher priority. Select **Critical** to give the highest PD priority on the port. Select **High** to set the switch to assign the remaining power to the port after all critical priority ports are served. Select **Low** to set the switch to assign the remaining power to the port after all the critical and high priority ports are served.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 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.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

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 IEEE 802.1Q VLAN terminology.

Table 13 IEEE 802.1Q VLAN 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 VLAN Terminology (continued)

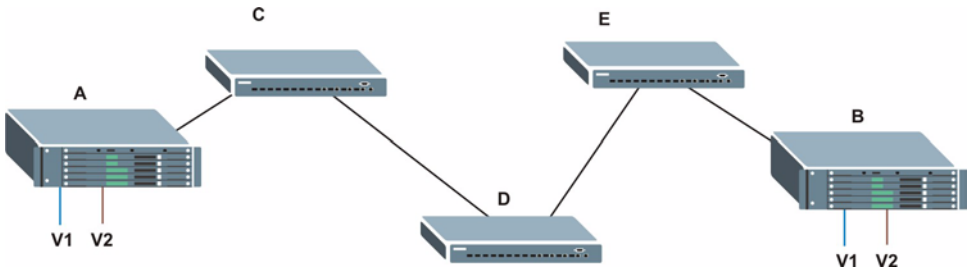
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable frame type	You may choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.
	Ingress filtering	If set, the switch discards 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).

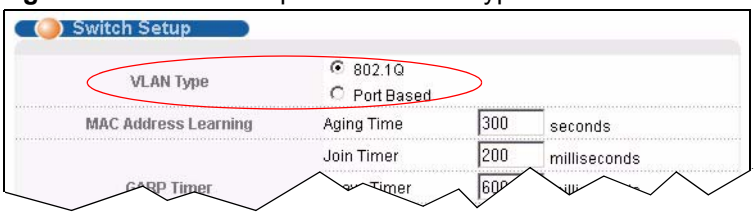
Figure 32 Port VLAN Trunking



8.4 Select the VLAN Type

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

Figure 33 Switch Setup: Select VLAN Type



8.5 Static VLAN

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

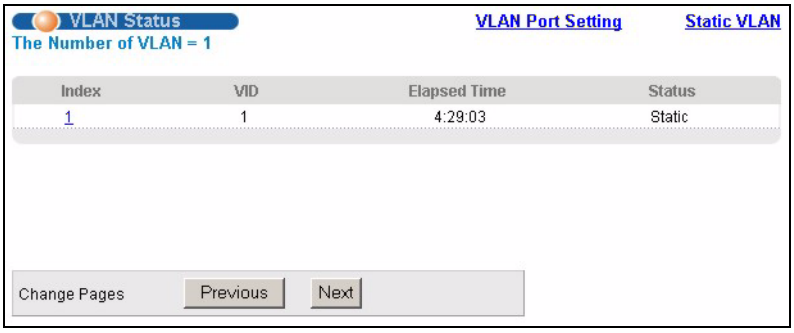
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

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. Refer to Section 8.1 on page 78 for more information on static VLAN.

Figure 34 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. Click an index number to display detailed VLAN status.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.

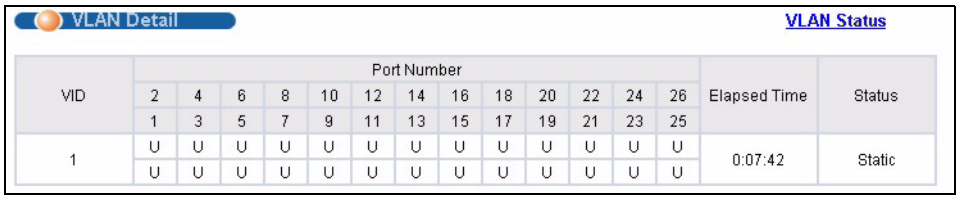
Table 14 VLAN: VLAN Status (continued)

LABEL	DESCRIPTION
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; **dynamic** - using GVRP, **static** - added as a permanent entry or **other** - added using Multicast VLAN Registration (MVR).
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

8.5.2 VLAN Detail

Click an index number in the VLAN Status screen to display the VLAN Detail screen. Use this screen to view detailed port settings and status of the VLAN group. Refer to Section 8.1 on page 78 for more information on static VLAN.

Figure 35 VLAN Status: Detail



The following table describes the labels in this screen.

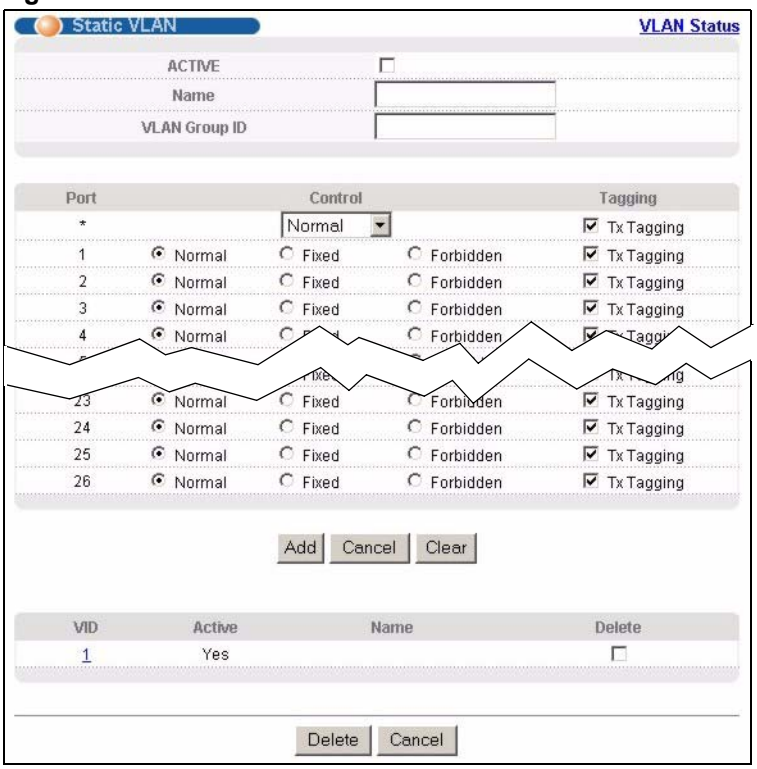
Table 15 VLAN Status: Detail

LABEL	DESCRIPTION
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN 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; **dynamic** - using GVRP, **static** - added as a permanent entry or **other** - added using Multicast VLAN Registration (MVR).

8.5.3 Configure a Static VLAN

To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen. Use this screen to configure and view 802.1Q VLAN parameters for the switch. Refer to Section 8.1 on page 78 for more information on static VLAN.

Figure 36 VLAN: Static VLAN



The following table describes the related labels in this screen.

Table 16 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.
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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.

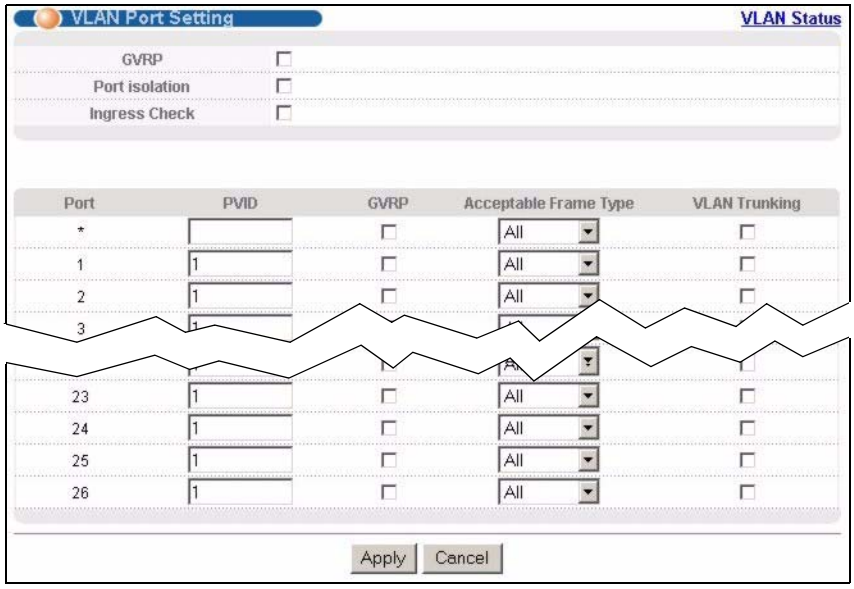
Table 16 VLAN: Static VLAN (continued)

LABEL	DESCRIPTION
Add	Click **Add** to add the settings as a new entry in the summary table below. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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.

8.5.4 Configure VLAN Port Settings

Use the **VLAN Port Setting** screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Refer to Section 8.1 on page 78 for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 37 VLAN: VLAN Port Setting



The following table describes the labels in this screen.

Table 17 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** allows each port (1 to 26) to communicate only with the CPU management port and the uplink ports but not communicate with each other. 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.
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 33 on page 81) and then click **VLAN** from the navigation panel to display the next screen.

Figure 38 Port Based VLAN Setup (All Connected)

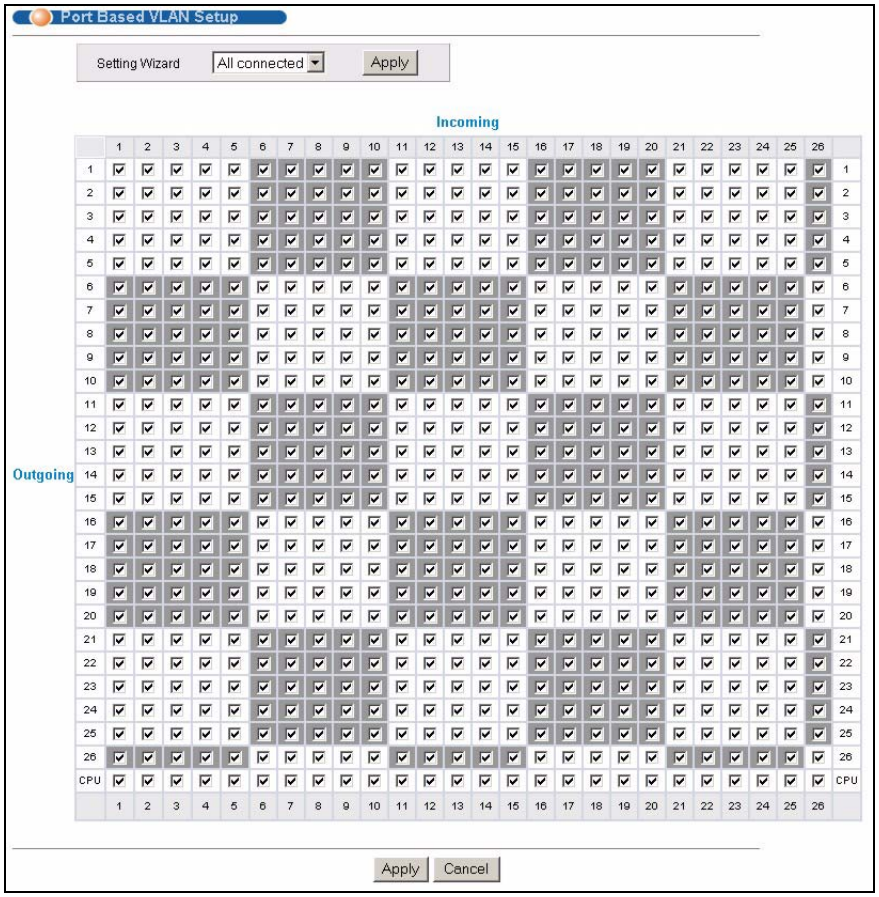
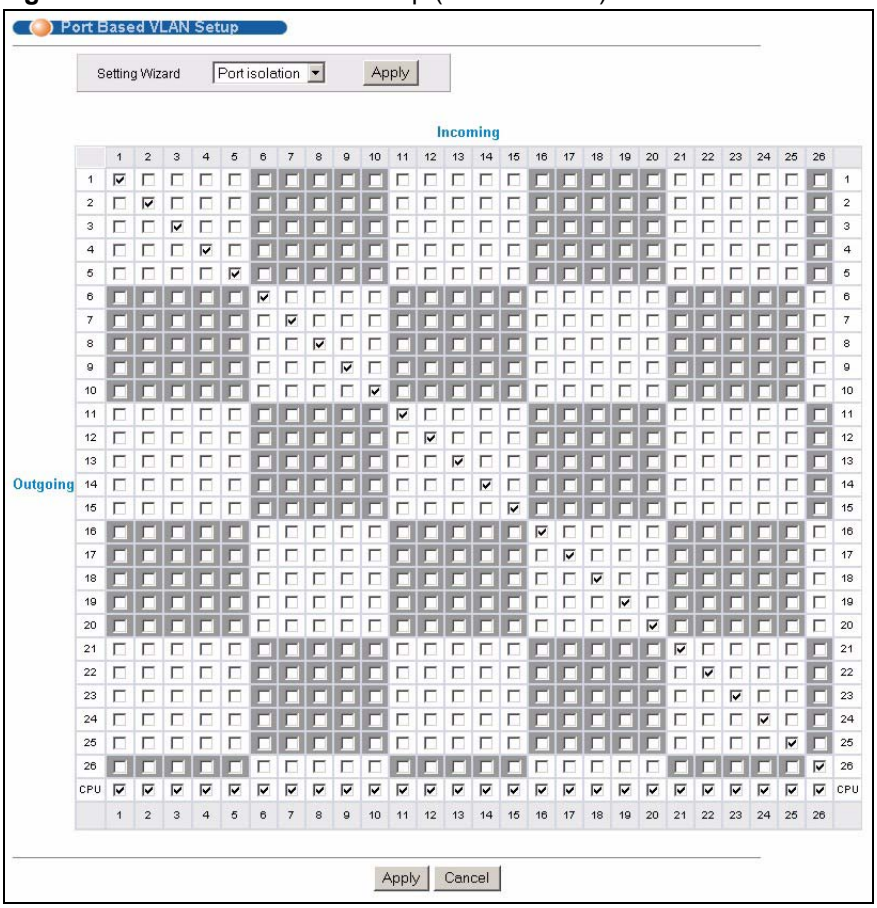


Figure 39 Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 18 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.

Table 18 Port Based VLAN Setup (continued)

LABEL	DESCRIPTION
Outgoing	These are the egress ports; an egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the 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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 Static MAC Forwarding Overview

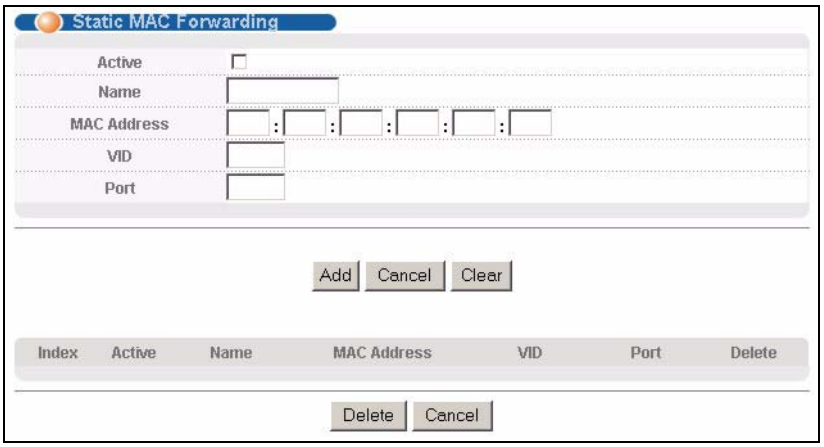
A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

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 118 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 40 Static MAC Forwarding



The following table describes the labels in this screen.

Table 19 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	Enter the number of 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. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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.
VID	This field displays the VLAN identification number.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
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.

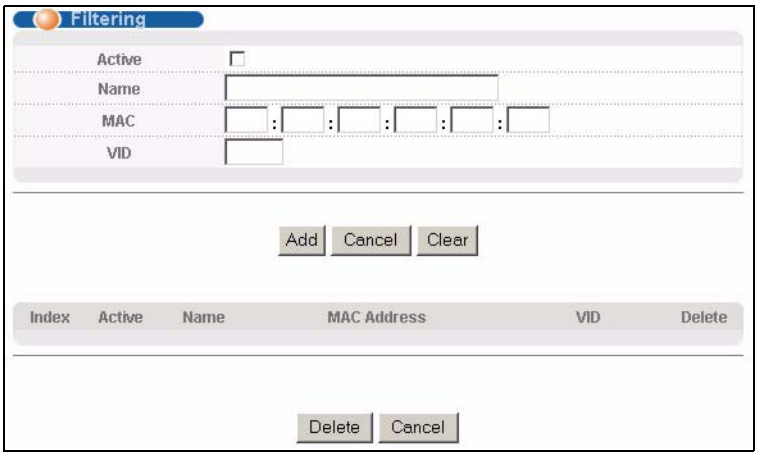
10.1 Filtering Overview

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 41 Filtering



The following table describes the related labels in this screen.

Table 20 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 20 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. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 ID of the VLAN to which this filter applies.
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) and Rapid Spanning Tree Protocol (RSTP).

11.1 STP/RSTP Overview

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

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

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

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 21 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.

11.2 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.

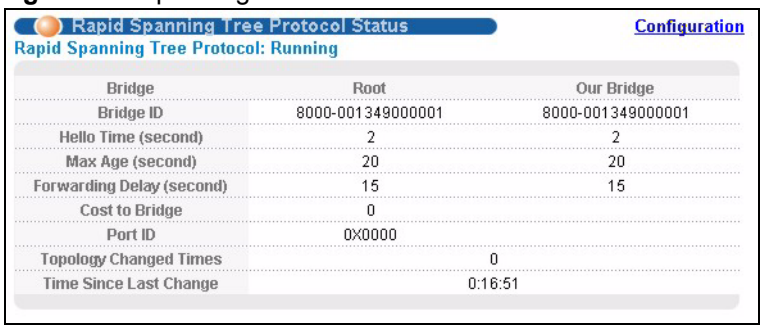
Table 22 STP Port States

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.

11.3 STP Status

Click **Advanced Application**, **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. Refer to Section 11.1 on page 94 for more information on STP (Spanning Tree Protocol).

Figure 42 Spanning Tree Protocol: Status



The following table describes the labels in this screen.

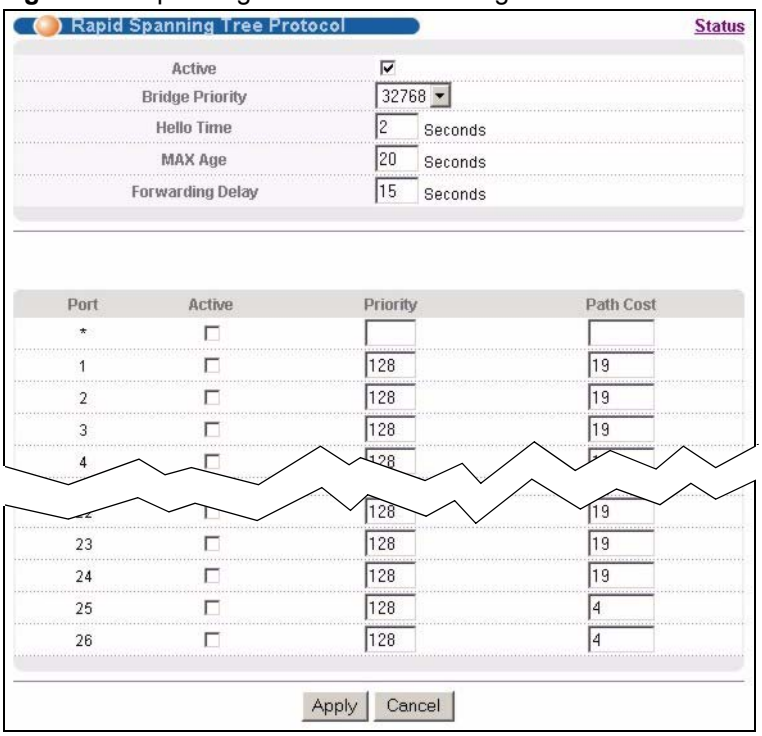
Table 23 Spanning Tree Protocol: Status

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 11.4 on page 96.
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.

11.4 Configuring STP

To configure STP, click the **Configuration** link in the **Spanning Tree Protocol** screen as shown next. Refer to Section 11.1 on page 94 for more information on STP (Spanning Tree Protocol).

Figure 43 Spanning Tree Protocol: Configuration



The following table describes the labels in this screen.

Table 24 Spanning Tree Protocol: Configuration

LABEL	DESCRIPTION
Status	Click **Status** to display the **Spanning Tree Protocol Status** screen (see Figure 42 on page 96).
Active	Select this check box to activate STP. Clear this checkbox to disable STP.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. 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.

Table 24 Spanning Tree Protocol: Configuration (continued)

LABEL	DESCRIPTION
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.
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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 21 on page 94 for more information.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 12
Bandwidth Control

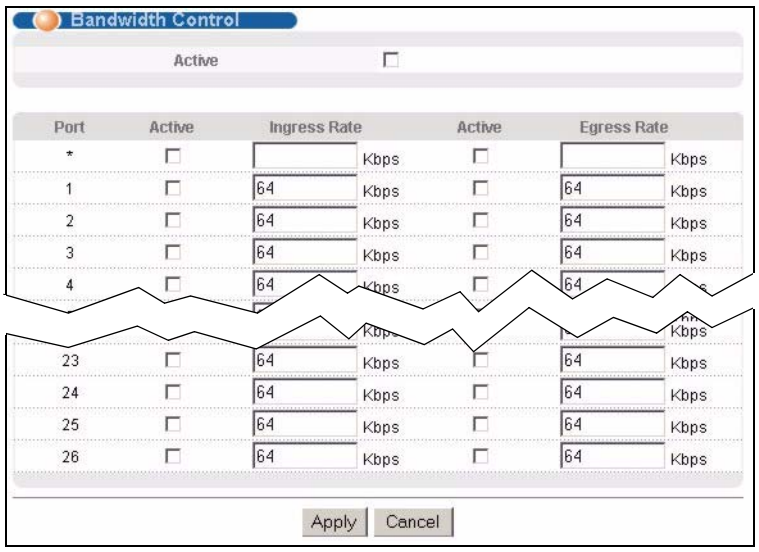
This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

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 44 Bandwidth Control



The following table describes the related labels in this screen.

Table 25 Bandwidth Control

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

Table 25 Bandwidth Control (continued)

LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
Active	Make sure to select this check box to activate ingress rate limit on this port.
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.
Active	Select this check box to activate egress rate limit on this port.
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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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.

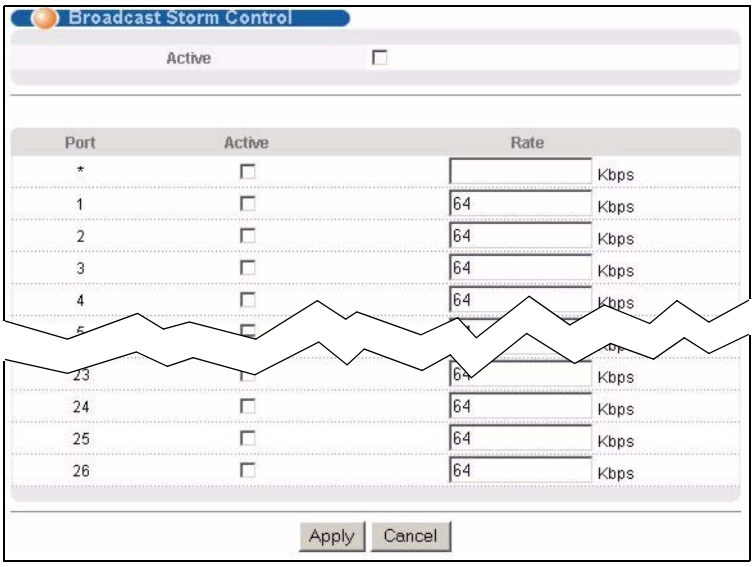
13.1 Broadcast Storm Control Overview

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 45 Broadcast Storm Control



The following table describes the labels in this screen.

Table 26 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.

Table 26 Broadcast Storm Control (continued)

LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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 to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 14
Mirroring

This chapter discusses the Mirror setup screens.

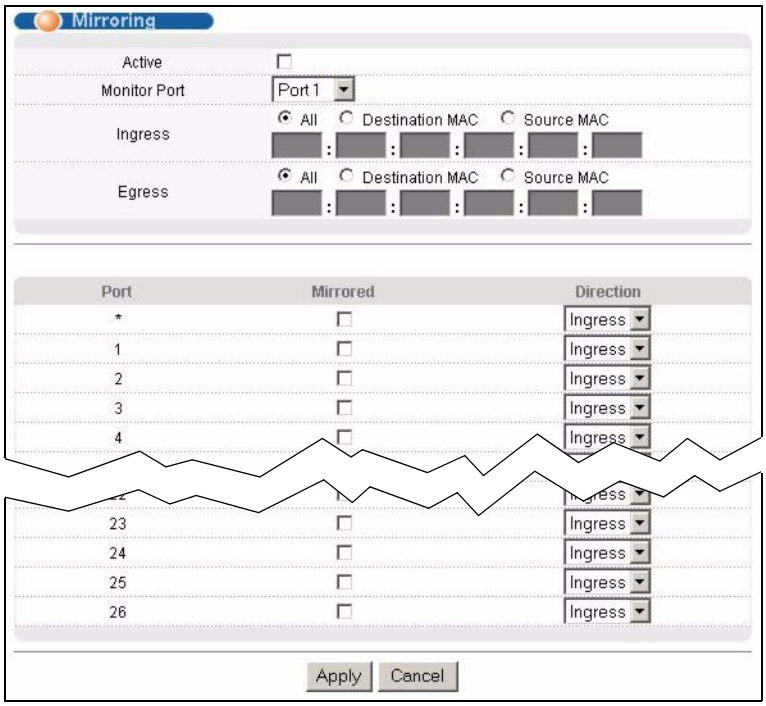
14.1 Mirroring Overview

Port mirroring allows you to copy a traffic flow to a monitor 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 monitor port and specify the traffic flow to be copied to the monitor port.

Figure 46 Mirroring



The following table describes the labels in this screen.

Table 27 Mirroring

LABEL	DESCRIPTION
Active	Clear this check box to deactivate port mirroring on the switch.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Select this port from this drop-down list box.
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.
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.

Table 27 Mirroring (continued)

LABEL	DESCRIPTION
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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 Link Aggregation 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 28 Link Aggregation ID: Local Switch

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

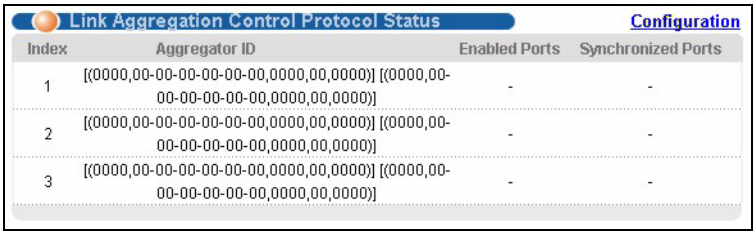
Table 29 Link Aggregation ID: Peer Switch

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. Refer to Section 15.1 on page 108 for more information on link aggregation control.

Figure 47 Link Aggregation Control Protocol Status



The following table describes the labels in this screen.

Table 30 Link Aggregation Control Protocol Status

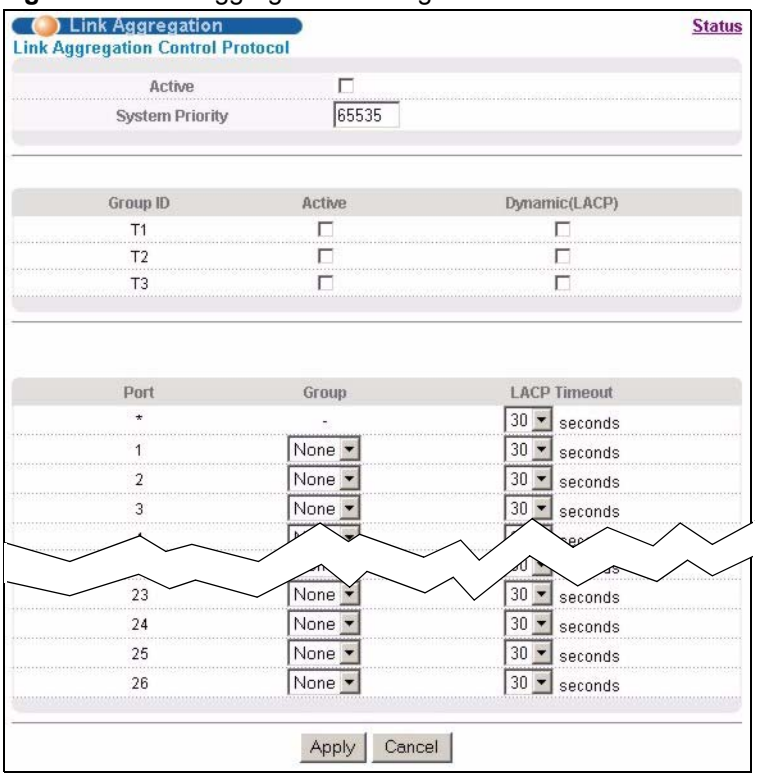
LABEL	DESCRIPTION
Index	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Aggregator ID	This field displays the link aggregation ID. Link aggregation ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.2.1 on page 109 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.

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

15.4 Link Aggregation Setup

Click **Configuration** in the **Link Aggregation Control Protocol Status** screen to display the screen shown next. Refer to Section 15.1 on page 108 for more information on link aggregation control.

Figure 48 Link Aggregation: Configuration



The following table describes the labels in this screen.

Table 31 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.

Table 31 Link Aggregation Control Protocol: Configuration (continued)

LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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 to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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. See Chapter 30 on page 182 for information on how to use the commands to configure additional RADIUS server settings as well as multiple RADIUS server configuration.

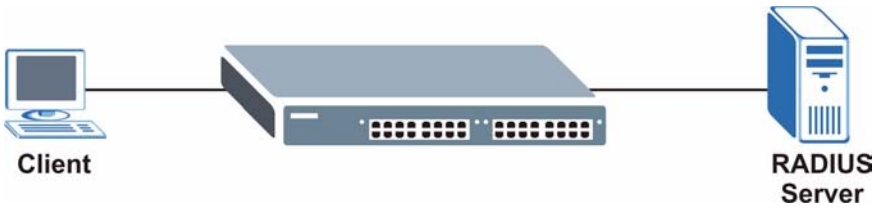
16.1 Port Authentication Overview

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 49 RADIUS Server



16.1.1.1 Vendor Specific Attribute

A Vendor Specific Attribute (VSA) is an attribute-value pair that is sent between a RADIUS server and the switch. Configure VSAs on the RADIUS sever to set the switch to perform the following actions on an authenticated user:

- Limit bandwidth on incoming or outgoing traffic
- Assign account privilege levels

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.

Note: Refer to the documentation that comes with your RADIUS server on how to configure a VSA.

The following table describes the VSAs supported on the switch.

Table 32 Supported VSA

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	`Vendor-Id = 890` (ZyXEL) `Vendor-Type = 1` `Vendor-data =` ingress rate (decimal)
Egress Bandwidth Assignment	`Vendor-Id = 890` (ZyXEL) `Vendor-Type = 2` `Vendor-data =` egress rate (decimal)

Privilege Assignment	`Vendor-ID = 890` (ZyXEL)
	`Vendor-Type = 3`
	`Vendor-Data = "shell:priv-lvl=N"`
	or
	`Vendor-ID = 9` (CISCO)
	`Vendor-Type = 1` (CISCO-AVPAIR)
	`Vendor-Data = "shell:priv-lvl=N"`
	where `N` is a privilege level (from 0 to 14).
	Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the switch, the user is assigned a privilege level from the database (RADIUS or local) the switch uses first for user authentication.

16.1.1.2 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server to assign a port on the switch to a VLAN (fixed, untagged). This will also set the port's VID. Refer to RFC 3580 for more information.

Table 33 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE

VLAN Assignment	`Tunnel-Type = VLAN(13)`
	`Tunnel-Medium-Type = 802(6)`
	`Tunnel-Private-Group-ID =` VLAN ID
	Note: You must also create a VLAN with the specified VID on the switch.

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.

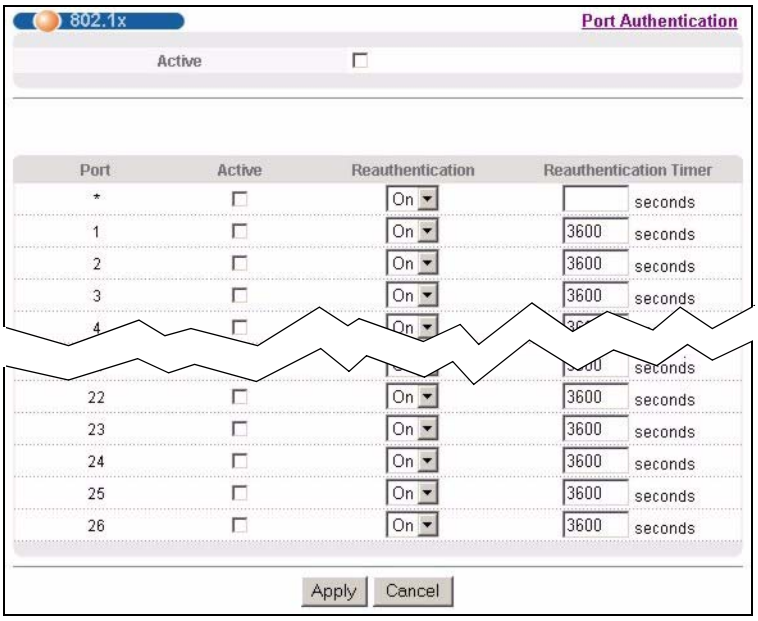
Figure 50 Port Authentication

16.3 Activating IEEE 802.1x Security

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

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

Figure 51 Port Authentication: 802.1x



The following table describes the labels in this screen.

Table 34 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.

Table 34 Port Authentication: 802.1x (continued)

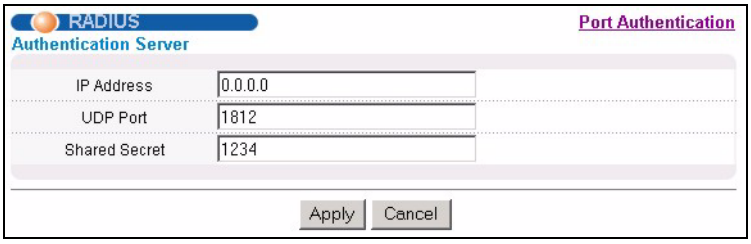
LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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 to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.4 Configuring RADIUS Server Settings

From the **Port Authentication** screen, click **RADIUS** to display the configuration screen as shown. You can configure two RADIUS servers on the switch. Use this screen to configure the first RADIUS server.

Note: Use the CLI to configure the first or second RADIUS server.

Figure 52 Port Authentication: RADIUS



The following table describes the labels in this screen.

Table 35 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.

Table 35 Port Authentication: RADIUS (continued)

LABEL	DESCRIPTION
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 to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 Port Sercurity 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.

Functionally the switch allows for three possible outcomes with port security. You can configure the ports to:

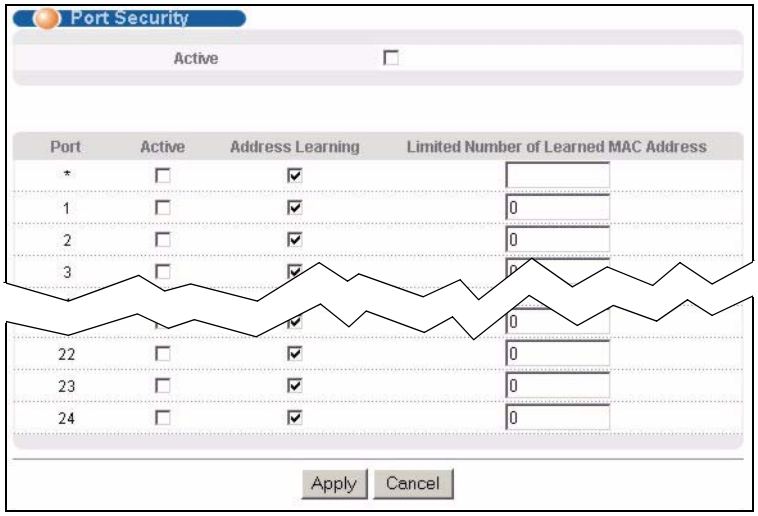
- Forward all packets and learn all MAC addresses.
- Drop all packets from unknown MAC addresses and do not learn MAC addresses.
- Drop all packets from unknown MAC addresses and learn a limited number of MAC addresses.

Note: The switch supports five possible configurations for port security. See Section 17.3 on page 120 for supported configurations and an example.

17.2 Port Security Setup

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

Figure 53 Port Security



The following table describes the labels in this screen.

Table 36 Port Security

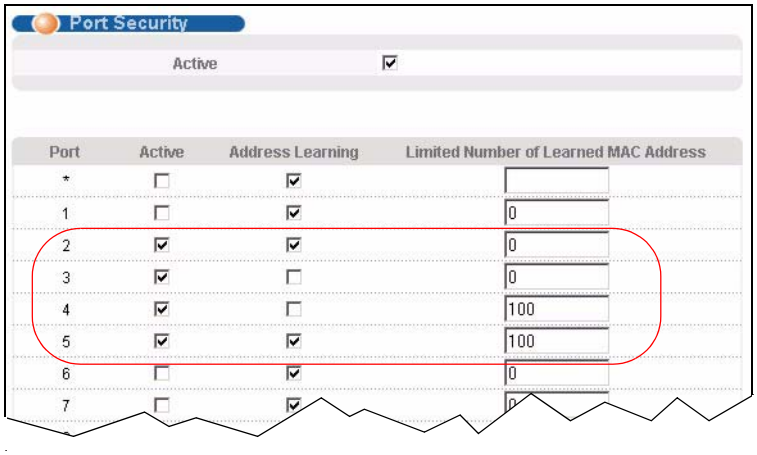
LABEL	DESCRIPTION
Active	Select this check box to enable the port security feature on the switch.
Port	This field displays a port number.
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
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. "0" means this feature is disabled. The switch can learn up to 8K MAC addresses.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.3 Port Security Example

The following example demonstrates the various settings and results associated with different port security configurations. Ports 1 to 5 are configured to:

- Port 1 - Forward all packets and learn all MAC addresses.
- Port 2 - Forward all packets and learn all MAC addresses.
- Port 3 - Drop all packets from unknown MAC addresses and do not learn MAC addresses.
- Port 4 - Drop all packets from unknown MAC addresses and do not learn MAC addresses.
- Port 5 - Drop all packets from unknown MAC addresses but forward packets from up to 100 learned MAC addresses.

Figure 54 Port Security Example



The following table is a summary of configuration and results of this example.

Table 37 Port Security Example

PORT	SETTINGS			RESULT
	ACTIVATE PORT SECURITY	ACTIVATE ADDRESS LEARNING	LIMIT NO. OF LEARNED MAC ADDRESSES	
1		X	**0** (disables limits)	Forward all packets, learn all MAC addresses.
2	X	X	**0** (disables limits)	Forward all packets, learn all MAC addresses.
3	X		**0** (disables limits)	Drop all packets from unknown MAC addresses, do not learn MAC addresses.

Table 37 Port Security Example (continued)

PORT	SETTINGS			RESULT
	ACTIVATE PORT SECURITY	ACTIVATE ADDRESS LEARNING	LIMIT NO. OF LEARNED MAC ADDRESSES	
4	**X**		**100**	Drop all packets from unknown MAC addresses, do not learn MAC addresses.
5	**X**	**X**	**100**	Drop packets from unknown MAC addresses, learn up to 100 MAC addresses.

CHAPTER 18
Queuing Method

This chapter introduces the queuing methods supported.

18.1 Queuing Method 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 38 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)

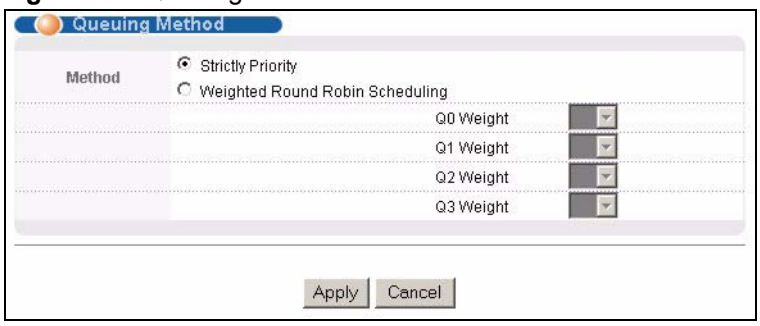
Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal 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 55 Queuing Method



The following table describes the labels in this screen.

Table 39 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 **Strict Priority**, it applies to Q3 only (with priority over all other queues). Q0 ~ Q2 will use **Weighted Round Robin Scheduling**.
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 to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 19
Multicast

This chapter shows you how to configure various multicast features.

19.1 Multicast Overview

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

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

19.1.1 IP Multicast Addresses

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

19.1.2 IGMP Filtering

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

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

19.1.3 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. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch.

19.2 Multicast Status

Click **Advanced Applications** and **Multicast** to display the screen as shown. This screen shows the multicast group information. Refer to Section 19.1 on page 124 for more information on multicast.

Figure 56 Multicast Status .

The following table describes the labels in this screen.

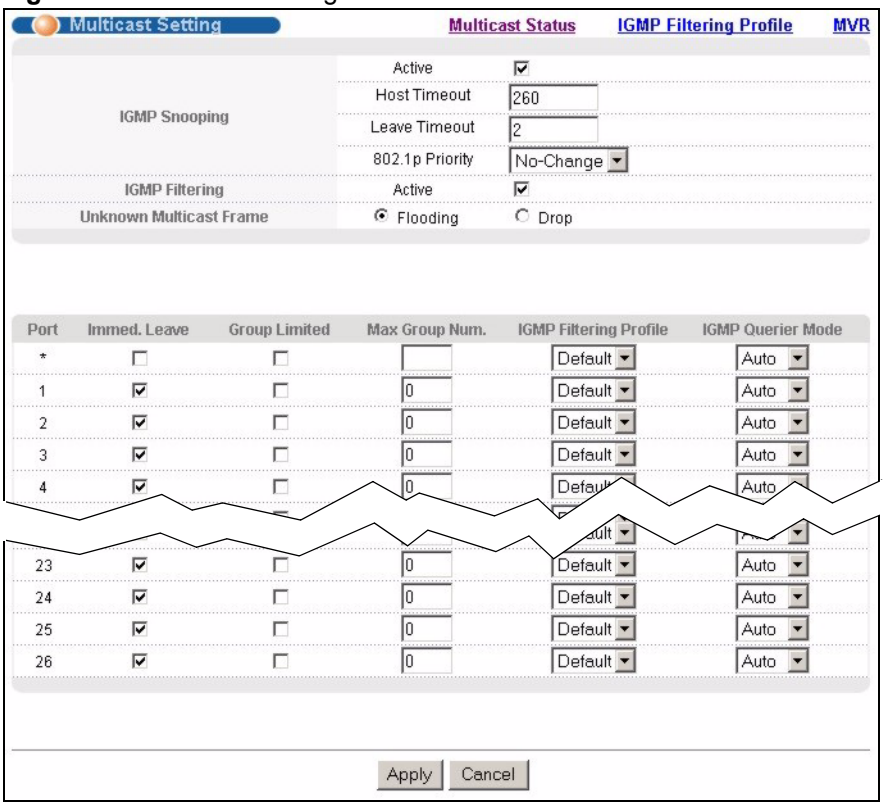
Table 40 Multicast Status

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

19.3 Multicast Setup

Click **Advanced Applications**, **Multicast** and the **Multicast Setting** link to display the screen as shown. Refer to Section 19.1 on page 124 for more information on multicast.

Figure 57 Multicast Setting



The following table describes the labels in this screen.

Table 41 Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Host Timeout	Specify the time (from 1 to 16,711,450) in seconds that elapses before the switch removes an IGMP group membership entry if it does not receive report messages from the port.
Leave Timeout	Enter an IGMP leave timeout value (from 1 to 16,711,450) in seconds. This defines how many seconds the switch waits before removing an IGMP snooping membership entry when an IGMP leave message is received from a host.
802.1p Priority	Select a priority level (0-7) to which the switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join.
Unknown Multicast Frame	Specify the action to perform when the switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.

Table 41 Multicast Setting (continued)

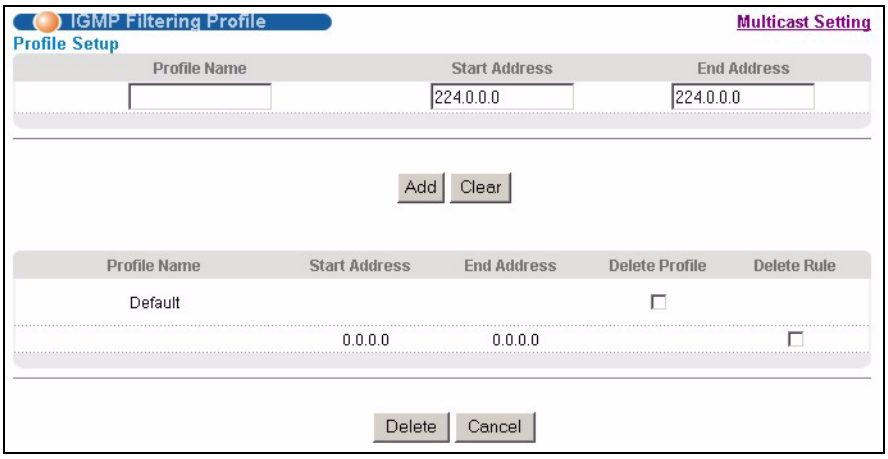
LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group.
IGMP Querier Mode	The switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the switch dynamically change to using the port as an IGMP query port after it receives IGMP query packets. Select **Fixed** to have the switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the switch from using the port as an IGMP query port. The switch will not keep any record of an IGMP router being connected to this port. The switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

19.4 IGMP Filtering Profile

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

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

Figure 58 Multicast: IGMP Filtering Profile



The following table describes the labels in this screen.

Table 42 Multicast: IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click **Add** to save the settings to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to clear the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

19.5 MVR Overview

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

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

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

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

Figure 59 MVR Network Example

19.5.1 Types of MVR Ports

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

19.5.2 MVR Modes

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

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

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

19.5.3 How MVR Works

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

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

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the switch to leave the multicast group. The switch sends a query to VLAN 1 on the receiver port (in this case, a DSL port on the switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the switch removes the receiver port from the forwarding table.

Figure 60 MVR Multicast Television Example

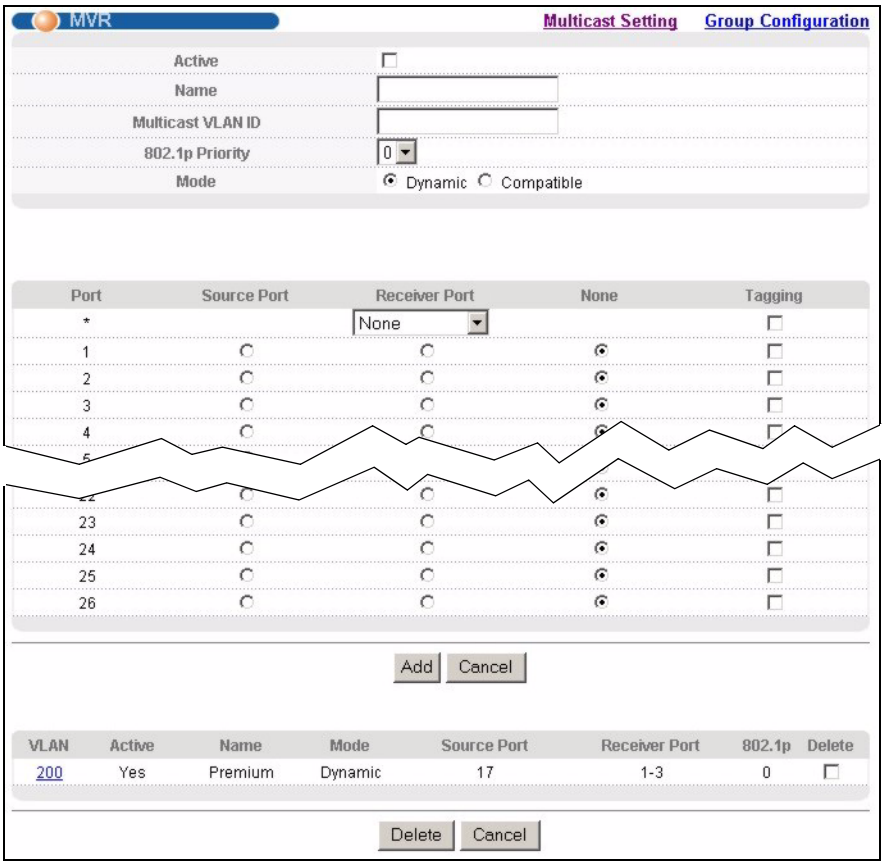
19.6 General MVR Configuration

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

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

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

Figure 61 MVR



The following table describes the related labels in this screen.

Table 43 MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the switch not to send IGMP reports.
Port	This field displays the port number on the switch.

Table 43 MVR (continued)

LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. **Note:** Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click **Add** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

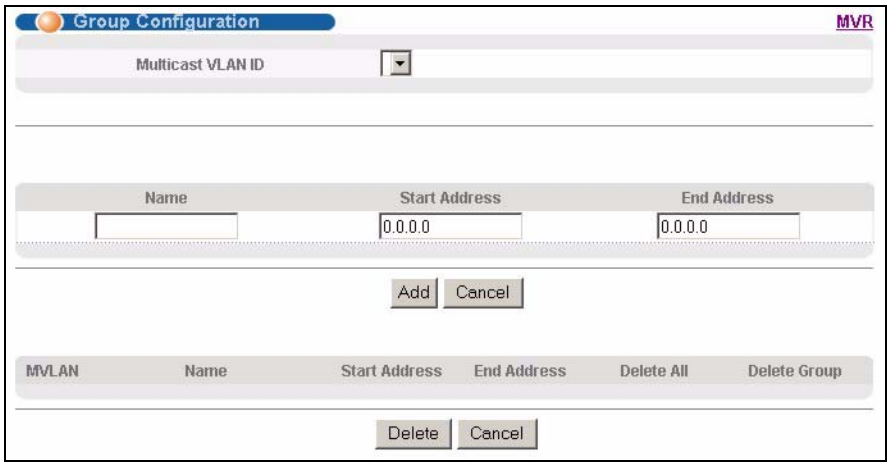
19.7 MVR Group Configuration

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

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

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

Figure 62 MVR: Group Configuration



The following table describes the labels in this screen.

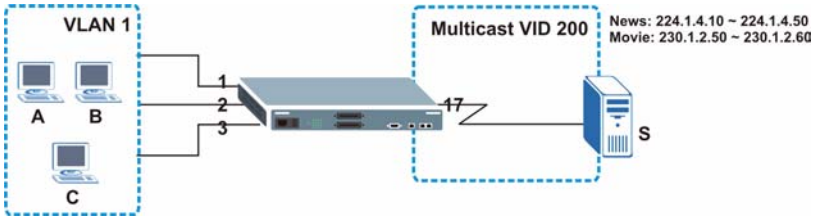
Table 44 MVR: Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 19.1.1 on page 124 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to Section 19.1.1 on page 124 for more information on IP multicast addresses.
Add	Click **Add** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select **Delete All** and click **Delete** to remove all entries from the table. Select **Delete Group** and click **Delete** to remove the selected entry(ies) from the table.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

19.7.1 MVR Configuration Example

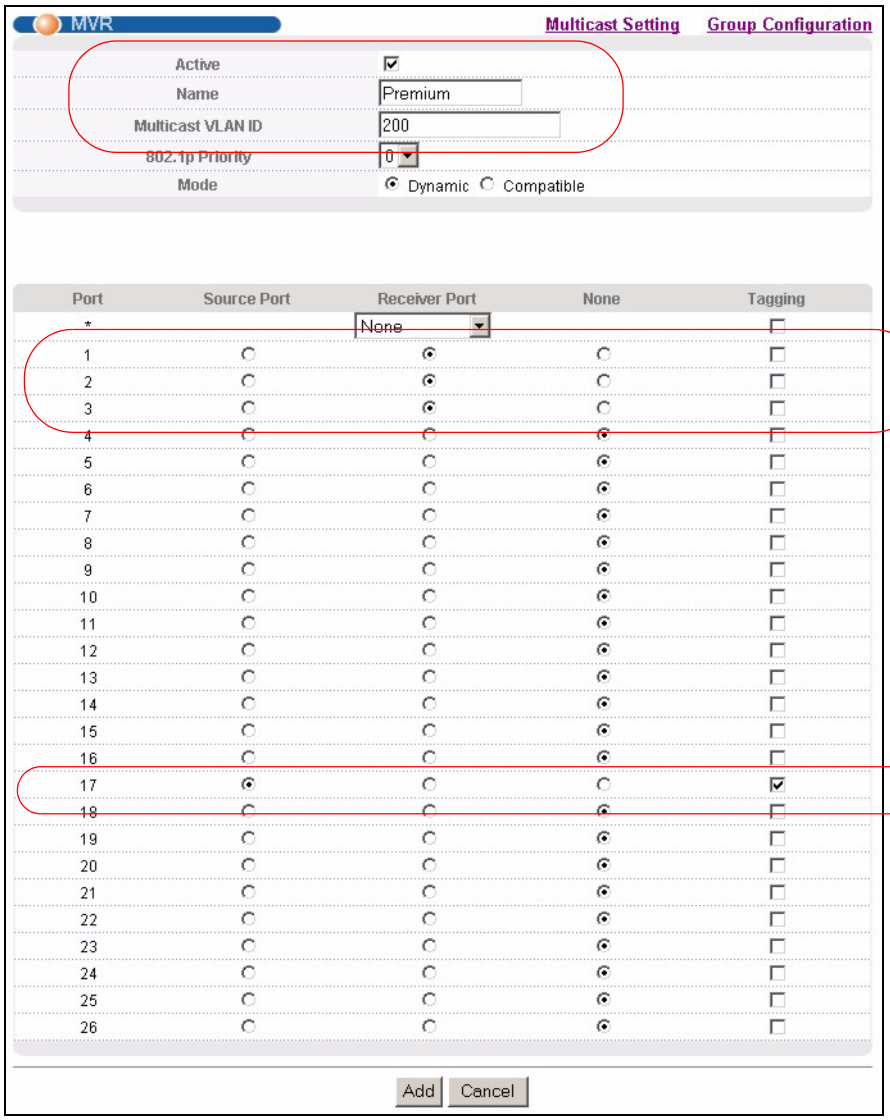
The following figure shows a network example where ports 1, 2 and 3 on the switch belong to VLAN 1. In addition, port 17 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers **A**, **B** and **C** in VLAN are able to receive the traffic.

Figure 63 MVR Configuration Example



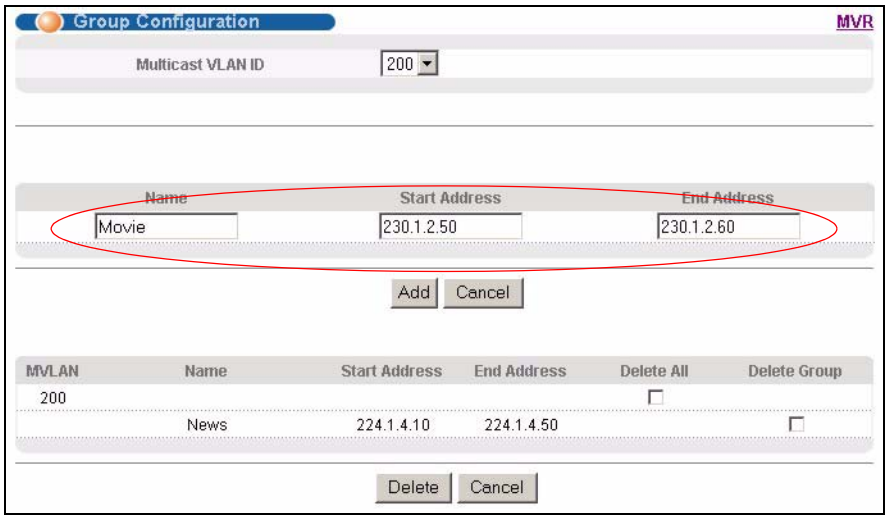
To configure the MVR settings on the switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 64 MVR Configuration Example



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

Figure 65 MVR Group Configuration Example



CHAPTER 20
Static Route

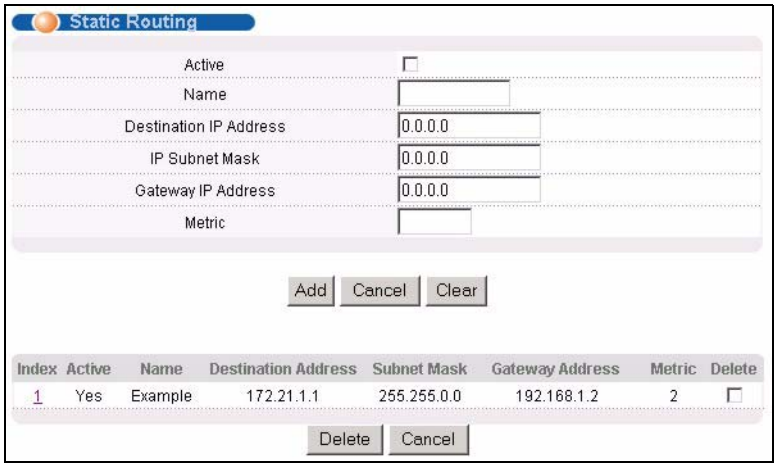
This chapter shows you how to configure static routes.

20.1 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 66 Static Routing



The following table describes the labels in this screen.

Table 45 Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 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 45 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	Clicking **Add** saves your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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 21
DiffServ Code Point

This chapter shows you how to set up Diffserv Code Point (DSCP) on each port and how to convert DSCP values to IEEE 802.1p values.

21.1 DiffServ Overview

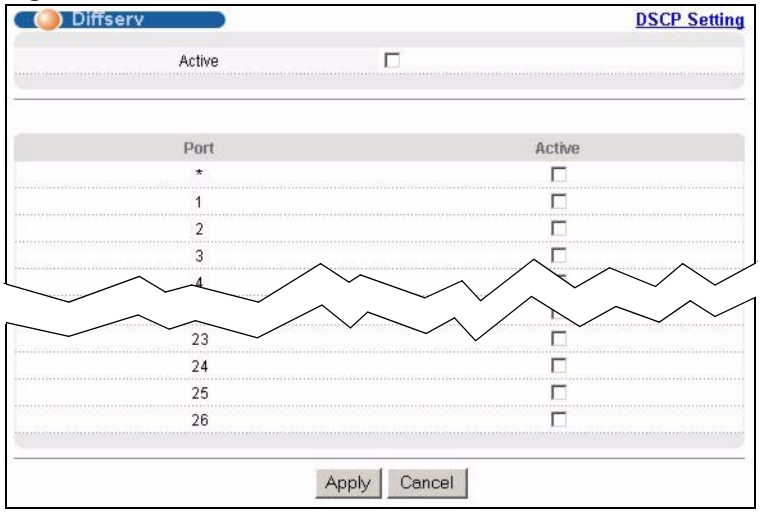
DiffServ Code Point is a field used for packet classification on DiffServ (Differentiated Services) networks. The higher the value, the higher the priority. Lower-priority packets may be dropped if the total traffic exceeds the capacity of the network.

21.2 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 67 DiffServ



The following table describes the labels in this screen.

Table 46 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.

Table 46 DiffServ (continued)

LABEL	DESCRIPTION
*	Use this row to configure all the ports at once. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port by port basis. **Note:** When you make changes in this row, the changes are copied to all the ports as soon as you make them.
Active	Select this option to enable DiffServ on the port.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring this screen again.

21.3 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.

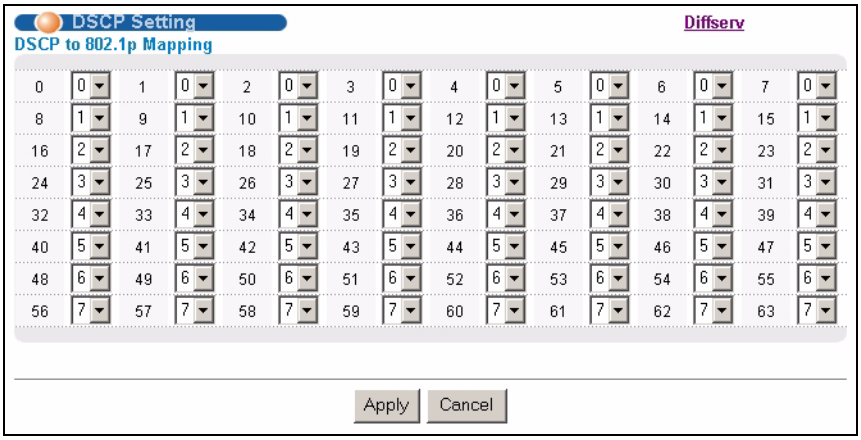
Table 47 Default DSCP-IEEE802.1p Mapping

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

21.3.1 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 68 DiffServ: DSCP Setting



The following table describes the labels in this screen.

Table 48 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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to discard all changes and start configuring the screen again.

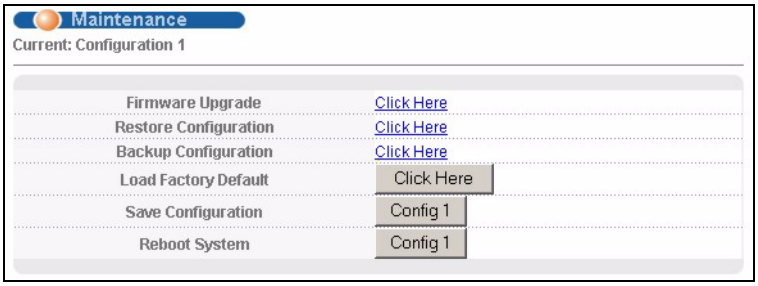
CHAPTER 22
Maintenance

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

22.1 The Maintenance Screen

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

Figure 69 Maintenance



The following table describes the labels in this screen.

Table 49 Maintenance

LABEL	DESCRIPTION
Current	This field displays the configuration file (**Configuration 1**) the switch is currently using.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Load Factory Default	Click **Click Here** to reset the current running configuration to the factory default settings.
Save Configuration	Click **Config 1** to save the current running configuration to the first configuration file.
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the switch. **Note:** Make sure to click the **Save** button in any screen to save your settings to the current configuration on the switch.

22.2 Load Factory Default

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 Default** to clear all switch configuration information you configured and return to the factory defaults. The following message appears.

Figure 70 Load Factory Default: Conformation

2. Click **OK** to reset all switch configurations to the factory defaults
3. In the web configurator, click the **Save** button to make the changes take effect. 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).

22.3 Save Configuration

To save the configuration changes permanently to switch, click **Config 1** next to **Save Configuration** in the main **Maintenance** screen. The switch saves the configuration to first configuration file.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes.

Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently.

All unsaved changes are erased after you reboot the switch.

22.4 Reboot System

Reboot System allows you to restart the switch without physically turning the power off. You also set the switch to use the first configuration file (**Config 1**) when you reboot the switch. Follow the steps below to reboot the switch.

1. In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load the first configuration file. The following screen displays.

Figure 71 Reboot System: Confirmation

2 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.

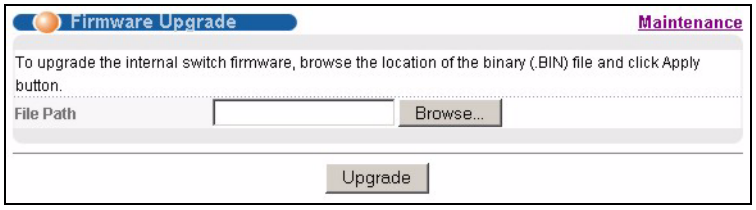
22.5 Firmware Upgrade

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 72 Firmware Upgrade



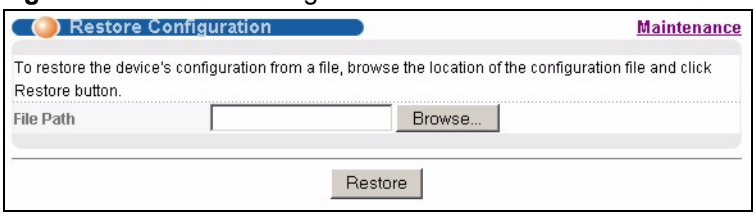
Type the path and file name of the firmware file you wish to upload to the switch in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

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

22.6 Restore a Configuration File

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

Figure 73 Restore Configuration



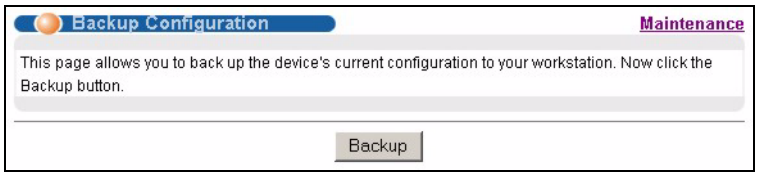
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file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

22.7 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 74 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.

22.8 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.

22.8.1 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 "sysname" file) is the system firmware and has a "bin" filename extension.

Table 50 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.rom	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.

22.8.1.1 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.

22.8.2 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. Enter the user name (for example, admin).
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 50 on page 148 for more information on filename conventions.

7 Enter `quit` to exit the ftp prompt.

22.8.3 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).

22.8.4 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 23
Access Control

This chapter describes how to control access to the switch.

23.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share four sessions, up to five web management sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 51 Access Control Overview

	Console Port	SSH	Telnet	FTP	Web	SNMP
Number of concurrent sessions allowed	1	SSH and Telnet share 4 sessions.		1	5	No limit

When multiple login is disabled and there is already a console port session, you cannot telnet to the switch. The following error message displays.

```
Connection to host lost.

C:\>
```

If you disable multiple login while another administrator is accessing the switch via telnet, the switch will immediately log out the administrator and disconnect the telnet session. The following error message displays.

```
multi-login is disabled, please exit immediately!!

Connection to host lost.

C:\>
```

See Section 30.2.1 on page 182 for more information on disabling multi-login.

23.2 The Access Control Main Screen

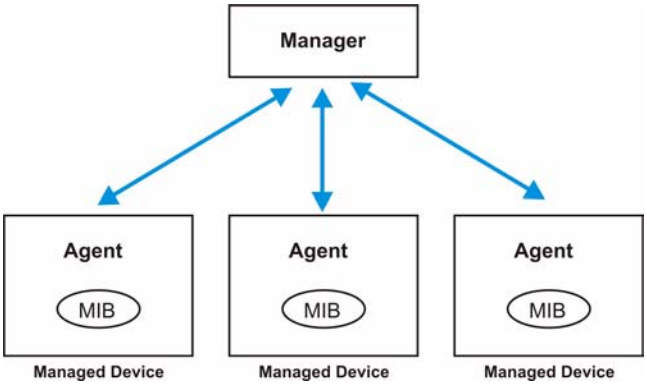
Click **Management**, **Access Control** in the navigation panel to display the main screen as shown. Use these links to configure remote management options and create user accounts on the switch.

Figure 75 Access Control

23.3 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 76 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 52 SNMP Commands

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

23.3.1 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
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP
- Private MIBs

23.3.2 SNMP Traps

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

Table 53 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv2 Traps		
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the switch is turned on.
WarmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the switch restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.

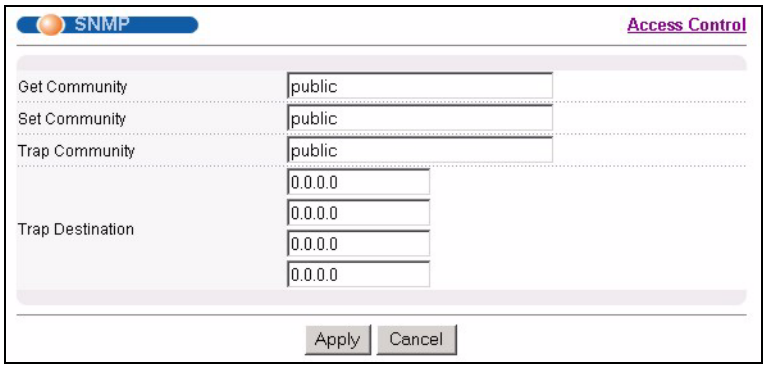
Table 53 SNMP Traps (continued)

OBJECT LABEL	OBJECT ID	DESCRIPTION
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP topology changes.
topology change	1.3.6.1.2.1.17.0.2	This trap is sent when the STP root switch changes.

23.3.3 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 77 Access Control: SNMP



The following table describes the labels in this screen.

Table 54 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 to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.4 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.

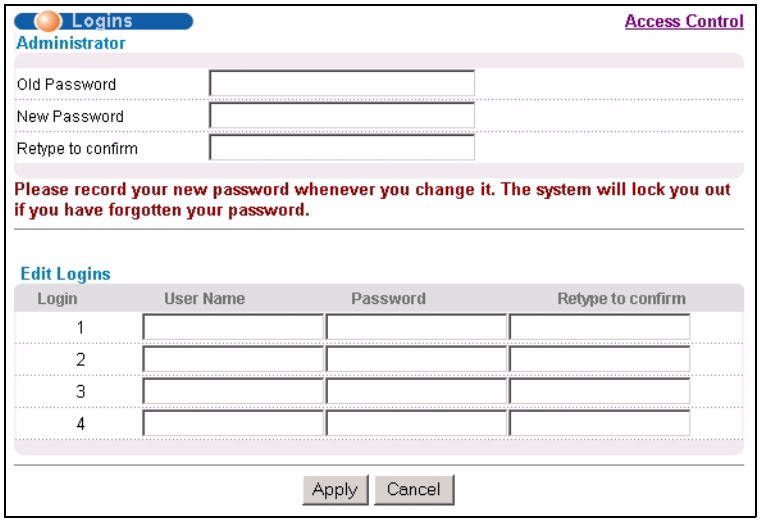
- An administrator is someone who can both view and configure switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

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 78 Access Control: Logins



The following table describes the labels in this screen.

Table 55 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.	

Table 55 Access Control: Logins (continued)

LABEL	DESCRIPTION
User Name	Set a user name (up to 32 characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.5 SSH Overview

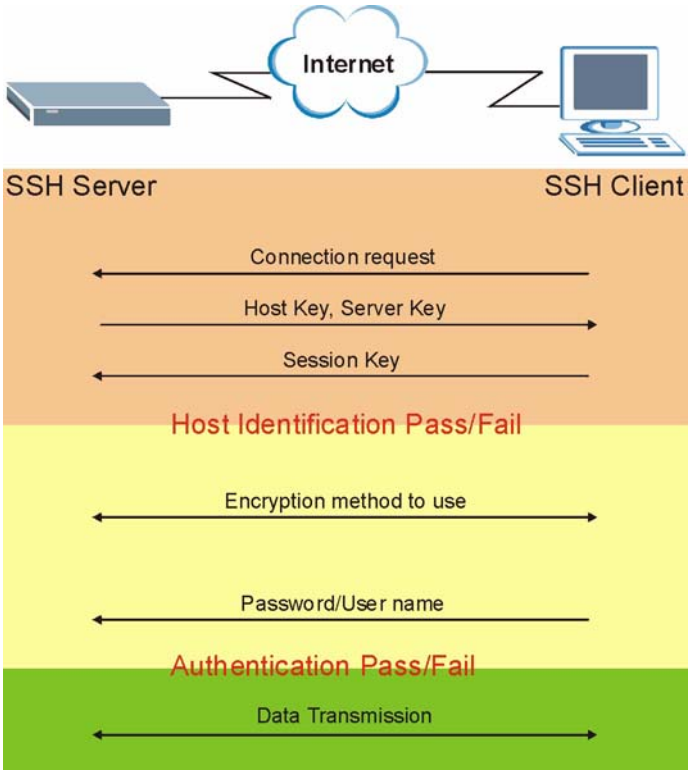
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 79 SSH Communication Example

23.6 How SSH works

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

Figure 80 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.

23.7 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.

23.7.1 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.

23.7.2 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 81 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.
sysname>
```

23.8 Introduction to HTTPS

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

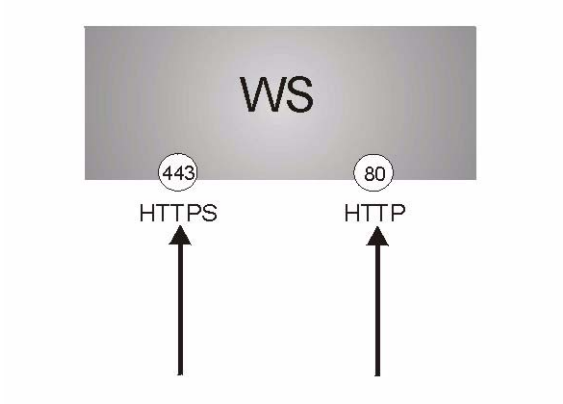
It relies upon certificates, public keys, and private keys.

HTTPS on the switch is used so that you may securely access the switch using the web configurator. The SSL protocol specifies that the SSL server (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 82 HTTPS Implementation



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

23.9 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.

23.9.1 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 83 Security Alert Dialog Box (Internet Explorer)

23.9.2 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 84 Security Certificate 1 (Netscape)

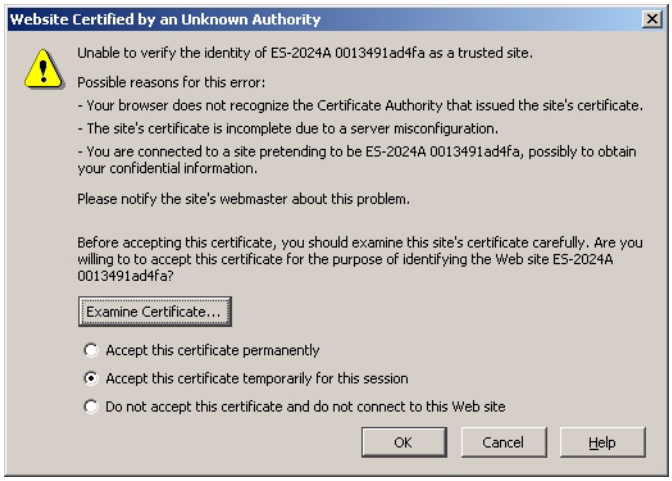
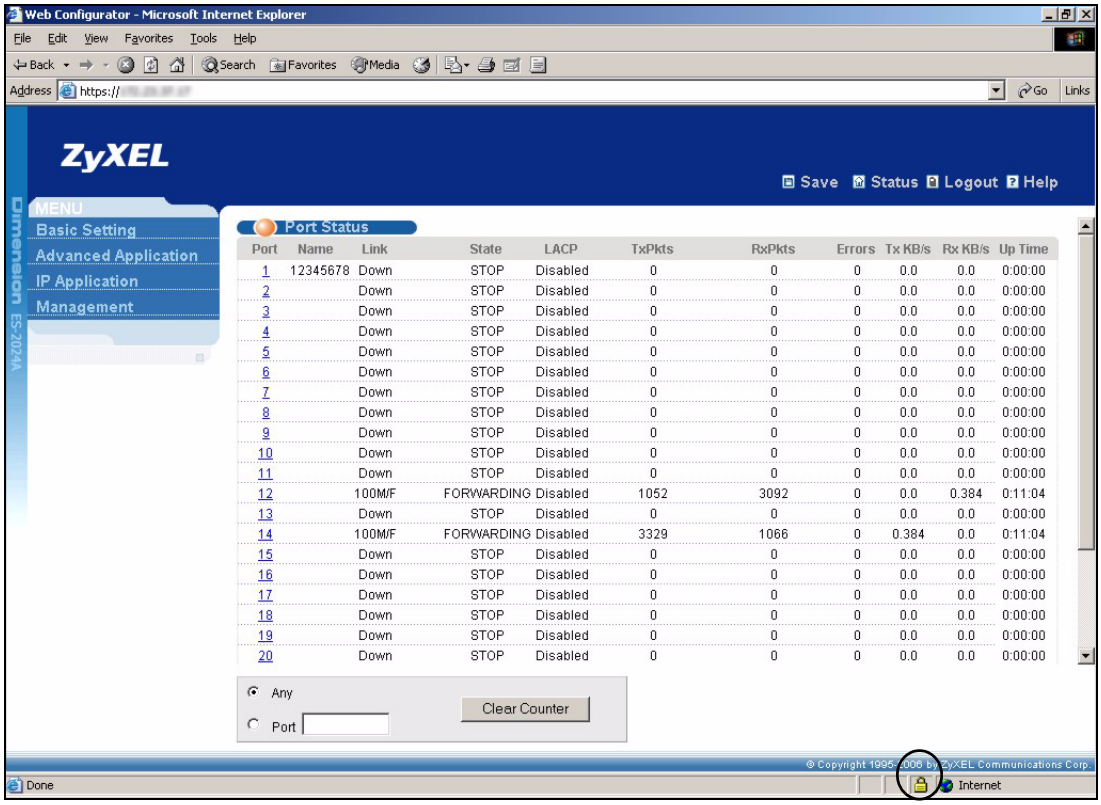


Figure 85 Security Certificate 2 (Netscape)

23.9.3 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.

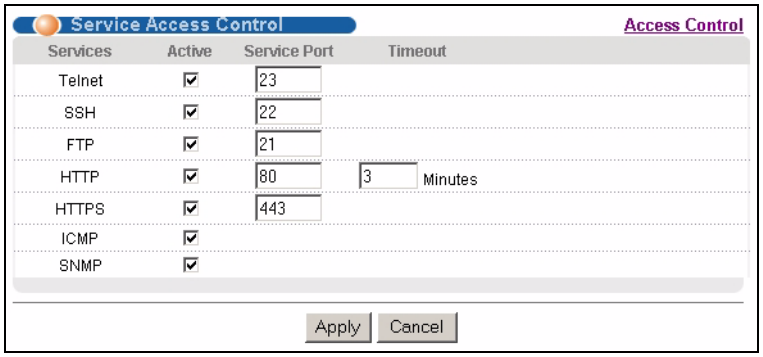
Figure 86 Example: Lock Denoting a Secure Connection



23.10 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 87 Access Control: Service Access Control



The following table describes the fields in this screen.

Table 56 Access Control: Service Access Control

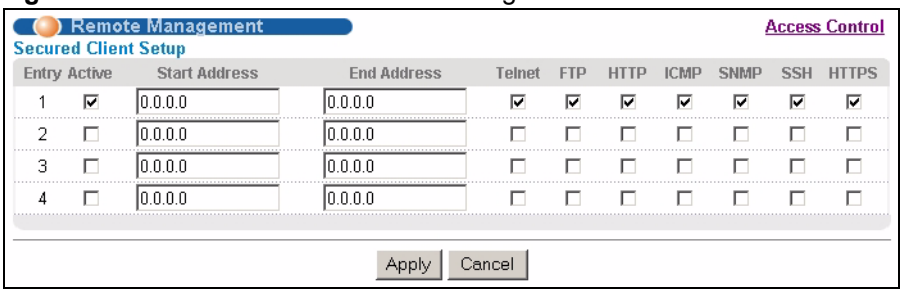
LABEL	DESCRIPTION
Services	Services you may use to access the switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the 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 timeouts may have security risks.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.11 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 88 Access Control: Remote Management



The following table describes the labels in this screen.

Table 57 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/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the switch from the specified trusted computers.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

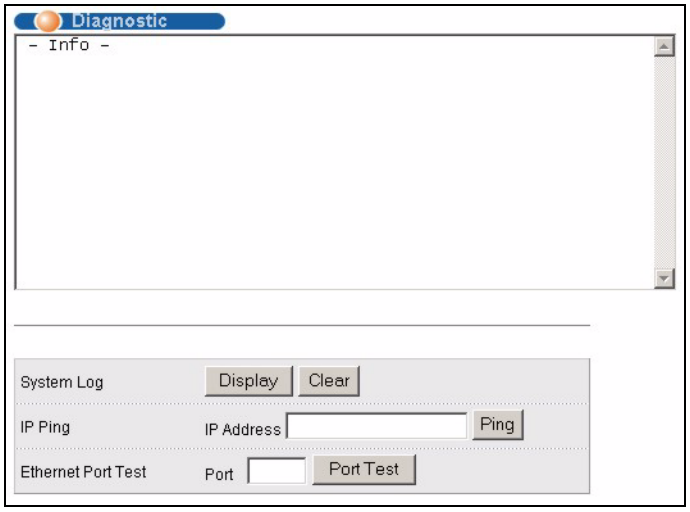
CHAPTER 24
Diagnostic

This chapter explains the **Diagnostic** screen.

24.1 Diagnostic

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

Figure 89 Diagnostic



The following table describes the labels in this screen.

Table 58 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	Enter a port number and click **Port Test** to perform internal loopback test.

CHAPTER 25
Syslog

This chapter explains the syslog screens.

25.1 Syslog Overview

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

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

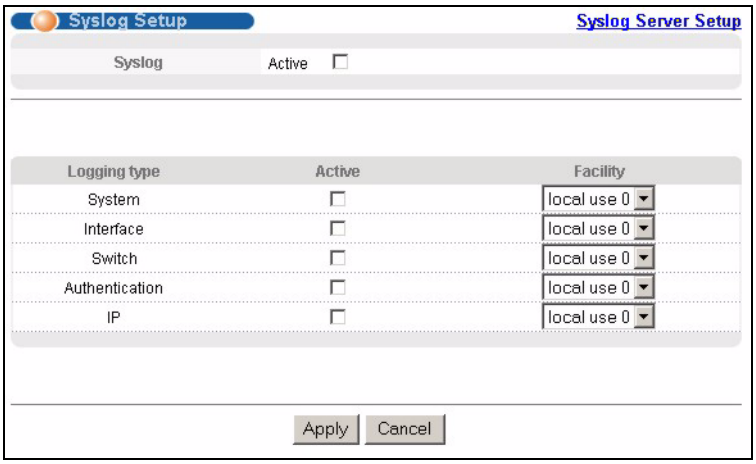
Table 59 Syslog Severity Levels

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

25.2 Syslog Setup

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

Figure 90 Syslog



The following table describes the labels in this screen.

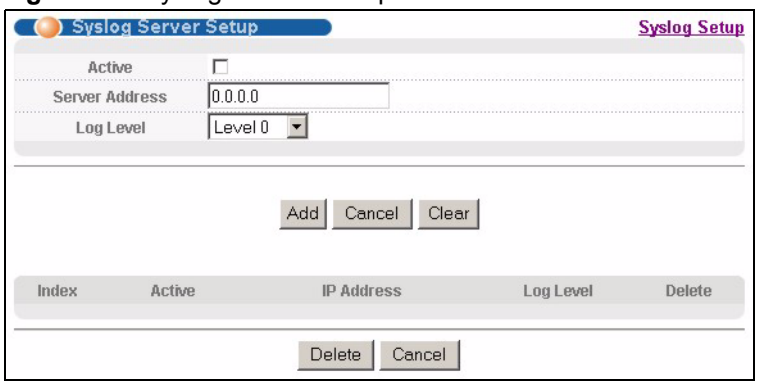
Table 60 Syslog

LABEL	DESCRIPTION
Syslog	Select **Active** to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

25.3 Syslog Server Setup

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

Figure 91 Syslog: Server Setup



The following table describes the labels in this screen.

Table 61 Syslog: Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to reset the fields.

CHAPTER 26
Cluster Management

This chapter introduces cluster management.

26.1 Cluster Management Overview

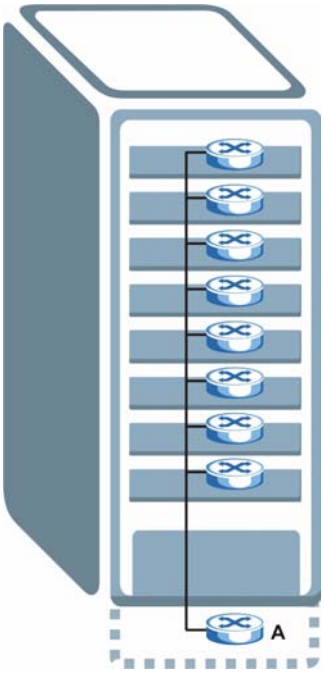
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 62 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 92 Clustering Application Example

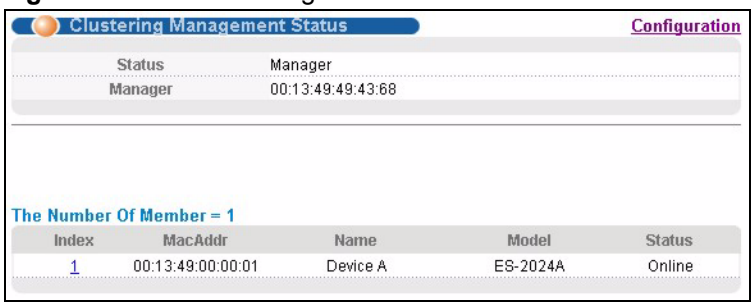


26.2 Cluster Management Status

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

Note: A cluster can only have one manager.

Figure 93 Cluster Management: Status



The following table describes the labels in this screen.

Table 63 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 94 on page 172).
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)

26.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then click on 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 94 Cluster Management: Cluster Member Web Configurator Screen

26.2.1.1 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 95 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         1459070 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group           49152 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-13-49-00-00-01
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-13-49-00-00-01
226 File sent OK
ftp: 297 bytes received in 0.01Seconds 19.80Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 370tx1.bin fw-00-13-49-00-00-01
200 Port command okay
150 Opening data connection for STOR fw-00-13-49-00-00-01
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 64 FTP Upload to Cluster Member Example

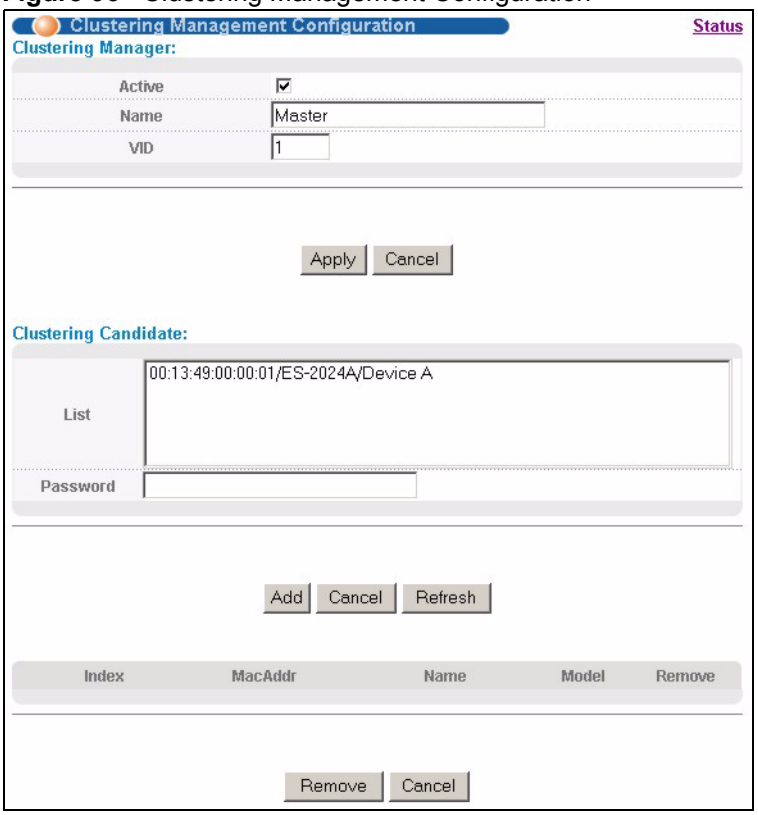
FTP PARAMETER	DESCRIPTION
`User`	Enter "admin".
`Password`	The web configurator password default is 1234.
`ls`	Enter this command to list the name of cluster member switch's firmware and configuration file.
`370tx1.bin`	This is the name of the firmware file you want to upload to the cluster member switch.
`fw-00-13-49-00-00-01`	This is the cluster member switch's firmware name as seen in the cluster manager switch.
`config-00-13-49-00-00-01`	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

26.3 Configuring Cluster Management

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

Refer to Section 26.1 on page 170 for more information.

Figure 96 Clustering Management Configuration



The following table describes the labels in this screen.

Table 65 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 32 printable characters (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 your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this part of the screen afresh.

Table 65 Clustering Management Configuration (continued)

LABEL	DESCRIPTION
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save this part of the screen to the switch. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
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.
MacAddr	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 27
MAC Table

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

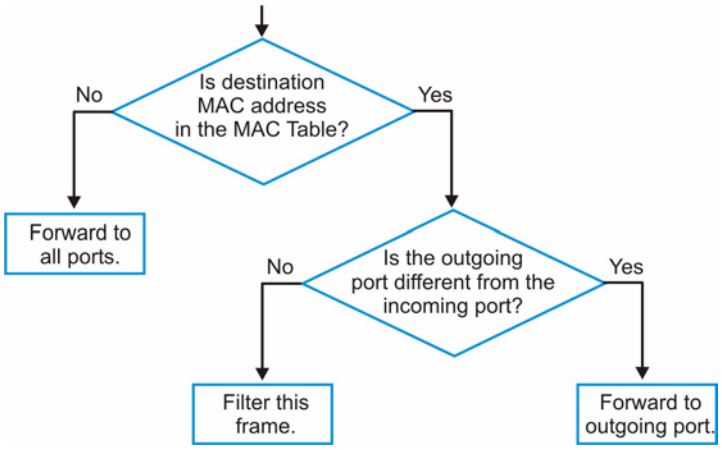
27.1 MAC Table Overview

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 97 MAC Table Flowchart

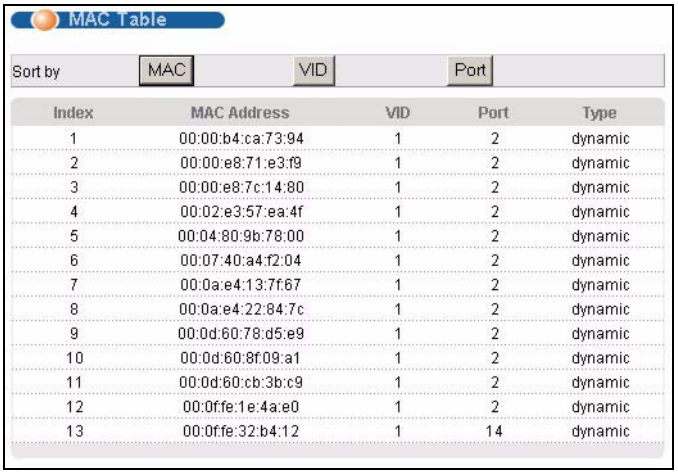


27.2 Viewing the MAC Table

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

Note: Click **MAC**, **VID** or **Port** in the **Sort by** field to display the MAC address entries.

Figure 98 MAC Table



The following table describes the labels in this screen.

Table 66 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 28
ARP Table

This chapter introduces ARP Table.

28.1 ARP Table 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.

28.1.1 How ARP Works

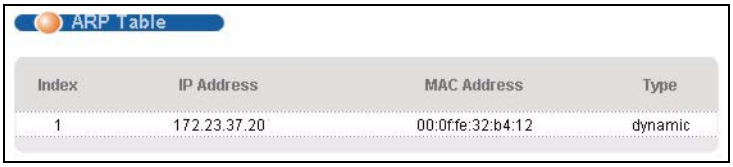
When an incoming packet destined for a host device on a local area network arrives at the switch, the switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

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.

28.2 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 99 ARP Table



The following table describes the labels in this screen.

Table 67 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).

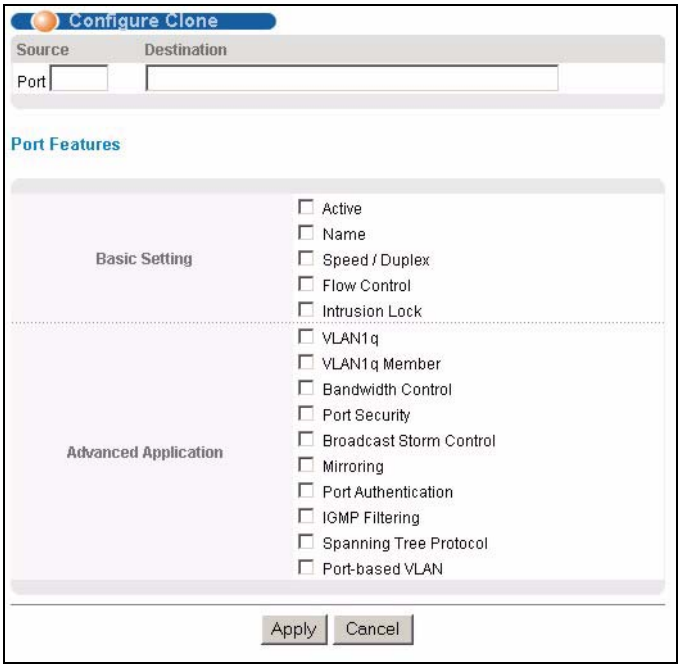
CHAPTER 29
Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

29.1 Clone a Port

Cloning allows you to copy the basic and advanced settings from a source port to one or more destination ports. Click **Management**, **Configure Clone** to open the following screen.

Figure 100 Configure Clone



The following table describes the labels in this screen.

Table 68 Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: • 2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports. • 2-6 indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (you configured in the **Basic Setting** screens) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the **Advanced Application** screens) should be copied to the destination ports.
Apply	Click **Apply** to save your changes to the switch's run-time memory. The switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields.

CHAPTER 30
Introducing the Commands

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

30.1 Overview

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

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

30.2 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.

30.2.1 Multiple Login

You can use a direct console connection or Telnet to access the command interpreter 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.

- By default, the multi-login feature is enabled to allow multiple CLI management sessions.
- 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. To disable this feature, use the `configure no multi-login` command.

30.2.2 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

30.2.2.1 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.

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
initialize switch, ethernet address: 00:13:49:00:00:01
Initializing VLAN Database...
Initializing IP Interface...
Initializing Advanced Applications...
Initializing Command Line Interface...
Initializing Web Interface...
Press ENTER to continue...
```

30.2.3 Telnet

Use the following steps to telnet into your switch.

1. 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**.
2. A login screen displays.

30.2.4 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.

```
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.
sysname>
```

30.3 The Login Screen

After you have successfully established a connection to the switch using a direct console connection or telnet, a login screen displays. The following shows the login prompt on the console port.

For your first login, enter the default administrator login username "admin" and password "1234".

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

30.4 Command Syntax Conventions

The rules of the commands are listed next.

- The command keywords are in `courier new` font.
- The required fields in a command are enclosed in angle brackets <>, for instance, `ping <ip>` means that you must specify an IP number for this command.

- The optional fields in a command are enclosed in square brackets `[]`, for instance,

  ```
  configure snmp-server [contact <system contact>] [location
  <system location>]
  ```

  means that the `contact` and `location` fields are optional.
- "Command" refers to a command used in the command line interface (CI command).
- The `|` symbol means "or".
- The entry `<cr>` in the command lines refers to carriage return. Press [ENTER] or carriage return after a command to execute the command.
- Use the up (↑) or down (↓) arrow key to scroll through the command history list.
- The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the switch automatically display the full command. For example, if you enter "`config`" and press [TAB], the full command of "`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.

30.5 Changing the Password

This command is used to change the password for Enable mode. By default the same password is used to enter the command line interface (CLI) and Enable and Config modes of the CLI.

The password you change with this command is required to enter Enable and Config modes of the CLI.

Syntax:

```
password <password>
```

where

`<password>`	=	Specifies the new password (up to 32 alphanumeric characters) users have to type in to enter Enable and Config modes.

30.6 Account Privilege Levels

You can use a command whose privilege level is equal to or less than that of your login account. For example, if your login account has a privilege level of 12, you can use all commands with privilege levels from 0 to 12. 0-privileged commands are available to all login accounts.

Note: If you use an external RADIUS server to authenticate users, you can use a VSA (Vendor Specific Attribute) to configure a privilege level for an account on the RADIUS server. See Section 16.1.1.1 on page 112 for more information.

30.7 Command Modes

There are three command modes: User, Enable and Configure. The modes (and commands) available to you depend on what level of privilege your account has. Use the `logins username` command in Configure mode to set up accounts and privilege levels.

When you first log into the command interpreter with a read-only account (having a privilege of 0 to 12), the initial mode is 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 using a read-only account, type `enable` and enter the administrator password when prompted (the default is 1234). When you enter Enable mode, the command prompt changes to the pound sign (#). If you log into the command interpreter as an administrator you automatically enter Enable mode.

The following table describes command interpreter modes and how to access them..

Table 69 Command Interpreter Mode Summary

MODE	.DESCRIPTION	HOW TO LOGIN/ ACCESS	PROMPT
User	Commands available in this mode are a subset of enable mode. You can perform basic tests and display general system information.	Default login level for a read-only account.	`sysname>` The first part of the prompt is the system name. In the CLI examples in this User's Guide, the system name is always "sysname".
Enable	Commands available in this mode allow you to save configuration settings, reset configuration settings as well as display further system information. This mode also contains the `configure` command which takes you to config mode.	Default login level for the administrator or accounts with a privilege of 13 or 14. Read-only accounts (with a privilege of 0 - 12) need to type the `enable` command and enter the Enable mode password.	`sysname#`
Config	Commands available in this mode allow you to configure settings that affect the switch globally.	Type `config` or `configure` in Enable mode.	`sysname(config)#`
Command modes that follow are sub-modes of the config mode and can only be accessed from within the config mode.			

Table 69 Command Interpreter Mode Summary (continued)

MODE	.DESCRIPTION	HOW TO LOGIN/ ACCESS	PROMPT
Config-vlan	This is a sub-mode of the config mode and allows you to configure VLAN settings.	Type `vlan` followed by a number (between 1 and 4094). For example, `vlan 10` to configure settings for VLAN 10.	`sysname(config-vlan)#`
Config-interface	This is a sub-mode of the config mode and allows you to configure port related settings.	Type `interface port-channel` followed by a port number. For example, `interface port-channel 10` to configure port 10 on the switch.	`sysname(config-interface)#`
Config-mvr	This is a sub-mode of the config mode and allows you to configure multicast VLAN settings.	To enter `MVR` mode, enter `mvr` followed by a VLAN ID (between 1 and 4094). For example, enter `mvr 2` to configure multicast settings on VLAN 2.	`sysname(config-mvr)#`

Enter `exit` to quit from the current mode or enter `logout` to exit the command interpreter.

30.8 Getting Help

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

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

30.8.1 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.

```
sysname> 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>
sysname>
```

```
sysname> ?
    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
sysname>
```

30.8.2 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.

```
sysname> ping help
  Commands available:
  ping <ip|host-name>
    <
      [ vlan <vlan-id> ]
      [ size <0-1472> ]
      [ -t ]
    >
sysname>
```

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

30.9 Using Command History

The switch keeps a list of 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.

```
sysname> history
  enable
  exit
  show ip
  history
sysname>
```

30.10 Saving Your Configuration

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

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.

```
sysname# write memory
```

30.10.1 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.

30.10.2 Logging Out

In User or Enable mode, enter the `exit` or `logout` command to log out of the CLI. In Config mode entering `exit` takes you out of the Config mode and into Enable mode and entering `logout` logs you out of the CLI.

30.11 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 alphabetical order. See the related section in the User's Guide for more background information.

30.11.1 User Mode

The following table describes the commands available for User mode.

Table 70 Command Summary: User Mode

COMMAND		DESCRIPTION	PRIVILEGE
`enable`		Accesses Enable (or privileged) mode. See Section 30.11.2 on page 191.	0
`exit`		Logs out from the CLI.	0
`help`		Displays help information.	0
`history`		Displays a list of previously command(s) that you have executed. The switch stores up to 256 commands in history.	0
`logout`		Exits from the CLI.	0
`ping`	`<ip|host-name>`	Sends Ping request to an Ethernet device.	0
	`<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.	0
	`help`	Displays command help information.	0
`show`	`ip`	Displays IP related information.	0
	`system-information`	Displays general system information.	0
`ssh`	`<1|2> <[user@]dest-ip>`	Connects to an SSH server with the specified SSH version.	0
`traceroute`	`<ip|host-name>`	Determines the path a packet takes to a device.	0

Table 70 Command Summary: User Mode (continued)

COMMAND		DESCRIPTION	PRIVILEGE
	`<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.	0
	`help`	Displays command help information.	0

30.11.2 Enable Mode

The following table describes the commands available for Enable mode.

Table 71 Command Summary: Enable Mode

COMMAND			DESCRIPTION	PRIVILEGE
`baudrate`	`<1|2|3|4|5>`		Changes the console port speed. Choices are 1 (9600), 2 (19200), 3(38400), 4 (57600) and 5 (115200).	13
`boot`	`config`		Restarts the system.	13
`cable-diagnostics`	`<port-list>`		Performs a basic connectivity test on the ports. Displays "Ok" if connector is inserted in the port, "Open" if no connector is inserted in the port or "Unknown" if this test cannot determine the status.	13
`configure`			Accesses Configuration mode. See Section 30.11.3 on page 196.	13
`copy`	`running-config`	`help`	Displays command help information.	13
		`interface port-channel <port-list>[bandwidth-limit ....]`	Copies the specified attributes from one port to other ports.	13
		`tftp <ip> <remote-file>`	Backs up running configuration to the specified TFTP server with the specified file name.	13
	`tftp`	`config <index> <ip> <remote-file>`	Restores configuration with the specified filename from the specified TFTP server.	13
		`flash <ip> <remote-file>`	Restores firmware via TFTP.	13
`disable`			Exits Enable (or privileged) mode.	13
`enable`			Accesses Enable (or privileged) mode.	13
`erase`	`running-config`	`help`	Displays command help information.	13

Table 71 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		interface [port-channel <port-list> [bandwidth-limit...]]	Resets to the factory default settings. You can reset sfeature ettings on a port.	13
exit			Exits Enable (or privileged) mode.	13
help			Displays help information.	13
history			Displays a list of command(s) that you have previously executed.	13
igmp-flush			Removes all IGMP information.	13
kick	tcp <Session ID>		Resets a TCP connection. Use the show ip tcp command to get the Session ID.	13
logout			Exits Enable (or privileged) mode.	13
mac-flush			Clears the MAC address table.	13
	<port-num>		Removes all learned MAC address on the specified port(s).	13
no	arp		Clears the ARP table.	13
	interface	<port-number>	Clears interface statistics.	13
	logging		Clears system logs.	13
ping	<ip|host-name>		Sends Ping request to an Ethernet device.	13
		[vlan <vlan-id>][size <0-1472>] [-t]	Sends Ping request to an Ethernet device in the specified VLAN(s).	13
	help		Displays command help information.	13
reload	config		Restarts the system.	13
show	cluster		Displays cluster management status.	13
		candidates	Displays cluster candidate information.	13
		member	Displays the MAC address of the cluster member(s).	13
		member config	Displays the configuration of the cluster member(s).	13
		member mac <mac-addr>	Displays the status of the cluster member(s).	13
	diffserv		Displays general DiffServ settings.	13
	garp		Displays GARP information.	13
	https		Displays the HTTPS information.	13
		certificate	Displays the HTTPS certificates.	13
		key <rsa|dsa>	Displays the HTTPS key.	13

Table 71 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`session`	Displays current HTTPS session(s).	13
		`timeout`	Displays the HTTPS session timeout.	13
	`igmp-filtering`	`profile`	Displays IGMP filter profile settings.	13
	`igmp-snooping`		Dispalys IGMP snooping setting.	13
	`interfaces`	`<port-list>`	Displays current interface status.	13
		`config <port-list>`	Displays current interface configuration.	13
		`bandwidth-control`	Displays bandwidth control settings.	13
		`bstorm-control`	Displays broadcast storm control settings.	13
		`egress`	Displays outgoing port information.	13
		`igmp-filtering`	Displays IGMP filter profile settings on the port(s).	13
		`igmp-group-limited`	Displays IGMP group settings on the port(s).	13
		`igmp-immediate-leave`	Displays IGMP immediate leave settings on the port(s).	13
		`igmp-query-mode`	Displays IGMP query mode settings on the port(s).	13
	`ip`		Displays IP related information.	13
		`arp`	Displays the ARP table.	13
		`route`	Displays IP routing information.	13
		`route static`	Displays IP static route information.	13
		`tcp`	Displays TCP related information.	13
		`udp`	Displays UDP related information.	13
	`lacp`		Displays LACP (Link Aggregation Control Protocol) settings.	13
	`logging`		Displays system logs.	13
	`loginPrecedence`		Displays login precedence settings.	13
	`logins`		Displays login account information.	13
	`mac`	`address-table all <sort>`	Displays MAC address table. You can sort by MAC address, VID or port. `sort` = `mac`, `vid` or `port`	13
		`address-table count`	Displays the number of static MAC address tables.	13

Table 71 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		address-table static	Displays static MAC address table.	13
	mac-aging-time		Displays MAC learning aging time.	13
	multicast		Displays multicast settings.	13
	multi-login		Displays multi-login information	13
	mvr		DIsplays all MVR (Multicast VLAN Registration) settings.	13
		<vlan-id>	DIsplays specified MVR information.	13
	plt		DIsplays PLT (Port Loopback Test) information.	13
	port-access-authenticator		Displays all port authentication settings.	13
		<port-list>	Displays port authentication settings on the specified port(s).	13
	port-security		Displays all port security settings.	13
		<port-list>	Displays port security settings on the specified port(s).	13
	pwr		Displays PoE (Power over Ethernet) settings on the switch. Only available on models with the PoE feature.	13
	radius-server		Displays RADIUS server settings.	13
	remote-management		Displays all secured client information.	13
		<index>	Displays the specified secured client information.	13
	running-config		Displays current operating configuration.	13
		help	Displays detailed information and parameters for this command.	13
		interface port-channel <port-list> [bandwidth-limit ...]	Displays current operating configuration on a port by port basis. Optionally specifies which settings are displayed.	13
	service-control		Displays service control settings.	13
	snmp-server		Displays SNMP settings.	13
	spanning-tree	config	Displays Spanning Tree Protocol (STP) settings.	13
	ssh		Displays general SSH settings.	13
		key <rsa1|rsa|dsa>	Displays internal SSH public and private key information.	13

Table 71 Command Summary: Enable Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		known-hosts	Displays known SSH hosts information.	13
		session	Displays current SSH session(s).	13
	system-information		Displays general system information.	13
	time		Displays current system time and date.	13
	timesync		Displays time server information.	13
	trunk		Displays link aggregation information.	13
	vlan		Displays the status of all VLANs.	13
		<vlan-id>	Displays the status of the specified VLAN.	13
	vlan1q	gvrp	Displays GVRP settings.	13
		ingress-check	Displays the ingress check setting.	13
		port-isolation	Displays port isolation settings.	13
ssh	<1|2> <[user@]dest-ip>		Connects to an SSH server with the specified SSH version.	13
		[command </>]	Connects to an SSH server with the specified SSH version and addition commands to be executed on the server.	13
traceroute	<ip|host-name> [vlan <vlan-id>][ttl <1-255>] [wait <1-60>] [queries <1-10>]		Determines the path a packet takes to a device.	13
	help		Displays command help information.	13
write	memory		Saves current configuration to the configuration file the switch is currently using.	13

30.11.3 General Configuration Mode

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

Table 72 Command Summary: Configuration Mode

COMMAND			DESCRIPTION	PRIVILEGE
admin-password	<pw-string> <confirm-string>		Changes the administrator password.	14
bandwidth-control			Enables bandwidth control.	13
cluster	<vlan-id>		Sets the cluster management VLAN ID.	13
	member <mac-address>	password <password-str>	Sets the cluster member switch's hardware MAC address and password.	13
	name <cluster name>		Configures a name to identify the cluster manager.	13
	rcommand <mac-address>		Logs into a cluster member switch.	13
diffserv			Enables DiffServ.	13
	dscp <0-63> priority <0-7>		Sets the DSCP-to-IEEE 802.1p mappings.	13
exit			Exits from the CLI.	13
garp	join <100-65535> leave <msec> leaveall <msec>		Configures GARP time settings.	13
help			Displays help information.	13
history			Displays a list of previous command(s) that you have executed.	13
hostname	<name_string>		Sets the switch's name for identification purposes. **Note:** Spaces are allowed in the CLI only when the system name is in "quotation marks". For example, "Device A"	13
https	cert-regeneration <rsa|dsa>		Re-generates a certificate.	13
	timeout <0-65535>		Sets the HTTPS timeout period.	13
igmp-filtering			Enables IGMP filtering on the switch.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`profile <name> start-address <ip> end-address <ip>`		Sets the range of multicast address(es) in a profile.	13
`igmp-snooping`			Enables IGMP snooping.	13
	`8021p-priority <0-7>`		Sets a priority level (0-7) to which the switch changes the priority in outgoing IGMP control packets.	13
	`host-timeout <1 - 16711450>`		Sets the host timeout value.	13
	`leave-timeout <1 - 16711450>`		Sets the leave timeout value	13
	`unknown-multicast-frame <drop|flooding>`		Sets how to treat traffic from unknown multicast group.	13
`interface`	`port-channel <port-list>`		Enables a port or a list of ports for configuration. See Section 30.11.4 on page 205 for more details.	13
`ip`	`name-server`	`<ip>`	Sets the IP address of a domain name server.	13
	`route`	`<ip> <mask> <next-hop-ip>`	Creates a static route.	13
		`<ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive]`	Sets the metric of a static route or deactivates a static route.	13
`lacp`			Enables Link Aggregation Control Protocol (LACP).	13
	`system-priority`	`<1-65535>`	Sets the priority of an active port using LACP.	13
`loginPrecedence`	`<LocalOnly | LocalRADIUS | RADIUSOnly>`		Select which database the switch should use (first) to authenticate a user.	14
`logins`	`username <name>`	`password <pwd>`	Configures up to four login accounts.	14
		`privilege <0-14>`	Sets the access privilege for the existing login accounts. The higher the value, the more commands are allowed.	14
`logout`			Exits from the CLI.	13
`mac-aging-time`	`<10-3000>`		Sets learned MAC aging time.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
mac-filter	name <name> mac <mac-addr> vlan <vlan-id>		Configures a static MAC address port filtering rule.	13
		inactive	Disables a static MAC address port filtering rule.	13
mac-forward	name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>		Configures a static MAC address forwarding rule.	13
		inactive	Disables a static MAC address forwarding rule.	13
mirror-filter	egress	mac <mac-addr>	Sets port mirroring for the MAC address on the outgoing traffic.	13
		type <all|dest|src>	Sets the direction of the outgoing traffic for port mirroring.	13
	ingress	mac <mac-addr>	Sets port mirroring for the MAC address on the incoming traffic.	13
		type <all|dest|src>	Sets the direction of the incoming traffic for port mirroring.	13
mirror-port			Enables port mirroring.	13
	<port-num>		Sets the monitor port.	13
mode	zynos		Changes the CLI mode to the ZyNOS format.	13
multi-login			Enables multi-login.	14
mvr <vlan-id>			Enters the MVR (Multicast VLAN Registration) configuration mode. See Section 30.11.5 on page 208 for more information.	13
no	bandwidth-control		Disable bandwidth control on the switch.	13
	cluster		Disables cluster management on the switch.	13
	cluster member	<mac-address>	Removes the cluster member.	13
	diffserv		Disables the DiffServ settings.	13
	https	timeout	Resets the session timeout to the default of 300 seconds.	13
	igmp-filtering			13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`profile <name> start-address <ip> end-address <ip>`	Deletes a rule in the IGMP filtering profile.	13
	`igmp-snooping`		Disables IGMP snooping.	13
	`ip`		Sets the management IP address to the default value.	13
		`route <ip> <mask>`	Removes a specified IP static route.	13
		`route <ip> <mask> inactive`	Enables a specified IP static route.	13
	`lacp`		Disables the link aggregation control protocol (dynamic trunking) on the switch.	13
	`logins`	`username <name>`	Disables login access to the specified name.	14
	`mac-filter`	`mac <mac-addr> vlan <vlan-id>`	Disables the specified MAC filter rule.	13
		`mac <mac-addr> vlan <vlan-id> inactive`	Enables the specified MAC-filter rule.	13
	`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).	13
		`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).	13
	`mirror-port`		Disables port mirroring on the switch.	13
	`multi-login`		Disables another administrator from logging into Telnet.	14
	`mvr <vlan-id>`		Disables MVR on the switch.	13
	`port-access-authenticator`		Disables port authentication on the switch.	13
		`<port-list>`	Disables authentication on the listed ports.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		<port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).	13
	port-security		Disables port security on the switch.	13
		<port-list>	Disables port security on the specified ports.	13
		<port-list> learn inactive	Enables MAC address learning on the specified ports.	13
	pwr	interface <port-list>	Disable PoE on the specified ports. Only available on models with the PoE feature.	13
		mibtrap	Disables MIB traps.	13
	radius-server	<index>	Disables the use of authentication from the specified RADIUS server.	13
	remote-management	<index>	Clears a secure client set entry from the list of secure clients.	13
		<index> service <[telnet][ftp] [http][icmp] [snmp][ssh][https]>	Disables a secure client set entry number from using the selected remote management service(s).	13
	service-control	ftp	Disables FTP access to the switch.	13
		http	Disables web browser control to the switch.	13
		https	Disables secure web browser access to the switch.	13
		icmp	Disables ICMP access to the switch such as pinging and tracerouting.	13
		snmp	Disables SNMP management.	13
		ssh	Disables SSH (Secure Shell) server access to the switch.	13
		telnet	Disables telnet access to the switch.	13
	snmp-server	trap-destination <ip>	Disables sending of SNMP traps to a station.	13
	spanning-tree		Disables STP.	13
		<port-list>	Disables STP on listed ports.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	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.	13
		known-hosts <host-ip>	Removes the specified remote hosts from the list of all known hosts.	13
		known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]	Removes remote known hosts with the specified public key (1024-bit RSA1, RSA or DSA).	13
	storm-control		Disables broadcast storm control.	13
	timesync		Disables timeserver settings.	13
	trunk	<T1|T2|T3>	Disables the specified trunk group.	13
		<T1|T2|T3> interface <port-list>	Removes ports from the specified trunk group.	13
		<T1|T2|T3> lacp	Disables LACP in the specified trunk group.	13
	vlan <vlan-id>		Deletes the static VLAN entry.	13
	vlan1q	gvrp	Disables GVRP on the switch.	13
		ingress-check	Disables VLAN tag checking on incoming traffic.	13
		port-isolation	Disables port isolation.	13
password			Change the password for Enable mode.	14
port-access-authenticator			Enables 802.1x authentication on the switch.	13
	<port-list>		Enables 802.1x authentication on the specified port(s).	13
		reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	13
		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).	13
port-security			Enables port security on the switch.	13
	<port-list>		Enables the port security feature on the specified port(s).	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		`learn inactive`	Disables MAC address learning on the specified port(s).	13
		`address-limit <number>`	Limits the number of (dynamic) MAC addresses that may be learned on a port.	13
		`MAC-freeze`	Disables MAC address learning and enables port security. **Note:** All previously learned dynamic MAC addresses are saved to the static MAC address table.	13
`pwr`	`interface <port-list>`		Enables PoE (Power over Ethernet) on the specified port(s). Only available on models with the PoE feature.	13
		`priority <critical|high|low>`	Sets the PD priority on a port to allow the swtich to allocate power to higher priority ports when the remaining power is less than the consumed power. `criticl` > `high` >`low`	13
	`mibtrap`		Enables MIB traps on the switch. Traps are initiated when the usage reaches the limit set by the `pwr usagethreshold` command.	13
	`usagethreshold <1-99>`		Sets the percentage of power usage which initiates MIB traps.	13
`queue`	`priority <0-7> level <0-3>`		Sets the priority level-to-physical queue mapping.	13
`radius-server`	`host <index> <ip>`		Specifies the IP address of RADIUS server 1 or RADIUS server 2 (index =1 or index =2).	13
		`[auth-port <socket-number>] [key <key-string>]`	Sets the port number and key of the external RADIUS server.	13
	`mode <priority|round-robin>`		Specifies the mode for RADIUS server selection.	13
	`timeout <1-1000>`		Specifies the RADIUS server timeout value.	13
`remote-management`	`<index>`		Enables a specified secured client set.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		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.	13
service-control	ftp <socket-number>		Allows FTP access on the specified service port.	13
	http <socket-number> <timeout>		Allows HTTP access on the specified service port and defines the timeout period.	13
	https <socket-number>		Allows HTTPS access on the specified service port.	13
	icmp		Allows ICMP access for services such as Ping.	13
	snmp		Allows SNMP management.	13
	ssh <socket-number>		Allows SSH access on the specified service port.	13
	telnet <socket-number>		Allows Telnet access on the specified service port.	13
snmp-server	[contact <system contact>] [location <system location>]		Sets the geographic location and the name of the person in charge of this switch.	13
	get-community <property>		Sets the get community.	13
	set-community <property>		Sets the set community.	13
	trap-community <property>		Sets the trap community.	13
	trap-destination <ip>		Sets the IP addresses of up to four stations to send your SNMP traps to.	13
spanning-tree			Enables STP on the switch.	13
	<port-list>		Enables STP on a specified port.	13
		path-cost <1-65535>	Sets the STP path cost for a specified port.	13
		priority <0-255>	Sets the priority for a specified port.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	hello-time <1-10> maximum-age <6-40> forward-delay <4-30>		Sets Hello Time, Maximum Age and Forward Delay.	13
	help		Displays help information.	13
	priority <0-61440>		Sets the bridge priority of the switch.	13
spq			Sets the switch to use Strictly Priority Queuing (SPQ).	13
ssh	known-hosts <host-ip> <1024|ssh-rsa|ssh-dsa> <key>		Adds a remote host to which the switch can access using SSH service.	13
storm-control			Enables broadcast storm control on the switch.	13
syslog			Enables syslog logging on the switch.	13
	server <ip-address>		Enables syslog logging to the specified syslog server	13
		inactive	Disables syslog logging to the specified syslog server.	13
		level <level>	Sets the severity level.	13
	type <type> facility <0-7>		Sets the log type and file location on the syslog server. type = system, interface, switch, authentication or ip	13
time	<Hour:Min:Sec>		Sets the time in hour, minute and second format.	13
	date <month/day/year>		Sets the date in year, month and day format.	13
	help		Displays help information.	13
	timezone <-1200|...|1200>		Selects the time difference between UTC (formerly known as GMT) and your time zone.	13
timesync	<daytime|time|ntp>		Sets the time server protocol.	13
	server <ip>		Sets the IP address of your time server.	13
trunk	<T1|T2|T3>		Activates a trunk group.	13
	<T1|T2|T3>interface <port-list>		Adds a port(s) to the specified trunk group.	13
	<T1|T2|T3>lacp		Enables LACP for a trunk group.	13

Table 72 Command Summary: Configuration Mode (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`interface <port-list> timeout <lacp-timeout>`		Defines the port number and LACP timeout period.	13
`vlan`	`<1-4094>`		Enters the VLAN configuration mode. See Section 30.11.6 on page 209 for more information.	13
`vlan-type`	`<802.1q|port-based>`		Specifies the VLAN type.	13
`vlan1q`	`gvrp`		Enables GVRP.	13
	`ingress-check`		Enables VLAN tag checking on incoming traffic.	13
	`port-isolation`		Enables port-isolation.	13
`wrr`			Sets the switch to use Weighted Round Robin queuing (WRR).	13
	`<wt1><wt2> ... <wt4>`		Sets the WRR weight. A weight value of one to eight is given to each variable from `wt1` to `wt4`.	13

30.11.4 interface port-channel Commands

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

Table 73 interface port-channel Commands

COMMAND			DESCRIPTION	PRIVILEGE
`interface port-channel <port-list>`			Enables a port or a list of ports for configuration.	13
	`bandwidth-limit`	`egress`	Enables bandwidth control on for outgoing traffic on he port(s).	13
		`egress <Kbps>`	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).	13
		`ingress`	Enables bandwidth control on for incoming traffic on he port(s).	13
		`ingress <Kbps>`	Sets the maximum bandwidth allowed for incoming traffic on the port(s).	13
	`bmstorm-limit`		Enables broadcast storm control on the port.	13
		`<Kpbs>`	Sets the limit of broadcast storm packets in kilobit per second (Kbps).	13
	`diffserv`		Enables DiffServ on the port(s).	13

Table 73 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	`egress set <port-list>`		Sets the outgoing traffic port list for a port-based VLAN.	13
	`exit`		Exits from the interface port-channel command mode.	13
	`flow-control`		Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	13
	`frame-type <all|tagged>`		Choose to accept both tagged and untagged incoming frames or just tagged incoming frames on a port.	13
	`gvrp`		Enables this function to permit VLAN groups beyond the local switch.	13
	`help`		Displays a description of the interface port-channel commands.	13
	`igmp-filtering profile <name>`		Sets the IGMP filtering profile for this port.	13
	`igmp-group-limited`		Limits the number of multicast groups.	13
		`number <number>`	Sets the number of multicast groups this port is allowed to join.	13
	`igmp-immediate-leave`		Enables IGMP immediate leave on the port.	13
	`igmp-querier-mode <auto|fixed|edge>`		Sets the IGMP querier mode of a port. Selects `auto` to treat the IGMP queries normally, `fixed` to always treat the port as a querier port no matter there is a query or `edge` to treat the port as a non-querier port which drops any IGMP queries received.	13
	`inactive`		Disables the specified port(s) on the switch.	13
	`intrusion-lock`		Enables intrusion lock on a port and a port cannot be connected again after you disconnected the cable.	13
	`mirror`		Enables port mirroring in the interface.	13

Table 73 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		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.	13
	name <port-name-string>		Sets a name for the port(s). Enter a descriptive name (up to nine printable ASCII characters).	13
	no	bandwidth-limit egress	Disables bandwidth limit for outgoing traffic.	13
		bandwidth-limit ingress	Disables bandwidth limit for incoming traffic.	13
		bmstorm-limit	Disables broadcast storm control limit on the port(s).	13
		diffserv	Disables DiffServ on the port(s).	13
		egress set <port-list>	Sets the outgoing traffic port list for a port-based VLAN.	13
		flow-control	Disables flow control on the port(s).	13
		gvrp	Disable GVRP on the port(s).	13
		igmp-filtering profile	Disables IGMP filtering on the port.	13
		igmp-group-limited	Disables IGMP group limitation.	13
		igmp-immediate-leave	Disables IGMP immediate leave on the port.	13
		inactive	Enables the port(s) on the switch.	13
		intrusion-lock	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	13
		mirror	Disables port mirroring on the port(s).	13
		vlan-trunking	Disables VLAN trunking on the port(s).	13
	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.	13
	qos priority <0 .. 7>		Sets the quality of service priority for an interface.	13

Table 73 interface port-channel Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
	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.	13
	test		Performs an interface loopback test.	13
	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.	13

30.11.5 mvr Commands

The following table lists the mvr commands in Configure mode.

Table 74 mvr Commands

COMMAND			DESCRIPTION	PRIVILEGE
mvr <1-4094>			Enters the MVR (Multicast VLAN Registration) configuration mode.	13
	8021p-priority <0 - 7>		Sets a priority level (0-7) to which the switch changes the priority in outgoing IGMP control packets.	13
	exit		Exist from the MVR configuration mode.	13
	group <name-str> start-address <ip> end-address <ip>		Sets the multicast group range for the MVR.	13
	inactive		Disables MVR settings.	13
	mode <dynamic|compatible>		Sets the MVR mode (dynamic or compatible).	13
	name <name-str>		Sets the MVR name for identification purposes.	13
	no	group	Disables all MVR group settings.	13

Table 74 mvr Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		group <name-str>	Disables the specified MVR group setting.	13
		inactive	Enables MVR.	13
		receiver-port <port-list>	Disables the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
		source-port <port-list>	Disables the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
		tagged <port-list>	Sets the port(s) to untag VLAN tags.	13
	receiver-port <port-list>		Sets the receiver port(s). An MVR receiver port can only receive multicast traffic in a multicast VLAN.	13
	source-port <port-list>		Sets the source port(s). An MVR source port can send and receive multicast traffic in a multicast VLAN.	13
	tagged <port-list>		Sets the port(s) to tag VLAN tags.	13

30.11.6 config-vlan Commands

The following table lists the `vlan` commands in Configure mode.

Table 75 Command Summary: config-vlan Commands

COMMAND			DESCRIPTION	PRIVILEGE
vlan <1-4094>			Creates a new VLAN group.	13
	exit		Leaves the VLAN configuration mode.	13
	fixed <port-list>		Specifies the port(s) to be a permanent member of this VLAN group.	13
	forbidden <port-list>		Specifies the port(s) you want to prohibit from joining this VLAN group.	13
	help		Displays a list of available VLAN commands.	13
	inactive		Disables the specified VLAN.	13
	ip address	<ip-address> <mask>	Sets the IP address and subnet mask of the switch in the specified VLAN.	13

Table 75 Command Summary: config-vlan Commands (continued)

COMMAND			DESCRIPTION	PRIVILEGE
		<ip-address> <mask> [manageable]	Sets the management IP address and subnet mask of the switch in the specified VLAN.	13
		default-gateway <ip-address>	Sets a default gateway IP address for this VLAN.	13
		default-management dhcp-bootp	Sets the dynamic in-band IP address	13
		default-management <ip-address> <mask>	Sets a static in-band IP address and subnet mask.	13
		default-management dhcp-bootp release	Releases the dynamic in-band IP address.	13
		default-management dhcp-bootp renew	Updates the dynamic in-band IP address.	13
	name <name-str>		Specifies a name for identification purposes.	13
	no	fixed <port-list>	Sets fixed port(s) to normal port(s).	13
		forbidden <port-list>	Sets forbidden port(s) to normal port(s).	13
		inactive	Enables the specified VLAN.	13
		ip address <ip-address> <mask>	Deletes the IP address and subnet mask from this VLAN.	13
		ip address default-gateway	Deletes the default gateway from this VLAN.	13
		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.	13
		untagged <port-list>	Enables VLAN tagging for outgoing traffic on the specified port(s).	13
	normal <port-list>		Specifies the port(s) to dynamically join this VLAN group using GVRP	13
	untagged <port-list>		Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.	13

CHAPTER 31
Command Examples

This chapter describes some commands in more detail.

31.1 Overview

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

31.2 show Commands

These are the commonly used `show` commands.

31.2.1 show interface

Syntax:

```
show interfaces <port-number>
```

This command displays port statistics of the specified port(s). The following example shows that port 12 is up and the related information.

```
sysname# show interfaces 12
  Port Info     Port NO.                :12
                Link                    :100M/F
                Status                  :FORWARDING
                LACP                    :Disabled
                TxPkts                  :14466
                RxPkts                  :43798
                Errors                  :0
                Tx KBs/s                :0.592
                Rx KBs/s                :1.47
                Up Time                 :16:42:54
  TX Packet     Tx Packets              :14466
                Multicast               :21
                Broadcast               :116
                Pause                   :0
  RX Packet     Rx Packets              :43798
                Multicast               :2923
                Broadcast               :25032
                Pause                   :0
  TX Collison   Single                  :0
                Multiple                :0
                Excessive               :0
                Late                    :0
  Error Packet  RX CRC                  :0
                Runt                    :0
  Distribution  64                      :25535
                65 to 127               :4373
                128 to 255              :3952
                256 to 511              :862
                512 to 1023             :1401
                1024 to 1518            :7675
                Giant                   :0

sysname#
```

31.2.2 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.

```
sysname> show ip
IP Interface
     IP[172.23.37.107], Netmask[255.255.255.0], VID[1]

sysname>
```

31.2.3 show logging

Syntax:

```
show logging
```

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

```
sysname# show logging
   0 Thu Jan 01 00:01:38 1970 PSSV  ERROR Port 2 link up
   1 Thu Jan 01 00:01:38 1970 PSSV -WARN  SNMP TRAP 2: link down
   2 Thu Jan 01 00:01:38 1970 PSSV  ERROR Port 3 link up
   3 Thu Jan 01 00:01:38 1970 PSSV -WARN  SNMP TRAP 2: link down
   4 Thu Jan 01 00:01:38 1970 PSSV  ERROR Port 4 link up
   5 Thu Jan 01 00:01:38 1970 PSSV -WARN  SNMP TRAP 2: link down
   6 Thu Jan 01 00:01:38 1970 PSSV  ERROR Port 5 link up
   7 Thu Jan 01 00:01:38 1970 PSSV -WARN  SNMP TRAP 2: link down
   8 Thu Jan 01 00:01:38 1970 PSSV  ERROR Port 6 link up
   9 Thu Jan 01 00:01:38 1970 PSSV -WARN  SNMP TRAP 2: link down
  10 Thu Jan 01 00:01:38 1970 PSSV  ERROR Port 7 link up
Clear Error Log (y/n):
```

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

31.2.4 show mac address-table all

Syntax:

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

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.

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

31.2.5 show pwr

Syntax:

```
show pwr
```

This command displays the PoE settings on the ports and the PoE status on the device. The following shows an example.

```
ES-2024PWR# show pwr

Averaged Junction Temperature: 33 (c), 91 (f).

Port   State   PD  Class  Priority  Consumption (mW)  MaxPower(mW)
----  ------  ---  -----  --------  ----------------  ------------
   1  Enable  off      0       Low                 0             0
   2  Enable  off      0       Low                 0             0
   3  Enable  off      0       Low                 0             0
   4  Enable  off      0       Low                 0             0
   5  Enable  off      0       Low                 0             0
   5  Enable  off      0       Low                 0             0
   7  Enable  off      0       Low                 0             0
   8  Enable  off      0       Low                 0             0
   9  Enable  off      0       Low                 0             0
  10  Enable  off      0       Low                 0             0
  11  Enable  off      0       Low                 0             0
  12  Enable  off      0       Low                 0             0
  13  Enable  off      0       Low                 0             0
  14  Enable  off      0       Low                 0             0
  15  Enable  off      0       Low                 0             0
  16  Enable  off      0       Low                 0             0
  17  Enable  off      0       Low                 0             0
  18  Enable  off      0       Low                 0             0
  19  Enable  off      0       Low                 0             0
  20  Enable  off      0       Low                 0             0
  21  Enable  off      0       Low                 0             0
  22  Enable  off      0       Low                 0             0
  23  Enable  off      0       Low                 0             0
  24  Enable  off      0       Low                 0             0

Total Power:185.0(W)
Consuming Power:0.0(W)
Allocated Power:0.0(W)
Remaining Power:185.0(W)
ES-2024PWR#
```

31.2.6 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.

```
sysname> show system-information
System Name             : ES-2024A
System Contact          :
System Location         :
Ethernet Address        : 00:13:49:49:43:68
ZyNOS F/W Version       : V3.70(TX.0)b1 | 06/06/2006
RomRasSize              : 1459070
System up Time          :    50:23:02 (114c475 ticks)
Bootbase Version        : V1.07 | 04/20/2005
sysname>
```

31.3 ping

Syntax:

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

where

`<ip|host-name>`	=	The IP address or host name 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`.

```
sysname# 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
sysname#
```

31.4 traceroute

Syntax:

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

where

`<ip|host-name>`	=	The IP address or host name 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`.

```
sysname> 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:
```

31.5 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.

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

31.6 Copy Port Attributes

Use the `copy running-config` command to copy attributes of one port to another port or ports.

Syntax:

```
copy running-config interface port-channel <port> <port-list>
copy running-config interface port-channel <port> <port-list> [active]
[name] [speed-duplex] [flow-control] [intrusion-lock] [vlan1q] [vlan1q-
member] [bandwidth-limit] [port-security] [broadcast-storm-control]
[mirroring] [port-access-authenticator] [queuing-method] [igmp-filtering]
[spanning-tree] [port-based-vlan]
```

where

`copy running-config interface port-channel <port> <port-list>`	=	Copies all of the possible attributes from one port to another port or ports.
`copy running-config interface port-channel <port> <port-list> [active ... ]`	=	Copies only the specified port attributes from one port to another port or ports.

An example is shown next.

- Copy all attributes of port 1 to port 2
- Copy selected attributes (active, bandwidth limit and STP settings) to ports 5-10

```
sysname# copy running-config interface port-channel 1 2
sysname# copy running-config interface port-channel 1 5-10 active
bandwidth-limit spanning-tree
```

31.7 Configuration File Maintenance

The following sections shows how to manage the configuration files.

31.7.1 Resetting to the Factory Default

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

1. Enter `erase running config` to reset the current running configuration.
2. Enter `write memory` to save the changes to the current configuration file.

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

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

CHAPTER 32
Configuration Mode Commands

This chapter describes how to enable and configure your switch's features using commands. For more background information, see the feature specific chapters which proceed the commands chapters.

32.1 Setting Login Accounts

Syntax:

```
logins username <username> password <password>
logins username <username> privilege <0-14>
```

where

`username <username>`	=	Specifies a new user (up to 32 alphanumeric characters). Enter a user name to change the settings of an existing account.
`password <password>`	=	Specifies the new password (up to 32 alphanumeric characters) for this user.
`privilege <0-14>`	=	Assigns a privilege level for the user. Refer to Section 30.6 on page 185 for more information.

Use this command to configure a login account.

The following example creates a new login account with a user name of JohnDoe, a password of 12345678 and a privilege level of 12.

```
sysname# config
sysname(config)# logins username JohnDoe password 12345678
sysname(config)# logins username JohnDoe privilege 12
sysname(config)# exit
sysname# show logins
Login   Username                                  Privilege
1                                  JohnDoe              12
2                                                        0
3                                                        0
4                                                        0
sysname#
```

32.2 Enabling IGMP Snooping

To enable IGMP snooping on the switch. Enter `igmp-snooping` and press [ENTER]. You can also set how to treat traffic from an unknown multicast group by typing the `unknown-multicast-frame` parameter.

Syntax:

```
igmp-snooping
igmp-snooping host-timeout <1-16711450>
igmp-snooping leave-timeout <1-16711450>
igmp-snooping unknown multicast-frame <drop|flooding>
```

where

`igmp-snooping`	=	Enables IGMP snooping on the switch.
`host-timeout <1-16711450>`	=	Specifies the timeout period of the switch with respect to IGMP report queries. If an IGMP report for a multicast group was not received for a host-timeout period, from a specific port, this port is deleted from the member list of that multicast group.
`leave-timeout <1-16711450>`	=	Specifies the time that the switch will wait for multicast members to respond to a leave report. If no response is received in the timeout period, the switch deletes the port from the multicast group.
`unknown multicast-frame <drop|flooding>`	=	Specifies whether you want to discard packets from unknown multicast groups or whether you want to forward them to all ports.

An example is shown next.

- Enable IGMP snooping on the switch.
- Set the `host-timeout` and `leave-timeout` values to 30 seconds
- Set the switch to drop packets from unknown multicast groups.

```
sysname(config)# igmp-snooping
sysname(config)# igmp-snooping host-timeout 30
sysname(config)# igmp-snooping leave-timeout 30
sysname(config)# igmp-snooping unknown-multicast-frame drop
```

32.3 Configuring an IGMP Filter

Use the following commands in the `config` mode to configure IGMP filtering profiles.

Syntax:

```
igmp-filtering
igmp-filtering profile <name> start-address <ip> end-address <ip>
```

where

`igmp filtering`	=	Enables IGMP filtering on the switch
`profile <name>`	=	Specifies a name (up to 32 alphanumeric characters) for this IGMP profile. If you want to edit an existing IGMP profile enter the existing profile name followed by `start-address` and `end-address` parameters.
`start-address <ip>`	=	Specifies the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile. IP address in the range 224.0.0.0 to 239.255.255.255 are used for IP multicasting.
`end-address <ip>`	=	Specifies the ending multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile. IP address in the range 224.0.0.0 to 239.255.255.255 are used for IP multicasting.

An example is shown next.

- Enable IGMP filtering on the switch.
- Create an IGMP filtering profile `filter1` and specify the multicast IP addresses in the range `224.255.255.0` to `225.255.255.255` to belong to this profile.

```
sysname(config)# igmp-filtering
sysname(config)# igmp-filtering profile filter1 start-address 224.255.255.0
end-address 225.255.255.255
```

32.4 Enabling STP

Use the `spanning-tree` or commands to enable and configure STP on the switch.

Syntax:

```
spanning-tree
spanning-tree priority <0-61440>
spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>
spanning-tree <port-list> path-cost <1-65535>
spanning-tree <port-list> priority <0-255>
```

where

`spanning-tree`	=	Enables STP on the switch.
`priority <0-61440>`	=	Specifies the bridge priority for the switch. The lower the numeric value you assign, the higher the priority for this bridge. 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. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
`hello-time <1-10>`	=	Specifies the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
`maximum-age <6-40>`	=	Specifies 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.
`forward-delay <4-30>`	=	Specifies 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.
`path-cost <1-65535>`	=	Specifies the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge.
`priority <0-255>`	=	Specifies the priority for each port. 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.

An example using `spanning-tree` command is shown next.

- Enable STP on the switch.
- Set the bridge priority of the switch to 0.
- Set the Hello Time to 4, Maximum Age to 20 and Forward Delay to 15 on the switch.
- Enable STP on port 10 with a path cost of 150.

- Set the priority for port 10 to 20.

```
sysname(config)# spanning-tree
sysname(config)# spanning-tree priority 0
sysname(config)# spanning-tree hello-time 4 maximum-age 20 forward-delay 15
sysname(config)# spanning-tree 10 path-cost 150
sysname(config)# spanning-tree 10 priority 20
```

32.5 no Command Examples

These are the commonly used command examples that belong to the `no` group of commands. The `no` group commands are commands which are preceded by keyword `no`. This command negates the intended action of the command. In most cases the `no` command disables, resets or clears settings. There are cases, however, where the `no` command can activate features. This section shows some uses of these commands.

32.5.1 Disable Commands

Use the `no` command to disable features on the switch.

Syntax:

```
no spanning-tree
```

This command disables STP on the switch.

32.5.2 Resetting Commands

Use the `no` command to reset switch settings to their default values.

Syntax:

```
no https timeout
```

This command resets the HTTPS session timeout to the default.

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

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

32.5.3 Re-enabling Commands

The no command can also be used to re-enable features which have been disabled.

Syntax:

```
no ip route <ip> <mask> inactive
```

where

`<ip> <mask> inactive`	=	Re-enables an IP route with the specified IP address and subnet mask.

An example is shown next.

- Enable the IP route with the IP address of 192.168.11.1 and subnet mask of 255.255.255.0. This IP route must have already been created and made inactive prior to re-enable command being applied.

```
sysname(config)# no ip route 192.168.11.1 255.255.255.0 inactive
```

32.5.4 Other Examples of no Commands

In some cases the `no` command can disable a feature, disable an option of a feature or disable a feature on a port-by-port basis.

32.5.4.1 no trunk

Syntax:

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

where

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

An example is shown next.

- Disable trunk one (T1).
- Disable LACP on trunk three (T3).
- Remove ports one, three, four and five from trunk two (T2).

```
sysname(config)# no trunk T1
sysname(config)# no trunk T3 lacp
sysname(config)# no trunk T2 interface 1,3-5
```

32.5.4.2 no port-access-authenticator

Syntax:

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

where

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

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.

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

32.5.4.3 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>`	=	Removes a specific remote host from the list of all known hosts.
`known-hosts <host-ip> [1024|ssh-rsa|ssh-dsa]`	=	Removes remote known hosts with a specified public key type (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.

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

32.6 pwr Commands

On the ES-2024PWR, use the `pwr` commands in Configure mode to enable PoE and configure PoE settings on the ports.

Syntax:

```
pwr interface <port-list>
pwr interface <port-list> priority <critical|high|low>
pwr mibtrap
pwr usagethreshold <1-99>
```

where

`<port-list>`	=	Enables PoE on the specified port(s).
`priority <critical|high|low>`	=	Sets the PD priority on a port to allow the switch to allocate power to higher priority ports when the remaining power goes below 16W. `criticl` > `high` >`low`
`mibtrap`	=	Enables MIB traps on the switch. Traps are initiated when the usage reaches the limit set by the `pwr usagethreshold` command.
`usagethreshold <1-99>`		Sets the percentage of power usage which initiates MIB traps.

The following figure shows an example.

- Activates PoE on port 1.
- Sets the PoE priority to critical.
- Enables MIB traps.
- Set the usage threshold to 15.
- Displays PoE settings.

```
ES-2024PWR# config
ES-2024PWR(config)# pwr interface 1
ES-2024PWR(config)# pwr interface 1 priority critical
ES-2024PWR(config)# pwr mibtrap
ES-2024PWR(config)# pwr usagethreshold 15
ES-2024PWR(config)# exit
ES-2024PWR# show pwr

Averaged Junction Temperature: 33 (c), 91 (f).

Port   State   PD  Class  Priority  Consumption (mW)  MaxPower(mW)
----  ------  ---  -----  --------  ----------------  ------------
   1  Enable  off      0  Critical                 0             0
   2  Enable  off      0       Low                 0             0
   3  Enable  off      0       Low                 0             0
   4  Enable  off      0       Low                 0             0
   5  Enable  off      0       Low                 0             0
   6  Enable  off      0       Low                 0             0
   7  Enable  off      0       Low                 0             0
   8  Enable  off      0       Low                 0             0
   9  Enable  off      0       Low                 0             0
  10  Enable  off      0       Low                 0             0
  11  Enable  off      0       Low                 0             0
  12  Enable  off      0       Low                 0             0
  13  Enable  off      0       Low                 0             0
  14  Enable  off      0       Low                 0             0
  15  Enable  off      0       Low                 0             0
  16  Enable  off      0       Low                 0             0
  17  Enable  off      0       Low                 0             0
  18  Enable  off      0       Low                 0             0
  19  Enable  off      0       Low                 0             0
  20  Enable  off      0       Low                 0             0
  21  Enable  off      0       Low                 0             0
  22  Enable  off      0       Low                 0             0
  23  Enable  off      0       Low                 0             0
  24  Enable  off      0       Low                 0             0

Total Power:185.0(W)
Consuming Power:0.0(W)
Allocated Power:0.0(W)
Remaining Power:185.0(W)
ES-2024PWR#
```

32.7 Queuing Method Commands

You can use the queuing method commands to configure queuing for outgoing traffic on the switch. You can only select one queuing method for the switch.

Syntax:

```
spq
wrr
wrr <wt1><wt2> ... <wt4>
```

where

`spq`	=	Sets the queuing method to SPQ (Strictly Priority Queuing).
`wrr`	=	Sets the queuing method to WRR (Weighted Round Robin).
`wrr <wt1><wt2> ... <wt4>`	=	You may want to configure weights for specific queues on the switch if you use WRR..

An example is shown next.

- Set the queueing method to SPQ.

```
sysname(config)# spq
```

32.8 Static Route Commands

You can create and configure static routes on the switch by using the `ip route` command.

Syntax:

```
ip route <ip> <mask> <next-hop-ip>
ip route <ip> <mask> <next-hop-ip> [metric <metric>][name <name>]
[inactive]
```

where

`<ip>`	=	Specifies the network IP address of the final destination.
`<mask>`	=	Specifies the subnet mask of this destination.
`<next-hop-ip>`	=	Specifies 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.
`[metric <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.

`[name <name>]`	=	Specifies a descriptive name (up to 32 printable ASCII characters) for identification purposes.
`[inactive]`	=	Deactivates a static route

An example is shown next.

- Create a static route with the destination IP address of `172.21.1.104`, subnet mask of `255.255.0.0` and the gateway IP address of `192.168.1.2`.
- Assigns a metric value of `2` to the static route.
- Assigns the name `route1` to the static route.

```
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 metric 2
sysname(config)# ip route 172.21.1.104 255.255.0.0 192.168.1.2 name route1
```

32.9 Enabling MAC Filtering

You can create a filter to drop packets based on the MAC address of the source or the destination.

Syntax:

```
mac-filter name <name> mac <mac-addr> vlan <vlan-id>
```

where

`name <name>`	=	Names the filtering rule.
`mac <mac-addr>`	=	Specifies the MAC address you want to filter.
`vlan <vlan-id>`	=	Specifies which VLAN this rule applies to.

An example is shown next.

- Create a filtering rule called "filter1".
- Drop packets coming from and going to MAC address 00:12:00:12:00:12 on VLAN.

```
sysname(config)# mac-filter name filter1
sysname(config)# mac-filter name filter1 mac 00:12:00:12:00:12 vlan 1
```

32.10 Enabling Trunking

To create and enable a trunk, enter `trunk` followed by the ports which you want to group and press [ENTER].

Syntax:

```
trunk <T1|T2|T3>
trunk <T1|T2|T3> interface <port-list>
trunk <T1|T2|T3> lacp
```

where

`<T1|T2|T3>`	=	Enables the trunk.
`<T1|T2|T3> interface <port-list>`	=	Places ports in the trunk.
`<T1|T2|T3> lacp`	=	Enables LACP in the trunk.

An example is shown next.

- Enable trunk 1 on the switch.
- Place ports 1-3 in trunk 1.
- Enable dynamic link aggregation (LACP) on trunk 1.

```
sysname(config)# trunk t1
sysname(config)# trunk t1 interface 1-3
sysname(config)# trunk t1 lacp
```

32.11 Enabling Port Authentication

To enable a port authentication, you need to specify your RADIUS server details and select the ports which require external authentication. You can set up multiple RADIUS servers and specify how the switch will process authentication requests.

32.11.1 RADIUS Server Settings

Configuring multiple RADIUS servers is only available via the command interpreter mode. Use the `radius-server` command to set up your RADIUS server settings.

Syntax:

```
radius-server host <index> <ip>
radius-server host <index> <ip> [auth-port <socket-number>][key <key-
string>]
radius-server timeout <1-1000>
radius-server mode <priority|round-robin>
```

where

`radius-server host <index> <ip>`	=	Specifies the IP address of the RADIUS server.
`[auth-port <socket-number>]`	=	Changes the UDP port of the RADIUS server from the default (1812).
`[key <key-string>]`	=	Specifies a password (up to 32 alphanumeric characters) as the key to be shared between the RADIUS server and the switch.
`radius-server timeout <1-1000>`	=	Specifies the timout period (in seconds) the switch will wait for a response from a RADIUS server. If 2 RADIUS servers are configured and are in priority mode, this is the total time the switch will wait for a response from either server.
`mode <priority|round-robin>`	=	Specifies the way the switch will process requests from the clients to the RADIUS server. (Only applicable with multiple RADIUS servers configured.) `priority` - When a client sends an authentication request through the switch to the RADIUS server. The switch will forward the request to the RADIUS server. If no response within half the timeout period, it will forward the request to the second RADIUS server. `round-robin` - When a client sends an authentication request through the switch to the RADIUS server. The switch will forward the request to the first RADIUS server. If there is no response within the timeout period, the request times out. The client sends an authentication request again and the switch forwards the request to the second RADIUS server.

See Section 32.11.2 on page 232 for an example.

32.11.2 Port Authentication Settings

Use the `port-access-authenticator` command to configure port security on the switch.

Syntax:

```
port-access-authenticator
port-access-authenticator <port-list>
port-access-authenticator <port-list> reauthenticate
port-access-authenticator <port-list> reauth-period <reauth-period>
```

where

`port-access-authenticator`	=	Enables port authentication on the switch.
`port-access-authenticator <port-list>`	=	Specifies which ports require authentication.
`reauthenticate`	=	Enables reauthentication on the port.
`reauth-period <reauth-period>`	=	Specifies how often a client has to re-enter his or her username and password to stay connected to the port.

An example is shown next.

- Specify RADIUS server 1 with IP address 10.10.10.1, port 1890 and the string `secretKey` as the password. See Section 32.11.1 on page 231 for more information on RADIUS server commands.
- Specify the timeout period of 30 seconds that the switch will wait for a response from the RADIUS server.
- Enable port authentication on ports 4 to12.
- Activate reauthentication on the ports.
- Specify 1800 seconds as the interval for client reauthentication.

```
sysname(config)# radius-server host 1 10.10.10.1 auth-port 1890 key secretKey
sysname(config)# radius-server timeout 30
sysname(config)# port-access-authenticator
sysname(config)# port-access-authenticator 4-12
sysname(config)# port-access-authenticator 4-12 reauthenticate
sysname(config)# port-access-authenticator 4-12 reauth-period 1800
```

CHAPTER 33
Interface Commands

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

33.1 Overview

The interface commands allow you to configure the switch on a port by port basis.

33.2 Interface Command Examples

This section provides examples of some frequently used interface commands.

33.2.1 interface port-channel

Use this command to enable the specified ports for configuration. Indicate multiple, non-sequential ports separated by a comma. Use a dash to specify a port range.

Syntax:

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

An example is shown next.

- Enter the configuration mode.
- Enable ports 1, 3, 4 and 5 for configuration.
- Begin configuring for those ports.

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

33.2.2 bandwidth-limit

The `bandwidth-limit` command enables bandwidth control on the switch.

Syntax:

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

where

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

An example is shown next.

- Enable port one for configuration.
- Enable bandwidth control on the outgoing traffic.
- Set the outgoing traffic bandwidth limit to 5000Kbps.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# bandwidth-limit egress
sysname(config-interface)# bandwidth-limit egress 5000
```

33.2.3 mirror

The `mirror` command enables port mirroring on the interface.

Syntax:

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

where

`dir <ingress|egress|both>`	=	Enables port mirroring for incoming, outgoing or both incoming and outgoing traffic. Port mirroring copies traffic from one port to another port for external analysis.

An example is shown next.

- Enable port mirroring.
- Enable the monitor port 3.
- Enable ports 1, 4, 5 and 6 for configuration.
- Enable port mirroring on the ports.

- Enable port mirroring for outgoing traffic. Traffic is copied from ports 1, 4, 5 and 6 to port three in order to examine it in more detail without interfering with the traffic flow on the original ports.

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

33.2.4 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 VLAN groups beyond the local switch.

An example is shown next.

- Enable IEEE 802.1Q tagged VLAN to configure tagged VLAN for the switch.
- Enable ports one, three, four and five for configuration.
- Enable GVRP on the interface.

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

33.2.5 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.

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

33.2.6 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).

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

33.2.7 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).

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

33.2.8 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.

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

33.2.9 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 100 Mbps in half duplex mode.

```
sysname(config)# interface port-channel 1,3-5
sysname(config-interface)# speed-duplex 100-half
```

33.2.10 test

You can perform local loopback test on a port. The test returns `Passed!` or `Failed!`

An example is shown next.

- Enters interface command mode to configure port 1.
- Execute the `test` command.
- View the results.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# test
Testing internal loopback on port  1 :Passed!
  Ethernet Port 1 Test ok.
sysname(config-interface)#
```

33.3 Interface no Command Examples

Similar to the `no` commands in Enable and Config modes, the `no` commands for the Interface sub mode also disable certain features. In this mode, however, this takes place on a port-by-port basis.

33.3.1 no bandwidth-limit

You can disable broadcast storm limit on port 1 simply by placing the `no` command in front of the `bwstorm-limit` command.

Syntax:

```
no bmstorm-limit
```

An example is shown next:

- Disable bandwidth limit on port one.

```
sysname(config)# interface port-channel 1
sysname(config-interface)# no bwstorm-limit
```

CHAPTER 34
IEEE 802.1Q Tagged VLAN Commands

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

34.1 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.

```
sysname(config)# vlan 2000
sysname(config-vlan)# name up1
sysname(config-vlan)# fixed 10-12
sysname(config-vlan)# no untagged 10-12
sysname(config-vlan)# exit
sysname(config)# interface port-channel 10-12
sysname(config-interface)# pvid 2000
sysname(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.

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

34.2 Global VLAN1Q Tagged VLAN Configuration Commands

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

34.2.1 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.

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

34.2.2 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.

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

34.2.3 GVRP Timer

Syntax:

```
show vlan1q gvrp
```

This command shows the switch's GVRP settings.

An example is shown next.

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

34.2.4 Enable GVRP

Syntax:

```
vlan1q gvrp
```

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

34.2.5 Disable GVRP

Syntax:

```
no vlan1q gvrp
```

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

34.3 Port VLAN Commands

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

34.3.1 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.

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

34.3.2 Set Acceptable Frame Type

Syntax:

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

where

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

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

34.3.3 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.

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

34.3.4 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.

34.3.4.1 Modify a Static VLAN Table Example

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

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

34.3.4.2 Forwarding Process Example

34.3.4.2.1 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.

34.3.4.2.2 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.

34.3.5 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.

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

34.4 Enable VLAN

Syntax:

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

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

34.5 Disable VLAN

Syntax:

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

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

34.6 Show VLAN Setting

Syntax:

```
show vlan
```

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

An example is shown next.

- VID is the VLAN identification number.
- Status shows whether the VLAN is static or active.
- Elap-Time is the time since the VLAN was created on the switch.
- The `TagCtl` section of the last column shows which ports are tagged and which are untagged.

```
sysname# show vlan
  The Number of VLAN:    3
  Idx. VID   Status    Elap-Time    TagCtl
  ---- ----  -------- ------------ ------------------------
   1     1    Static     0:12:13  Untagged :1-28
                                    Tagged   :

   1   100    Static     0:00:17  Untagged :
                                    Tagged   :1-24

   1   200    Static     0:00:07  Untagged :1-12
                                    Tagged   :13-28
```

CHAPTER 35
Troubleshooting

This chapter covers potential problems and possible remedies.

35.1 Problems Starting Up the Switch

Table 76 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.

35.2 Problems Accessing the Switch

Table 77 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.

35.2.1 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.

35.2.1.1 Internet Explorer Pop-up Blockers

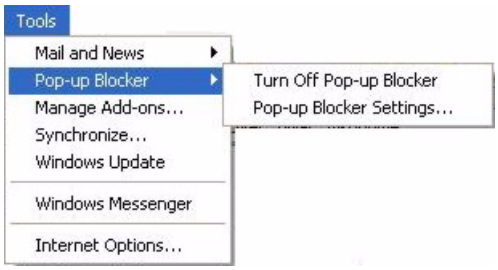
You may have to disable pop-up blocking to log into your device.

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.

35.2.1.1.1 Disable pop-up Blockers

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

Figure 101 Pop-up Blocker

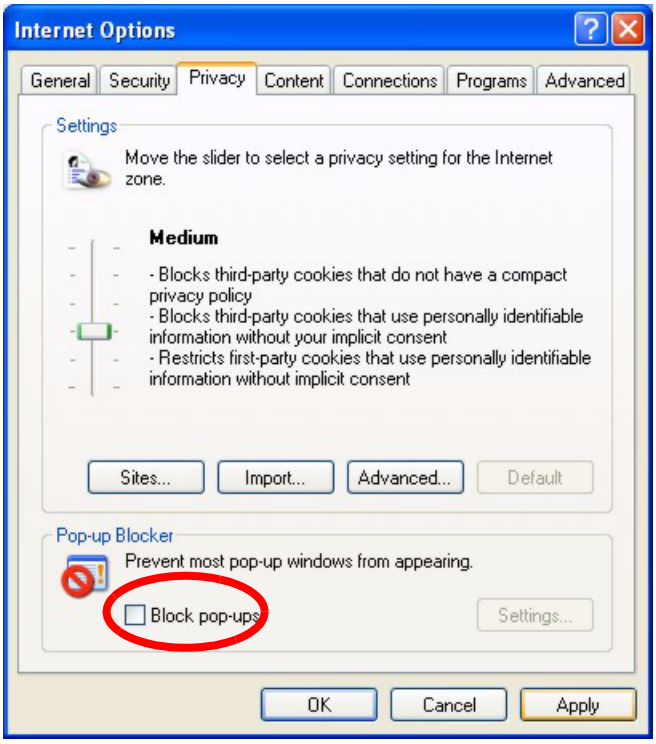


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

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 102 Internet Options



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

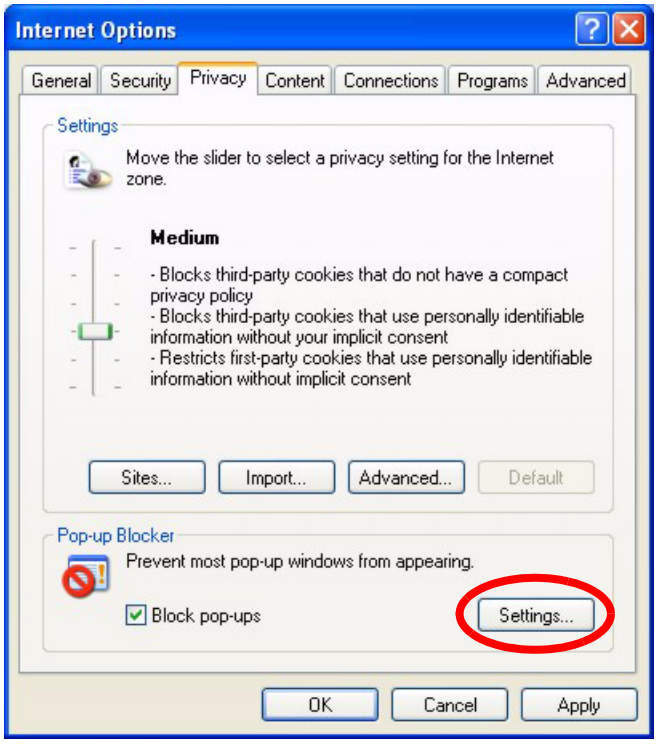
35.2.1.1.2 Enable pop-up Blockers with Exceptions

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.

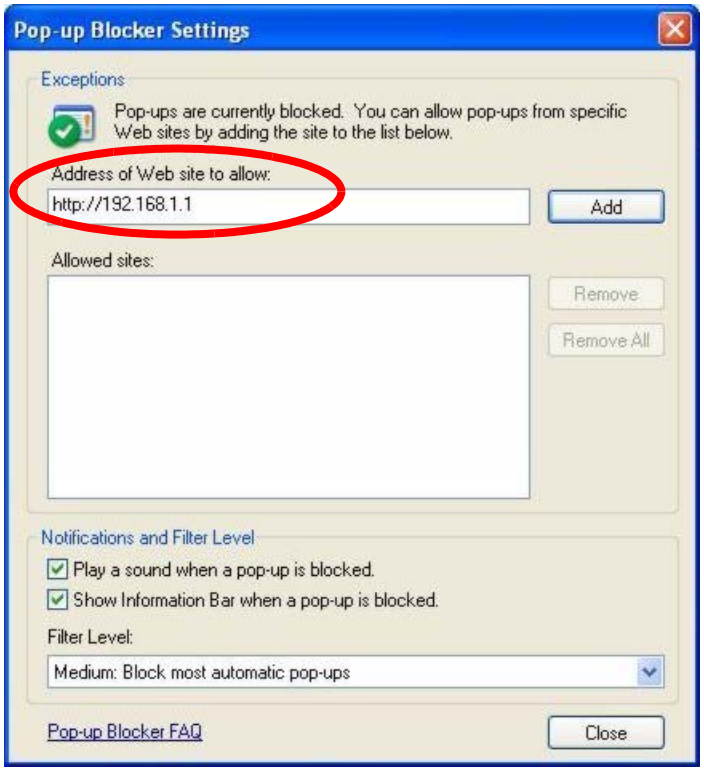
Figure 103 Internet Options



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 104 Pop-up Blocker Settings



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

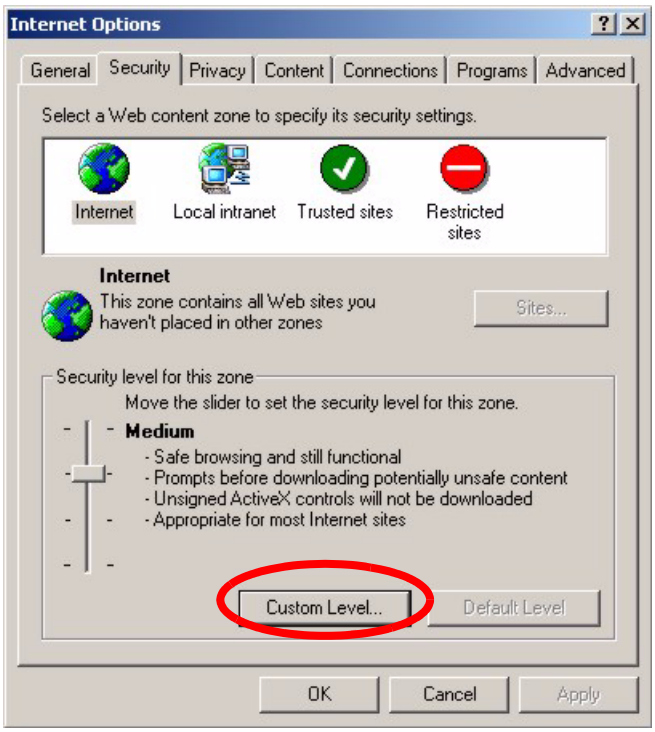
6 Click **Apply** to save this setting.

35.2.1.2 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 105 Internet Options



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

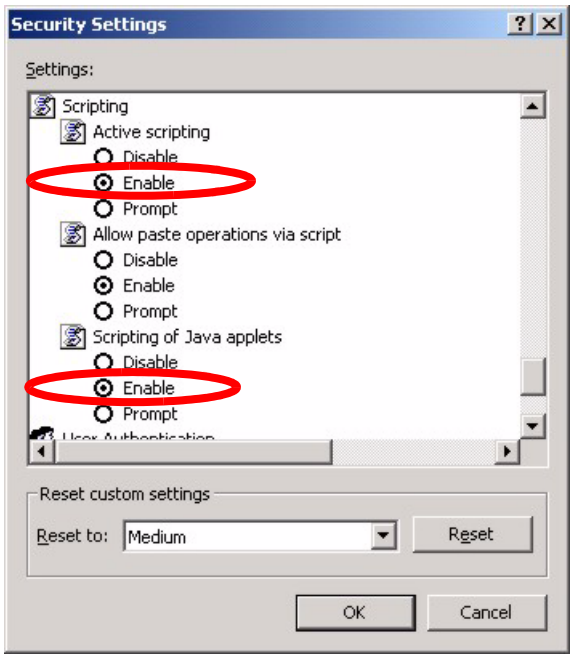
3 Scroll down to **Scripting**.

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.

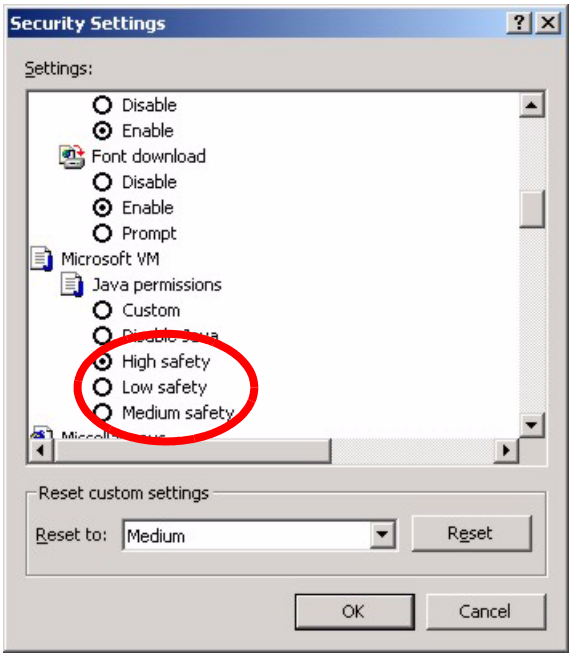
Figure 106 Security Settings - Java Scripting



35.2.1.3 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 107 Security Settings - Java



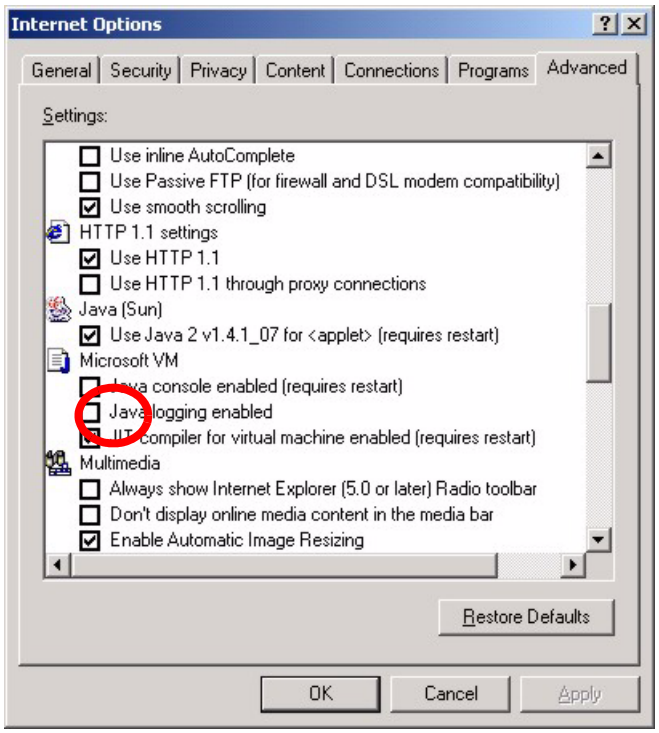
35.2.1.3.1 JAVA (Sun)

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 108 Java (Sun)



35.3 Problems with the Password

Table 78 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 79 General Product Specifications

Ethernet Interface	24 10/100 Base-TX interfaces Auto-negotiation Auto-MDI/MDIX Compliant with IEEE 802.3/3u Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x) RJ-45 Ethernet cable connector Rate limiting at 64Kbps steps
Gigabit Interface	Two Gigabit Ethernet/mini-GBIC ports
PoE	IEEE 802.3af compliant Inline power to 24 PoE ports (max. 15.4 Watt/port, 185Watt/system) Power budget management
Bridging	8K MAC addresses Static MAC address filtering (port lock) Broadcast storm control Limited maximum number of MAC addresses per port
Switching	Switching fabric: 8.8Gbps, non-blocking Max. Frame size: 1522 bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II, PPPoE Prevent the forwarding of corrupted packets
STP	IEEE 802.1d spanning tree protocol IEEE 802.1w, rapid reconfiguration to recover network failure
QoS	IEEE 802.1p Four priority queues Supports RFC 2475 DiffServ, DSCP to IEEE 802.1p priority mapping
Security	IEEE 802.1x port-based authentication Static MAC Address Forward (256 rules)
VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K (256 static VLANs) Supports GVRP
Link aggregation	Supports IEEE 802.3ad; static and dynamic (LACP) port trunking Three groups (two for fast Ethernet and one for Gigabit Ethernet)

Table 79 General Product Specifications (continued)

Port mirroring	All ports support port mirroring
Multicast	IGMP filtering IGMP snooping MVR

Table 80 Management Specifications

System Control	Alarm/Status surveillance LED indication for alarm and system status Performance monitoring Line speed Four RMON groups (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/TFTP 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 64management IP address in different VLAN Clustering: up to 24 switches can be manage 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) Private MIBs

Table 81 Physical and Environmental Specifications

LEDs	Per switch: PWR, SYS, ALM Per Ethernet port: LNK/ACT, FDX/COL (ES-2024A), PoE (ES-2024PWR)
Dimension	Standard 19" rack mountable ES-2024A: 438 mm (W) x 173 mm (D) x 44.5 mm (H) ES-2024PWR: 438 mm (W) x 270 mm (D) x 44.5 mm (H)

Table 81 Physical and Environmental Specifications (continued)

Weight	ES-2024A: 2.2 Kg ES-2024PWR: 4 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)
Power Supply	100-240VAC, 50/60Hz, ES-2024A: 0.4A ES-2024PWR: 2A
Power Consumption	ES-2024A: 24W ES-2024PWR: 200W
Safety	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 Addresses and Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

The following table shows the network number and host ID arrangement for classes A, B and C.

Table 82 Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	**Network number**	Host ID	Host ID	Host ID
Class B	**Network number**	**Network number**	Host ID	Host ID
Class C	**Network number**	**Network number**	**Network number**	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have $2^8 - 2$, or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have $2^{16} - 2$, or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have $2^{24} - 2$ hosts, or approximately 16 million hosts.

IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

Table 83 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
Class E (reserved)	**1111**0000 to **1111**1111	240 to 255

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 bits. If a bit in the subnet mask 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 like IP addresses. The "natural" masks for class A, B and C IP addresses are as follows.

Table 84 "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 leftmost 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 85 Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

Table 85 Alternative Subnet Mask Notation (continued)

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

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 86 Two Subnets Example

IP/SUBNET MASK	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").

To make two 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 make 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 87 Subnet 1

IP/SUBNET MASK	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

Table 87 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 88 Subnet 2

IP/SUBNET MASK	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	

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 (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 zeroes is the subnet itself, all ones is the broadcast address on the subnet).

Table 89 Subnet 1

IP/SUBNET MASK	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

Table 89 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 90 Subnet 2

IP/SUBNET MASK	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 91 Subnet 3

IP/SUBNET MASK	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 92 Subnet 4

IP/SUBNET MASK	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 eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

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

Table 93 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	225	254	255

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

Table 94 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 82 on page 263) available for subnetting.

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

Table 95 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

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Z