ES-2024 Series

Ethernet Switch

User's Guide

Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 3.90
Edition 1, 12/2008

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ES-2024 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide contains information on setting up your hardware.

- Web Configurator Online Help

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

- CLI Reference Guide

  The CLI Reference Guide is intended for people who want to configure the ES-2024 via commands.

Note: It is recommended you use the web configurator to configure the Switch.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- 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.

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

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033
- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

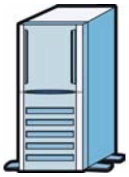
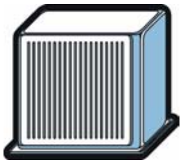
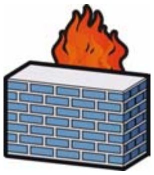
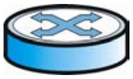
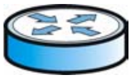
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ES-2024A and ES-2024PWR may be referred to as the "ES-2024", "Switch", the "device", the "system" or the "product" in this User's Guide. Differentiation is made where needed.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- Command keywords are in `courier new font`.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- An arrow (`-->`) indicates that this line is a continuation of the previous line.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User’s Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- 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.
- ONLY qualified service personnel should service or disassemble this device.
- 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.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- This product is recyclable. Dispose of it properly.

Contents Overview

Table of Contents

PART I
Introduction

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.

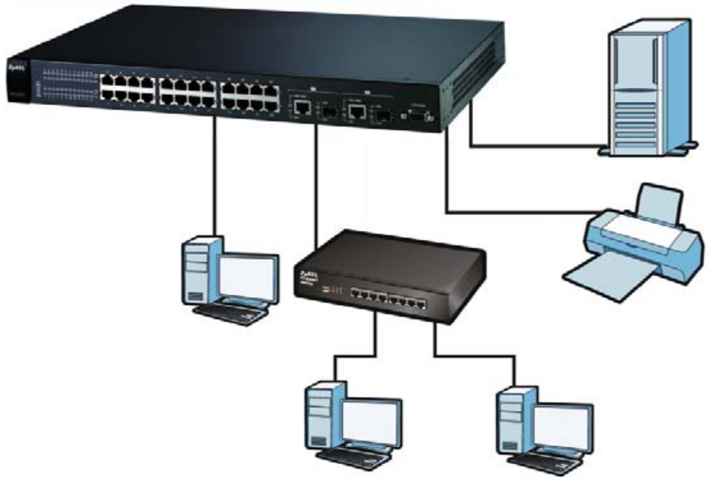
See Appendix A on page 279 for a full list of software features available on the Switch.

1.1.1 Backbone 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 and servers 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

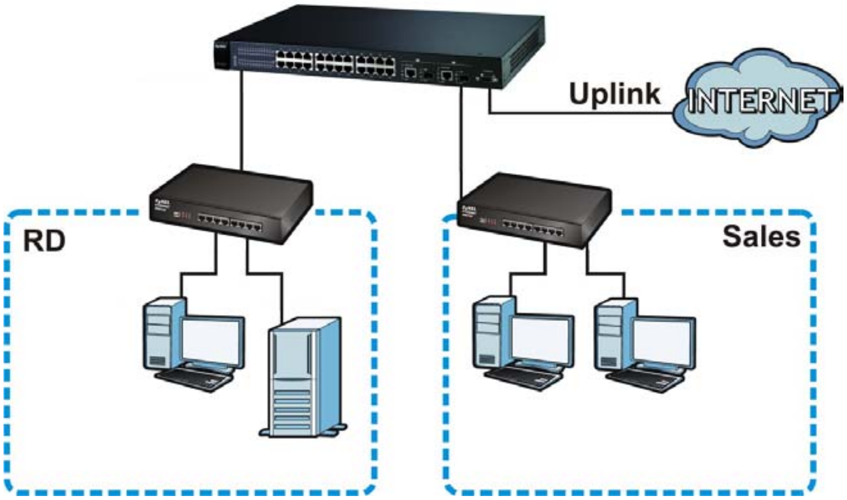


1.1.2 Bridging Example

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

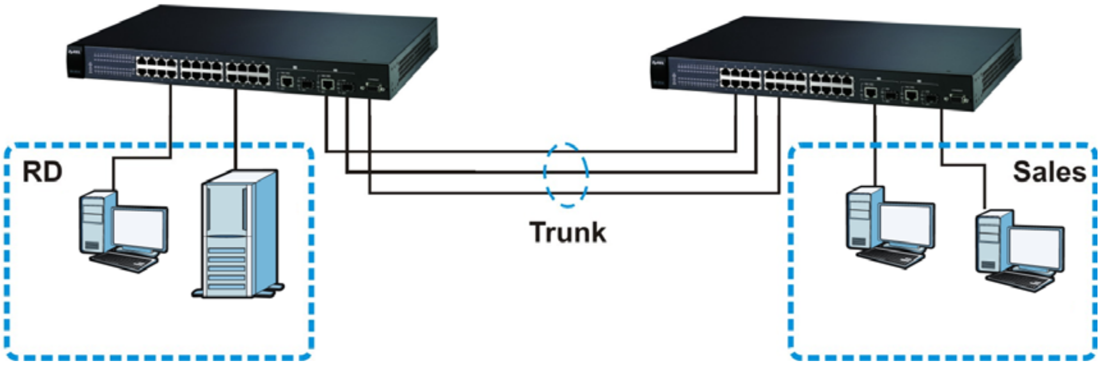


1.1.3 High Performance Switching Example

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 Workgroup Application



1.1.4 IEEE 802.1Q VLAN Application Examples

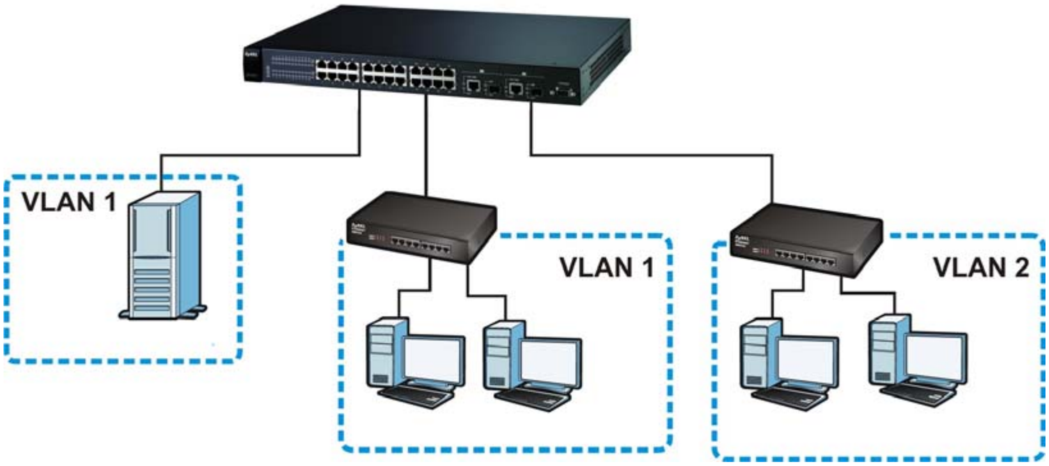
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one group. A station can belong to more than one group. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s)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

For more information on VLANs, refer to Chapter 9 on page 91.

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.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 41.
- Command Line Interface. Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/ restore. See Section 28.8 on page 229.
- SNMP. The device can be monitored and/or managed by an SNMP manager. See Section 29.3 on page 234.

1.3 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that’s not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

2

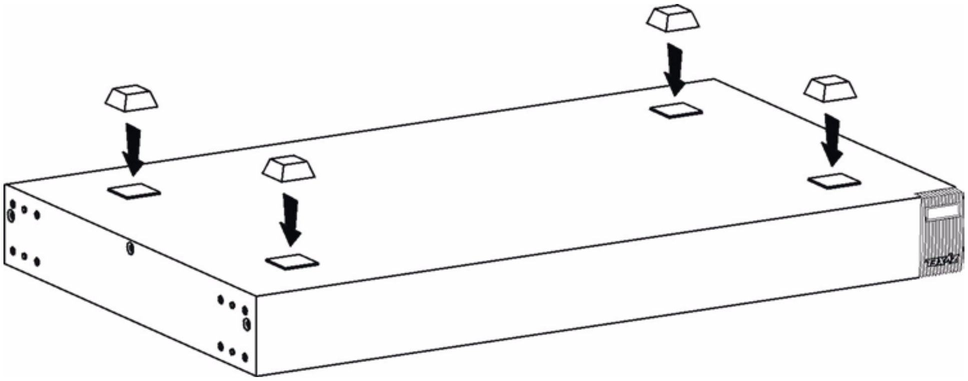
Hardware Installation and Connection

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 5 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.

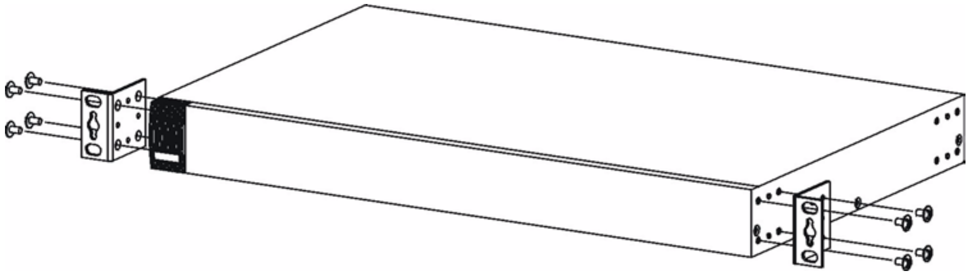
2.2.1.1 Precautions

- 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 6 Attaching the Mounting Brackets



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

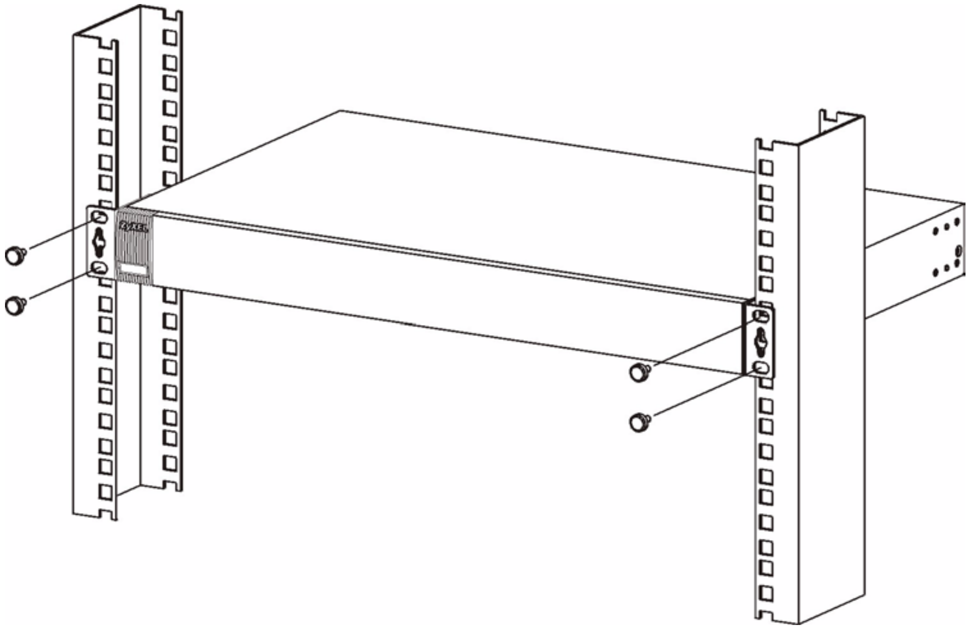
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

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 7 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.

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 8 Front Panel: ES-2024A

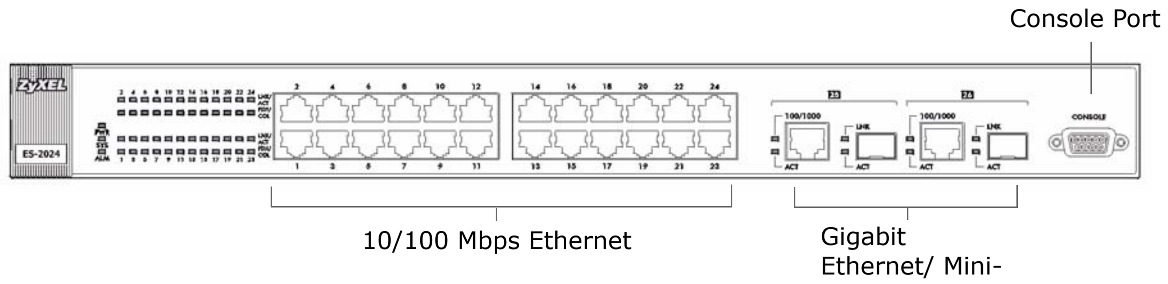
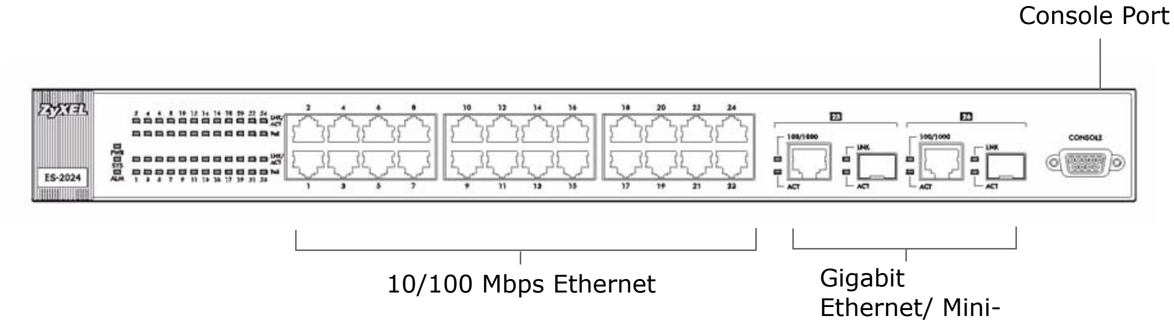


Figure 9 Front Panel: ES-2024PWR



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.
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 10/100-Mbps auto-negotiating, auto-crossover Ethernet ports. In 10/100 Mbps Fast Ethernet, the speed can be 10 Mbps or 100 Mbps 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 100 Mbps or 1000 Mbps 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 (10/100 Mbps) 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)

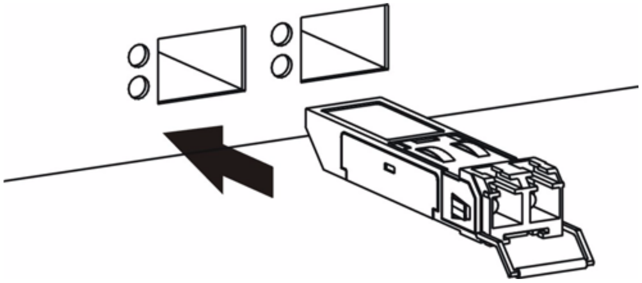
Note: To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

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.

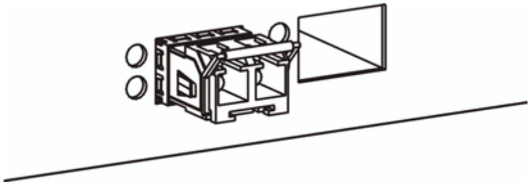
Figure 10 Transceiver Installation Example



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 11 Installed Transceiver

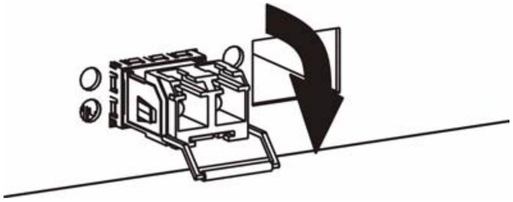


3.1.3.2 Transceiver Removal

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

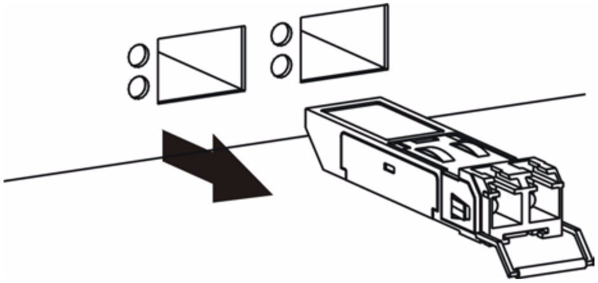
1 Open the transceiver's latch (latch styles vary).

Figure 12 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

Figure 13 Transceiver Removal Example



3.2 Rear Panel

The following figures show the rear panel of the Switch. The power receptacle is on the rear panel.

Figure 14 AC Rear Panel

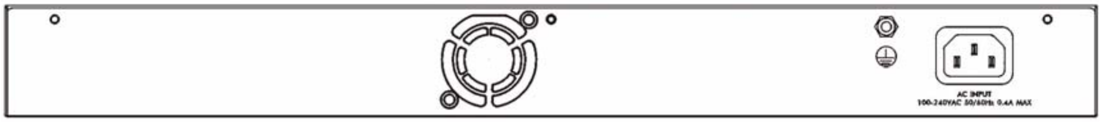
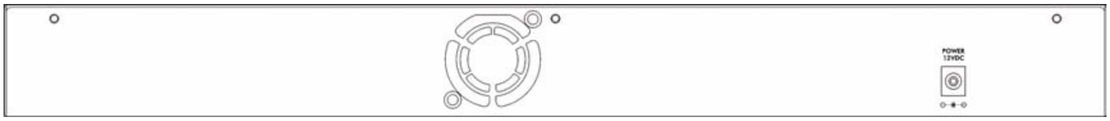


Figure 15 DC Rear Panel



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	COLO R	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			

Table 2 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
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.
ACT	Green	Blinking	The port is sending or receiving data.
		Off	The port is not sending or receiving data.

PART II
Basic Configuration

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).

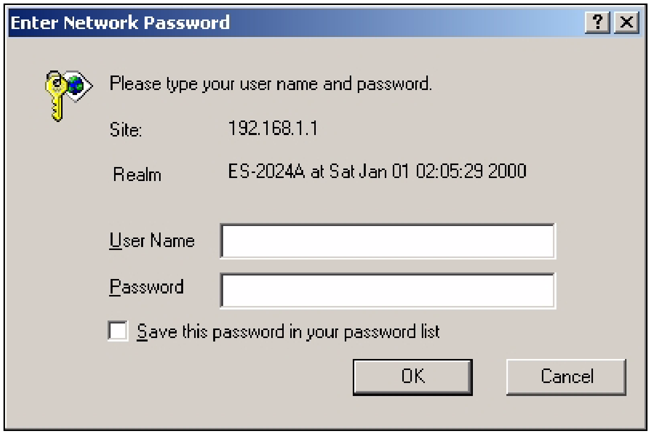
4.2 System Login

1 Start your web browser.

2 Type 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



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm ES-2024A at Sat Jan 01 02:05:29 2000

User Name

Password

□ Save this password in your password list

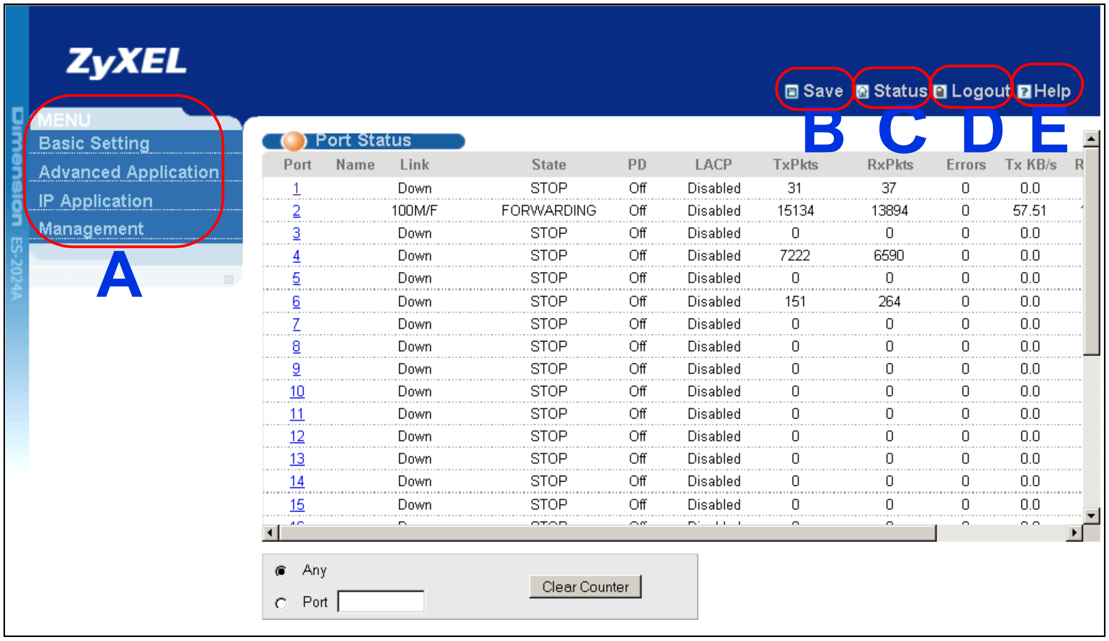
4 Click **OK** to view the first web configurator screen.

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)



Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	R
1		Down	STOP	Off	Disabled	31	37	0	0.0	
2		100M/F	FORWARDING	Off	Disabled	15134	13894	0	57.51	
3		Down	STOP	Off	Disabled	0	0	0	0.0	
4		Down	STOP	Off	Disabled	7222	6590	0	0.0	
5		Down	STOP	Off	Disabled	0	0	0	0.0	
6		Down	STOP	Off	Disabled	151	264	0	0.0	
7		Down	STOP	Off	Disabled	0	0	0	0.0	
8		Down	STOP	Off	Disabled	0	0	0	0.0	
9		Down	STOP	Off	Disabled	0	0	0	0.0	
10		Down	STOP	Off	Disabled	0	0	0	0.0	
11		Down	STOP	Off	Disabled	0	0	0	0.0	
12		Down	STOP	Off	Disabled	0	0	0	0.0	
13		Down	STOP	Off	Disabled	0	0	0	0.0	
14		Down	STOP	Off	Disabled	0	0	0	0.0	
15		Down	STOP	Off	Disabled	0	0	0	0.0	

● Any
○ Port

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 quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is saved in the configuration file from which the Switch booted from and it stays the same even if the Switch's power is turned off. See Section 28.3 on page 226 for information on saving your settings to a specific configuration file.

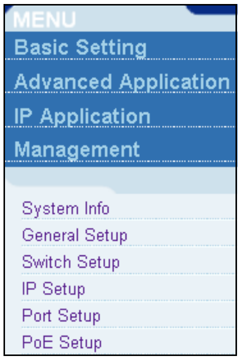
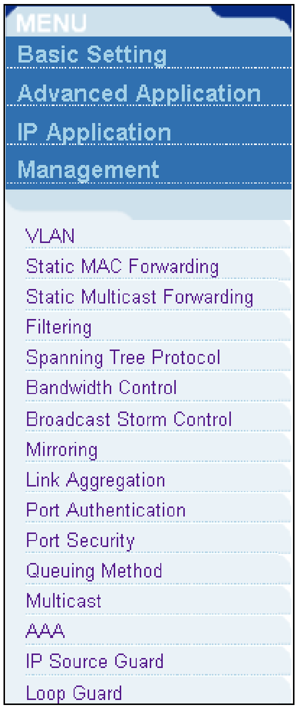
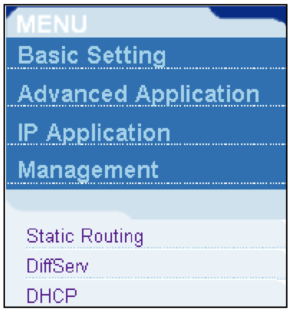
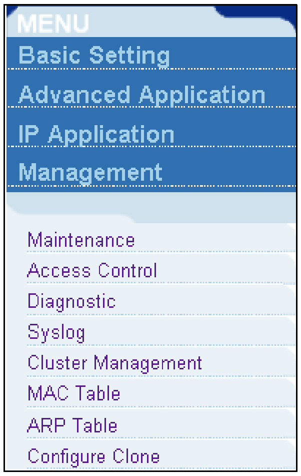
C - Click this link to go to the status page of the Switch.

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.

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

Table 3 Navigation Panel Sub-links Overview

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

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 General Setup Switch Setup IP Setup Port Setup PoE Setup	VLAN VLAN Port Setting Static VLAN Static MAC Forwarding Static Multicast Forwarding Filtering Spanning Tree Protocol Configuration RSTP MSTP Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Link Aggregation Setting Link Aggregation Control Protocol Port Authentication 802.1x Port Security Queuing Method Multicast Multicast Setting IGMP Snooping VLAN IGMP Filtering Profile MVR Group Configuration AAA RADIUS Server Setup TACACS+ Server Setup AAA Setup IP Source Guard Static Binding ARP Inspection Status LogStatus Configure Port VLAN Loop Guard	Static Routing DiffServ DSCP Setting DHCP Global Relay VLAN Setting	Maintenance Firmware Upgrade Restore Configuration Backup Configuration Load Factory Default Save Configuration Reboot System Access Control SNMP Trap Group Logins Service Access Control Remote Management Diagnostic Syslog Syslog Server Setup Cluster Management Clustering Management Configuration MAC Table ARP Table Configure Clone

The following table describes the links in the navigation panel.

Table 5 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up IP routing domains.
Port Setup	This link takes you to screens where you can configure settings for individual Switch ports.
PoE Setup	This link take you to a screen where you can set priorities so that the Switch is able to reserve and allocate power to certain PDs.
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.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast 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 RSTP/MSTP 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 IEEE 802.1x port authentication.
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 queuing with associated queue weights.

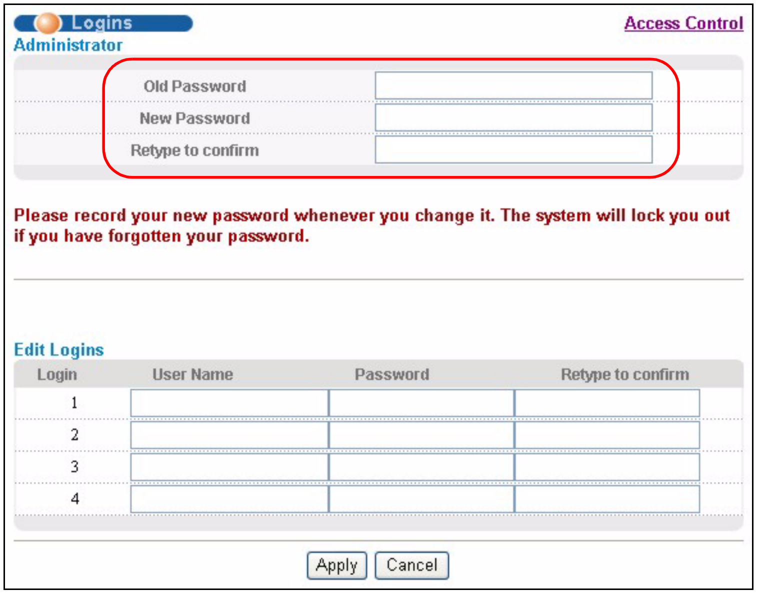
Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
Multicast	This link takes you to a screen where you can configure various multicast features and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to a screen where you can configure filtering of unauthorized ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
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.
DHCP	This link takes you to a screen where you can configure the DHCP settings.
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.
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 copy attributes of one port to other ports.

4.3.1 Change Your Password

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

Figure 18 Change Administrator Login Password



Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

Login	User Name	Password	Retype to confirm
1			
2			
3			
4			

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 using in-band-management (managing through the data ports) if you do one of the following:

1 Delete the management VLAN (default is VLAN 1).

2 Delete all port-based VLANs with the CPU port as a member. The “CPU port” is the management port of the Switch.

3 Filter all traffic to the CPU port.

4 Disable all ports.

5 Misconfigure the text configuration file.

6 Forget the password and/or IP address.

7 Prevent all services from accessing the Switch.

8 Change a service port number but forget 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) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the 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 9600 bps with 8 data bits, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

1 Connect to the console port using a computer with terminal emulation software. See Section 3.1.1 on page 34 for details.

2 Disconnect and reconnect the Switch’s power to begin a session. When you reconnect the Switch’s power, you will see the initial screen.

3 When you see the message “`Press any key to enter Debug Mode within 3 seconds ...`” press any key to enter debug mode.

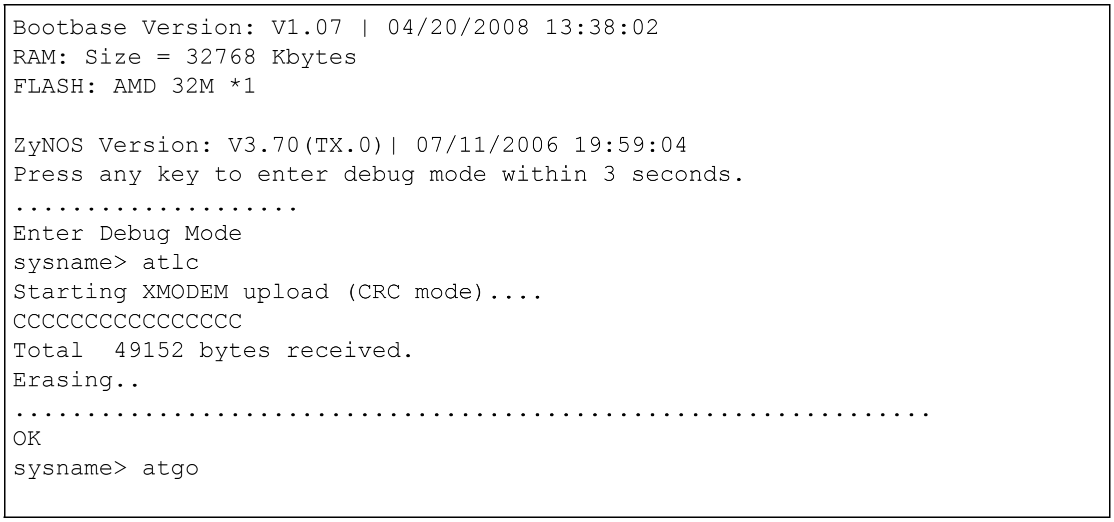
4 Type `atlc` after the “`Enter Debug Mode`” message.

5 Wait for the "`Starting XMODEM upload`" message before activating XMODEM upload on your terminal.

6 After a configuration file upload, type `atgo` to restart the Switch.

An example is shown below.

Figure 19 Resetting the Switch: Via the Console Port



```
Bootbase Version: V1.07 | 04/20/2008 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
sysname> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCCC
Total  49152 bytes received.
Erasing..
................................................................
OK
sysname> atgo
```

The Switch is now reinitialized with a 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 for security reasons.

Figure 20 Web Configurator: Logout Screen

Thank you for using the Web Configurator.Goodbye!

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.

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

Before you begin, you should log in to the web configurator.

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.

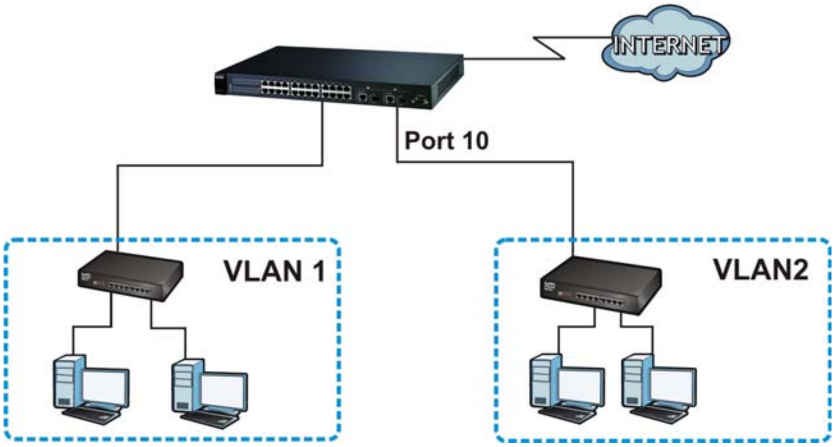
See Section 4.2 on page 41 for more information.

5.1.1 Creating a VLAN

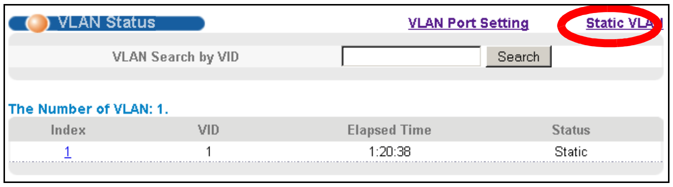
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

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.

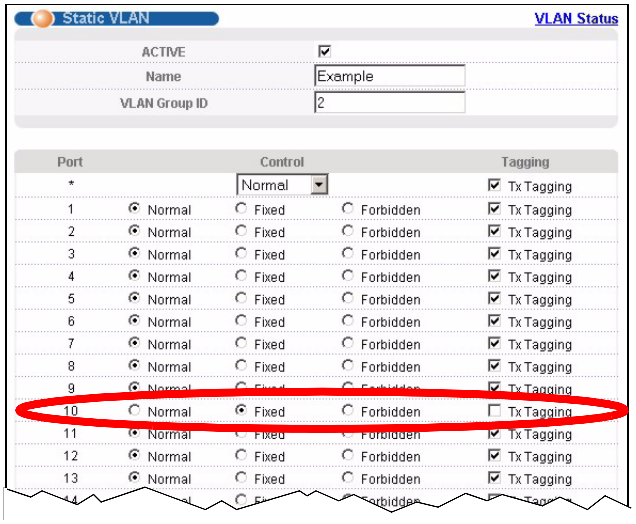


VLAN Search by VID

The Number of VLAN: 1.

Index	VID	Elapsed Time	Status
1	1	1:20:38	Static

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.



ACTIVE	☑
Name	Example
VLAN Group ID	2

Port	Control			Tagging
*	Normal			☑ Tx Tagging
1	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
2	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
3	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
4	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
5	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
8	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
9	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
10	○ Normal	● Fixed	○ Forbidden	☐ Tx Tagging
11	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
12	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
13	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

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.

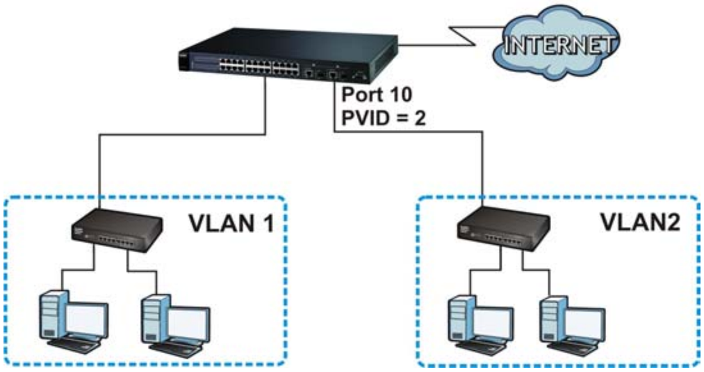
5 Click **Add** to create the static VLAN and click the **Save** button to save the settings.

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.

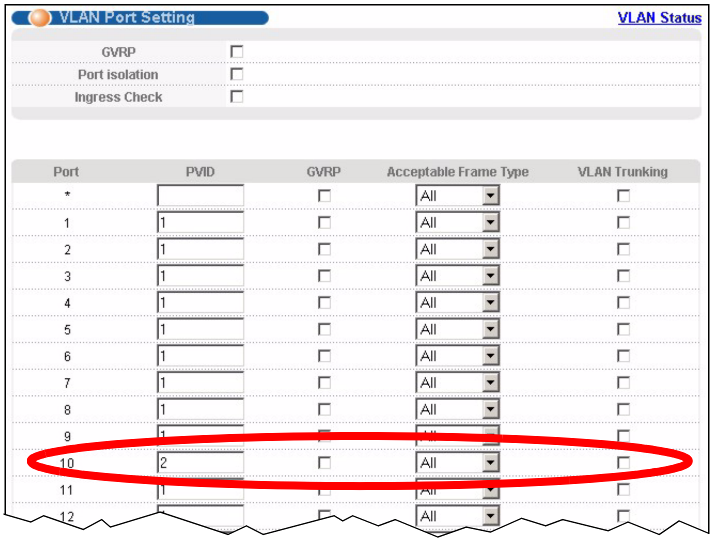
In the example network, configure 2 as the port VID on port 10 so that any untagged frames received on that port get sent to VLAN 2.

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.



VLAN Port Setting

VLAN Status

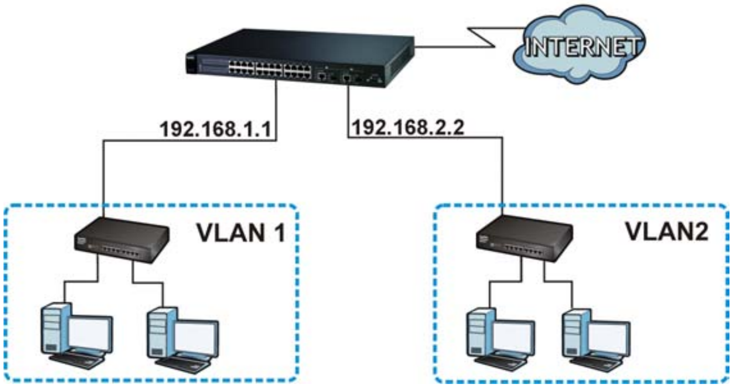
GVRP	□
Port isolation	□
Ingress Check	□

Port	PVID	GVRP	Acceptable Frame Type	VLAN Trunking
*		□	All	□
1	1	□	All	□
2	1	□	All	□
3	1	□	All	□
4	1	□	All	□
5	1	□	All	□
6	1	□	All	□
7	1	□	All	□
8	1	□	All	□
9	1	□	All	□
10	2	□	All	□
11	1	□	All	□
12		□	All	□

5.1.3 Configuring Switch Management IP Address

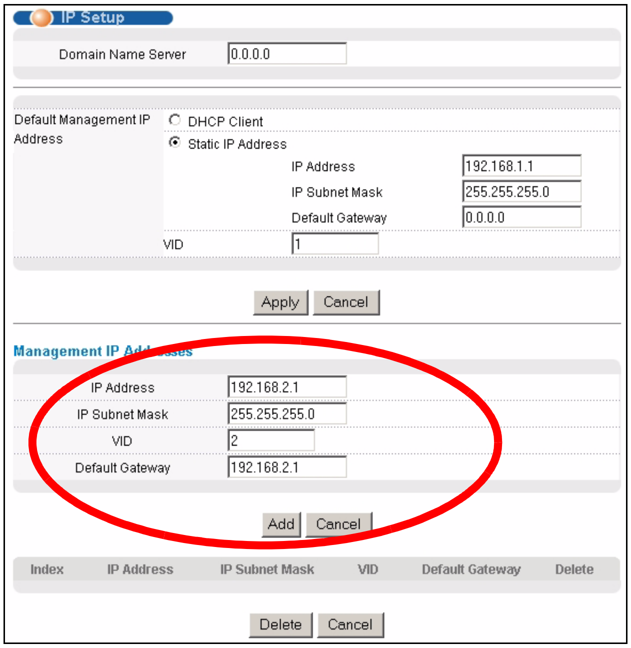
The default management IP address of the Switch is 192.168.1.1. You can configure another IP address in a different subnet for management purposes. The following figure shows an example.

Figure 23 Initial Setup Example: Management IP Address



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

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



Domain Name Server: 0.0.0.0

Default Management IP Address: ○ DHCP Client ● Static IP Address

- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0

VID: 1

- IP Address: 192.168.2.1
- IP Subnet Mask: 255.255.255.0
- VID: 2
- Default Gateway: 192.168.2.1

Index	IP Address	IP Subnet Mask	VID	Default Gateway	Delete

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

3 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.

4 Click **Add**.

6

Tutorials

This chapter provides an example of using the web configurator to set up and use the Switch.

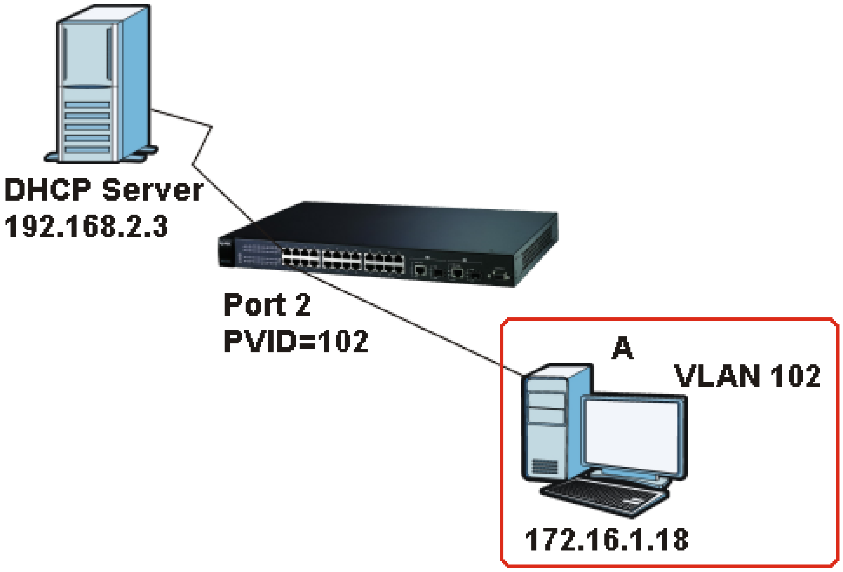
6.1 How to Use DHCP Relay on the Switch

This tutorial describes how to configure your Switch to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

6.1.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 in VLAN 102.

Figure 24 Tutorial: DHCP Relay Scenario



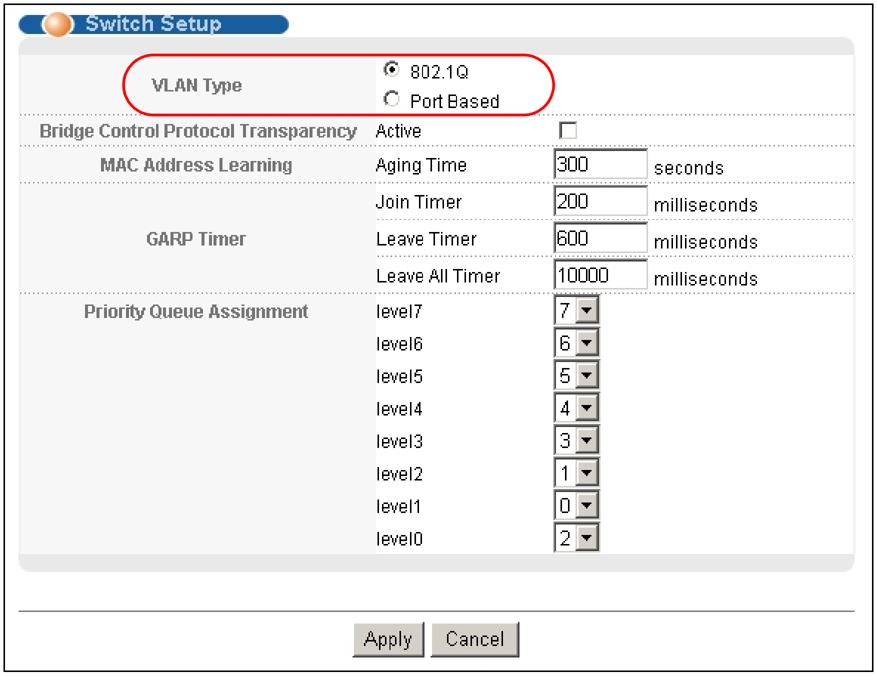
6.1.2 Creating a VLAN

Follow the steps below to configure port 2 as a member of VLAN 102.

1 Access the web configurator through the Switch's management port.

2 Go to **Basic Setting** > **Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.

Figure 25 Tutorial: Set VLAN Type to 802.1Q



VLAN Type	● 802.1Q ○ Port Based		
Bridge Control Protocol Transparency	Active	□	
MAC Address Learning	Aging Time	300	seconds
GARP Timer	Join Timer	200	milliseconds
	Leave Timer	600	milliseconds
	Leave All Timer	10000	milliseconds
Priority Queue Assignment	level7	7	
	level6	6	
	level5	5	
	level4	4	
	level3	3	
	level2	1	
	level1	0	
	level0	2	

3 Click **Advanced Application** > **VLAN > Static VLAN**.

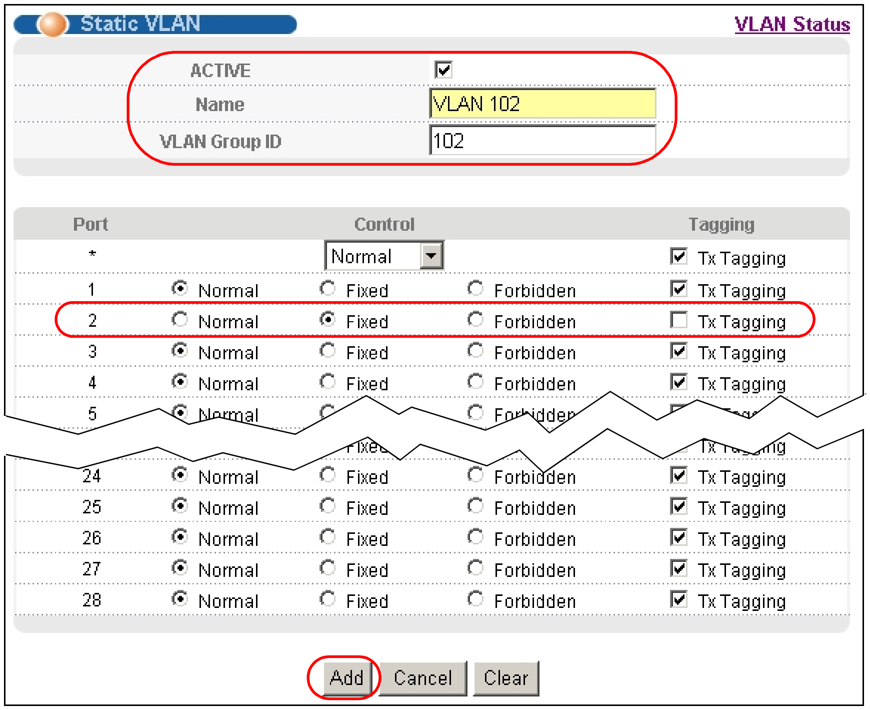
4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VALN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field.

5 Select **Fixed** to configure port 2 to be a permanent member of this VLAN.

6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch’s power is turned off.

Figure 26 Tutorial: Create a Static VLAN

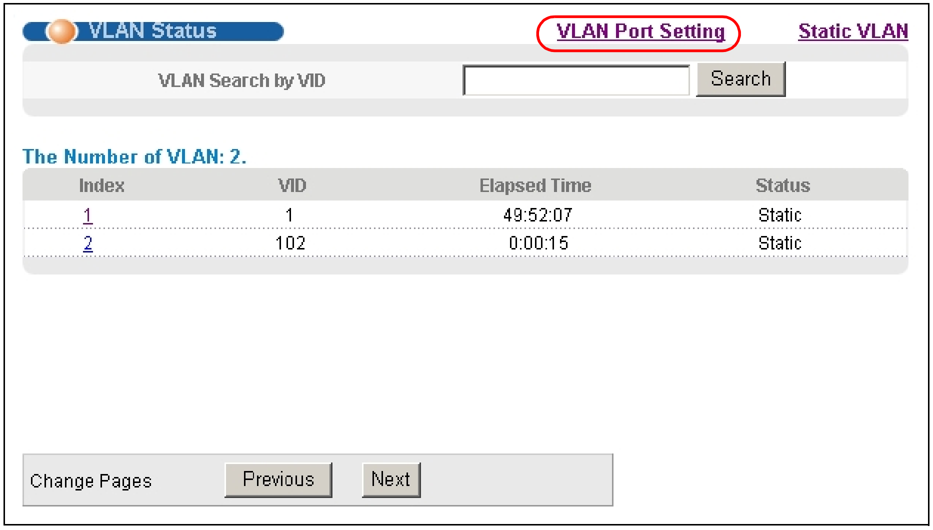


ACTIVE	☑
Name	VLAN 102
VLAN Group ID	102

Port	Control			Tagging
*	Normal			☑ Tx Tagging
1	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
2	○ Normal	● Fixed	○ Forbidden	□ Tx Tagging
3	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
4	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
5	● Normal	○	○ Forbidden	
24	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
25	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
26	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
27	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
28	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

8 Click the **VLAN Status** link in the **Static VLAN** screen and then the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 27 Tutorial: Click the VLAN Port Setting Link



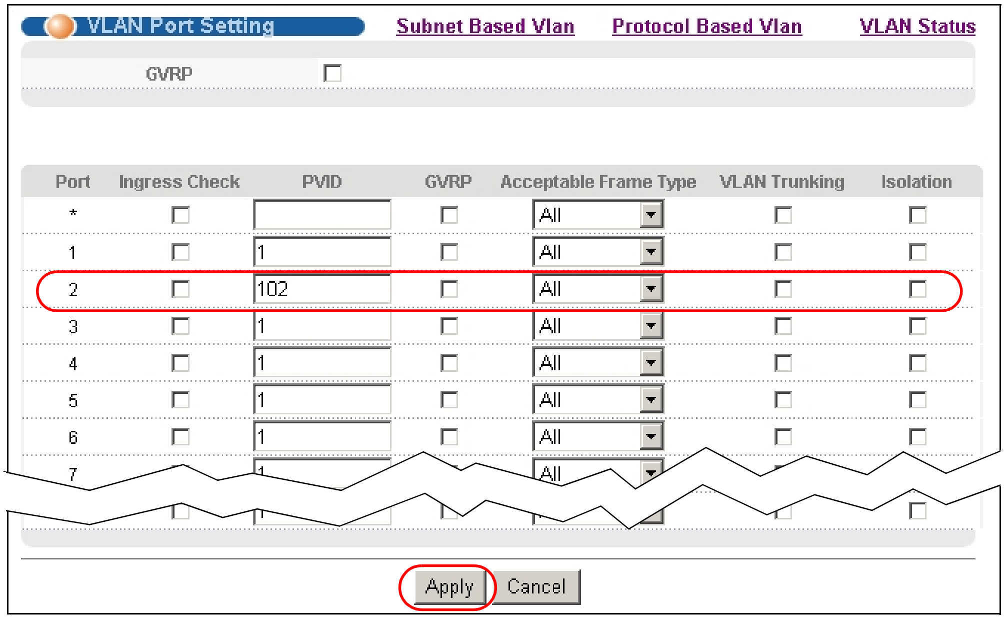
The Number of VLAN: 2.

Index	VID	Elapsed Time	Status
1	1	49:52:07	Static
2	102	0:00:15	Static

9 Enter 102 in the **PVID** field for port 2 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.

10 Click **Apply** to save your changes back to the run-time memory.

Figure 28 Tutorial: Add Tag for Frames Received on Port 2



GVRP □

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	□		□	All	□	□
1	□	1	□	All	□	□
2	□	102	□	All	□	□
3	□	1	□	All	□	□
4	□	1	□	All	□	□
5	□	1	□	All	□	□
6	□	1	□	All	□	□
7		1		All		

11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

6.1.3 Configuring DHCP Relay

Follow the steps below to enable DHCP relay on the Switch and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

1 Click **IP Application > DHCP** and then the **Global** link to open the **DHCP Relay** screen.

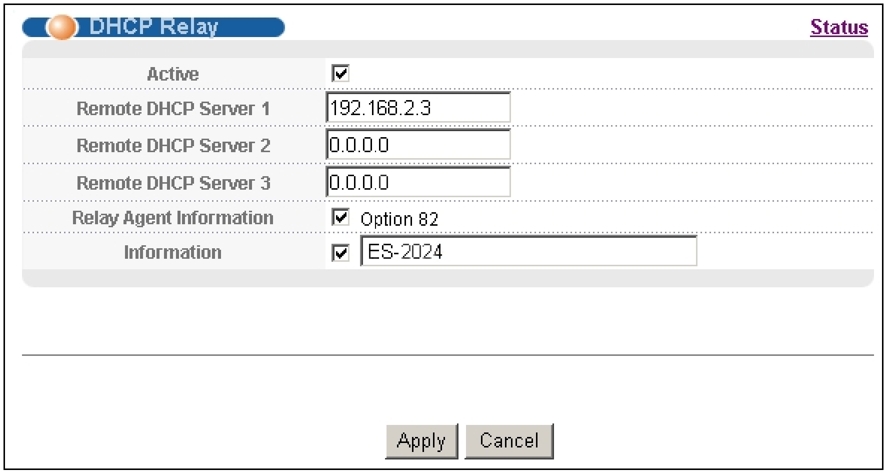
2 Select the **Active** check box.

3 Enter the DHCP server’s IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.

4 Select the **Option 82** and the **Information** check boxes.

5 Click **Apply** to save your changes back to the run-time memory.

Figure 29 Tutorial: Set DHCP Server and Relay Information



DHCP Relay

Status

Active	☑
Remote DHCP Server 1	192.168.2.3
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	☑ Option 82
Information	☑ ES-2024

6 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

7 The DHCP server can then assign a specific IP address based on the DHCP request.

6.1.4 Troubleshooting

Check the client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

1 Client **A** is connected to the Switch's port 2 in VLAN 102.

2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.

3 You clicked the **Save** link on the Switch to have your settings take effect.

7

System Status and Port Statistics

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

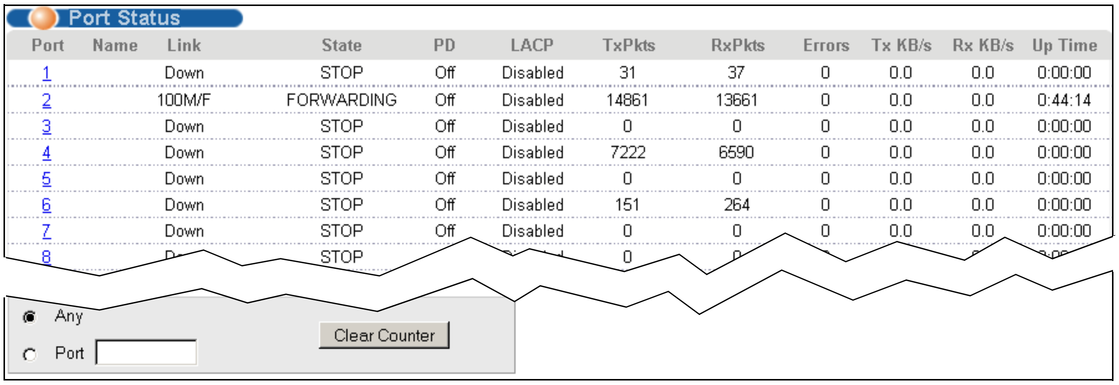
7.1 Overview

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

7.2 Port Status Summary

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

Figure 30 Status



Port Status

Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Off	Disabled	31	37	0	0.0	0.0	0:00:00
2		100M/F	FORWARDING	Off	Disabled	14861	13661	0	0.0	0.0	0:44:14
3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Off	Disabled	7222	6590	0	0.0	0.0	0:00:00
5		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Off	Disabled	151	264	0	0.0	0.0	0:00:00
7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
8			STOP			0					

● Any

○ Port

The following table describes the labels in this screen.

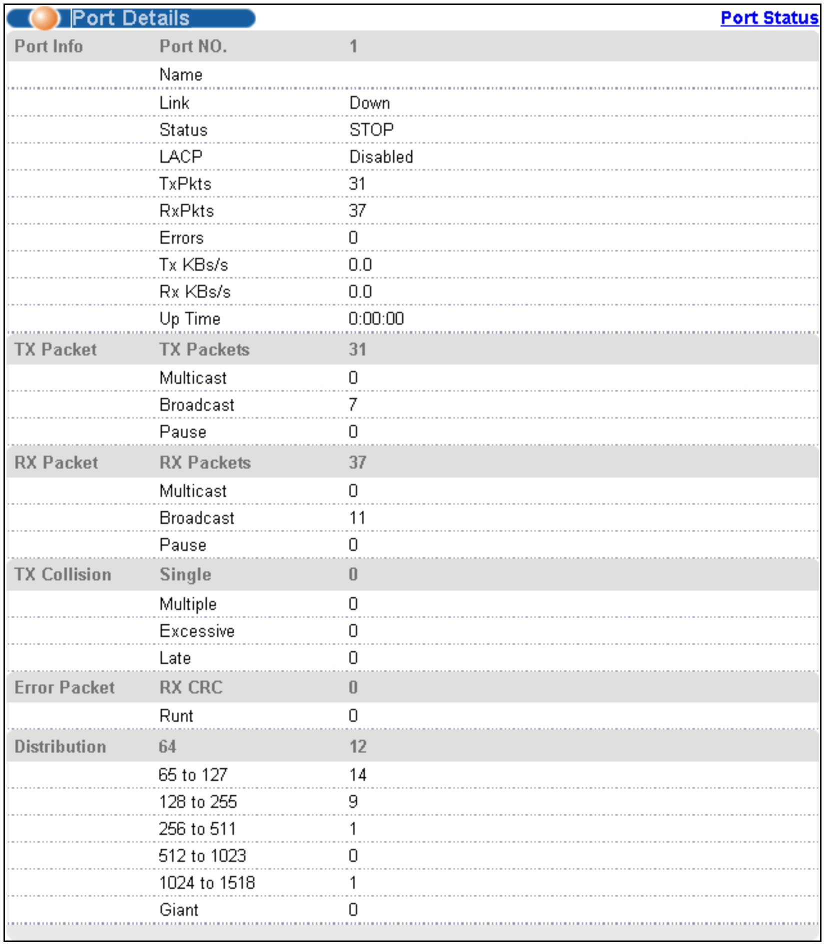
Table 6 Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 31 on page 67).
Name	This is the name you assigned to this port in the **Basic Setting**, **Port Setup** screen.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half). It also shows the cable type (**Copper** or **Fiber**) for the combo ports.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 13.1.3 on page 117 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
PD (PWR model only)	This field displays the current amount of power consumed by devices (powered devices, or PD) that use Power over Ethernet (PoE) to get power from the Switch 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	Enter a port number and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

7.2.1 Status: Port Details

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

Figure 31 Status: Port Details



Port Details

Port Status

Port Info	Port NO.	1
	Name	
	Link	Down
	Status	STOP
	LACP	Disabled
	TxPkts	31
	RxPkts	37
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	0:00:00
TX Packet	TX Packets	31
	Multicast	0
	Broadcast	7
	Pause	0
RX Packet	RX Packets	37
	Multicast	0
	Broadcast	11
	Pause	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Runt	0
Distribution	64	12
	65 to 127	14
	128 to 255	9
	256 to 511	1
	512 to 1023	0
	1024 to 1518	1
	Giant	0

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either **10M** for 10Mbps, **100M** for 100Mbps or **1000M** for 1000Mbps) and the duplex (**F** for full duplex or **H** for half duplex). It also shows the cable type (**Copper** or **Fiber**).

LABEL	DESCRIPTION
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 13.1.3 on page 117 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP.
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 packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	The following fields display detailed information about packets received that were in error.
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).

LABEL	DESCRIPTION
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets dropped because they were bigger than the maximum frame size.

8

Basic Setting

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

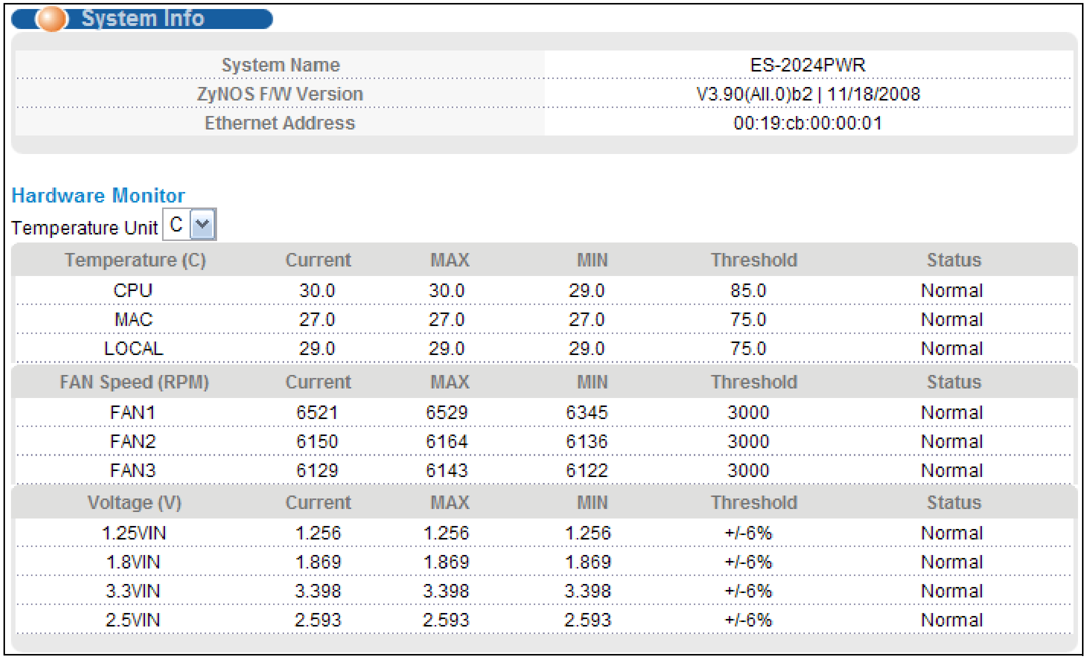
8.1 Overview

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

8.2 System Information

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

Figure 32 Basic Setting > System Info



System Name	ES-2024PWR
ZyNOS F/W Version	V3.90(AII.0)b2 | 11/18/2008
Ethernet Address	00:19:cb:00:00:01

Hardware Monitor

Temperature Unit C

Temperature (C)	Current	MAX	MIN	Threshold	Status
CPU	30.0	30.0	29.0	85.0	Normal
MAC	27.0	27.0	27.0	75.0	Normal
LOCAL	29.0	29.0	29.0	75.0	Normal
FAN Speed (RPM)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
FAN1	6521	6529	6345	3000	Normal
FAN2	6150	6164	6136	3000	Normal
FAN3	6129	6143	6122	3000	Normal
Voltage (V)	**Current**	**MAX**	**MIN**	**Threshold**	**Status**
1.25VIN	1.256	1.256	1.256	+/-6%	Normal
1.8VIN	1.869	1.869	1.869	+/-6%	Normal
3.3VIN	3.398	3.398	3.398	+/-6%	Normal
2.5VIN	2.593	2.593	2.593	+/-6%	Normal

The following table describes the labels in this screen.

Table 7 Basic Setting > 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.
Hardware Monitor (This section is available for the ES-2024 PWR model only)	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**MAC**, **CPU** and **LOCAL** refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature 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.

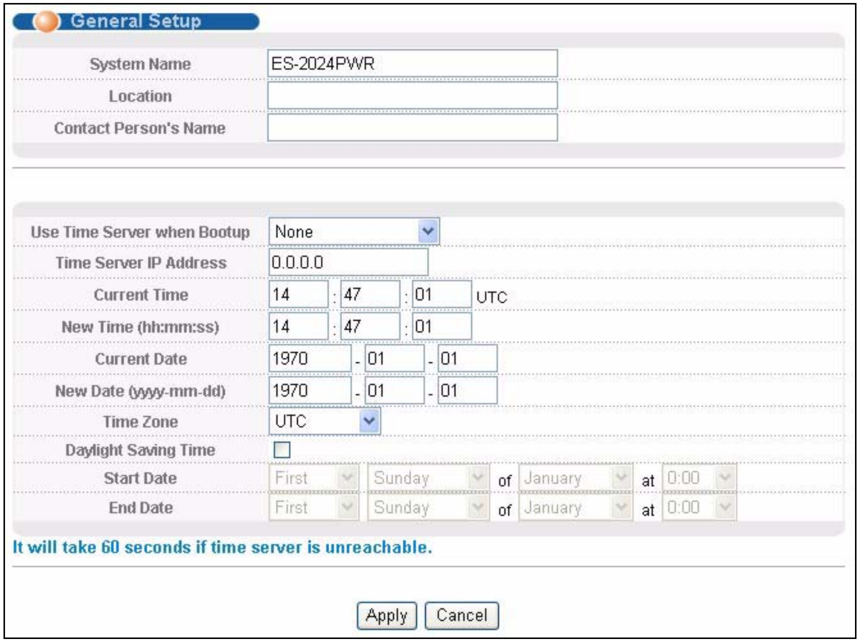
Table 7 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the 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.

8.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

Figure 33 Basic Setting > General Setup



General Setup

System Name	ES-2024PWR
Location	
Contact Person's Name	

Use Time Server when Bootup	None
Time Server IP Address	0.0.0.0
Current Time	14 : 47 : 01 UTC
New Time (hh:mm:ss)	14 : 47 : 01
Current Date	1970 - 01 - 01
New Date (yyyy-mm-dd)	1970 - 01 - 01
Time Zone	UTC
Daylight Saving Time	□
Start Date	First Sunday of January at 0:00
End Date	First Sunday of January at 0:00

It will take 60 seconds if time server is unreachable.

The following table describes the labels in this screen.

Table 8 Basic Setting > 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 of your Switch. You can use up to 32 English keyboard characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 English keyboard characters; spaces are allowed.

Table 8 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your timeserver uses. 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 1970-1-1 0:0:0.
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.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 8 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
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.

8.4 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.

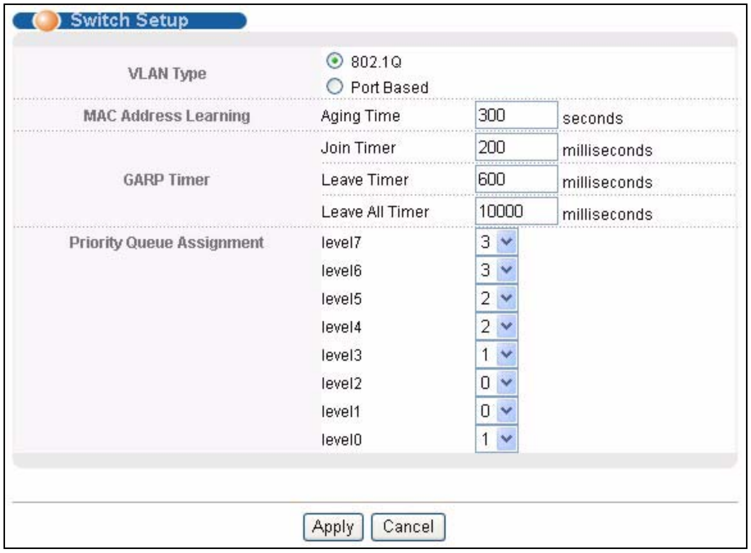
Note: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 9 on page 91 for information on port-based and 802.1Q tagged VLANs.

8.5 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 34 Basic Setting > Switch Setup



Switch Setup

VLAN Type	● 802.1Q ○ Port Based		
MAC Address Learning	Aging Time	300	seconds
GARP Timer	Join Timer	200	milliseconds
	Leave Timer	600	milliseconds
	Leave All Timer	10000	milliseconds
Priority Queue Assignment	level7	3	
	level6	3	
	level5	2	
	level4	2	
	level3	1	
	level2	0	
	level1	0	
	level0	1	

The following table describes the labels in this screen.

Table 9 Basic Setting > 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 9 on page 91 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; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.

Table 9 Basic Setting > 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**; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
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 following 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 begin configuring this screen afresh.

8.6 IP Setup

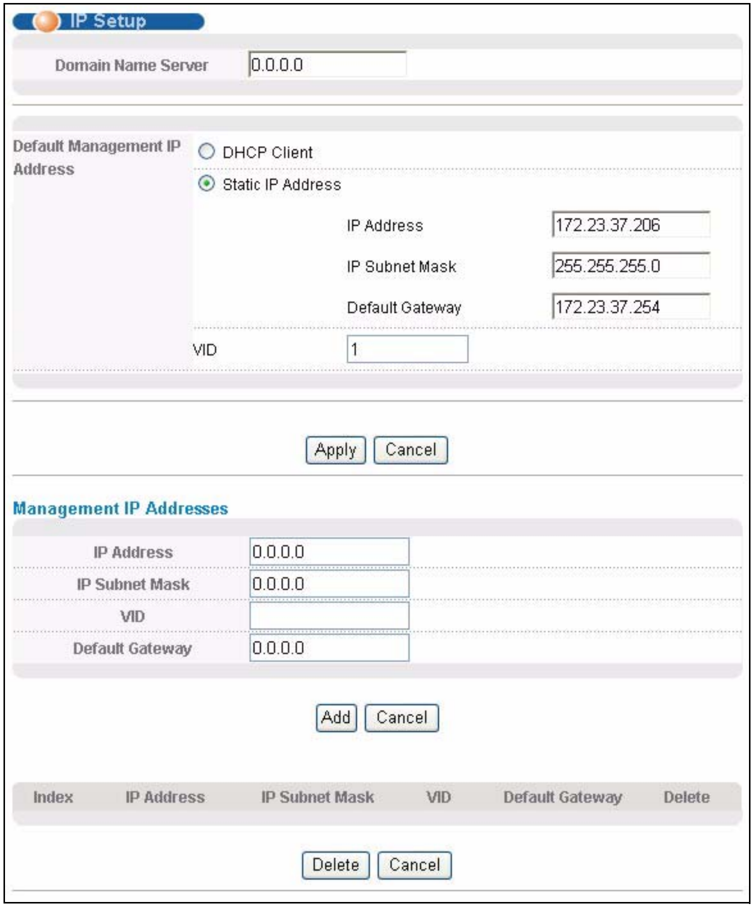
Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.

8.6.1 IP Interfaces

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.

Configure IP addresses for accessing and managing the Switch from the ports belonging to the pre-defined VLAN(s). See Table 102 on page 283 for how many IP addresses you can configure.

Figure 35 Basic Setting > IP Setup



IP Setup

Domain Name Server: 0.0.0.0

Default Management IP Address
○ DHCP Client
● Static IP Address
IP Address: 172.23.37.206
IP Subnet Mask: 255.255.255.0
Default Gateway: 172.23.37.254
VID: 1

Management IP Addresses

IP Address: 0.0.0.0
IP Subnet Mask: 0.0.0.0
VID:
Default Gateway: 0.0.0.0

Index	IP Address	IP Subnet Mask	VID	Default Gateway	Delete

The following table describes the labels in this screen.

Table 10 Basic Setting > 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.	

Table 10 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address and subnet mask, a default gateway IP address and a domain name server IP address.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254
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.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254
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.

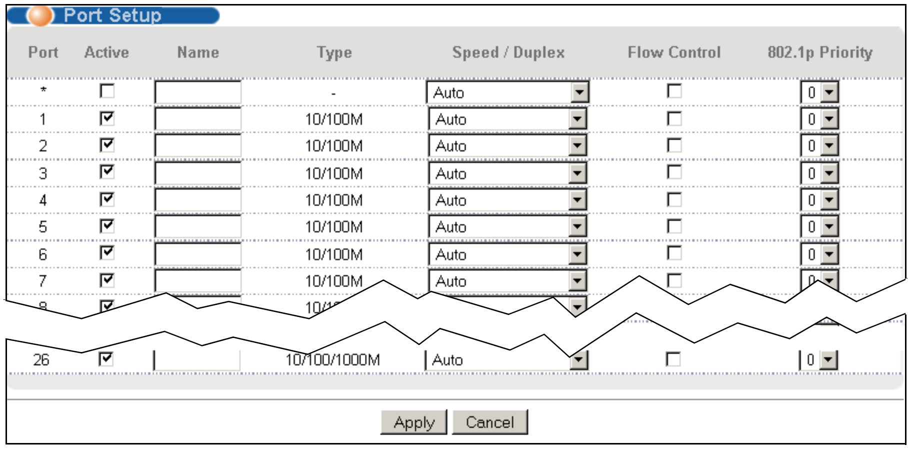
Table 10 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
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.

8.7 Port Setup

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

Figure 36 Basic Setting > Port Setup



Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority
*	□		-	Auto	□	0
1	☑		10/100M	Auto	□	0
2	☑		10/100M	Auto	□	0
3	☑		10/100M	Auto	□	0
4	☑		10/100M	Auto	□	0
5	☑		10/100M	Auto	□	0
6	☑		10/100M	Auto	□	0
7	☑		10/100M	Auto	□	0
26	☑		10/100/1000M	Auto	□	0

The following table describes the labels in this screen.

Table 11 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. 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.

Table 11 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
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/Fast Ethernet connection and **10/100/1000M** for Gigabit connections.
Speed/ Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. Choices are **Auto**, **10M/Half Duplex**, **10M/Full Duplex**, **100M/ Half Duplex**, **100M/Full Duplex** and **1000M/Full Duplex** (for Gigabit ports only). Selecting **Auto** (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses 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 9 on page 77 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.

8.8 PoE Status

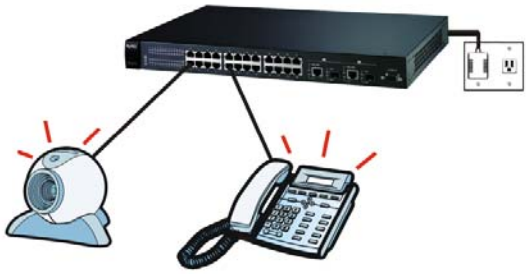
Note: The following screens are available for the ES-2024 PWR model only. Some features are only available for the Fast Ethernet ports (1 to 24).

Your Switch supports IEEE 802.3af Power over Ethernet (PoE).

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.

In the figure below, the IP camera and IP phone get their power directly from the Switch. Aside from minimizing the need for cables and wires, PoE removes the hassle of trying to find a nearby electric outlet to power up devices.

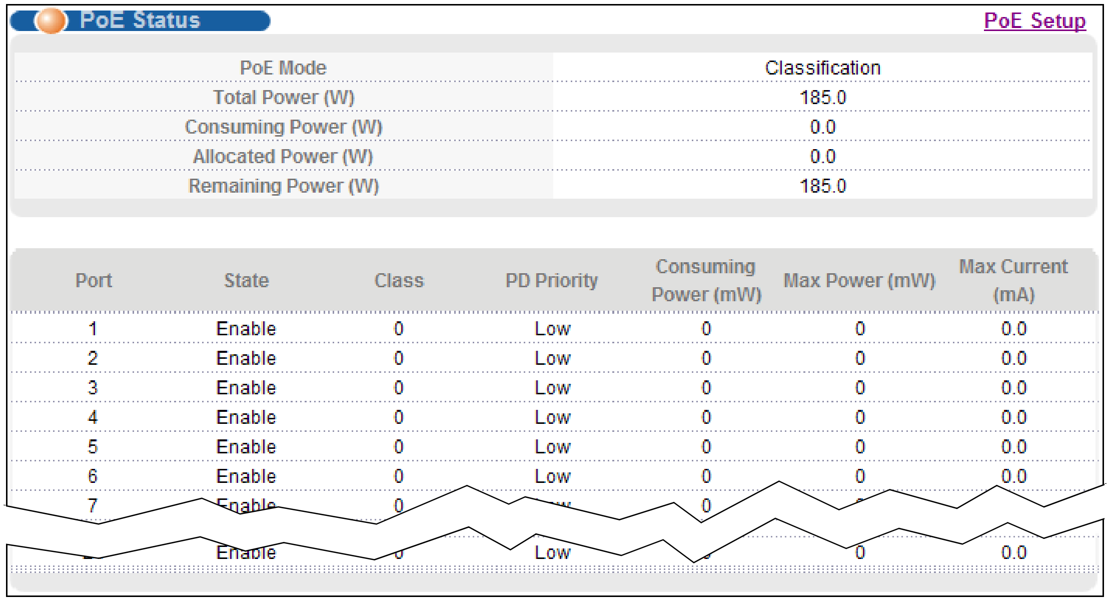
Figure 37 Powered Device Examples



You can also set priorities so that the Switch is able to reserve and allocate power to certain PDs.

To view the current amount of power that PDs are receiving from the Switch, click **Basic Setting** > **PoE Setup**.

Figure 38 Basic Setting > PoE Status



PoE Mode	Classification
Total Power (W)	185.0
Consuming Power (W)	0.0
Allocated Power (W)	0.0
Remaining Power (W)	185.0

Port	State	Class	PD Priority	Consuming Power (mW)	Max Power (mW)	Max Current (mA)
1	Enable	0	Low	0	0	0.0
2	Enable	0	Low	0	0	0.0
3	Enable	0	Low	0	0	0.0
4	Enable	0	Low	0	0	0.0
5	Enable	0	Low	0	0	0.0
6	Enable	0	Low	0	0	0.0
7	Enable	0		0		
	Enable		Low		0	0.0

The following table describes the labels in this screen.

Table 12 Basic Setting > PoE Status

LABEL	DESCRIPTION
PoE Status	
PoE Mode	*This field displays the power management mode used by the Switch, whether it is in* **Classification** *or* **Consumption** *mode.*
Total Power	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). **Consuming Power (W)** can be less than or equal but not more than the **Allocated Power (W)**.
Remaining Power (W)	This field displays the amount of power the Switch can still provide for PoE. Note: The Switch must have at least 16 W of remaining power in order to supply power to a PoE device, even if the PoE device needs less than 16W.
Port	This is the port index number.
State	This field shows which ports can receive power from the Switch. You can set this in Section 8.8.1 on page 85. • **Disable** - The PD connected to this port cannot get power supply. • **Enable** - The PD connected to this port can receive power.

Table 12 Basic Setting > PoE Status (continued)

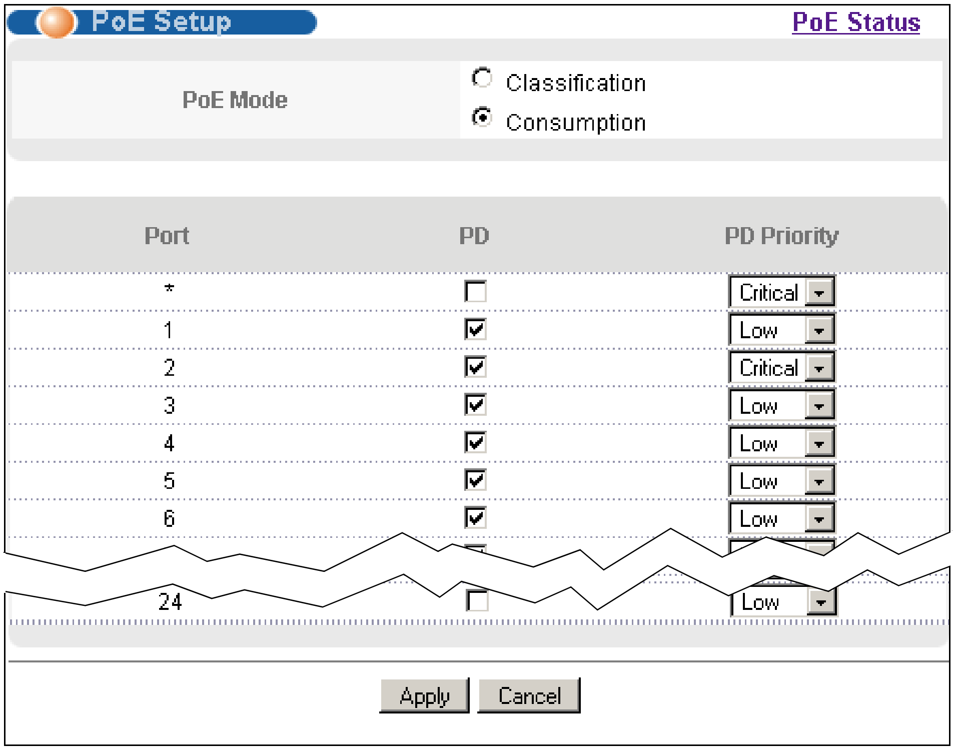
LABEL	DESCRIPTION
Class	This shows the IEEE 802.3af power classification of the PD. This is a number from 0 to 4, where each value represents a range of power (W) and power current (mA) that the PD requires to function. The ranges are as follows. • **Class 0** - Default, 0.44 to 12.94 • **Class 1** - Optional, 0.44 to 3.84 • **Class 2** - Optional , 3.84 to 6.49 • **Class 3** - Optional, 6.49 to 12.95 • **Class 4** - Reserved (PSEs classify as Class 0)
PD Priority	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 first. • **Critical** has the highest priority. • **High** has the Switch assign power to the port after all critical priority ports are served. • **Low** has the Switch assign power to the port after all critical and high priority ports are served.
Consuming Power (mW)	This field displays the current amount of power consumed by the PD from the Switch on this port.
Max Power (mW)	This field displays the maximum amount of power the PD could use from the Switch on this port.
Max Current (mA)	This field displays the maximum amount of current drawn by the PD from the Switch on this port.

8.8.1 PoE Setup

Use this screen to set the priority levels for the Switch in distributing power to PDs.

Click the **PoE Setup** link in the **Basic Setting > PoE Status** screen. The following screen opens.

Figure 39 Basic Setting > PoE Setup



PoE Mode ○ Classification ● Consumption

Port	PD	PD Priority
*	□	Critical
1	☑	Low
2	☑	Critical
3	☑	Low
4	☑	Low
5	☑	Low
6	☑	Low
24	□	Low

The following table describes the labels in this screen.

Table 13 Basic Setting > PoE Setup

LABEL	DESCRIPTION
PoE Mode	*Select the power management mode you want the Switch to use.* • **Classification** - Select this if you want the Switch to reserve the Max Power (mW) to each PD according to the priority level. If the total power supply runs out, PDs with lower priority do not get power to function. • **Consumption** - Select this if you want the Switch to manage the total power supply so that each connected PD gets a resource. However, the power allocated by the Switch may be less than the Max Power (mW) of the PD. PDs with higher priority also get more power than those with lower priority levels.
Port	This is the port index number.
PD	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.

Table 13 Basic Setting > PoE Setup (continued)

LABEL	DESCRIPTION
PD Priority	This field is only available on the PWR model 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 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 begin configuring this screen afresh.

PART III
Advanced Setup

9

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.

9.1 Introduction to IEEE 802.1Q Tagged VLANs

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

9.1.1 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.

9.2 Automatic VLAN Registration

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

9.2.1 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.

9.2.1.1 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.

9.2.2 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 VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 14 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.

Table 14 IEEE 802.1Q VLAN Terminology (continued)

VLAN PARAMETER	TERM	DESCRIPTION
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 VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged 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

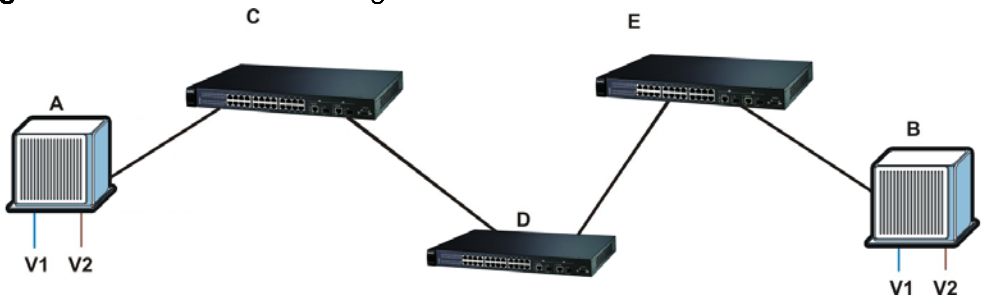
9.3 Port VLAN Trunking

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).

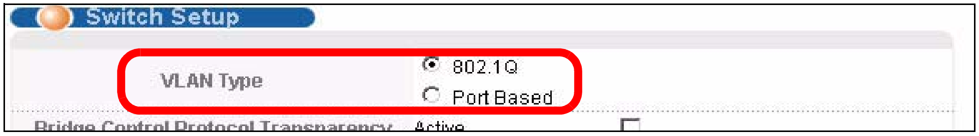
Figure 40 Port VLAN Trunking



9.4 Select the VLAN Type

Select a VLAN type in the **Basic Setting > Switch Setup** screen.

Figure 41 Switch Setup: Select VLAN Type



VLAN Type ● 802.1Q ○ Port Based

Bridge Control Protocol Transparency Active □

9.5 Static VLAN

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

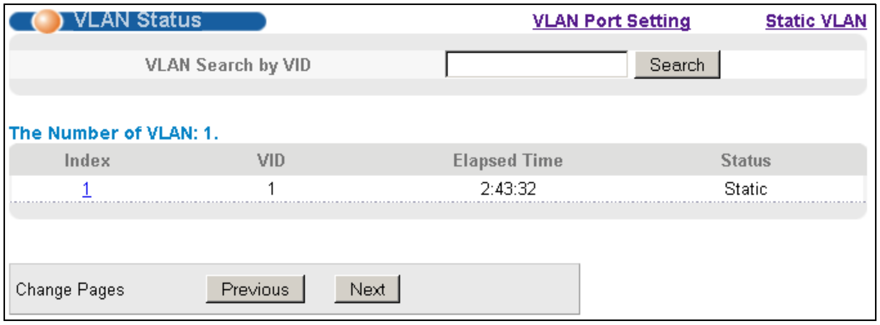
- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

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

9.5.1 Static VLAN Status

See Section 9.1 on page 91 for more information on Static VLAN. Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 42 Advanced Application > VLAN: VLAN Status



The Number of VLAN: 1.

Index	VID	Elapsed Time	Status
1	1	2:43:32	Static

The following table describes the labels in this screen.

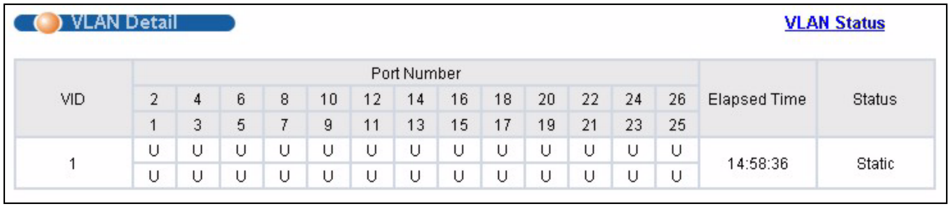
Table 15 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click **Search** to display only the specified VLAN(s) in the list below. Leave this field blank and click **Search** to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the **Search** button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
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 in another way such as via 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.

9.5.2 Static VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See Section 9.1 on page 91 for more information on static VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 43 Advanced Application > VLAN > VLAN Details



VLAN Detail

VLAN Status

VID	Port Number													Elapsed Time	Status
	2	4	6	8	10	12	14	16	18	20	22	24	26		
	1	3	5	7	9	11	13	15	17	19	21	23	25		
1	U	U	U	U	U	U	U	U	U	U	U	U	U	14:58:36	Static
	U	U	U	U	U	U	U	U	U	U	U	U	U		

The following table describes the labels in this screen.

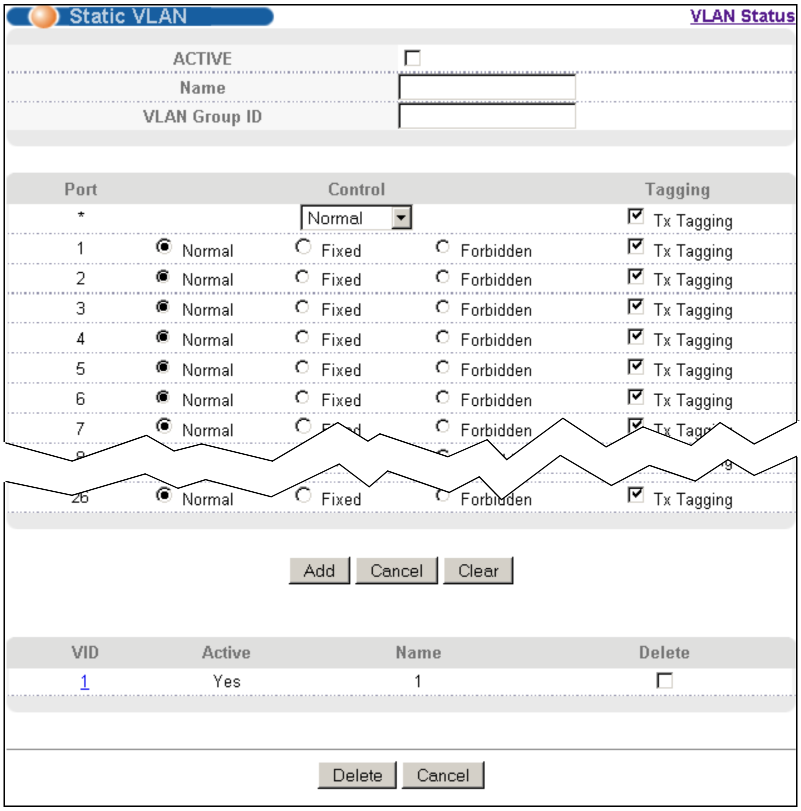
Table 16 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
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 in another way such as via Multicast VLAN Registration (MVR).

9.5.3 Configure a Static VLAN

Use this screen to configure and view 802.1Q VLAN parameters for the Switch. See Section 9.1 on page 91 for more information on static VLAN. To configure a static VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 44 Advanced Application > VLAN > Static VLAN



ACTIVE	□
Name	
VLAN Group ID	

Port	Control			Tagging
*	Normal			☑ Tx Tagging
1	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
2	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
3	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
4	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
5	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
6	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
7	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging
26	● Normal	○ Fixed	○ Forbidden	☑ Tx Tagging

VID	Active	Name	Delete
1	Yes	1	□

The following table describes the related labels in this screen.

Table 17 Advanced Application > 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. This name consists of up to 64 printable characters; spaces are allowed.
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.
*	Settings in this row apply to all ports. 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.

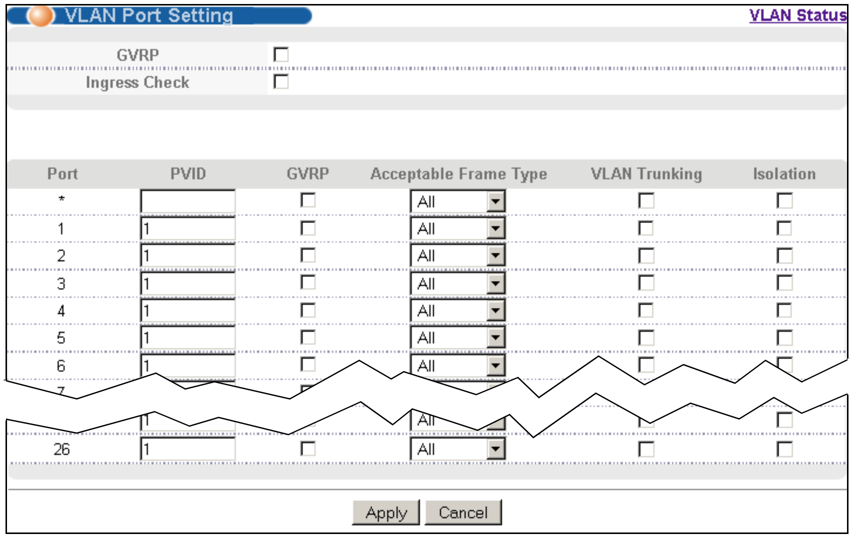
Table 17 Advanced Application > VLAN > Static VLAN (continued)

LABEL	DESCRIPTION
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save 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.
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.

9.5.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See Section 9.1 on page 91 for more information on static VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 45 Advanced Application > VLAN > VLAN Port Settings



GVRP □
Ingress Check □

Port	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*		□	All	□	□
1	1	□	All	□	□
2	1	□	All	□	□
3	1	□	All	□	□
4	1	□	All	□	□
5	1	□	All	□	□
6	1	□	All	□	□
26	1	□	All	□	□

The following table describes the labels in this screen.

Table 18 Advanced Application > 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.
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.
*	Settings in this row apply to all ports. 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.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled.
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.

9.6 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.

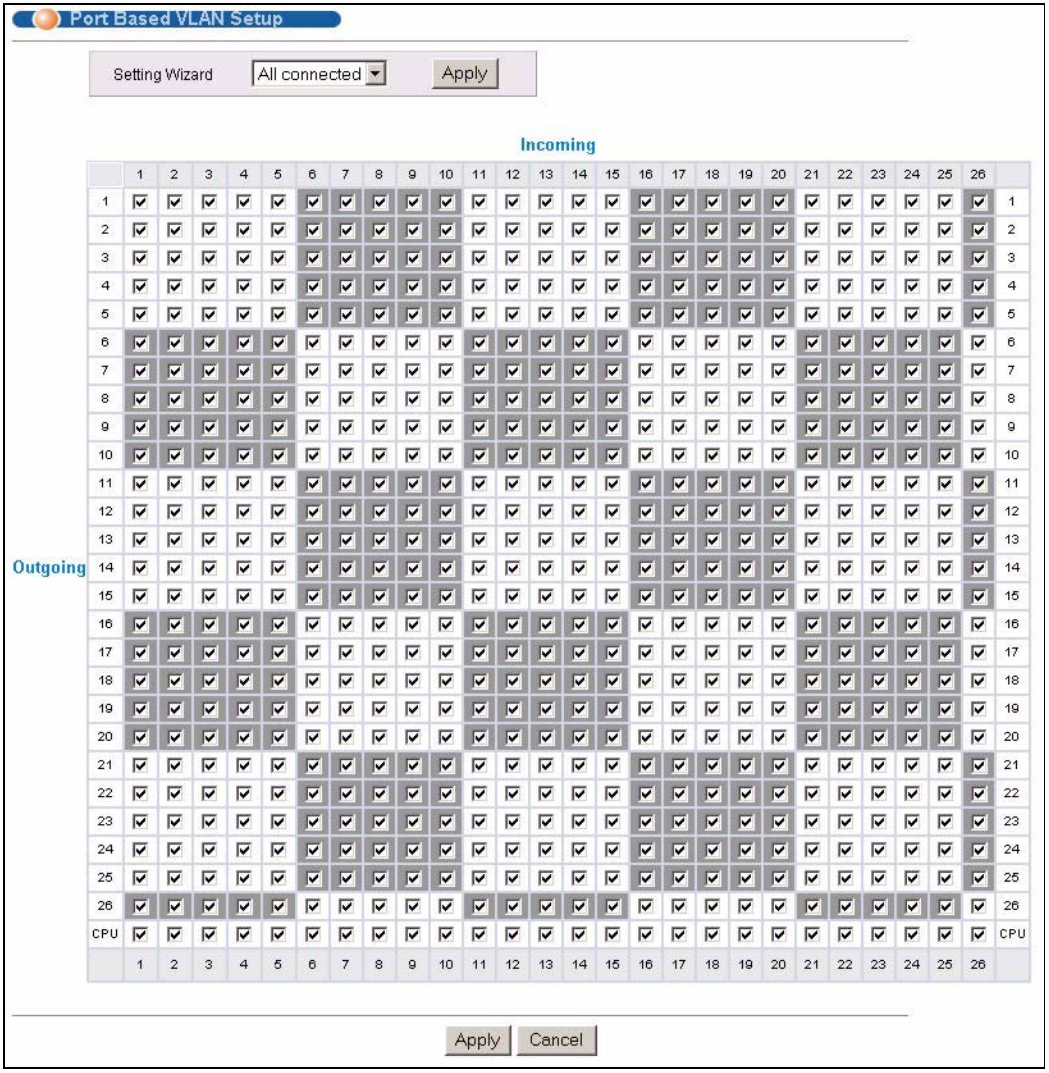
Note: In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

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

9.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN** from the navigation panel to display the next screen.

Figure 46 Advanced Application > VLAN: Port Based VLAN Setup (All Connected)



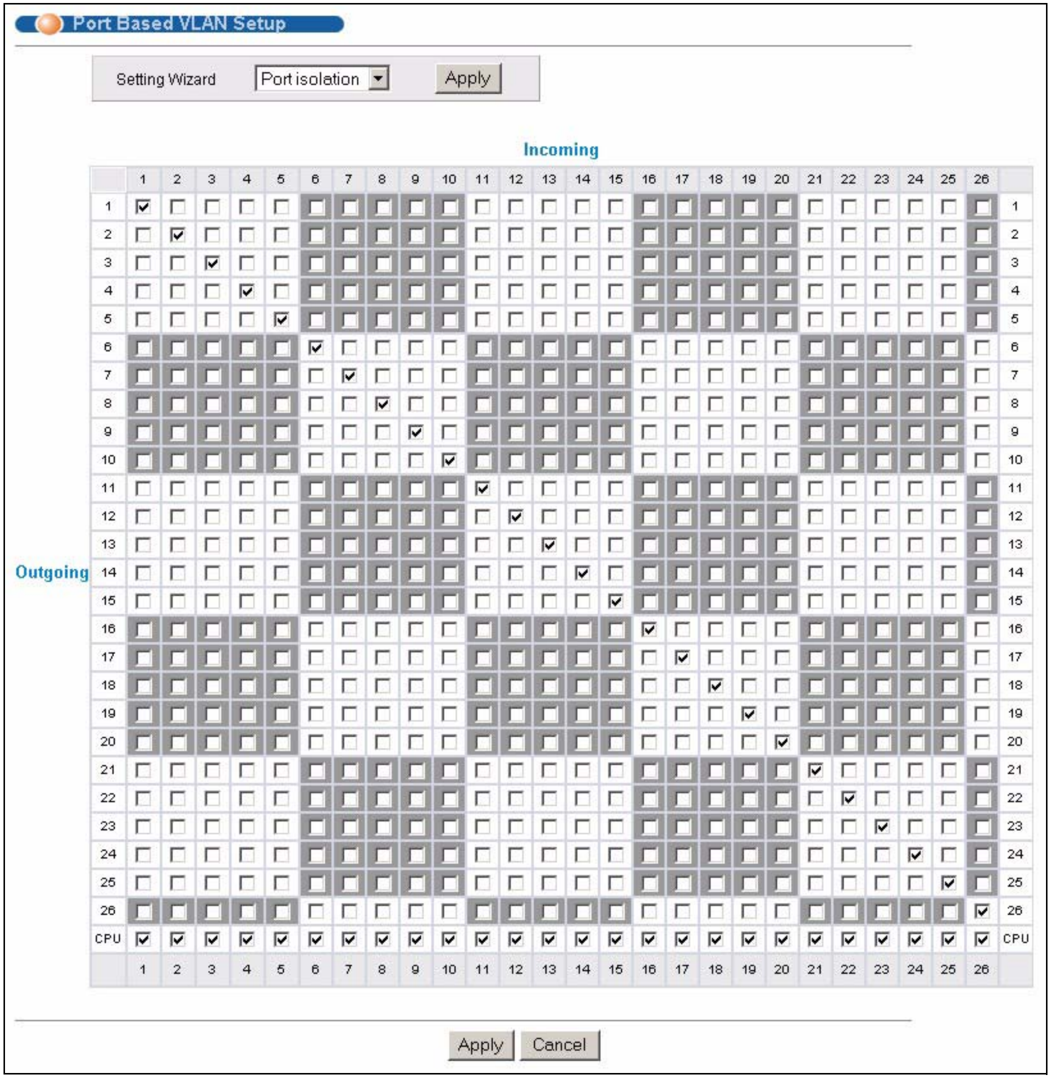
Setting Wizard: All connected

Incoming

Outgoing

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	1
2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	2
3	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	3
4	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	4
5	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	5
6	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	6
7	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	7
8	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	8
9	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	9
10	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	10
11	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	11
12	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	12
13	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	13
14	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	14
15	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	15
16	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	16
17	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	17
18	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	18
19	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	19
20	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	20
21	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	21
22	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	22
23	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	23
24	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	24
25	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	25
26	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	26
CPU	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	CPU
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	

Figure 47 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



Setting Wizard: Port isolation

Incoming

Outgoing

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
1	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	1
2	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	2
3	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	3
4	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	4
5	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	5
6	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	6
7	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	7
8	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	8
9	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	9
10	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	10
11	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	11
12	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	12
13	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	13
14	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	□	14
15	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	□	15
16	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	□	16
17	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	□	17
18	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	□	18
19	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	□	19
20	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	□	20
21	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	□	21
22	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	□	22
23	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	□	23
24	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	□	24
25	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	□	25
26	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	☑	26
CPU	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	CPU
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	

The following table describes the labels in this screen.

Table 19 Advanced Application > VLAN: Port Based VLAN Setup

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

10

Static MAC Forwarding

Use these screens to configure static MAC address forwarding.

10.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

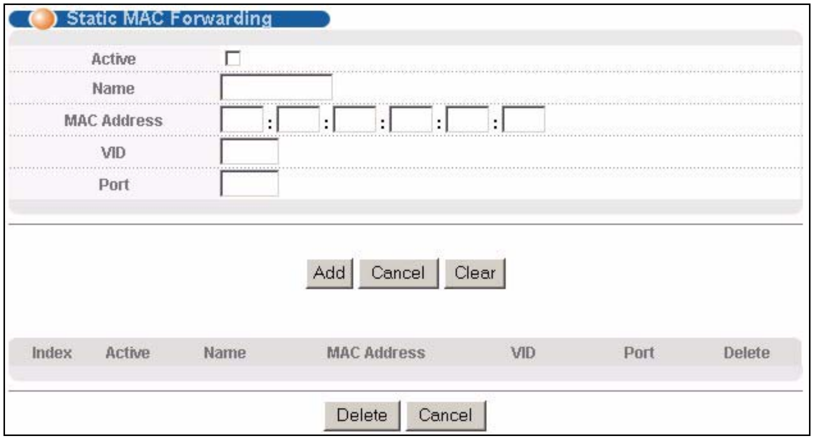
10.2 Configuring Static MAC Forwarding

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 19 on page 149 for more information on port security.

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

Figure 48 Advanced Application > Static MAC Forwarding



The following table describes the labels in this screen.

Table 20 Advanced Application > 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 port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save your rule to the Switch’s run-time memory. The Switch loses this rule 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.
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 ID number of the VLAN group.

Table 20 Advanced Application > Static MAC Forwarding (continued)

LABEL	DESCRIPTION
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.

11

Static Multicast Forwarding

Use these screens to configure static Multicast address forwarding.

11.1 Static Multicast Forwarding Overview

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. Figure 49 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. Figure 50 shows frames being forwarded to devices connected to port 3. Figure 51 shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 49 No Static Multicast Forwarding

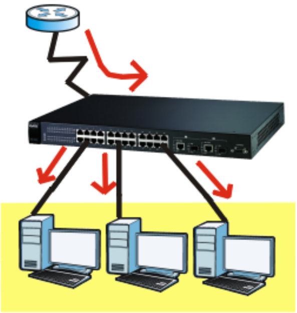


Figure 50 Static Mutlicast Forwarding to A Single Port

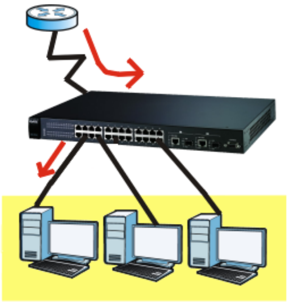
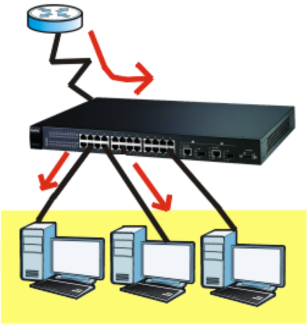


Figure 51 Static Mutlicast Forwarding to Multiple Ports

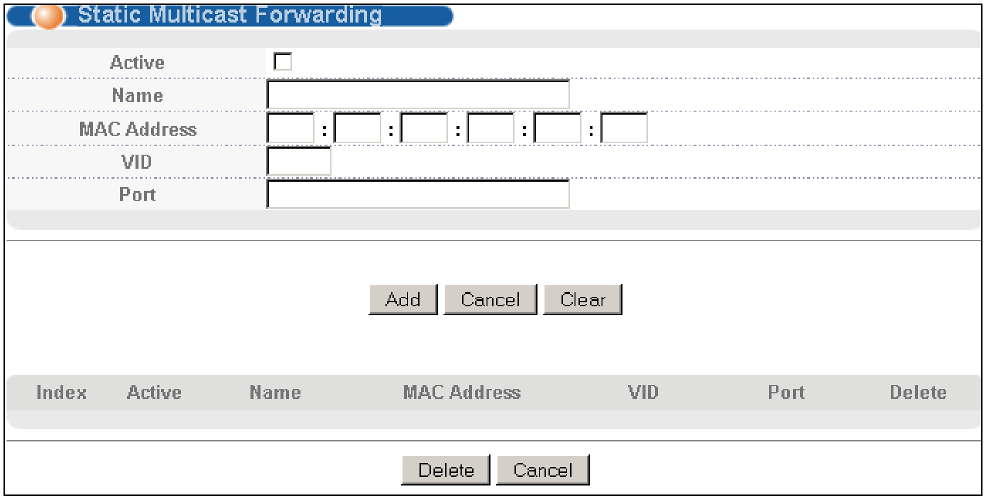


11.2 Configuring Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

Click **Advanced Applications** > **Static Multicast Forwarding** to display the configuration screen as shown.

Figure 52 Advanced Application > Static Multicast Forwarding



The following table describes the labels in this screen.

Table 21 Advanced Application > Static Multicast 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	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don’t have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter “3-5” for ports 3, 4, and 5. Enter “3,5,7” for ports 3, 5, and 7.
Add	Click **Add** to save your rule to the Switch’s run-time memory. The Switch loses this rule 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 their last saved values.
Clear	Click **Clear** to begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for port(s).

Table 21 Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
Active	This field displays whether a static multicast 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 a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

12

Filtering

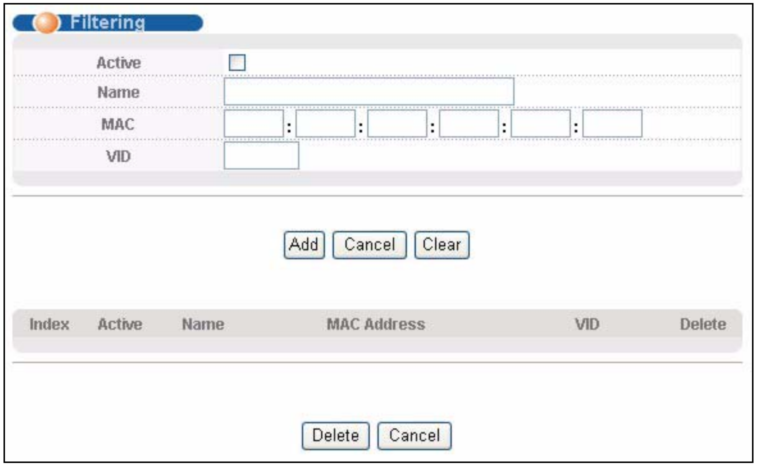
This chapter discusses MAC address port filtering.

12.1 Configure a Filtering Rule

Filtering means sifting traffic going through the Switch based on the MAC addresses and VLAN group (ID).

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

Figure 53 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 22 Advanced Application > 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 English keyboard characters) for this rule. This is for identification only.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.

Table 22 Advanced Application > Filtering (continued)

LABEL	DESCRIPTION
VID	Type the VLAN group identification number.
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 begin configuring this screen afresh.
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 MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

13

Spanning Tree Protocol

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

13.1 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 allows 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.

13.1.1 STP Terminology

The root bridge is the base of the spanning tree.

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

Table 23 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.

13.1.2 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.

13.1.3 STP Port States

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

Table 24 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. Note: The listening state does not exist in RSTP.
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.

13.1.4 Multiple STP

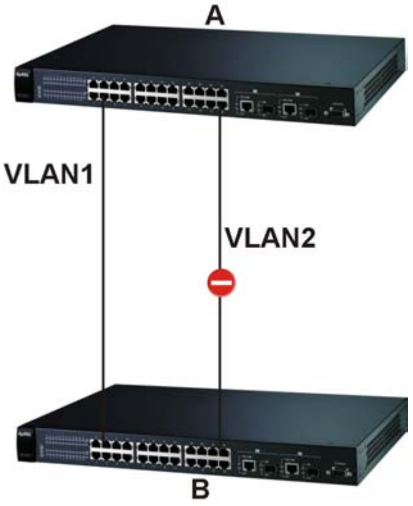
Multiple Spanning Tree Protocol (IEEE 802.1s) is backward compatible with STP/ RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network’s connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

13.1.4.1 MSTP Network Example

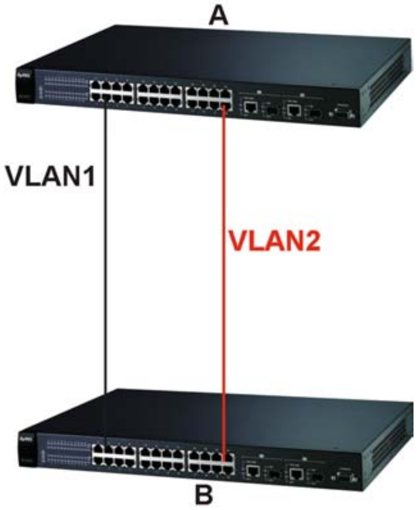
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 54 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 55 MSTP Network Example



13.1.4.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

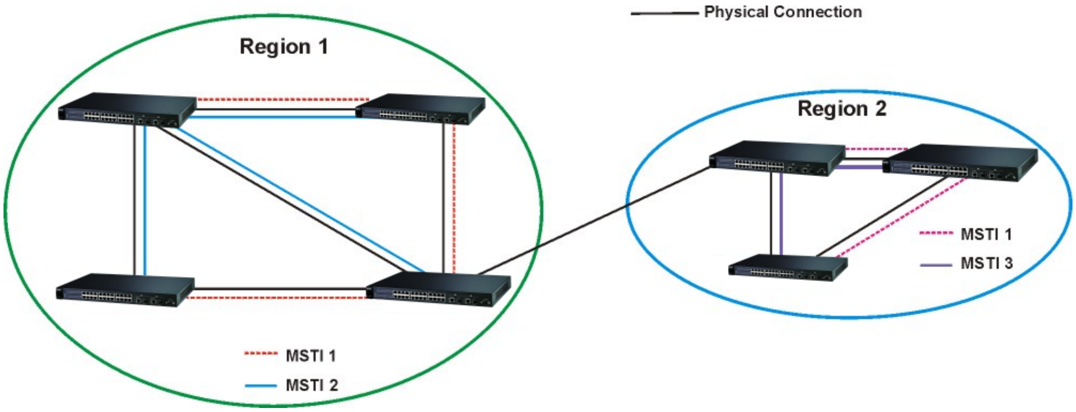
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

13.1.4.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

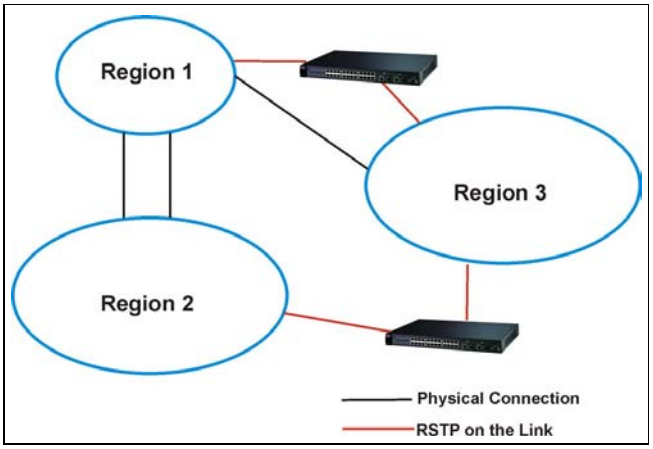
Figure 56 MSTIs in Different Regions



13.1.4.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

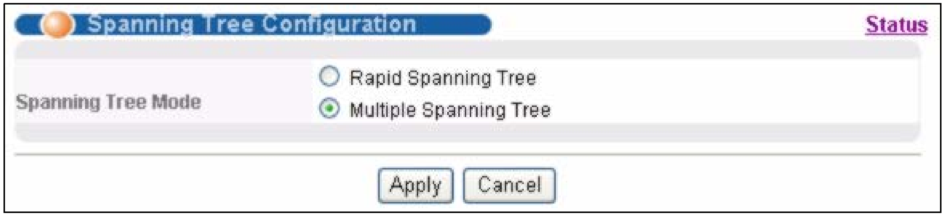
Figure 57 MSTP and Legacy RSTP Network Example



13.2 Spanning Tree Configuration Screen

Use this screen to select the STP mode for the Switch. To open this screen, click **Advanced Application > Spanning Tree Protocol > Configuration**.

Figure 58 Advanced Application> Spanning Tree Protocol > Configuration



Spanning Tree Mode
○ Rapid Spanning Tree
● Multiple Spanning Tree

The following table describes the labels in this screen.

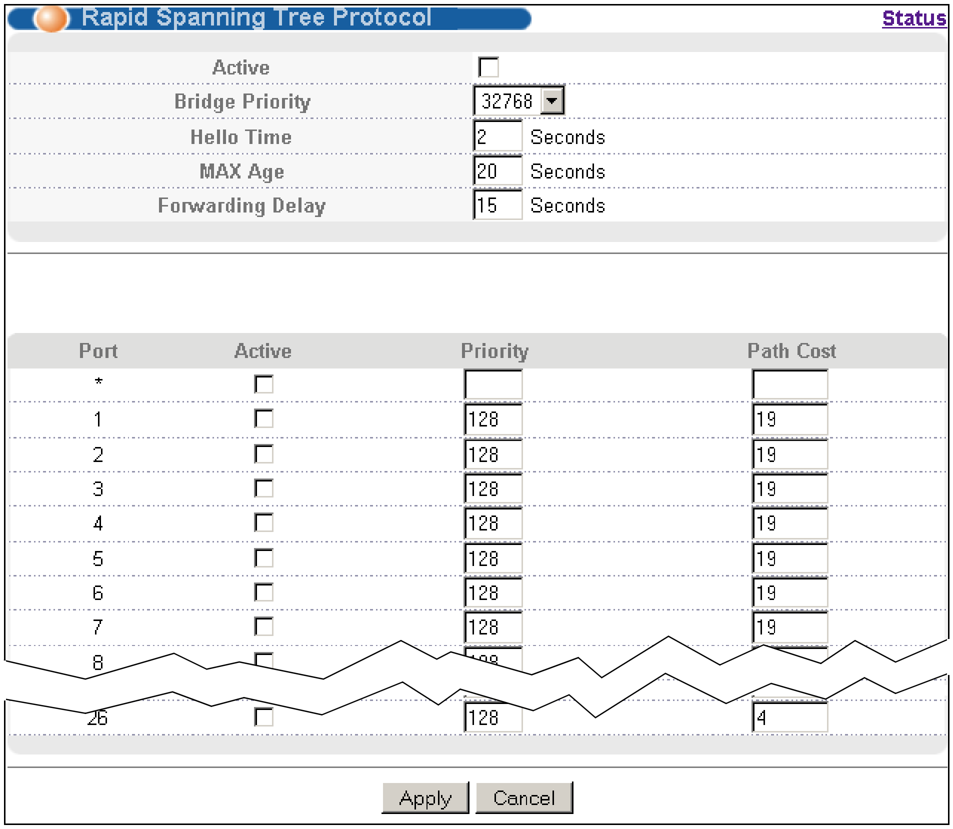
Table 25 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree** or **Multiple Rapid Spanning Tree**. See Section 13.1 on page 115 for background information on STP.
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.

13.3 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 13.1 on page 115 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 59 Advanced Application > Spanning Tree Protocol > RSTP



Active	□
Bridge Priority	32768 ▾
Hello Time	2 Seconds
MAX Age	20 Seconds
Forwarding Delay	15 Seconds

Port	Active	Priority	Path Cost
*	□		
1	□	128	19
2	□	128	19
3	□	128	19
4	□	128	19
5	□	128	19
6	□	128	19
7	□	128	19
8	□		
26	□	128	4

The following table describes the labels in this screen.

Table 26 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 60 on page 123).
Active	Select this check box to activate RSTP. Clear this check box to disable RSTP.

Table 26 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. 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 RSTP 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 recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. See Table 23 on page 116 for more information.

Table 26 Advanced Application > Spanning Tree Protocol > RSTP (continued)

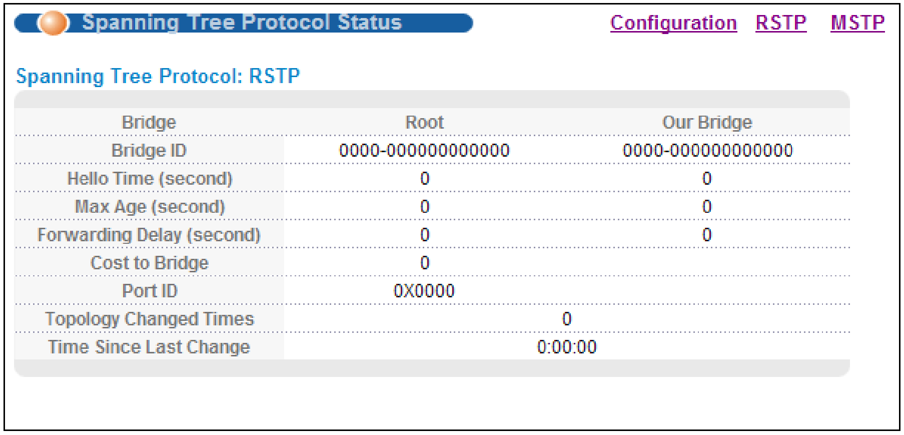
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click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

13.4 Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1 on page 115 for more information on RSTP.

Note: This screen is only available after you activate RSTP on the Switch.

Figure 60 Advanced Application > Spanning Tree Protocol > Status: RSTP



Spanning Tree Protocol Status

Spanning Tree Protocol: RSTP

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	
Port ID	0X0000	
Topology Changed Times	0	
Time Since Last Change	0:00:00	

The following table describes the labels in this screen.

Table 27 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **RSTP** to edit RSTP settings on the Switch.
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.

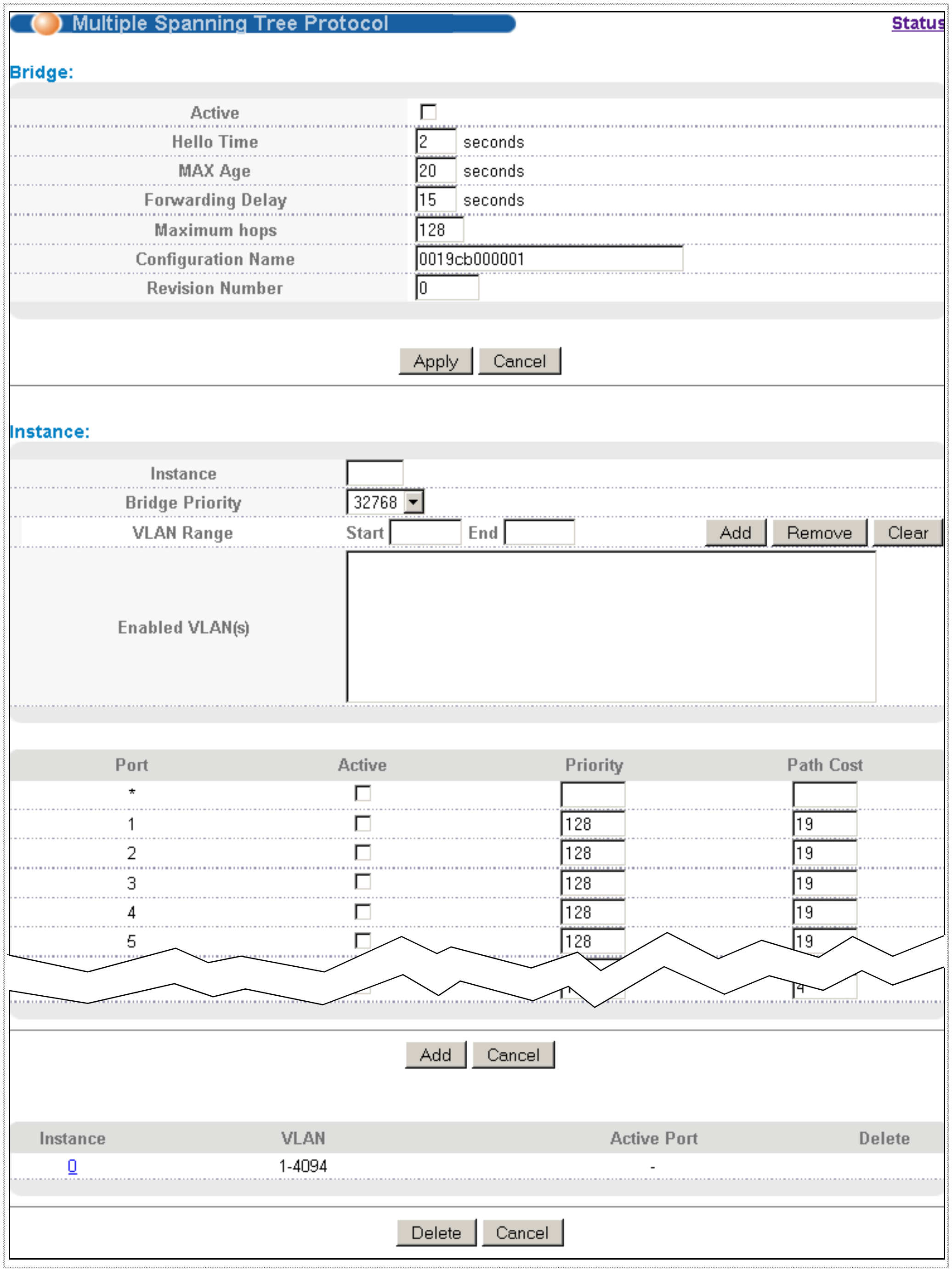
Table 27 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
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.

13.5 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 13.1.4 on page 117 for more information on MSTP.

Figure 61 Advanced Application > Spanning Tree Protocol > MSTP



Bridge:

Active	□
Hello Time	2 seconds
MAX Age	20 seconds
Forwarding Delay	15 seconds
Maximum hops	128
Configuration Name	0019cb000001
Revision Number	0

Instance:

Instance	
Bridge Priority	32768
VLAN Range	Start End
Enabled VLAN(s)	

Port	Active	Priority	Path Cost
*	□		
1	□	128	19
2	□	128	19
3	□	128	19
4	□	128	19
5	□	128	19

Instance	VLAN	Active Port	Delete
0	1-4094	-	

The following table describes the labels in this screen.

Table 28 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen (see Figure 62 on page 128).
Active	Select this check box to activate MSTP on the Switch. Clear this check box to disable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MAX Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
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.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-16.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).

Table 28 Advanced Application > Spanning Tree Protocol > MSTP (continued)

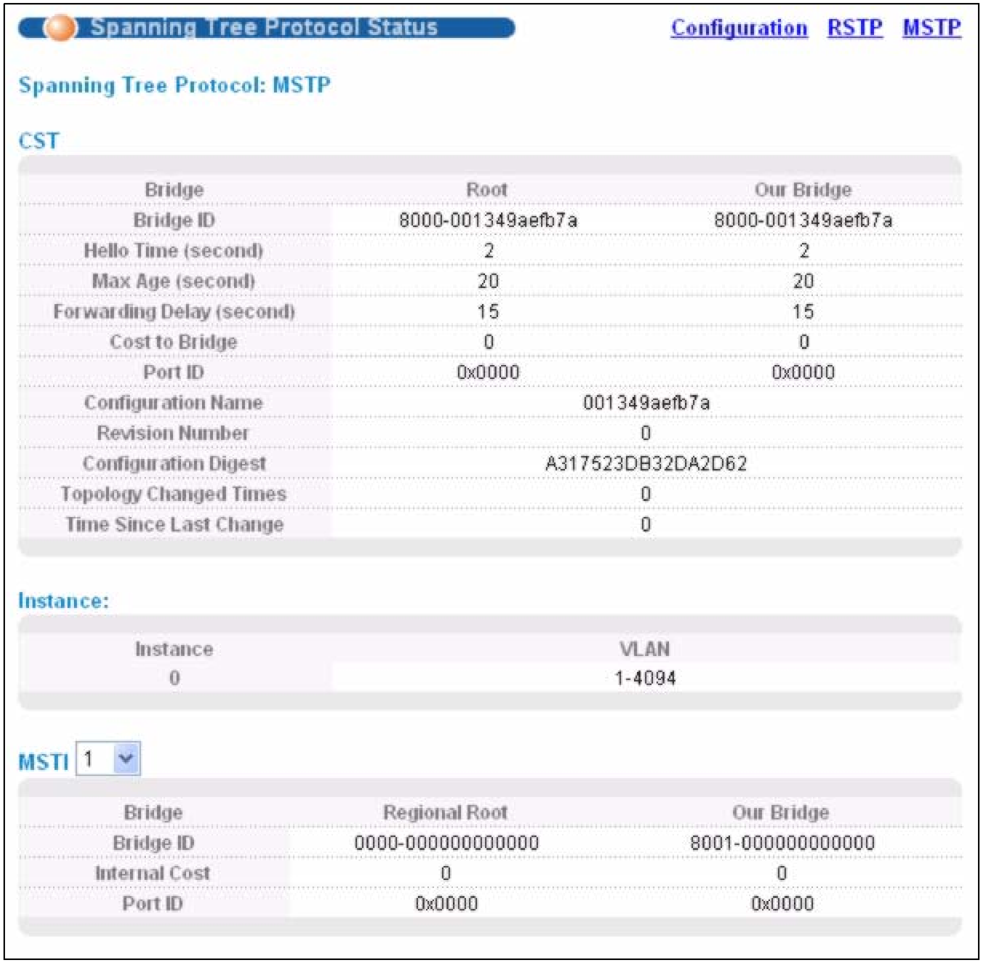
LABEL	DESCRIPTION
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **Start** field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **End** field. Next click: • **Add** - to add this range of VLAN(s) to be mapped to the MST instance. • **Remove** - to remove this range of VLAN(s) from being mapped to the MST instance. • **Clear** - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number.
*	Settings in this row apply to all ports. 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 add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the 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 recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. See Table 23 on page 116 for more information.
Add	Click **Add** to save this MST instance to the Switch's run-time memory. The Switch loses this change 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.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13.6 Multiple Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 13.1.4 on page 117 for more information on MSTP.

Note: This screen is only available after you activate MSTP on the Switch.

Figure 62 Advanced Application > Spanning Tree Protocol > Status: MSTP



Spanning Tree Protocol: MSTP

CST

Bridge	Root	Our Bridge
Bridge ID	8000-001349aefb7a	8000-001349aefb7a
Hello Time (second)	2	2
Max Age (second)	20	20
Forwarding Delay (second)	15	15
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	001349aefb7a	
Revision Number	0	
Configuration Digest	A317523DB32DA2D62	
Topology Changed Times	0	
Time Since Last Change	0	

Instance:

Instance	VLAN
0	1-4094

MSTI 1

Bridge	Regional Root	Our Bridge
Bridge ID	0000-000000000000	8001-000000000000
Internal Cost	0	0
Port ID	0x0000	0x0000

The following table describes the labels in this screen.

Table 29 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MSTP** to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
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.

Table 29 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
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.
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.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
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.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	**Root** refers to the base of the MST instance. **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.
Internal Cost	This is the path cost from the root port in this MST instance to the regional 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 MST instance.

14

Bandwidth Control

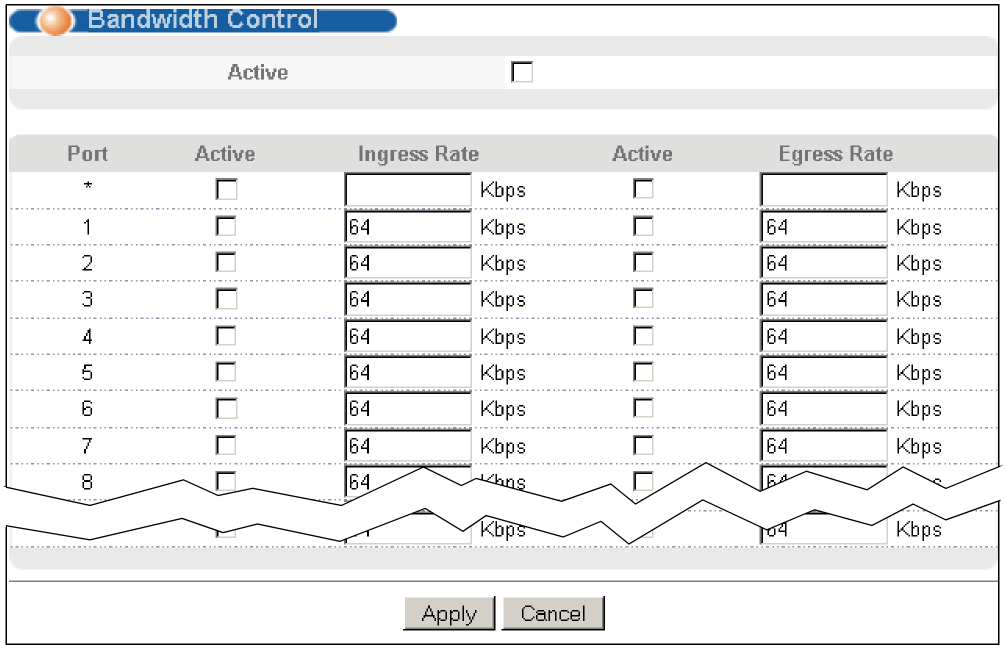
This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

14.1 Bandwidth Control Setup

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

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

Figure 63 Advanced Application > Bandwidth Control



Bandwidth Control

Active □

Port	Active	Ingress Rate		Active	Egress Rate	
*	□		Kbps	□		Kbps
1	□	64	Kbps	□	64	Kbps
2	□	64	Kbps	□	64	Kbps
3	□	64	Kbps	□	64	Kbps
4	□	64	Kbps	□	64	Kbps
5	□	64	Kbps	□	64	Kbps
6	□	64	Kbps	□	64	Kbps
7	□	64	Kbps	□	64	Kbps
8	□	64	Kbps	□	64	
			Kbps		64	Kbps

The following table describes the related labels in this screen.

Table 30 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. 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 begin configuring this screen afresh.

Broadcast Storm Control

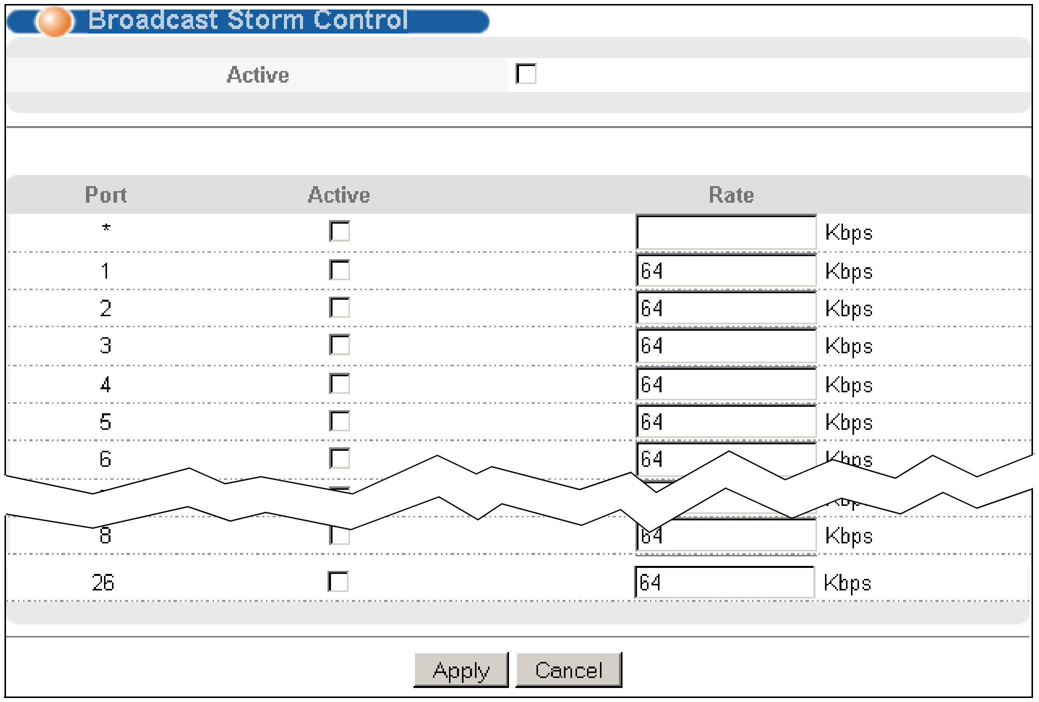
This chapter introduces and shows you how to configure the broadcast storm control feature.

15.1 Broadcast Storm Control Setup

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

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

Figure 64 Advanced Application > Broadcast Storm Control



Broadcast Storm Control

Active □

Port	Active	Rate
*	□	Kbps
1	□	64 Kbps
2	□	64 Kbps
3	□	64 Kbps
4	□	64 Kbps
5	□	64 Kbps
6	□	64 Kbps
8	□	64 Kbps
26	□	64 Kbps

The following table describes the labels in this screen.

Table 31 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays a port number.
*	Settings in this row apply to all ports. 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.

16

Mirroring

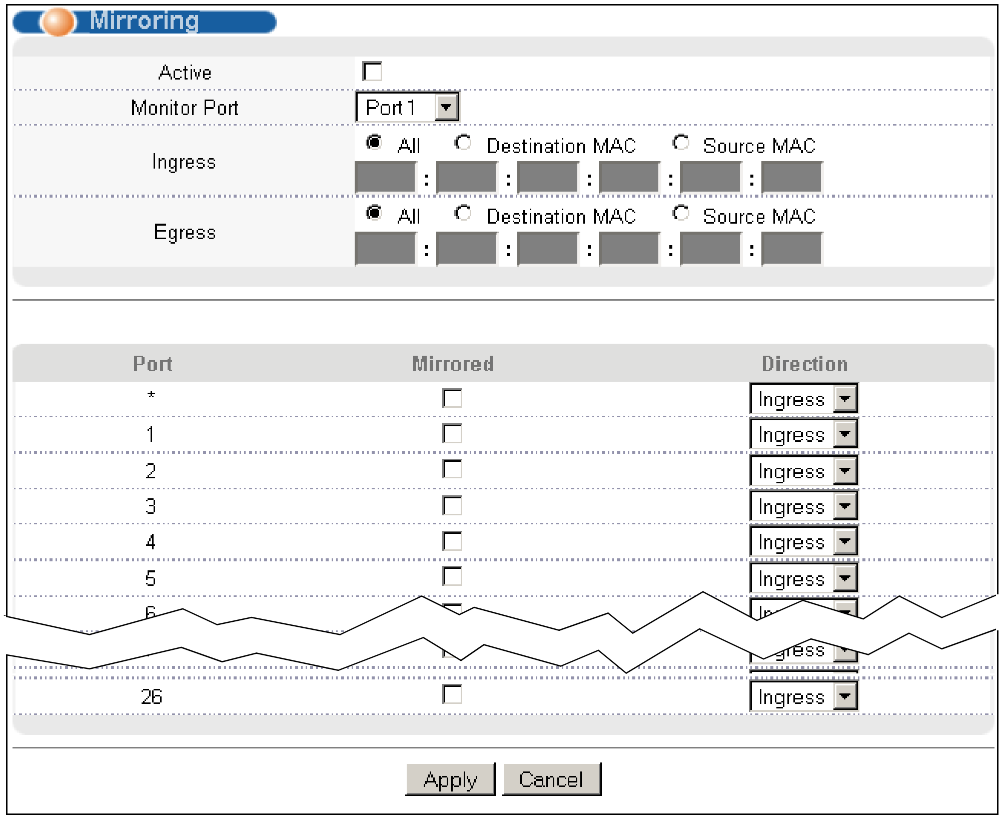
This chapter discusses port mirroring setup screens.

16.1 Port Mirroring Setup

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 monitor port without interference.

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 65 Advanced Application > Mirroring



Mirroring

Active	□
Monitor Port	Port 1
Ingress	● All ○ Destination MAC ○ Source MAC : : : : :
Egress	● All ○ Destination MAC ○ Source MAC : : : : :

Port	Mirrored	Direction
*	□	Ingress
1	□	Ingress
2	□	Ingress
3	□	Ingress
4	□	Ingress
5	□	Ingress
6		In
26	□	Ingress

The following table describes the labels in this screen.

Table 32 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
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). Enter the port number of the monitor port.
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.
*	Settings in this row apply to all ports. 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.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. 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 begin configuring this screen afresh.

17

Link Aggregation

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

17.1 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.

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See Section 17.6 on page 142 for a static port trunking example.

17.2 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.

17.2.1 Link Aggregation ID

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

Table 33 Link Aggregation ID: Local Switch

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

Table 34 Link Aggregation ID: Peer Switch

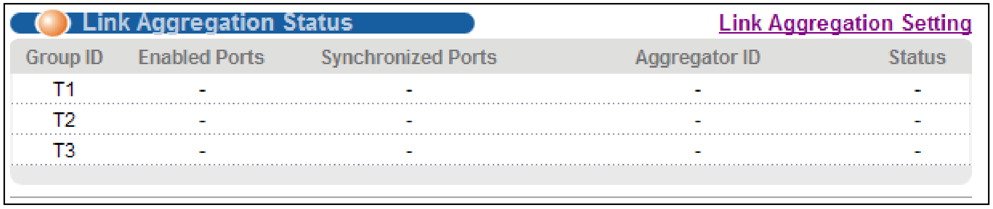
SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00	0000	00	0000

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

17.3 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 17.1 on page 137 for more information.

Figure 66 Advanced Application > Link Aggregation Status



Link Aggregation Status

Link Aggregation Setting

Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Status
T1	-	-	-	-
T2	-	-	-	-
T3	-	-	-	-

The following table describes the labels in this screen.

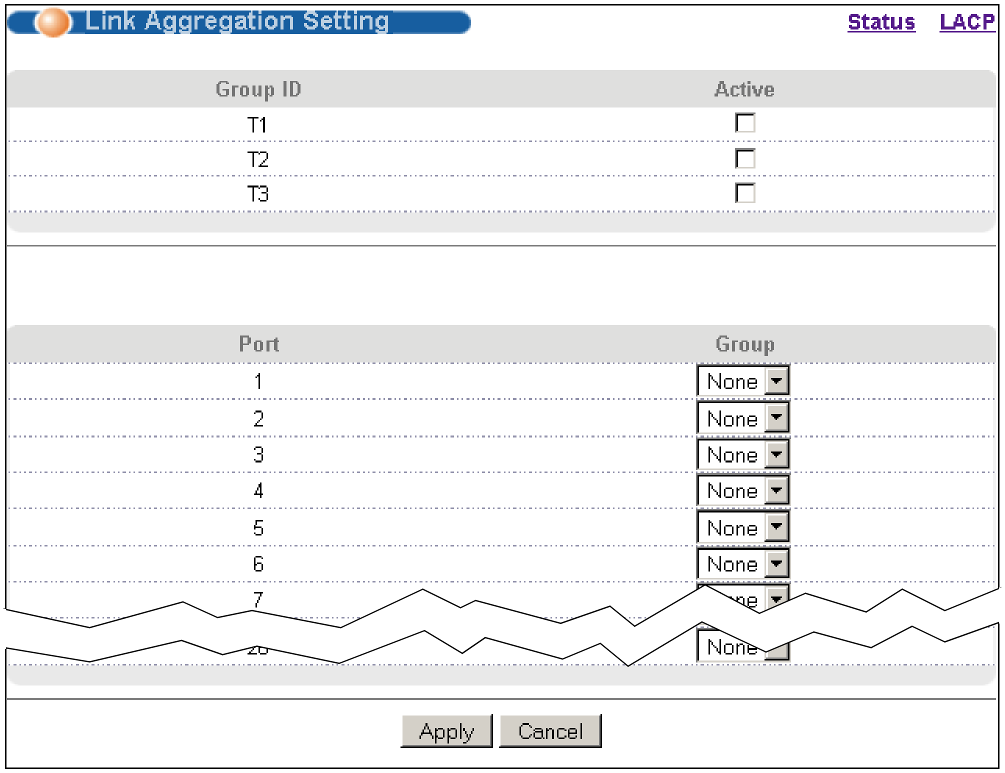
Table 35 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the trunk ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	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.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 17.2.1 on page 138 for more information on this field.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** - if the ports are configured as static members of a trunk group. • **LACP** - if the ports are configured to join a trunk group via LACP.

17.4 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation > Link Aggregation Setting** to display the screen shown next. See Section 17.1 on page 137 for more information on link aggregation.

Figure 67 Advanced Application > Link Aggregation > Link Aggregation Setting



Link Aggregation Setting

Group ID	Active
T1	□
T2	□
T3	□

Port	Group
1	None
2	None
3	None
4	None
5	None
6	None
7	None
28	None

The following table describes the labels in this screen.

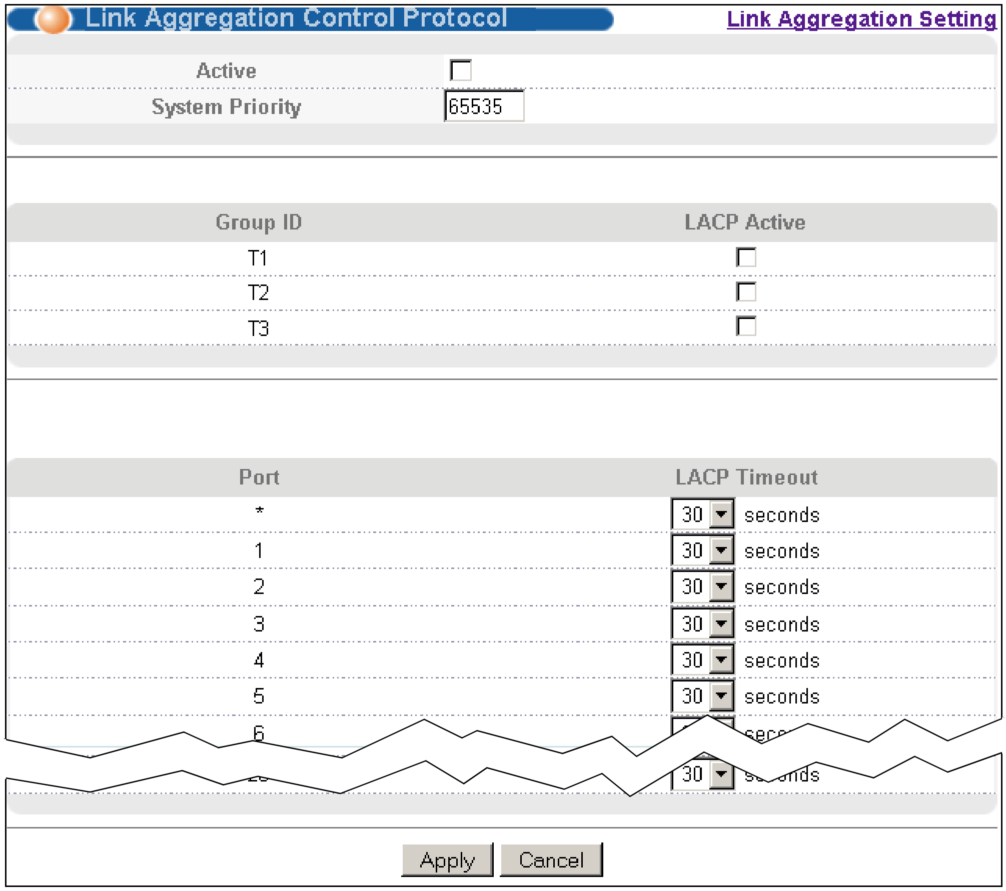
Table 36 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
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.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs.
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.

17.5 Link Aggregation Control Protocol

Click in the **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Section 17.2 on page 137 for more information on dynamic link aggregation.

Figure 68 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



Active	□
System Priority	65535

Group ID	LACP Active
T1	□
T2	□
T3	□

Port	LACP Timeout
*	30 seconds
1	30 seconds
2	30 seconds
3	30 seconds
4	30 seconds
5	30 seconds
6	
	30 seconds

The following table describes the labels in this screen.

Table 37 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).

Table 37 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

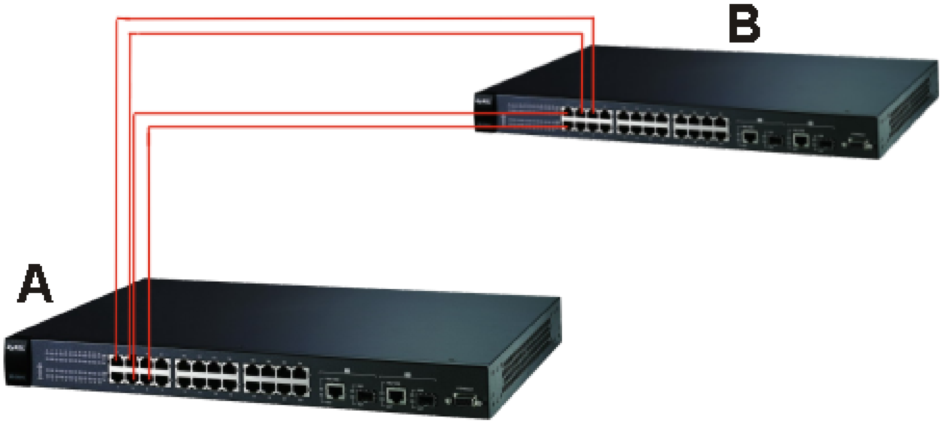
LABEL	DESCRIPTION
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority 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.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.
*	Settings in this row apply to all ports. 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.
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.

17.6 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

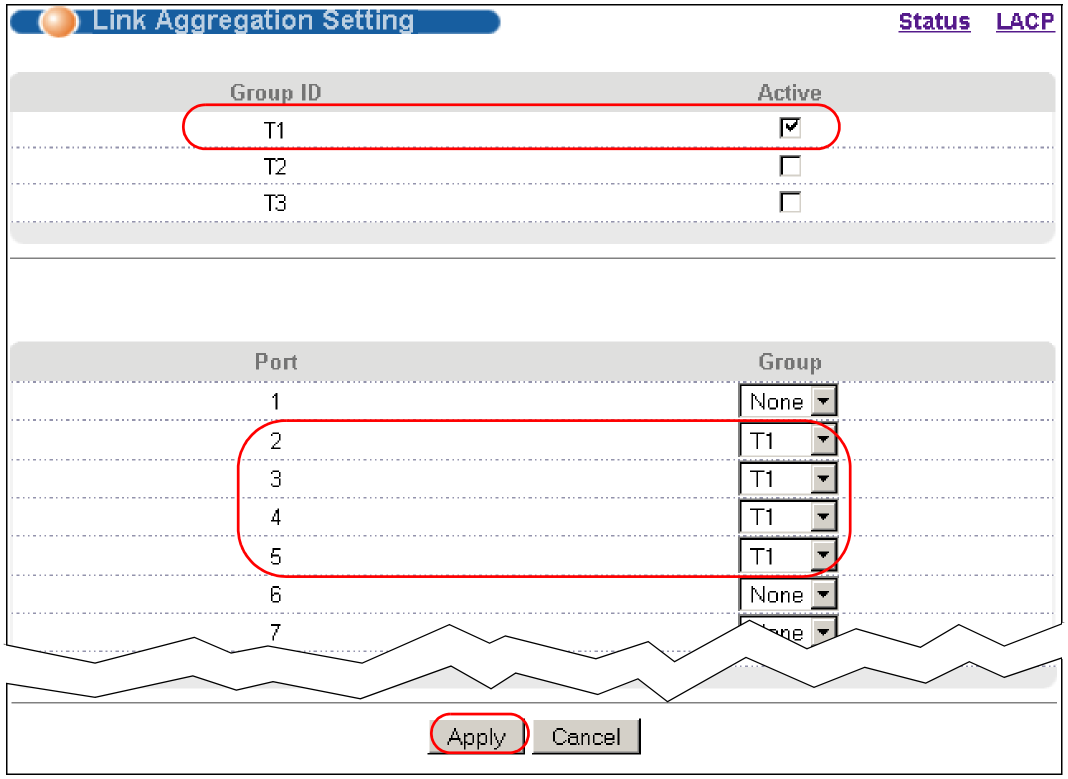
1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 69 Trunking Example - Physical Connections



2 **Configure static trunking** - Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. In this screen activate trunking group **T1** and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 70 Trunking Example - Configuration Screen



Link Aggregation Setting

Group ID	Active
T1	☑
T2	□
T3	□

Port	Group
1	None
2	T1
3	T1
4	T1
5	T1
6	None
7	[illegible]ne

Your trunk group 1 (**T1**) configuration is now complete; you do not need to go to any additional screens.

18

Port Authentication

This chapter describes the IEEE 802.1x methods.

18.1 Port Authentication Overview

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports **IEEE 802.1x**[2] authentication, in which an authentication server validates access to a port based on a username and password provided by the user.

This type of authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 22.1.2 on page 174 for more information on configuring your RADIUS server settings.

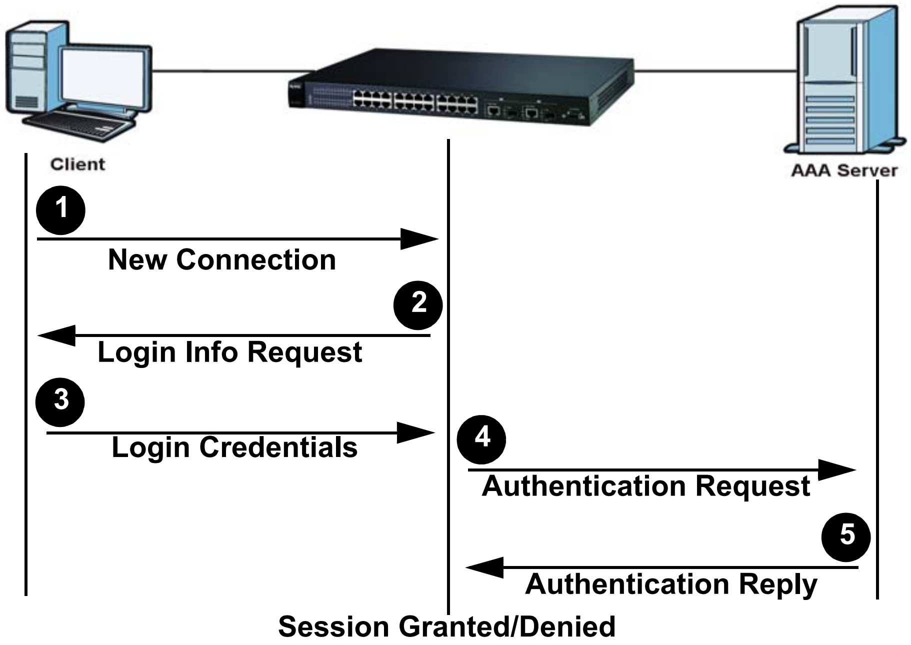
18.1.1 IEEE 802.1x Authentication

The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password. When the client provides the login credentials, the Switch sends an authentication

[2] At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 71 IEEE 802.1x Authentication Process

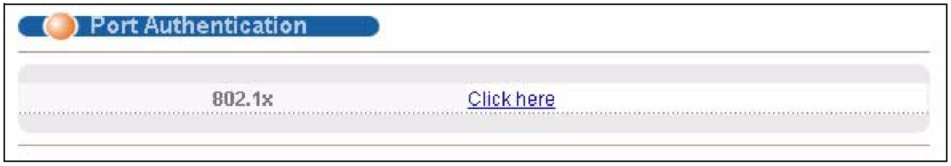


18.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method(s) you want to use (both on the Switch and the port(s)) then configure the RADIUS server settings in the **AAA > Radius Server Setup** screen.

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

Figure 72 Advanced Application > Port Authentication



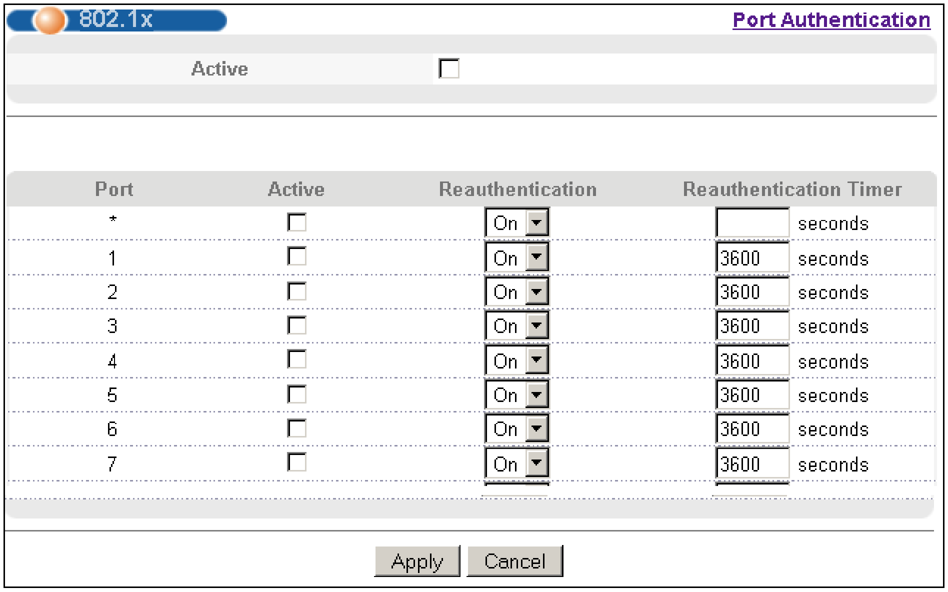
Port Authentication

802.1x	Click here

18.2.1 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

Figure 73 Advanced Application > Port Authentication > 802.1x



802.1x

Active	□

Port	Active	Reauthentication	Reauthentication Timer
*	□	On	seconds
1	□	On	3600 seconds
2	□	On	3600 seconds
3	□	On	3600 seconds
4	□	On	3600 seconds
5	□	On	3600 seconds
6	□	On	3600 seconds
7	□	On	3600 seconds

The following table describes the labels in this screen.

Table 38 Advanced Application > 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.
*	Settings in this row apply to all ports. 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 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.

Table 38 Advanced Application > Port Authentication > 802.1x (continued)

LABEL	DESCRIPTION
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.

19

Port Security

This chapter shows you how to set up port security.

19.1 Port Security 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. See Chapter 10 on page 105 for information on configuring static MAC address forwarding.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. By default, MAC address learning is still enabled even though the port security is not activated.

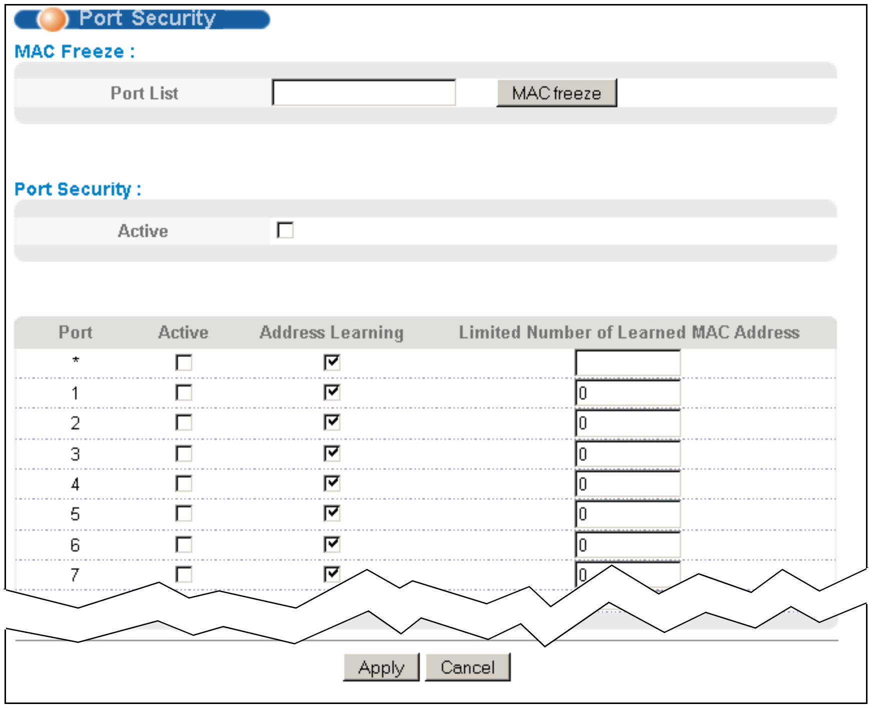
Functionally the Switch allows for three possible outcomes with port security. You can configure the ports to:

- 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 19.3 on page 151 for supported configurations and an example.

19.2 Port Security Setup

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



Port Security

MAC Freeze :

Port List		MAC freeze

Port Security :

Active	□

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	□	☑	
1	□	☑	0
2	□	☑	0
3	□	☑	0
4	□	☑	0
5	□	☑	0
6	□	☑	0
7	□	☑	0

Figure 74 Advanced Application > Port Security

The following table describes the labels in this screen.

Table 39 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click **MAC freeze**, all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the **Static MAC Forwarding** screen.
MAC freeze	Click **MAC freeze** to have the Switch automatically select the **Active** check boxes and clear the **Address Learning** check boxes only for the ports specified in the **Port list**.
Active	Select this check box to enable the port security feature on the Switch.
Port	This field displays a port number.
*	Settings in this row apply to all ports. 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 39 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
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 (activated in the **Basic Settings**, **Port Setup** screen) with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “8192”. “0” means that the limiting of learned addresses is disabled.
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.

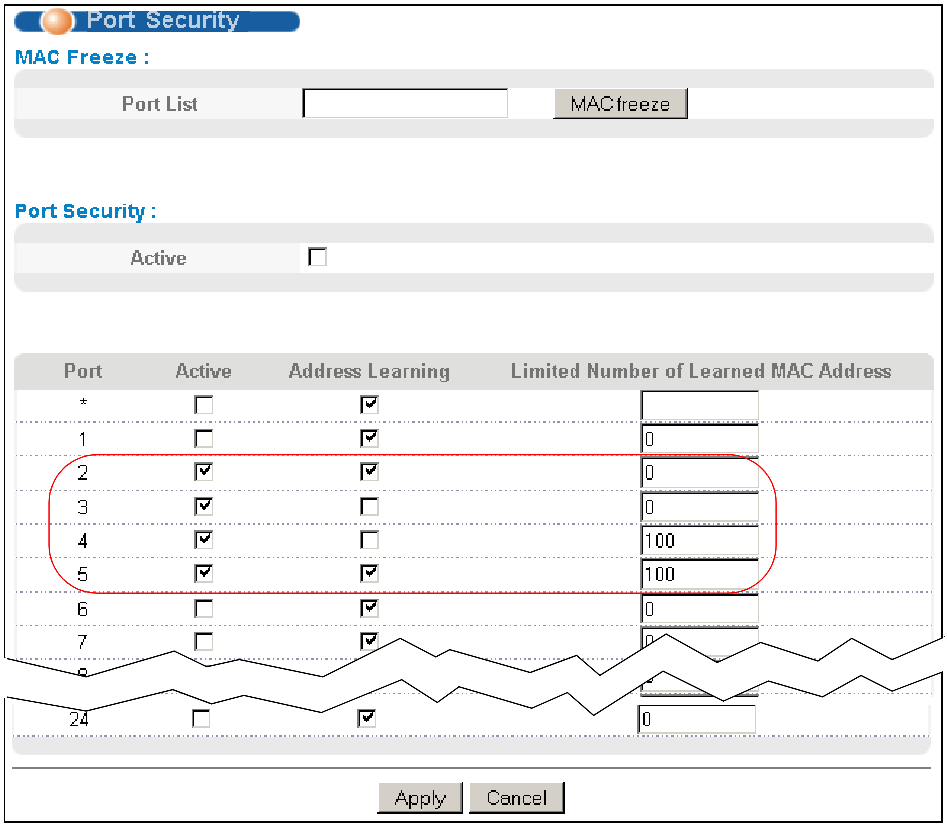
19.3 Port Security Example

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 75 Port Security Example



MAC Freeze :

Port List

Port Security :

Active ☐

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	☐	☑	
1	☐	☑	0
2	☑	☑	0
3	☑	☐	0
4	☑	☐	100
5	☑	☑	100
6	☐	☑	0
7	☐	☑	0
24	☐	☑	0

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

Table 40 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.
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.

20

Queuing Method

This chapter introduces the queuing methods supported.

20.1 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 41 Physical Queue Priority

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

20.1.1 Strictly Priority Queuing

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

20.1.2 Weighted Round Robin Scheduling (WRR)

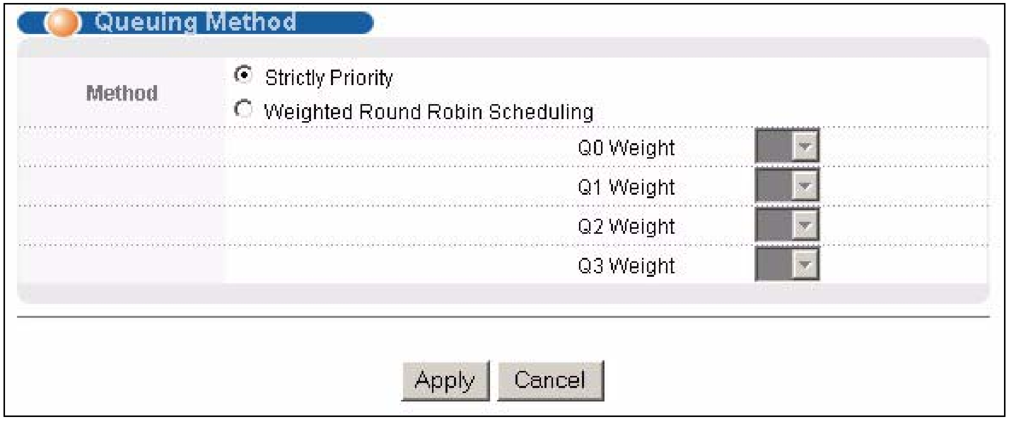
Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is a given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal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

20.2 Configuring Queuing

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

Figure 76 Advanced Application > Queuing Method



Queuing Method

Method ● Strictly Priority
○ Weighted Round Robin Scheduling

Q0 Weight

Q1 Weight

Q2 Weight

Q3 Weight

The following table describes the labels in this screen.

Table 42 Advanced Application > 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. 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.

21

Multicast

This chapter shows you how to configure various multicast features.

21.1 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 Management 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, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

21.1.1 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).

21.1.2 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.

21.1.3 IGMP Snooping

The Switch can passively snoop on IGMP 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.

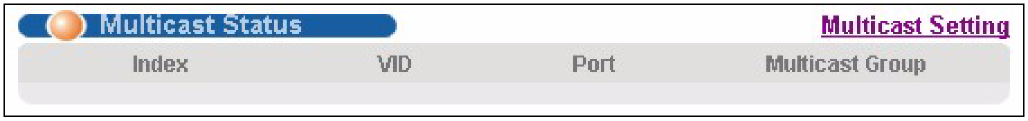
21.1.4 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

21.2 Multicast Status

Click **Advanced Applications > Multicast** to display the screen as shown. This screen shows the multicast group information. See Section 21.1 on page 157 for more information on multicasting.

Figure 77 Advanced Application > Multicast



Index	VID	Port	Multicast Group

The following table describes the labels in this screen.

Table 43 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.

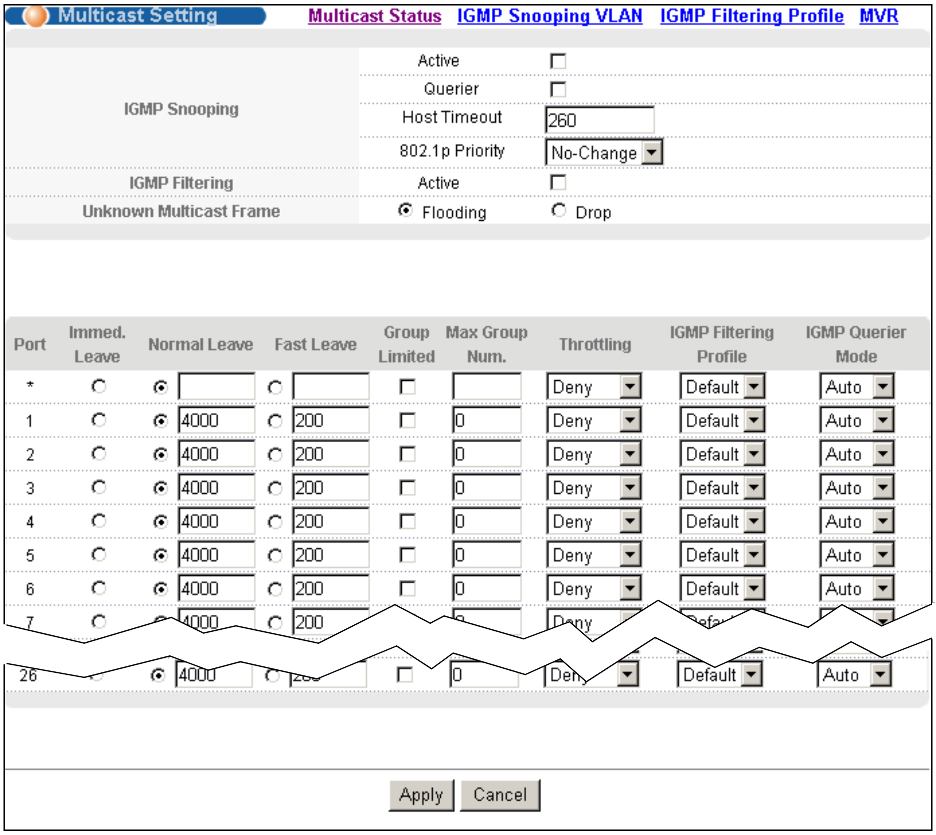
Table 43 Multicast Status (continued)

LABEL	DESCRIPTION
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

21.3 Multicast Setting

Click **Advanced Applications > Multicast > Multicast Setting** link to display the screen as shown. See Section 21.1 on page 157 for more information on multicasting.

Figure 78 Advanced Application > Multicast > Multicast Setting



IGMP Snooping	Active	□
	Querier	□
	Host Timeout	260
	802.1p Priority	No-Change
IGMP Filtering	Active	□
Unknown Multicast Frame	● Flooding	○ Drop

Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	○	●	○	□		Deny	Default	Auto
1	○	● 4000	○ 200	□	0	Deny	Default	Auto
2	○	● 4000	○ 200	□	0	Deny	Default	Auto
3	○	● 4000	○ 200	□	0	Deny	Default	Auto
4	○	● 4000	○ 200	□	0	Deny	Default	Auto
5	○	● 4000	○ 200	□	0	Deny	Default	Auto
6	○	● 4000	○ 200	□	0	Deny	Default	Auto
7	○	4000	○ 200			Deny		
26		● 4000	○	□	0	Den	Default	Auto

The following table describes the labels in this screen.

Table 44 Advanced Application > Multicast > 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.

Table 44 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
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.
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. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
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.
*	Settings in this row apply to all ports. 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 (0-255) 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. You can create IGMP filtering profiles in the **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** screen.

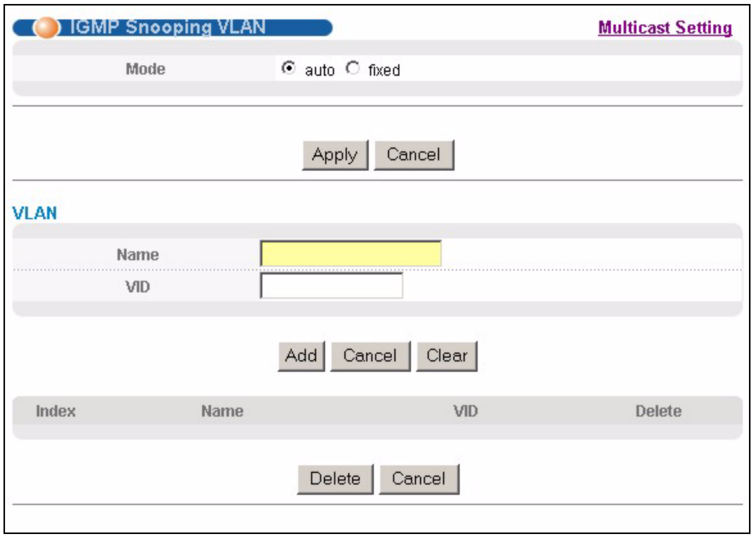
Table 44 Advanced Application > Multicast > Multicast Setting (continued)

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

21.4 IGMP Snooping VLAN

Click **Advanced Applications > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See Section 21.1.4 on page 158 for more information on IGMP Snooping VLAN.

Figure 79 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN



IGMP Snooping VLAN

Multicast Setting

Mode ● auto ○ fixed

VLAN

Name

VID

Index	Name	VID	Delete

The following table describes the labels in this screen.

Table 45 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

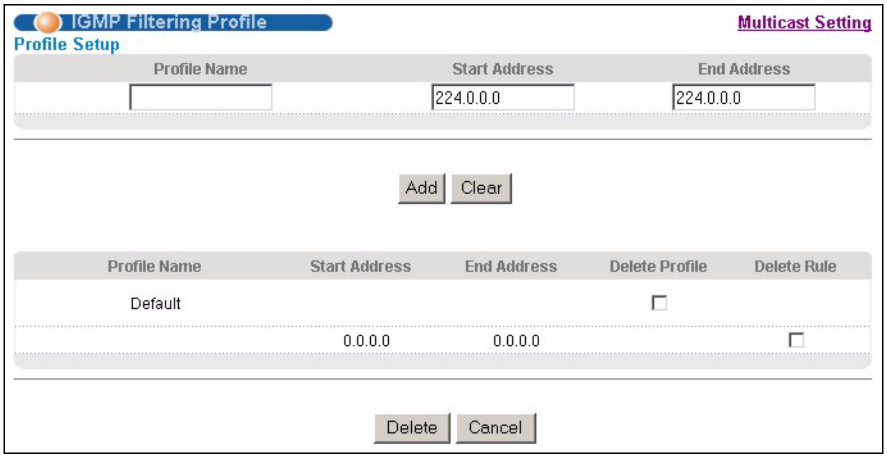
LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to three VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the **Multicast Setting** screen first.
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.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the **MVR** screen.
Add	Click **Add** to insert the entry in the summary table below and 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.
Clear	Click this to clear the fields.
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

21.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Applications** > **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** link to display the screen as shown.

Figure 80 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile



Profile Name	Start Address	End Address
	224.0.0.0	224.0.0.0

Profile Name	Start Address	End Address	Delete Profile	Delete Rule
Default			□	
	0.0.0.0	0.0.0.0		□

The following table describes the labels in this screen.

Table 46 Advanced Application > Multicast > Multicast Setting > 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 profile 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.

Table 46 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile (continued)

LABEL	DESCRIPTION
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.

21.6 MVR Overview

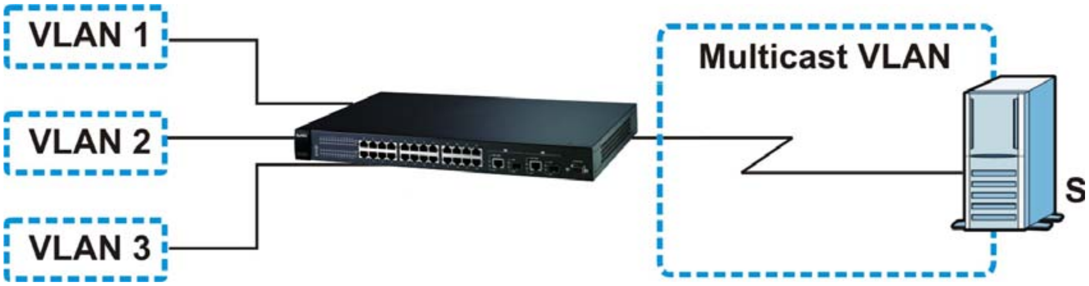
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

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.

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 81 MVR Network Example



21.6.1 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 traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

21.6.2 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.

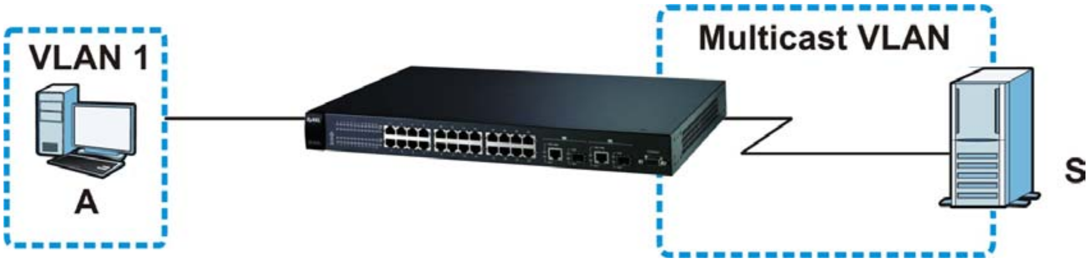
21.6.3 How MVR Works

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, an uplink 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 82 MVR Multicast Television Example



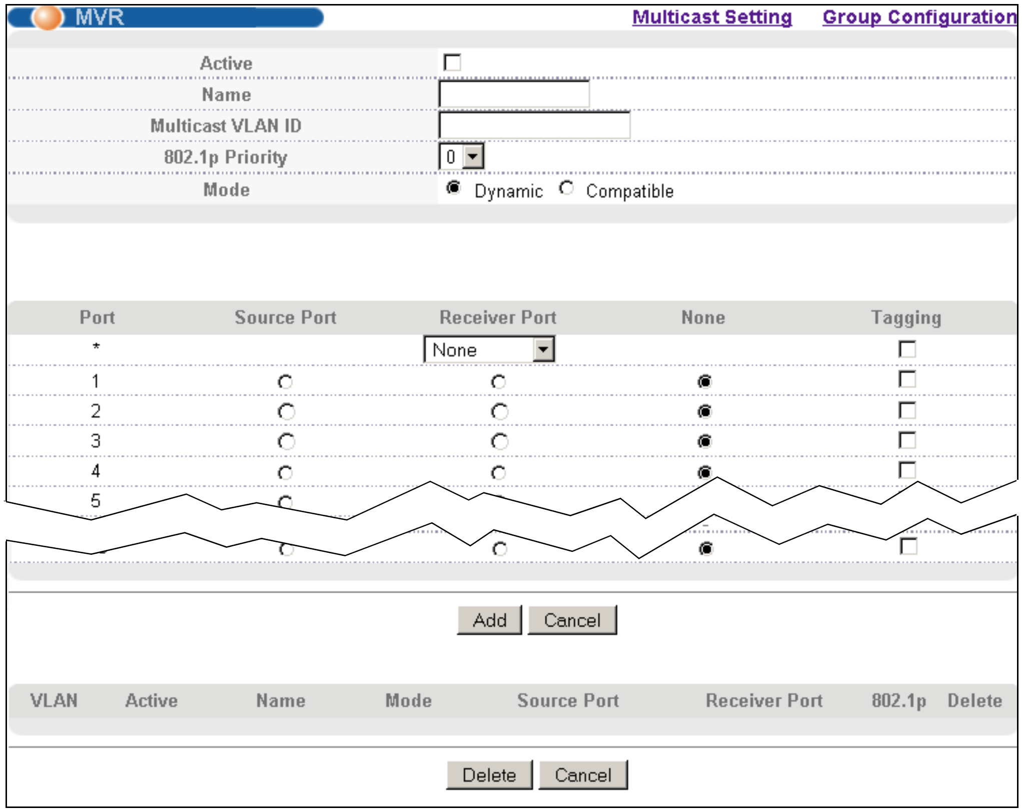
21.7 General MVR Configuration

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 > Multicast** > **Multicast Setting > 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.

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

Figure 83 Advanced Application > Multicast > Multicast Setting > MVR



Active	□
Name	
Multicast VLAN ID	
802.1p Priority	0
Mode	● Dynamic ○ Compatible

Port	Source Port	Receiver Port	None	Tagging
*		None		□
1	○	○	●	□
2	○	○	●	□
3	○	○	●	□
4	○	○	●	□
5	○			
	○	○	●	□

VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p	Delete

The following table describes the related labels in this screen.

Table 47 Advanced Application > Multicast > Multicast Setting > 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 English keyboard 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 47 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. 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 begin configuring this screen afresh.
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.

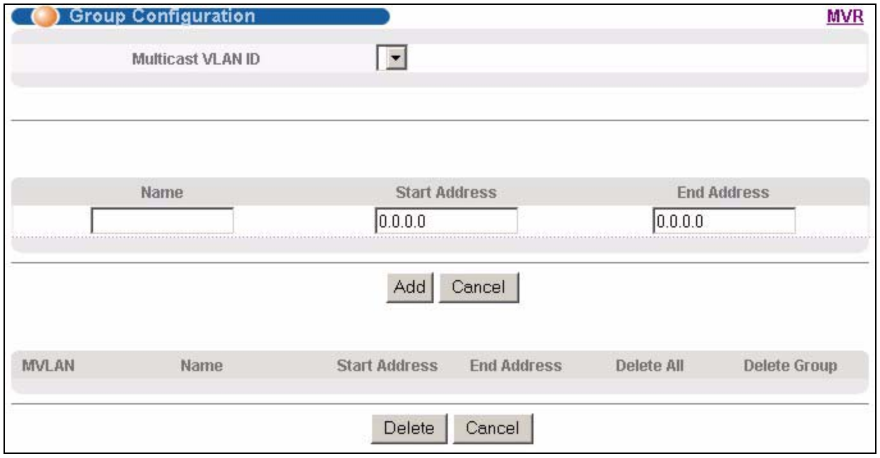
21.8 MVR Group Configuration

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 84 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration



The following table describes the labels in this screen.

Table 48 Advanced Application > Multicast > Multicast Setting > 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 21.1.1 on page 157 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 21.1.1 on page 157 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 begin configuring this screen afresh.
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.

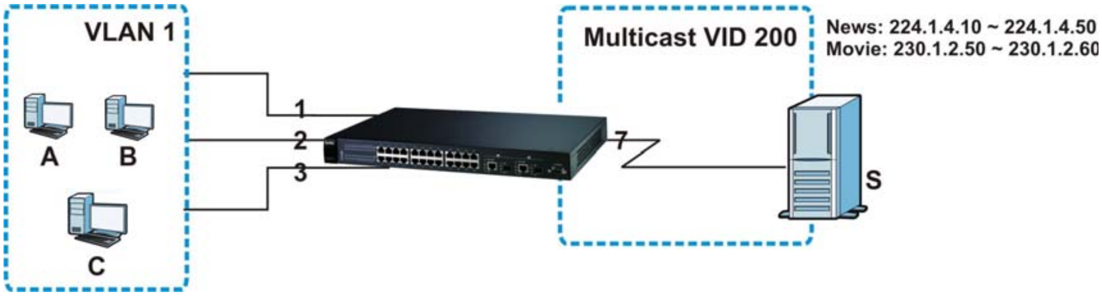
Table 48 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

LABEL	DESCRIPTION
Delete	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.

21.8.1 MVR Configuration Example

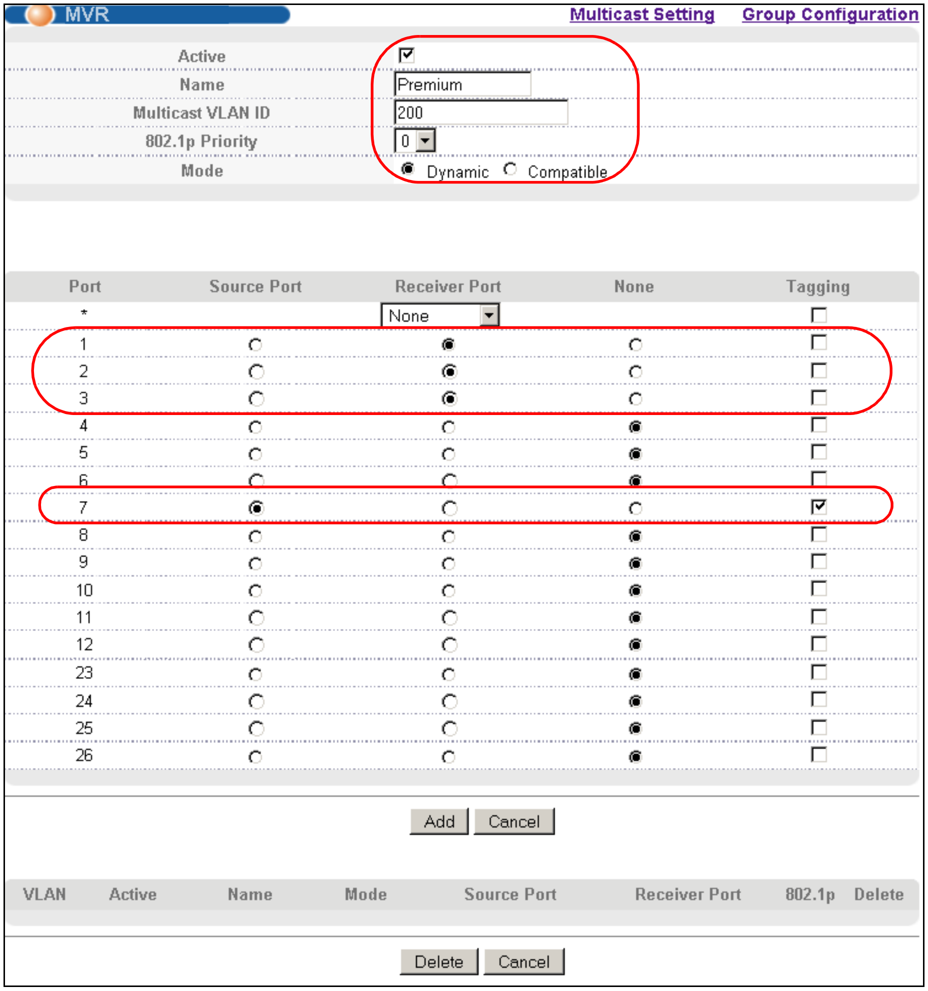
The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the **News** and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in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

Figure 85 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 86 MVR Configuration Example



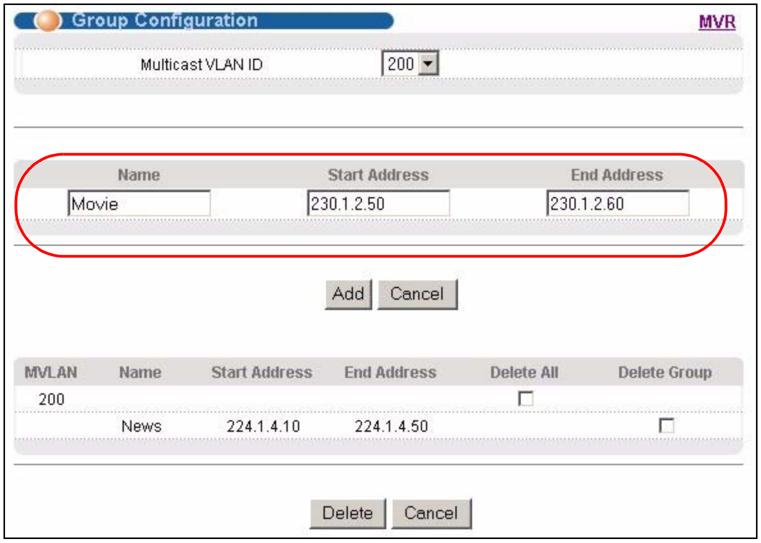
Active	☑
Name	Premium
Multicast VLAN ID	200
802.1p Priority	0
Mode	● Dynamic ○ Compatible

Port	Source Port	Receiver Port	None	Tagging
*		None		□
1	○	●	○	□
2	○	●	○	□
3	○	●	○	□
4	○	○	●	□
5	○	○	●	□
6	○	○	●	□
7	●	○	○	☑
8	○	○	●	□
9	○	○	●	□
10	○	○	●	□
11	○	○	●	□
12	○	○	●	□
23	○	○	●	□
24	○	○	●	□
25	○	○	●	□
26	○	○	●	□

VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p	Delete

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 87 MVR Group Configuration Example



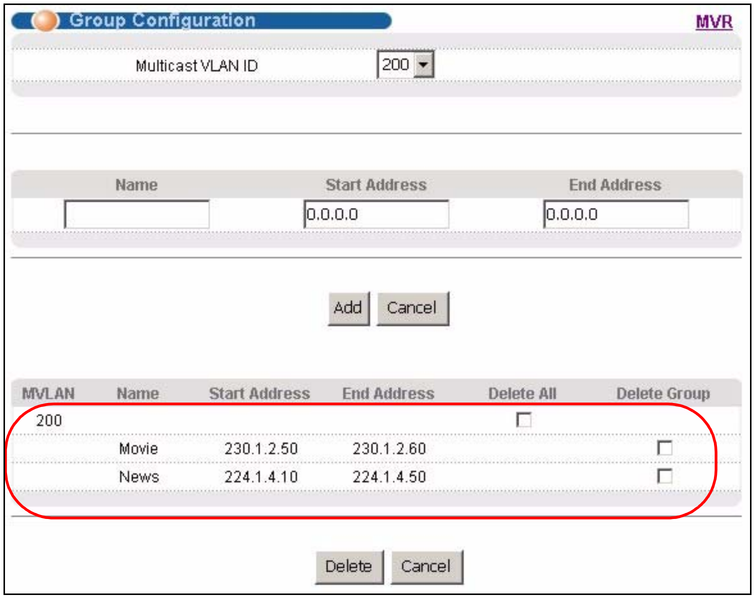
Group Configuration

Multicast VLAN ID: 200

Name	Start Address	End Address
Movie	230.1.2.50	230.1.2.60

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200				□	
	News	224.1.4.10	224.1.4.50		□

Figure 88 MVR Group Configuration Example



Group Configuration

Multicast VLAN ID: 200

Name	Start Address	End Address
	0.0.0.0	0.0.0.0

MVLAN	Name	Start Address	End Address	Delete All	Delete Group
200				□	
	Movie	230.1.2.50	230.1.2.60		□
	News	224.1.4.10	224.1.4.50		□

22

AAA

This chapter describes how to configure authentication and accounting settings on the Switch.

22.1 Authentication, Authorization and Accounting (AAA)

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users

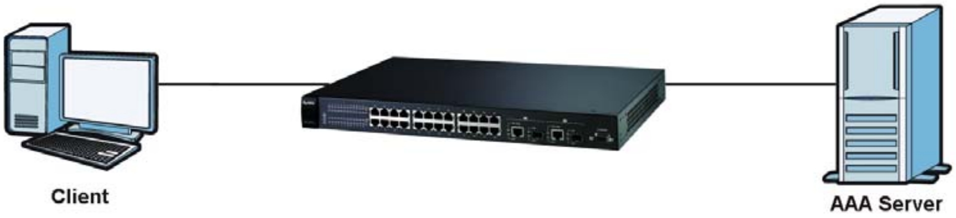
Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see Section 22.1.2 on page 174) and TACACS+ (Terminal Access Controller Access-Control System Plus, see Section

22.1.2 on page 174) as external authentication, authorization and accounting servers.

Figure 89 AAA Server



22.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See Chapter 29 on page 233).

22.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols 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 and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 49 RADIUS vs. TACACS+

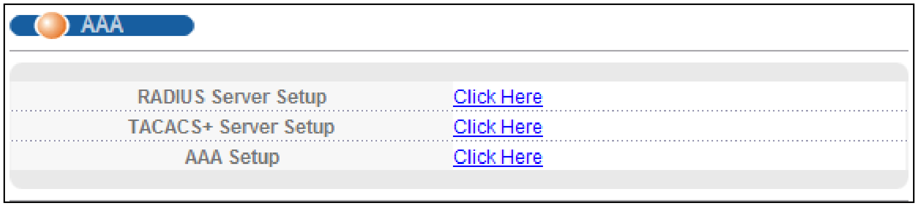
	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

22.2 AAA Screens

To enable authentication, accounting or both on the Switch. First, configure your authentication server settings (RADIUS, TACACS+ or both) and then set up the authentication priority and accounting settings.

Click **Advanced Application** > **AAA** in the navigation panel to display the screen as shown.

Figure 90 Advanced Application > AAA



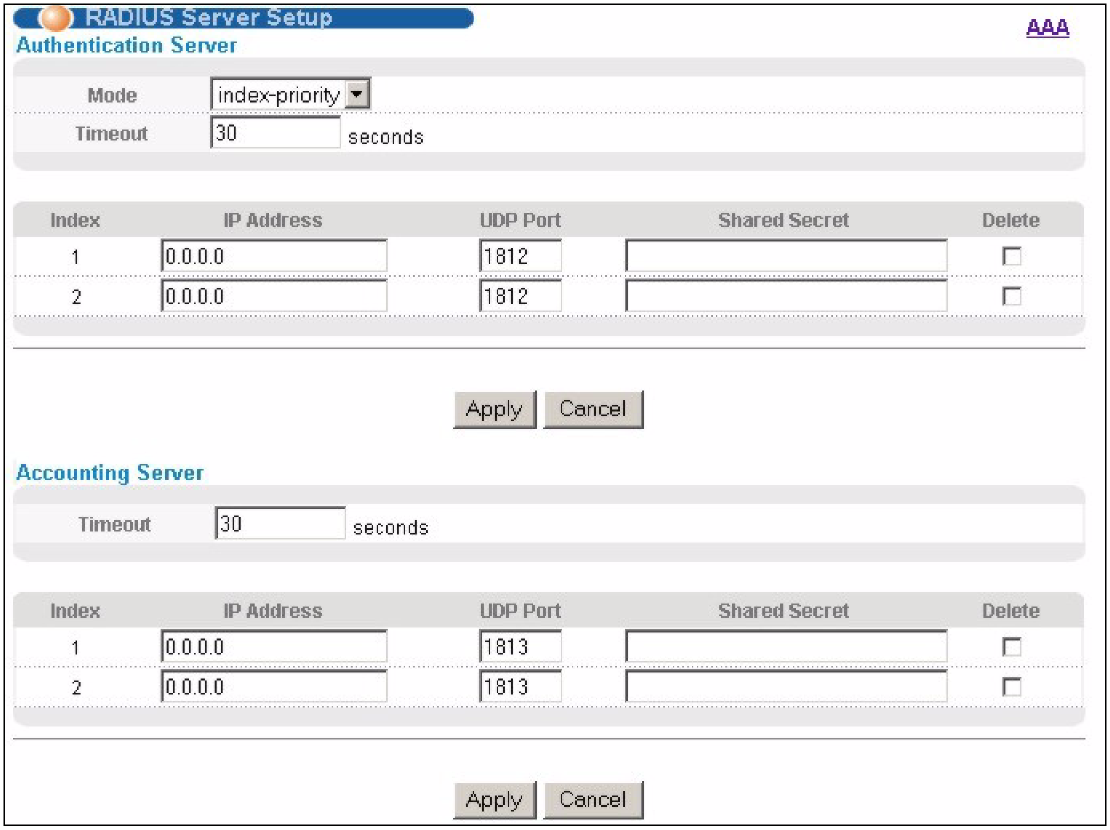
AAA

RADIUS Server Setup	Click Here
TACACS+ Server Setup	Click Here
AAA Setup	Click Here

22.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See Section 22.1.2 on page 174 for more information on RADIUS servers. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 91 Advanced Application > AAA > RADIUS Server Setup



RADIUS Server Setup

AAA

Authentication Server

Mode	index-priority
Timeout	30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1812		□
2	0.0.0.0	1812		□

Apply Cancel

Accounting Server

Timeout	30 seconds

Index	IP Address	UDP Port	Shared Secret	Delete
1	0.0.0.0	1813		□
2	0.0.0.0	1813		□

Apply Cancel

The following table describes the labels in this screen.

Table 50 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field is only valid if you configure multiple RADIUS servers. Select **index-priority** and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select **round-robin** to alternate between the RADIUS servers that it sends authentication requests to. Note: If you are using two different RADIUS servers, select **round-robin** in this field. If the designated server is not available, the connection times out instead of trying other available servers.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using **index-priority** for your authentication and you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **Apply**.
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.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.

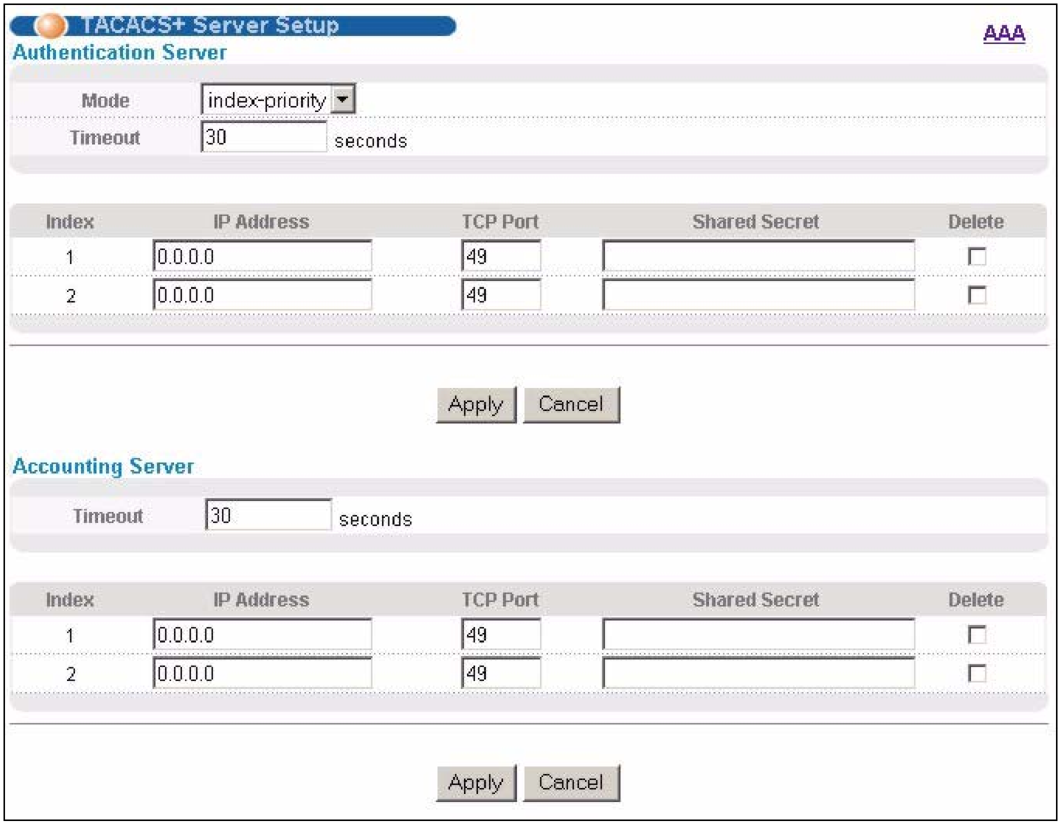
Table 50 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click **Apply**.
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.

22.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See Section 22.1.2 on page 174 for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 92 Advanced Application > AAA > TACACS+ Server Setup



Authentication Server

Mode: index-priority

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		□
2	0.0.0.0	49		□

Accounting Server

Timeout: 30 seconds

Index	IP Address	TCP Port	Shared Secret	Delete
1	0.0.0.0	49		□
2	0.0.0.0	49		□

The following table describes the labels in this screen.

Table 51 Advanced Application > AAA > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers. Select **index-priority** and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select **round-robin** to alternate between the TACACS+ servers that it sends authentication requests to. Note: If you are using two different TACACS+ servers, select **round-robin** in this field. If the designated server is not available, the connection times out instead of trying other available servers.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using **index-priority** for your authentication and you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click **Apply**.
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.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.

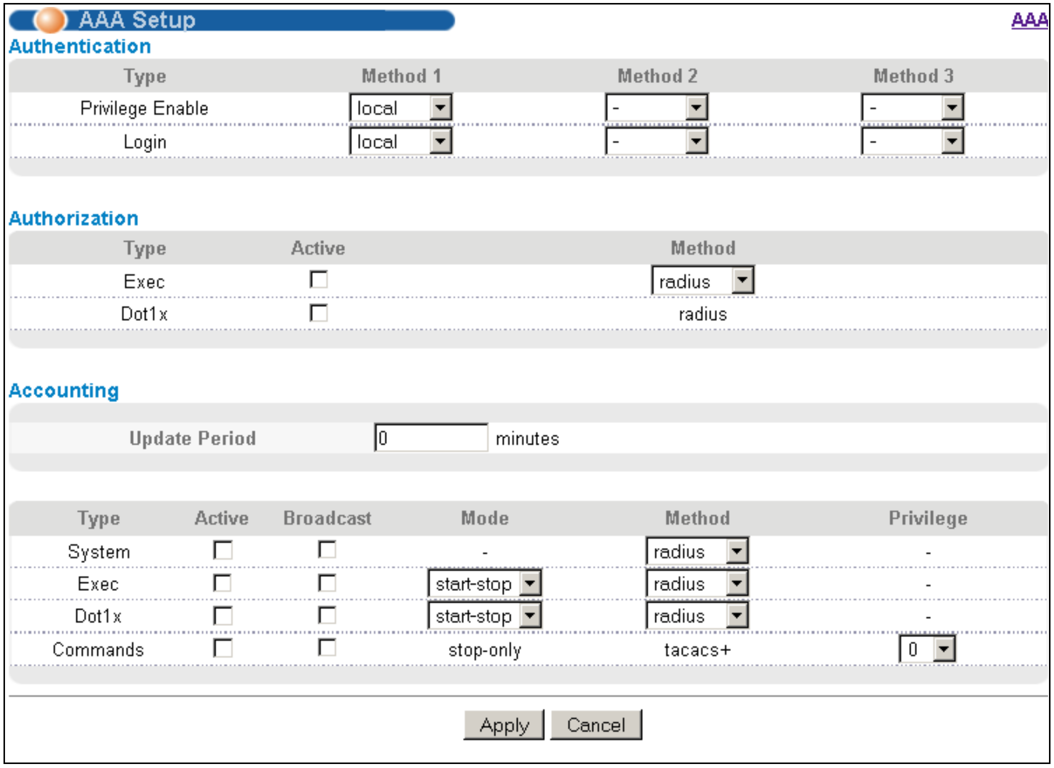
Table 51 Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
TCP Port	The default port of a TACACS+ accounting server is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click **Apply**.
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.

22.2.3 AAA Setup

Use this screen to configure authentication and accounting settings on the Switch. Click on the **AAA Setup** link in the **AAA** screen to view the screen as shown.

Figure 93 Advanced Application > AAA > AAA Setup



AAA Setup

AAA

Authentication

Type	Method 1	Method 2	Method 3
Privilege Enable	local	-	-
Login	local	-	-

Authorization

Type	Active	Method
Exec	□	radius
Dot1x	□	radius

Accounting

Update Period 0 minutes

Type	Active	Broadcast	Mode	Method	Privilege
System	□	□	-	radius	-
Exec	□	□	start-stop	radius	-
Dot1x	□	□	start-stop	radius	-
Commands	□	□	stop-only	tacacs+	0

Apply Cancel

The following table describes the labels in this screen.

Table 52 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management). Configure the access privilege of accounts via commands (see the CLI Reference Guide) for **local** authentication. The **TACACS+** and **RADIUS** are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for access privilege level specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the access privilege configured for local authentication. Select **radius** or **tacacs+** to have the Switch check the access privilege via the external servers.
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **Access Control > Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **Access Control > Logins** screen. Select **radius** to have the Switch check the administrator accounts via RADIUS servers configured in the **RADIUS Server Setup** screen. Select **tacacs+** to have the Switch check the administrator accounts via TACACS+ servers configured in the **TACACS+ Server Setup** screen.
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. • **Exec**: Allow an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned via the external server. • **Dot1x**: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.

Table 52 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Active	Select this to activate authorization for a specified event types.
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the **start-stop** option for the **Exec** or **Dot1x** entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • **System** - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled. • **Exec** - Configure the Switch to send information when an administrator logs in and logs out via the console port, Telnet or SSH. • **Dot1x** - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • **Commands** - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don’t select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn’t get a response from the accounting server then it tries the second accounting server.
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** - to have the Switch send information to the accounting server when a user begins a session, during a user’s session (if it lasts past the **Update Period**), and when a user ends a session. • **stop-only** - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. TACACS+ is the only method for recording **Commands** type of event.
Privilege	This field is only configurable for **Commands** type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on 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.

22.2.4 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (See the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 53 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	`Vendor-Id =` **890** `Vendor-Type =` **1** `Vendor-data =` ingress rate (Kbps in decimal format)

Table 53 Supported VSAs

FUNCTION	ATTRIBUTE

Egress Bandwidth Assignment	`Vendor-Id =` **`890`**
	`Vendor-Type =` **`2`**
	`Vendor-data =` egress rate (Kbps in decimal format)

Privilege Assignment	`Vendor-ID =` **`890`** `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.

22.2.4.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that the bolded values in the table are fixed values as defined in RFC 3580.

Table 54 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.

22.3 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

This appendix lists the attributes used by authentication and accounting functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

22.3.1 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

22.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name

- the format of the User-Name attribute is **$enab**#**$**, where # is the privilege level (1-14)

User-Password

NAS-Identifier

NAS-IP-Address

22.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

22.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

22.3.2 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

22.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 2007041917210300000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

22.3.2.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 55 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

Table 56 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-IP-Address	Y	Y	Y
Service-Type	Y	Y	Y
Calling-Station-Id	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y

Table 56 RADIUS Attributes - Exec Events via Telnet/SSH (continued)

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Session-Time		Y	Y
Acct-Terminate-Cause			Y

22.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 57 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	Y	Y	Y
NAS-IP-Address	Y	Y	Y
NAS-Port	Y	Y	Y
Class	Y	Y	Y
Called-Station-Id	Y	Y	Y
Calling-Station-Id	Y	Y	Y
NAS-Identifier	Y	Y	Y
NAS-Port-Type	Y	Y	Y
Acct-Status-Type	Y	Y	Y
Acct-Delay-Time	Y	Y	Y
Acct-Session-Id	Y	Y	Y
Acct-Authentic	Y	Y	Y
Acct-Input-Octets		Y	Y
Acct-Output-Octets		Y	Y
Acct-Session-Time		Y	Y
Acct-Input-Packets		Y	Y
Acct-Output-Packets		Y	Y
Acct-Terminate-Cause			Y
Acct-Input-Gigawords		Y	Y
Acct-Output-Gigawords		Y	Y

IP Source Guard

Use IP source guard to filter unauthorized ARP packets in your network.

23.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives an ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds from information provided manually by administrators (static bindings).

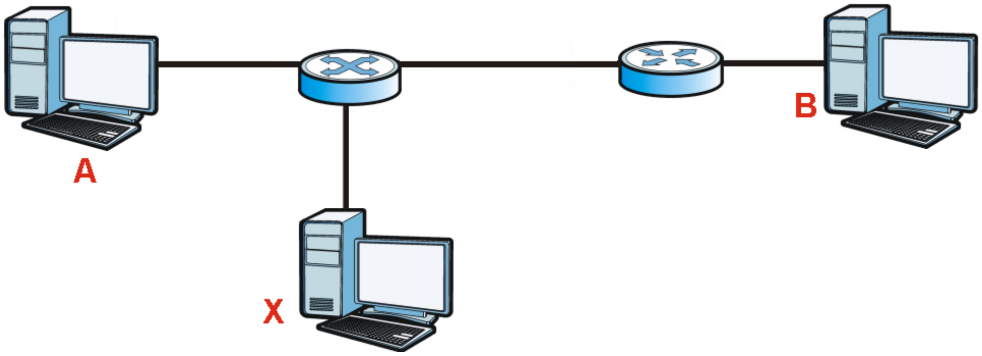
IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

23.1.1 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 94 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A.** Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A.** Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B.**
- It pretends to be computer **B** and sends a message to computer **A.**

As a result, all the communication between computer **A** and computer **B** passes through computer **X.** Computer **X** can read and alter the information passed between them.

23.1.1.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters (Chapter 12 on page 113).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

23.1.1.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports if the sender's information in the ARP packet does not match any of the current bindings.

23.1.1.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 31 on page 257) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

23.1.1.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1 Configure static bindings so the Switch can distinguish between authorized and unauthorized ARP packets.

2 Enable ARP inspection on the Switch.

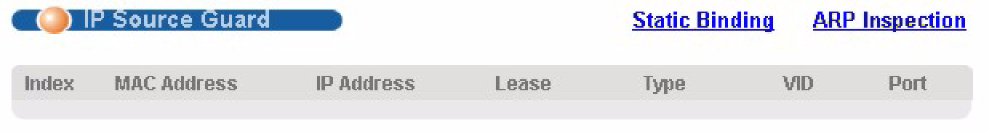
3 Enable ARP inspection on each VLAN.

4 Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

23.2 IP Source Guard

Use this screen to look at the current bindings for ARP inspection. Bindings are used by ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 95 IP Source Guard



Index	MAC Address	IP Address	Lease	Type	VID	Port

The following table describes the labels in this screen.

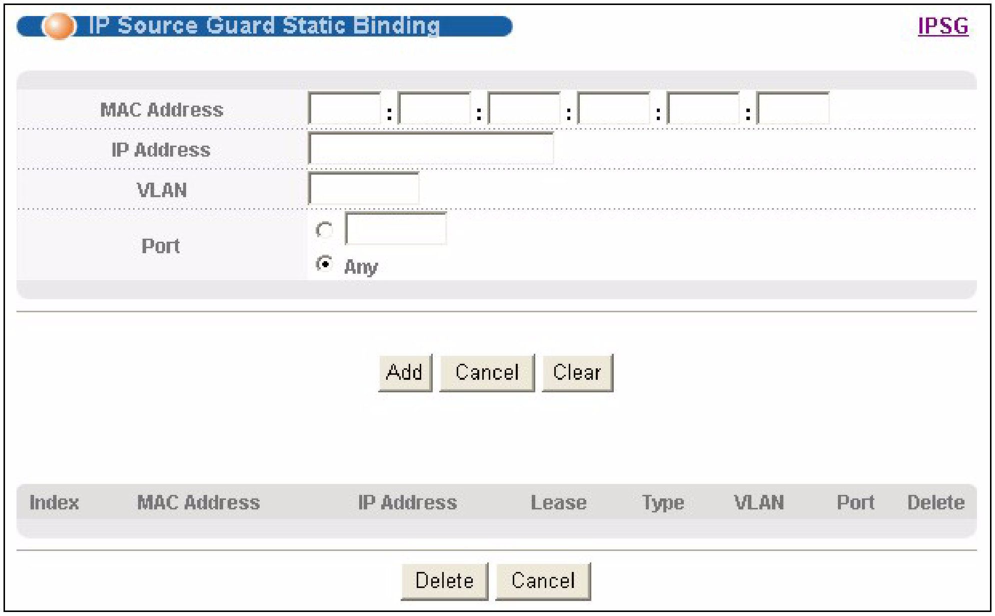
Table 58 IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

23.3 IP Source Guard Static Binding

Use this screen to manage static bindings for ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 96 IP Source Guard Static Binding



The following table describes the labels in this screen.

Table 59 IP Source Guard Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select **Any**.
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click this to clear the fields above.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.

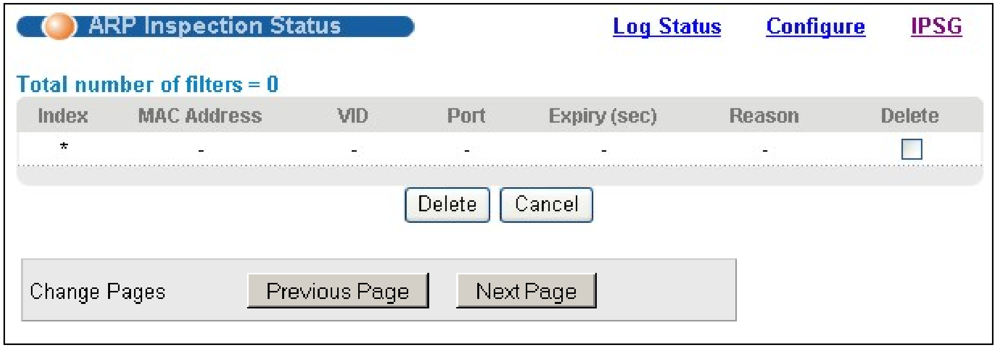
Table 59 IP Source Guard Static Binding (continued)

LABEL	DESCRIPTION
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

23.4 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 97 ARP Inspection Status



Total number of filters = 0

Index	MAC Address	VID	Port	Expiry (sec)	Reason	Delete
*	-	-	-	-	-	□

The following table describes the labels in this screen.

Table 60 ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).

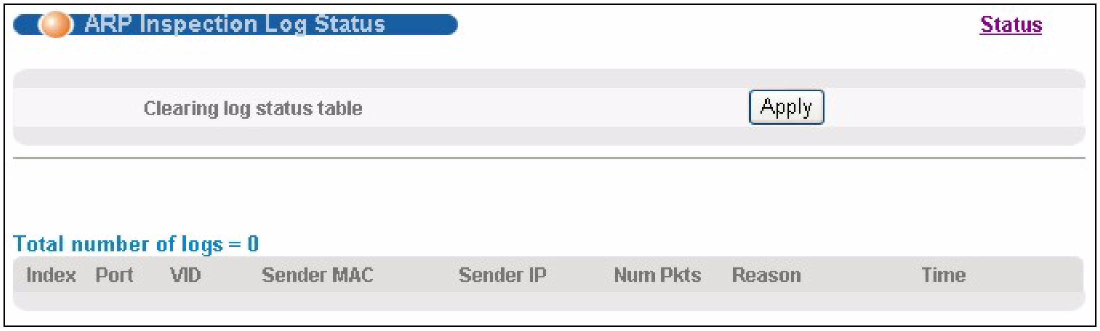
Table 60 ARP Inspection Status (continued)

LABEL	DESCRIPTION
Reason	This field displays the reason the ARP packet was discarded. **MAC+VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this, and click **Delete** to remove the specified entry.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the **Delete** check boxes above.
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

23.4.1 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 98 ARP Inspection Log Status



Total number of logs = 0

Index	Port	VID	Sender MAC	Sender IP	Num Pkts	Reason	Time

The following table describes the labels in this screen.

Table 61 ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click **Apply** to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.

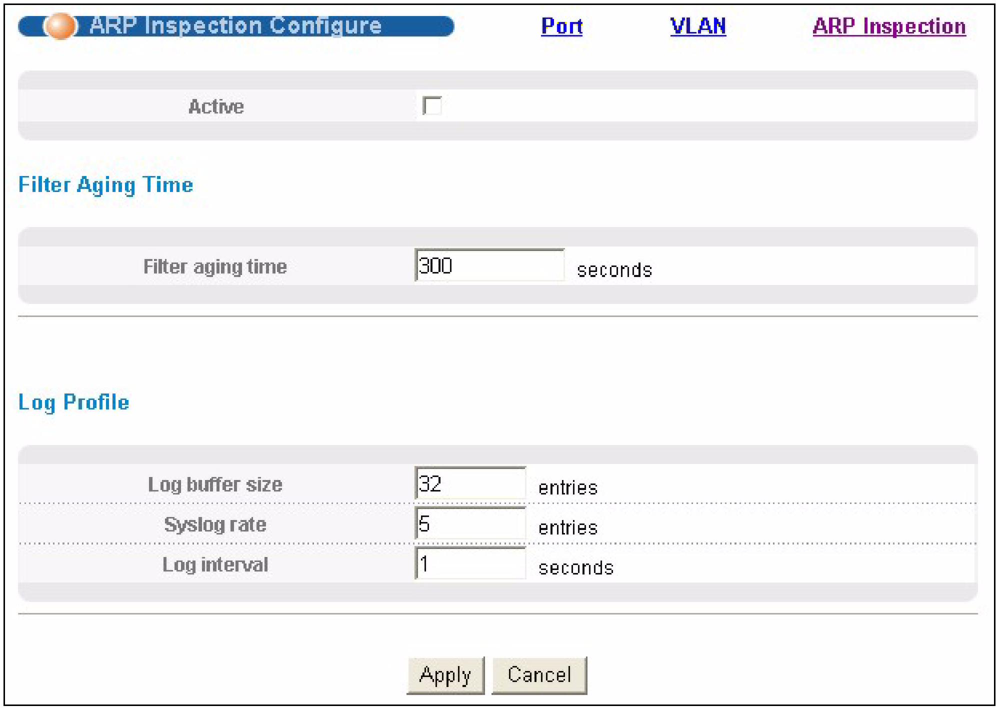
Table 61 ARP Inspection Log Status (continued)

LABEL	DESCRIPTION
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the **ARP Inspection Configure** screen. See Section 23.5 on page 194.
Reason	This field displays the reason the log message was generated. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **ARP Inspection VLAN Configure** screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 23.5.2 on page 198.
Time	This field displays when the log message was generated.

23.5 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 99 ARP Inspection Configure



Active □

Filter Aging Time

Filter aging time 300 seconds

Log Profile

Log buffer size 32 entries

Syslog rate 5 entries

Log interval 1 seconds

The following table describes the labels in this screen.

Table 62 ARP Inspection Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Enter 0 if you want the MAC address filter to be permanent.
Log Profile	

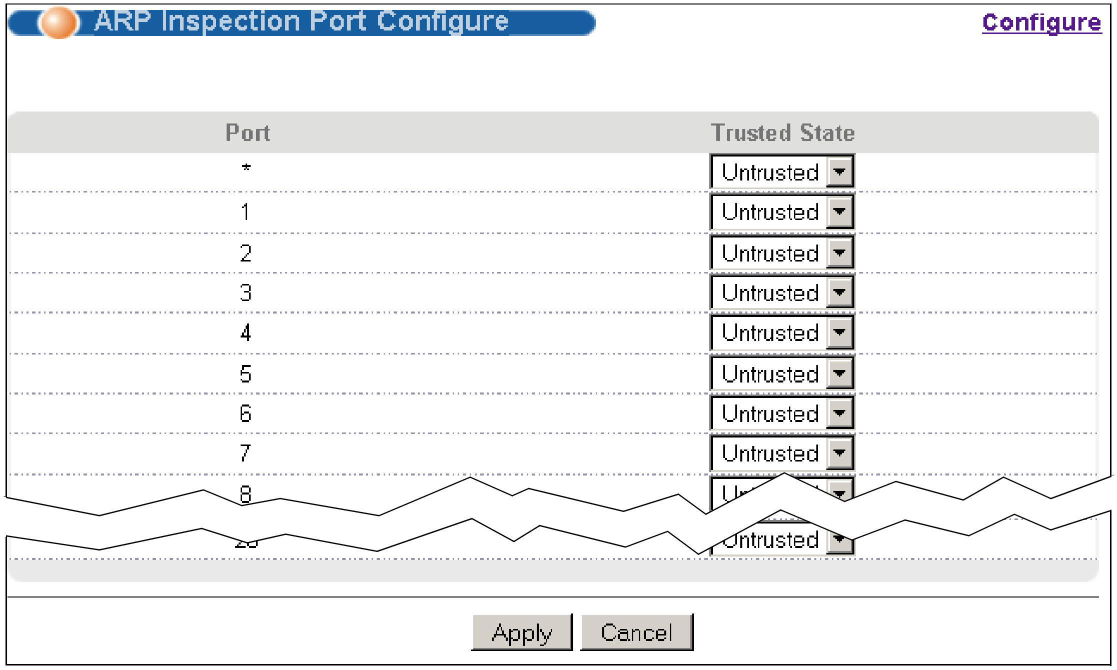
Table 62 ARP Inspection Configure (continued)

LABEL	DESCRIPTION
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified **Syslog rate** and **Log interval**. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click **Clearing log status table** in the **ARP Inspection Log Status** screen to clear the log and reset this counter. See Section 23.4.1 on page 193.
Syslog rate	Enter the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**. You must configure the syslog server (Chapter 31 on page 257) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog rate** and **Log interval** is illustrated in the following examples: • 4 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • 6 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 2: the Switch sends 10 syslog messages every 2 seconds.
Log interval	Enter how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See **Syslog rate** for an example of the relationship between **Syslog rate** and **Log interval**.
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 this to reset the values in this screen to their last-saved values.

23.5.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 100 ARP Inspection Port Configure



Port	Trusted State
*	Untrusted
1	Untrusted
2	Untrusted
3	Untrusted
4	Untrusted
5	Untrusted
6	Untrusted
7	Untrusted
8	Un
28	Untrusted

The following table describes the labels in this screen.

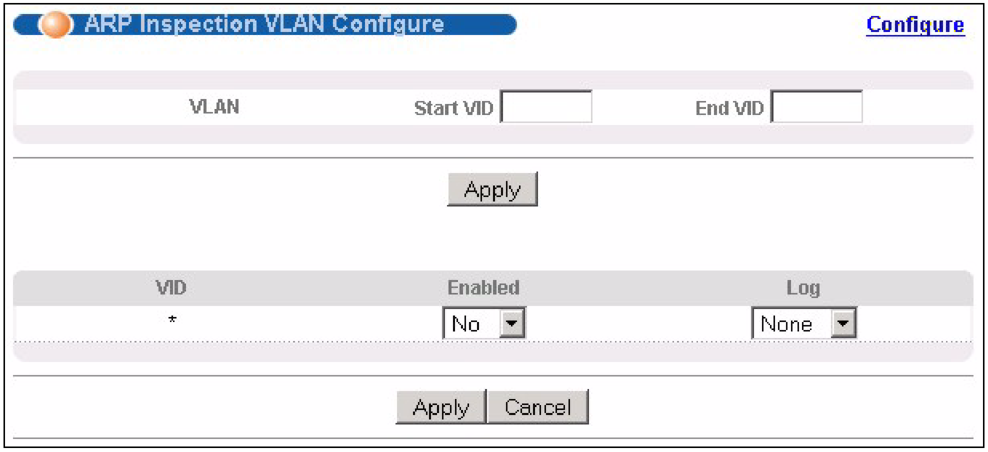
Table 63 ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports if the sender's information in the ARP packet does not match any of the current bindings.
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 this to reset the values in this screen to their last-saved values.

23.5.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 101 ARP Inspection VLAN Configure



The following table describes the labels in this screen.

Table 64 ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.

Table 64 ARP Inspection VLAN Configure (continued)

LABEL	DESCRIPTION
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the 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 this to reset the values in this screen to their last-saved values.

24

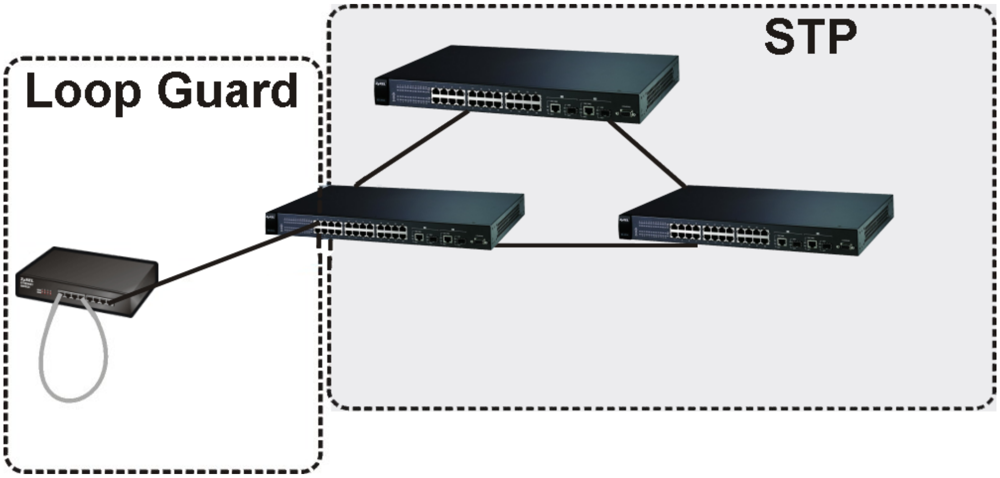
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

24.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network, STP cannot prevent loops that occur on the edge of your network.

Figure 102 Loop Guard vs. STP



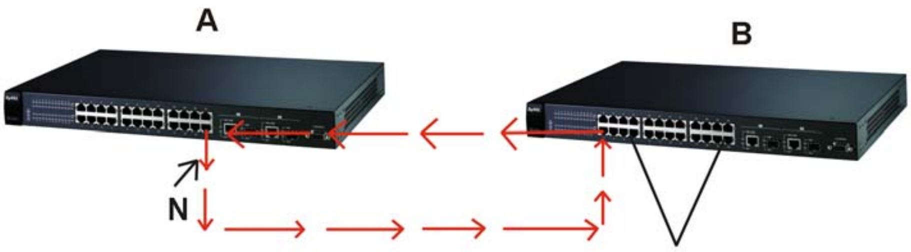
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from B.

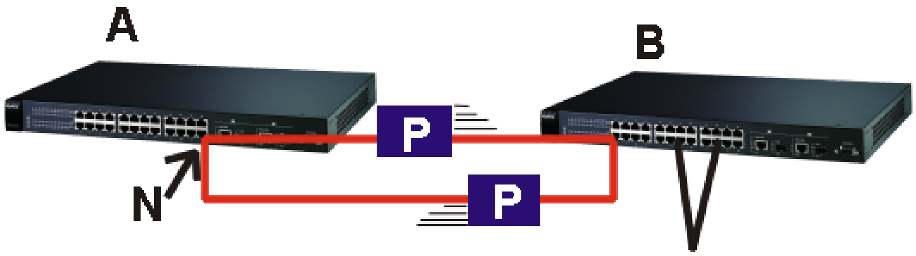
Figure 103 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

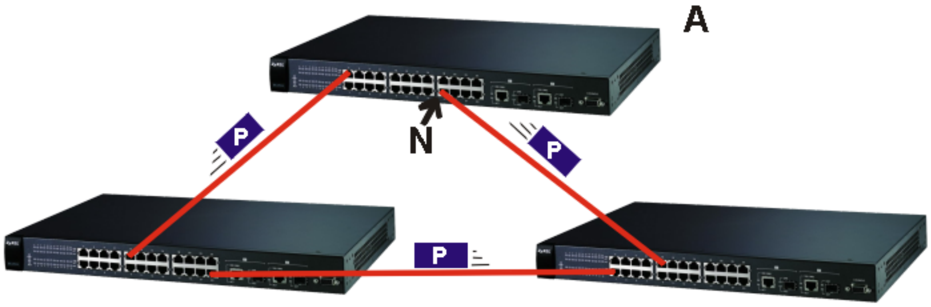
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 104 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N.** The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 105 Loop Guard - Network Loop



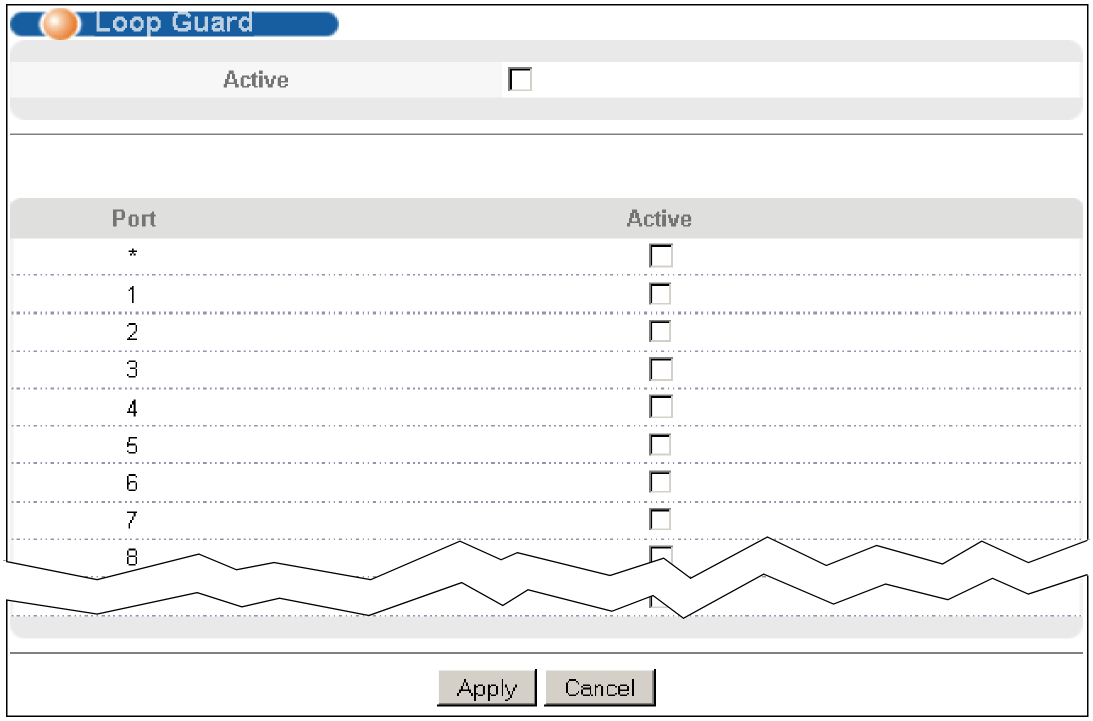
Note: After resolving the loop problem on your network you can re-activate the disabled port (see Section 8.7 on page 81).

24.2 Loop Guard Setup

Click **Advanced Application** > **Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP or MSTP) enabled.

Figure 106 Advanced Application > Loop Guard



Loop Guard

Active	□

Port	Active
*	□
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□

The following table describes the labels in this screen.

Table 65 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays a port number.
*	Use this row to make the setting the same for all ports. Use this row first 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 loop guard feature on this port. The Switch sends probe packets from this port to check if the Switch it is connected to is in loop state. If the Switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
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.

PART IV
IP Application

25

Static Route

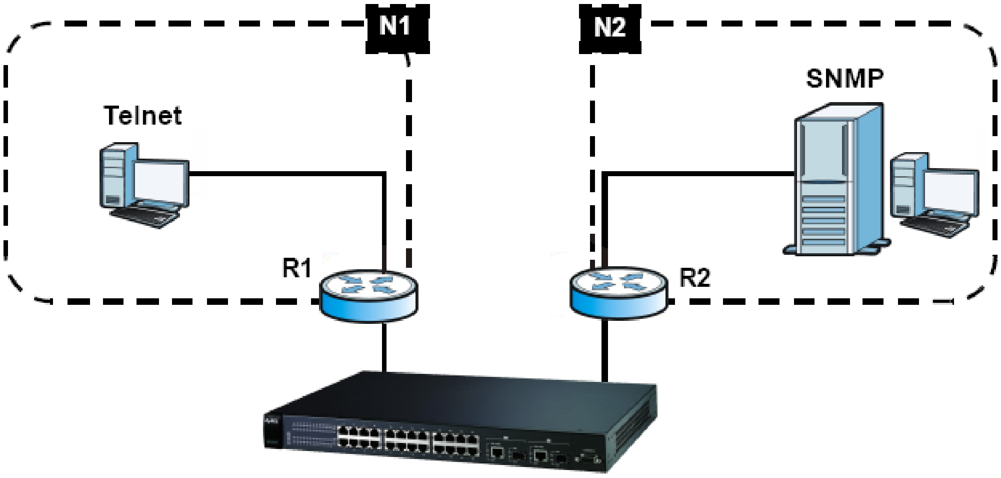
This chapter shows you how to configure static routes.

25.1 Static Routing Overview

The Switch uses IP for communication with management computers, for example using HTTP, telnet, SSH, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

This figure shows a **Telnet** session coming in from network **N1**. The Switch sends reply traffic to default gateway **R1** which routes it back to the manager's computer. The Switch needs a static route to tell it to use router **R2** to send traffic to an SNMP trap server on network **N2**.

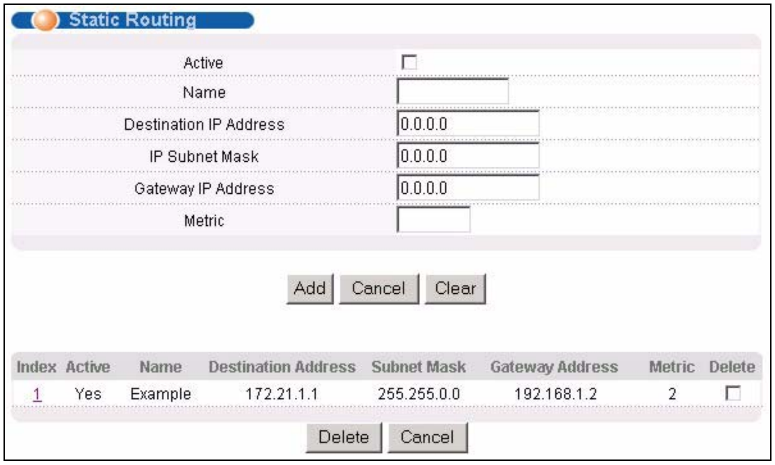
Figure 107 Static Routing Overview



25.2 Configuring Static Routing

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

Figure 108 IP Application > Static Routing



Active	□
Name	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Metric	

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	Yes	Example	172.21.1.1	255.255.0.0	192.168.1.2	2	□

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

Table 66 IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 32 English keyboard 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.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route 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.
Clear	Click **Clear** to set the above fields back to the factory defaults.

Table 66 IP Application > Static Routing (continued)

LABEL	DESCRIPTION
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **NO** when 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.

26

Differentiated Services

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

26.1 DiffServ Overview

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

26.1.1 DSCP and Per-Hop Behavior

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

Figure 109 DiffServ: Differentiated Service Field

DSCP (6 bits)	CU (2 bits)

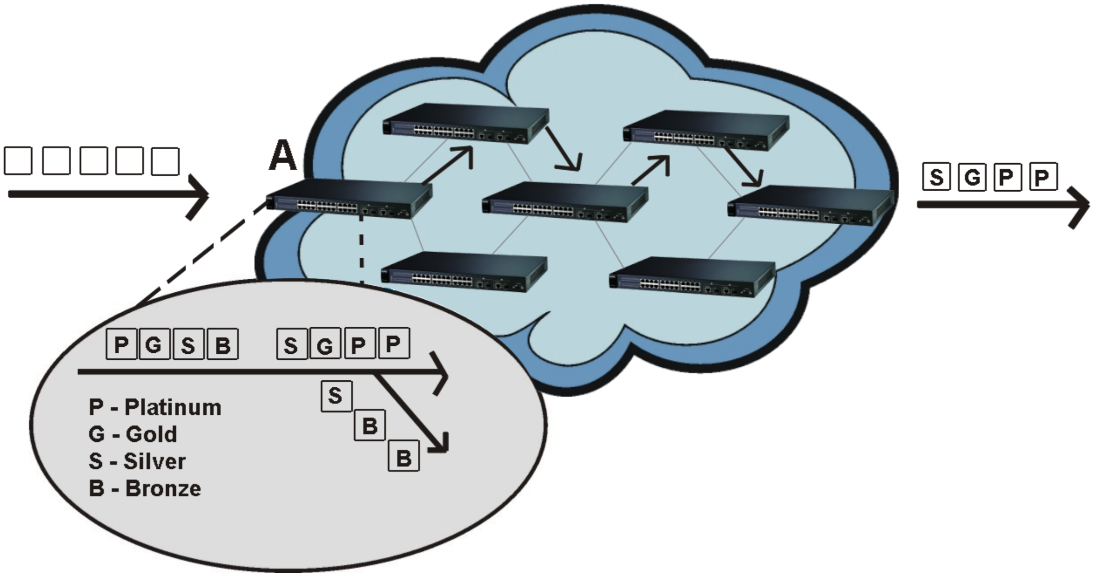
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

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

26.1.2 DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 110) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 110 DiffServ Network

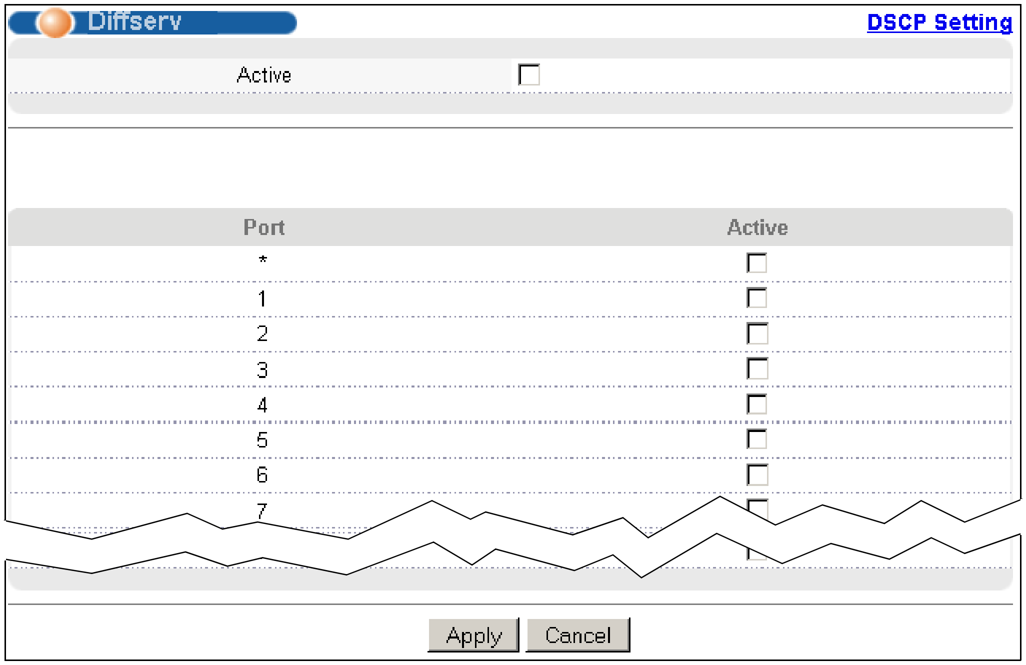


26.2 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

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

Figure 111 IP Application > DiffServ



The following table describes the labels in this screen.

Table 67 IP Application > 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.
*	Settings in this row apply to all ports. 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 **Active** 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 begin configuring this screen afresh.

26.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

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

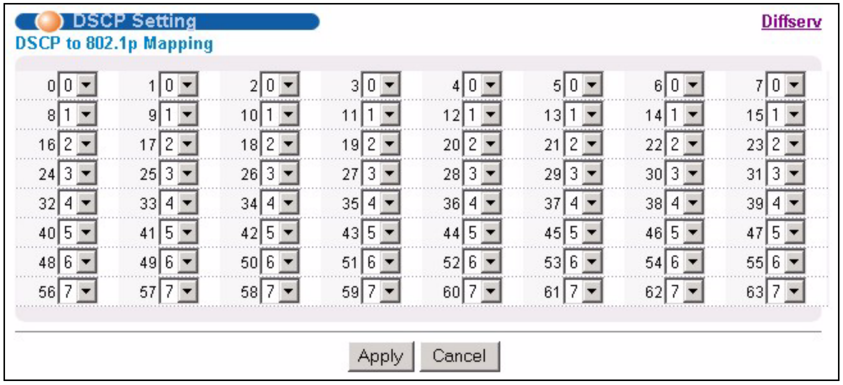
Table 68 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

26.3.1 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 112 IP Application > DiffServ > DSCP Setting



DSCP to 802.1p Mapping

0	0	1	0	2	0	3	0	4	0	5	0	6	0	7	0
8	1	9	1	10	1	11	1	12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2	20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3	28	3	29	3	30	3	31	3
32	4	33	4	34	4	35	4	36	4	37	4	38	4	39	4
40	5	41	5	42	5	43	5	44	5	45	5	46	5	47	5
48	6	49	6	50	6	51	6	52	6	53	6	54	6	55	6
56	7	57	7	58	7	59	7	60	7	61	7	62	7	63	7

The following table describes the labels in this screen.

Table 69 IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 … 63	This is the DSCP classification identification number. To set the IEEE 802.1p 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 begin configuring this screen afresh.

27

DHCP

This chapter shows you how to configure the DHCP feature.

27.1 DHCP Overview

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 relay agent. If you configure the Switch as a relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don’t configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

27.1.1 DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

27.1.2 DHCP Configuration Options

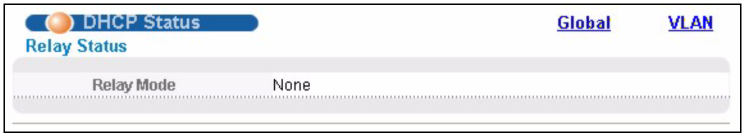
The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

27.2 DHCP Status

Click **IP Application** > **DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 113 IP Application > DHCP Status



Relay Status

Relay Mode	None

The following table describes the labels in this screen.

Table 70 IP Application > DHCP Status

LABEL	DESCRIPTION
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: • **None** - if the Switch is not configured as a DHCP relay agent. • **Global** - if the Switch is configured as a DHCP relay agent only. • **VLAN** - followed by a VLAN ID if it is configured as a relay agent for specific VLAN(s).

27.3 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

27.3.1 DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings** > **General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

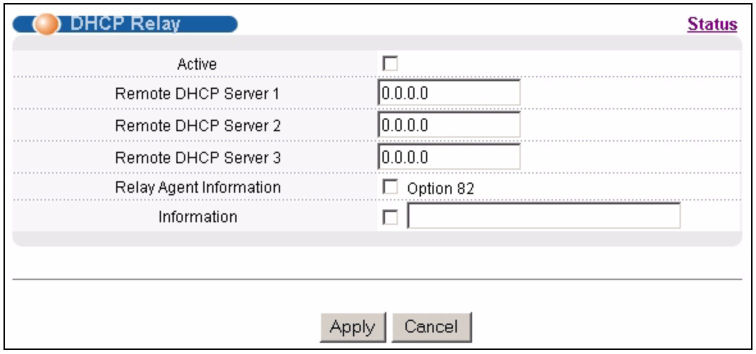
Table 71 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 32 bytes) This optional, read-only field is set according to system name set in **Basic Settings > General Setup.**

27.3.2 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 114 IP Application > DHCP > Global



Active	□
Remote DHCP Server 1	0.0.0.0
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	□ Option 82
Information	□

The following table describes the labels in this screen.

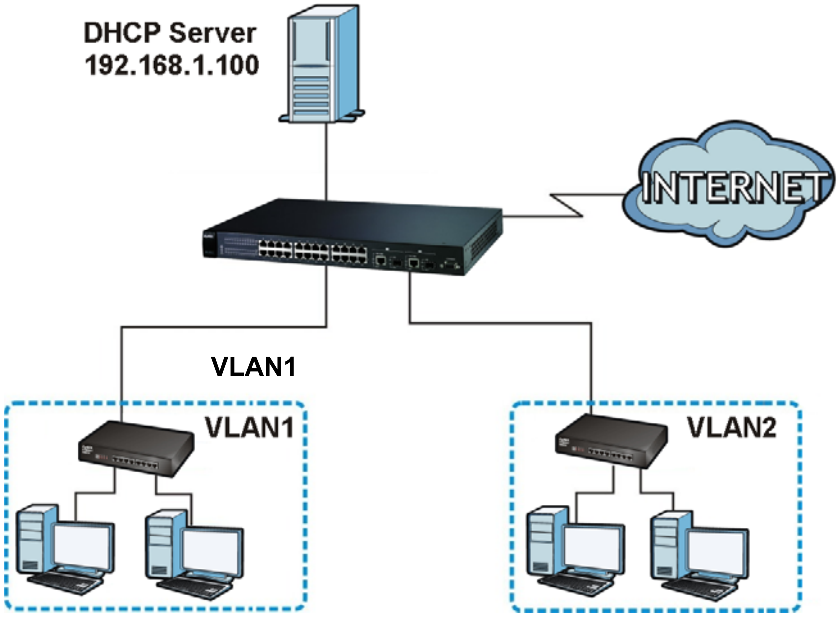
Table 72 IP Application > DHCP > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
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.

27.3.3 Global DHCP Relay Configuration Example

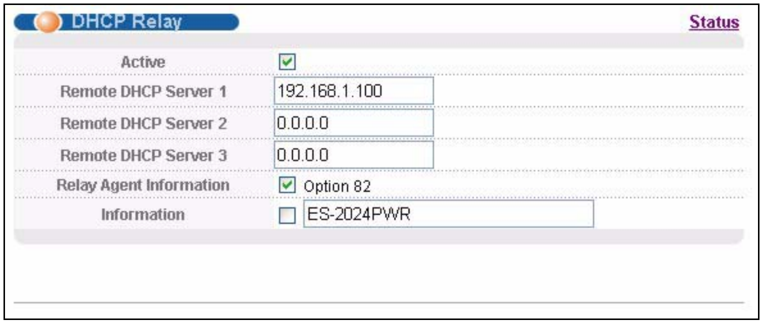
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 115 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 116 DHCP Relay Configuration Example



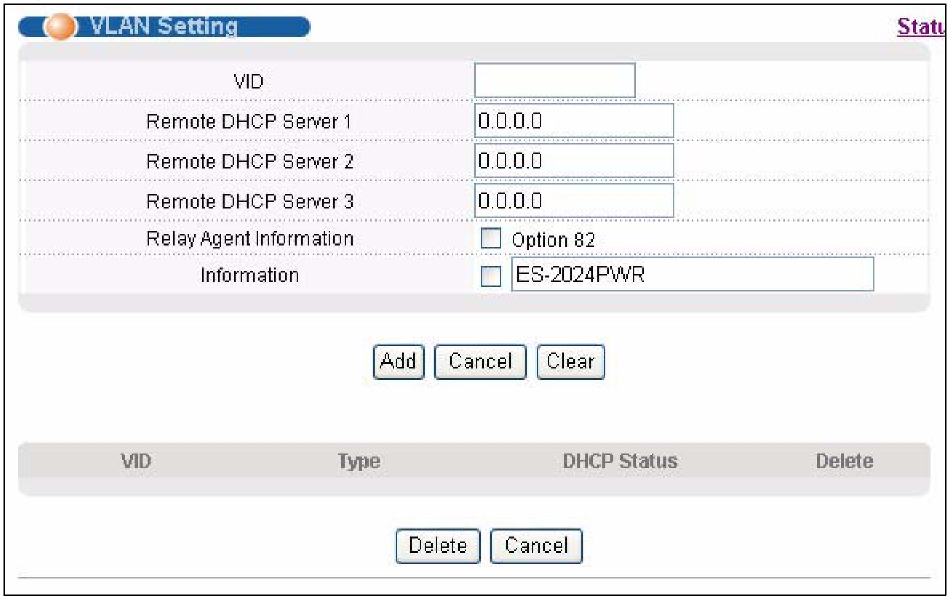
Active	☑
Remote DHCP Server 1	192.168.1.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	☑ Option 82
Information	□ ES-2024PWR

27.4 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** in the navigation panel, then click the **VLAN** link In the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See Section 8.6 on page 78 for information on how to do this.

Figure 117 IP Application > DHCP > VLAN



VID	
Remote DHCP Server 1	0.0.0.0
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	□ Option 82
Information	□ ES-2024PWR

VID	Type	DHCP Status	Delete

The following table describes the labels in this screen.

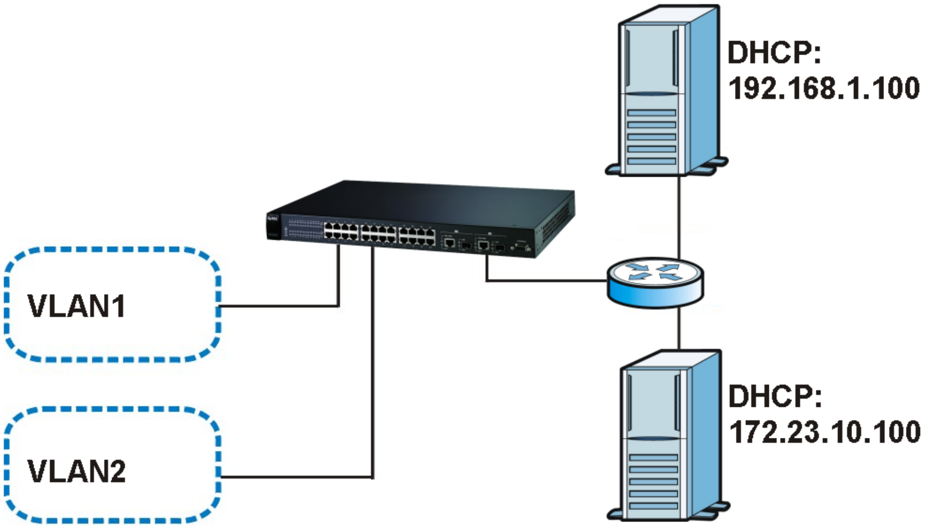
Table 73 IP Application > DHCP > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
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 begin configuring this screen afresh.
Clear	Click this to clear the fields above.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays **Relay** for the DHCP mode.
DHCP Status	This field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

27.4.1 Example: DHCP Relay for Two VLANs

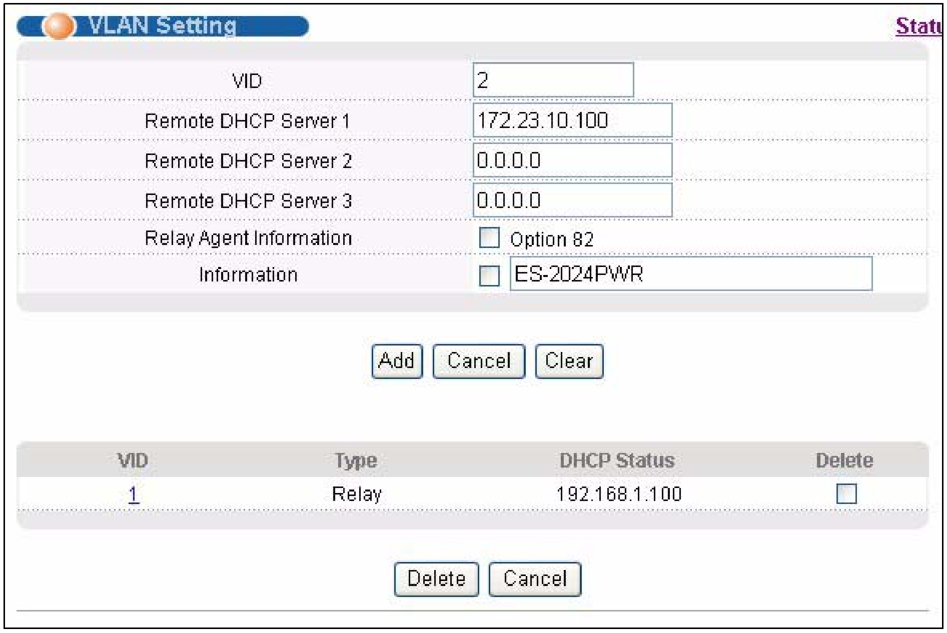
The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.23.10.100.

Figure 118 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 119 DHCP Relay for Two VLANs Configuration Example



VID	2
Remote DHCP Server 1	172.23.10.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Relay Agent Information	□ Option 82
Information	□ ES-2024PWR

VID	Type	DHCP Status	Delete
1	Relay	192.168.1.100	□

PART V
Management

28

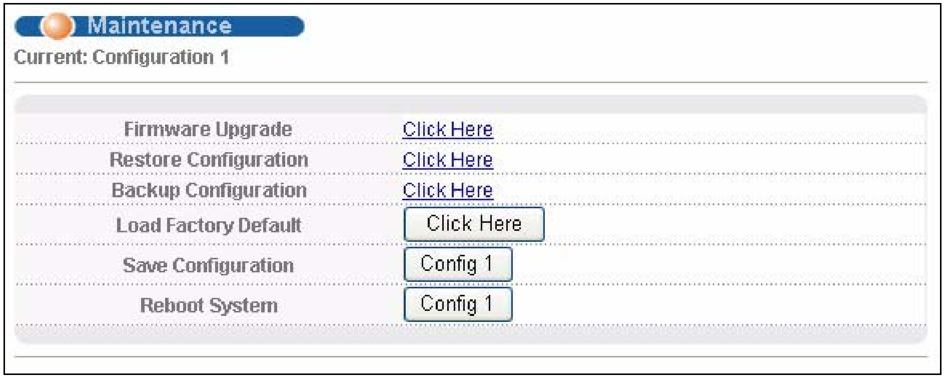
Maintenance

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

28.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 120 Management > Maintenance



Current: Configuration 1

Firmware Upgrade	Click Here
Restore Configuration	Click Here
Backup Configuration	Click Here
Load Factory Default	Click Here
Save Configuration	Config 1
Reboot System	Config 1

The following table describes the labels in this screen.

Table 74 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1**) is currently operating on the Switch.
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.

Table 74 Management > Maintenance (continued)

LABEL	DESCRIPTION
Load Factory Default	Click **Click Here** to reset the configuration to the factory default settings.
Save Configuration	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch.
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.

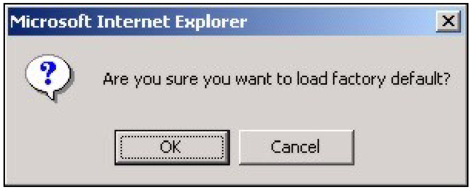
28.2 Load Factory Default

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.

2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 121 Load Factory Default: Start



Microsoft Internet Explorer

Are you sure you want to load factory default?

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).

28.3 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch.

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

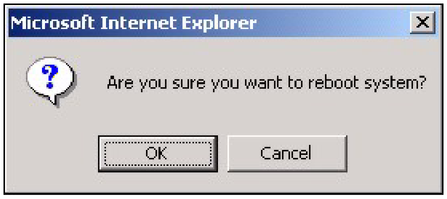
Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

28.4 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. The Switch loads configuration one (**Config 1**) when you reboot. 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 configuration one. The following screen displays.

Figure 122 Reboot System: Confirmation



Microsoft Internet Explorer

Are you sure you want to reboot system?

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.

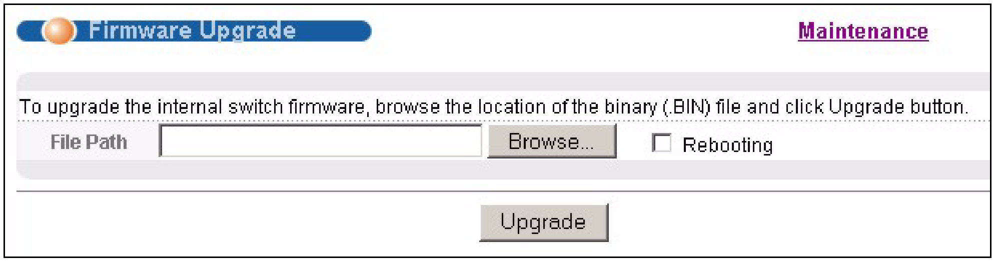
28.5 Firmware Upgrade

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

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

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

Figure 123 Management > Maintenance > Firmware Upgrade



Firmware Upgrade

To upgrade the internal switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

File Path

□ Rebooting

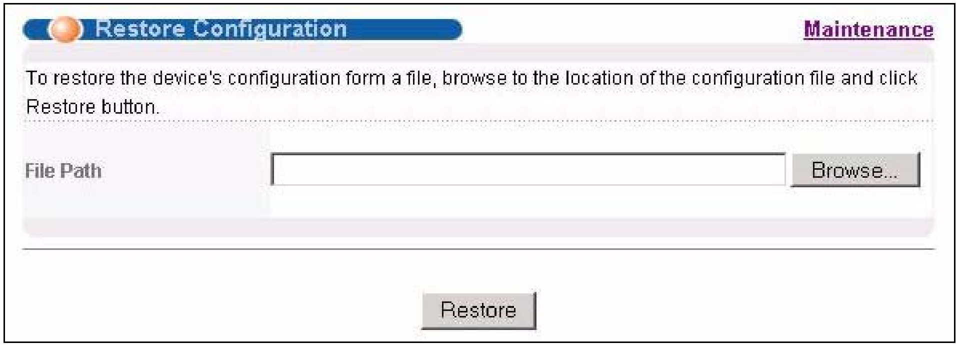
Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** check box if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

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

28.6 Restore a Configuration File

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

Figure 124 Management > Maintenance > Restore Configuration



To restore the device's configuration form a file, browse to the location of the configuration file and click Restore button.

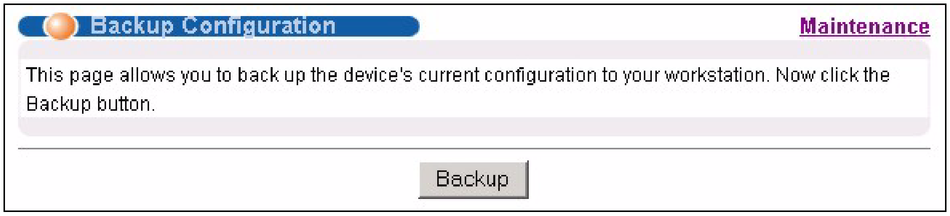
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen (below) from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file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

28.7 Backup 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 125 Management > Maintenance > Backup Configuration



This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.

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.

28.8 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.

28.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch’s settings, they can be saved back to your computer under a filename of your choosing.

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

Table 75 Filename Conventions

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

28.8.1.1 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.

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

28.8.2 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. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter `bin` to set transfer mode to binary.

6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See Table 75 on page 230 for more information on filename conventions.

7 Enter `quit` to exit the ftp prompt.

28.8.3 GUI-based FTP Clients

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

Table 76 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).

28.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) 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.

29

Access Control

This chapter describes how to control access to the Switch.

29.1 Access Control Overview

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

Table 77 Access Control Overview

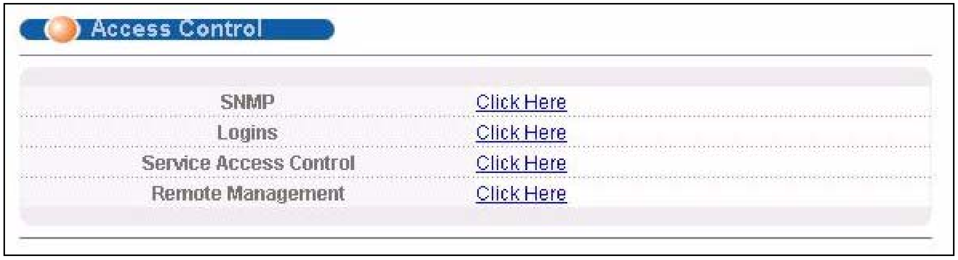
Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

29.2 The Access Control Main Screen

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

Figure 126 Management > Access Control

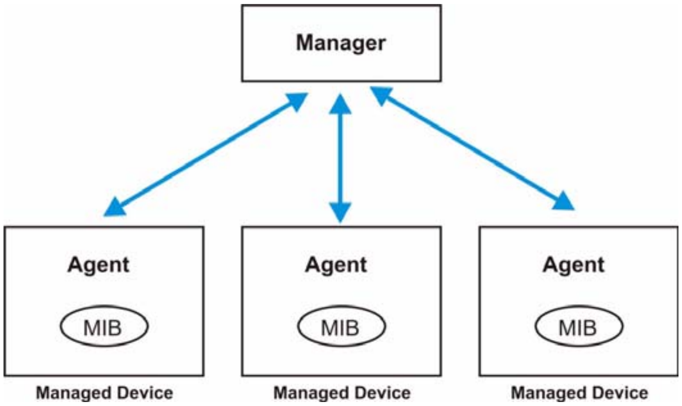


SNMP	Click Here
Logins	Click Here
Service Access Control	Click Here
Remote Management	Click Here

29.3 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), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 127 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 number of packets received, node port status and so on. 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 78 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.

29.3.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

29.3.2 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

29.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with "**1.3.6.1.4.1.890.1.5.8.16**" (ES-2024A) or "**1.3.6.1.4.1.890.1.5.8.27**" (ES-2024PWR) is defined in private MIBs. Otherwise, it is a standard MIB OID.

Table 79 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the fan speed returns to the normal operating range.
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the voltage returns to the normal operating range.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.

Table 79 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when the Switch fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the Switch gets the time and date from a time server.
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when loopguard shuts down a port.

Table 80 SNMP Interface Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when the Ethernet link is down.
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when an Ethernet interface auto-negotiates with the peer Ethernet interface.

Table 80 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
lldp	LLDPRemoteTopologyChange	1.0.8802.1.1.2.0.0.1	This trap is sent when the LLDP (Link Layer Discovery Protocol) remote topology changes.
transceiver-ddmi	transceiverddmiEventOn	1.3.6.1.4.1.890.1.5.8.45.27.2.1	This trap is sent when one of the device operating parameters (such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage) is above or below a factory set normal range.
	transceiverddmiEventClear	1.3.6.1.4.1.890.1.5.8.45.27.2.2	This trap is sent when all device operating parameters return to the normal operating range.

Table 81 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the RADIUS server can be reached.

Table 81 AAA Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
accounting	RADIUSAcctNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
	RADIUSAcctNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when the RADIUS accounting server can be reached.

Table 82 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

Table 83 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.16.107.70.1 1.3.6.1.4.1.890.1.5.8.27.107.70.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.16.107.70.2 1.3.6.1.4.1.890.1.5.8.27.107.70.2	This trap is sent when the MSTP root switch changes.

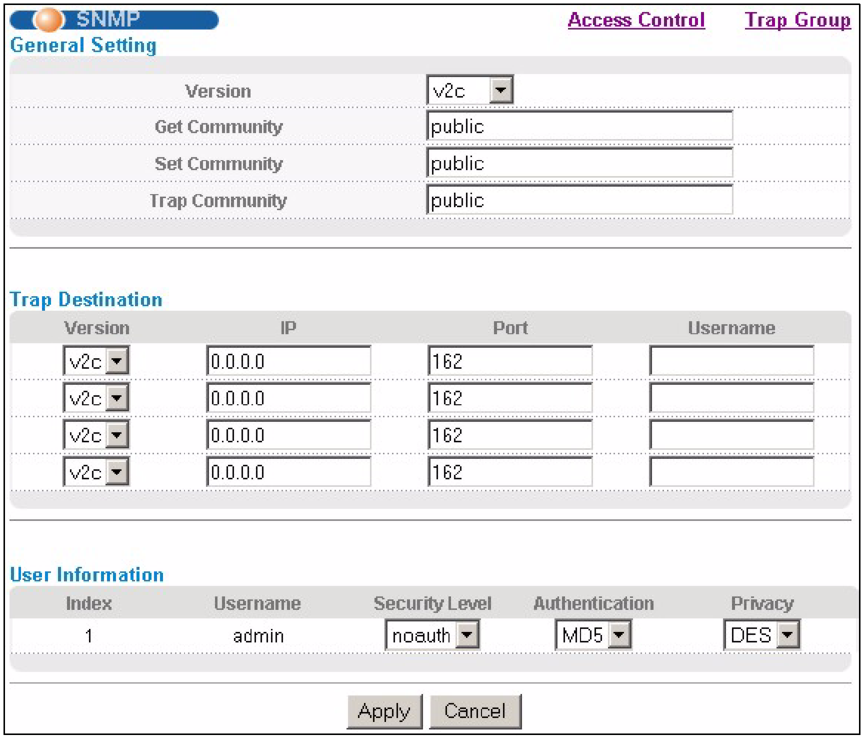
Table 83 SNMP Switch Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.16.27.2.1 1.3.6.1.4.1.890.1.5.8.27.27.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.16.27.2.2 1.3.6.1.4.1.890.1.5.8.27.27.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.4.1.890.1.5.1.1.15	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.4.1.890.1.5.1.1.16	This trap is sent when the variable falls below the RMON "falling" threshold.

29.3.4 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 128 Management > Access Control > SNMP



General Setting

Version: v2c
Get Community: public
Set Community: public
Trap Community: public

Trap Destination

Version	IP	Port	Username
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	

User Information

Index	Username	Security Level	Authentication	Privacy
1	admin	noauth	MD5	DES

The following table describes the labels in this screen.

Table 84 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext- requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the **Set Community**, which is the password for incoming Set-requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. Note: This username must match an existing account on the Switch (configured in **Management > Access Control > Logins** screen).
User Information	Use this section to configure users for authentication with managers using SNMP v3. Note: Use the username and password of the login accounts you specify in this section to create accounts on the SNMP v3 manager.
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the username of a login account on the Switch.

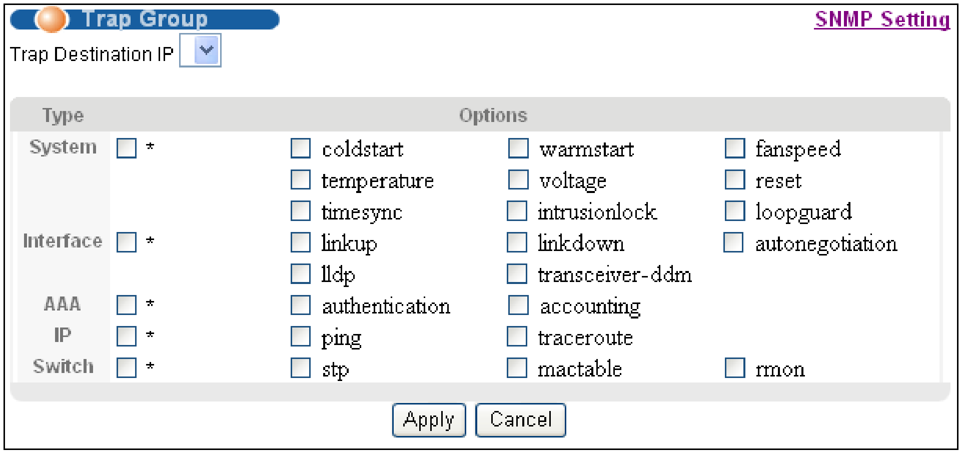
Table 84 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **noauth** -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • **auth** - to implement an authentication algorithm for SNMP messages sent by this user. • **priv** - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
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.

29.3.5 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 129 Management > Access Control > SNMP > Trap Group



Trap Destination IP

Type		Options		
System	□ *	□ coldstart	□ warmstart	□ fanspeed
		□ temperature	□ voltage	□ reset
		□ timesync	□ intrusionlock	□ loopguard
Interface	□ *	□ linkup	□ linkdown	□ autonegotiation
		□ lldp	□ transceiver-ddm	
AAA	□ *	□ authentication	□ accounting	
IP	□ *	□ ping	□ traceroute	
Switch	□ *	□ stp	□ mactable	□ rmon

The following table describes the labels in this screen.

Table 85 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the **SNMP Setting** screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See Section 29.3.3 on page 236 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
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.

29.3.6 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.

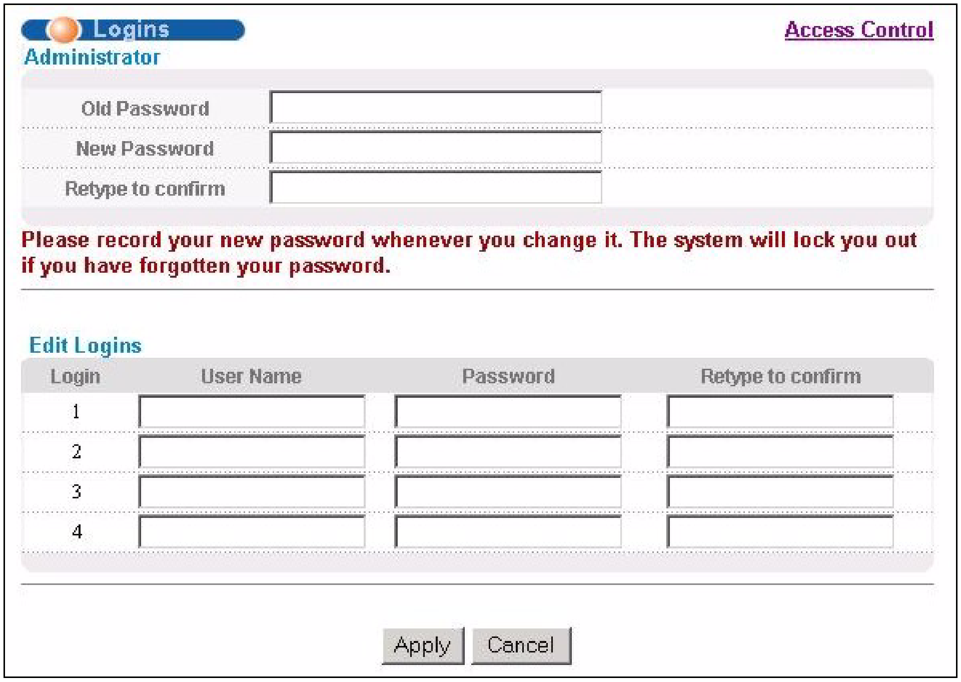
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

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 **Management > Access Control > Logins** to view the screen as shown.

Figure 130 Management > Access Control > Logins



Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.

The following table describes the labels in this screen.

Table 86 Management > 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.

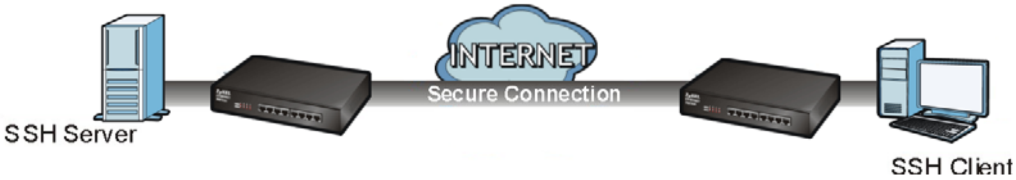
Table 86 Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These users have privilege level 0 (basic read-only access). You can give users higher privileges via the CLI. For more information on assigning privileges see the CLI Reference Guide.	
User Name	Set a user name (up to 32 English keyboard 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.

29.4 SSH Overview

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

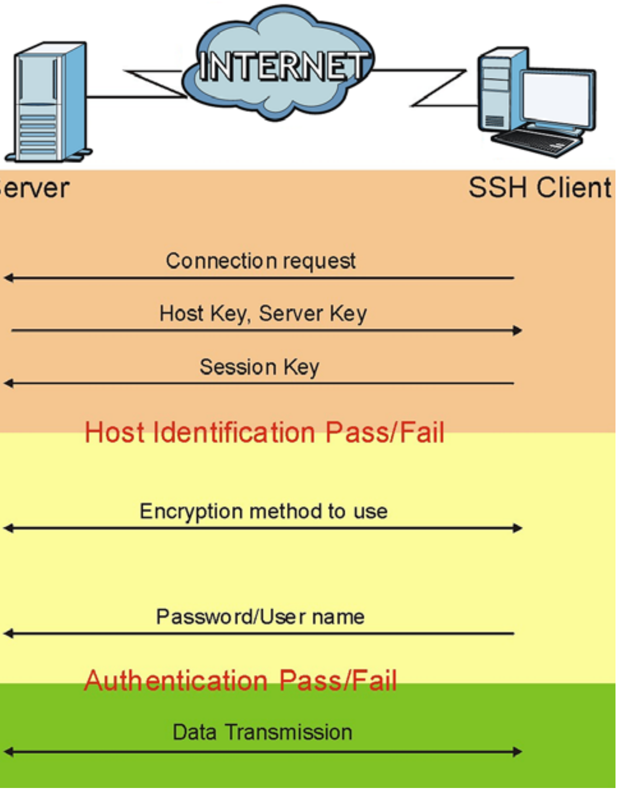
Figure 131 SSH Communication Example



29.5 How SSH works

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

Figure 132 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.

29.6 SSH Implementation on the Switch

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

29.6.1 Requirements for Using SSH

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

29.7 Introduction to HTTPS

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

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

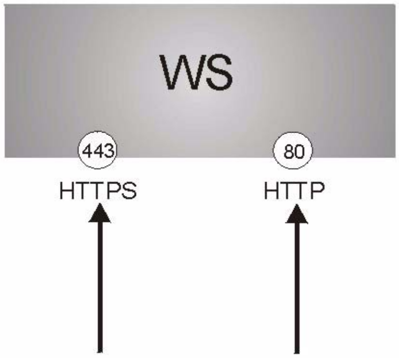
HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. When a computer requests an HTTPS (secure) connection, the Switch sends its certificate to the computer. The user decides if he wants to trust the certificate. If the user decides to trust the certificate, the certificate is used in building the HTTPS connection.

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 133 HTTPS Implementation



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

29.8 HTTPS Example

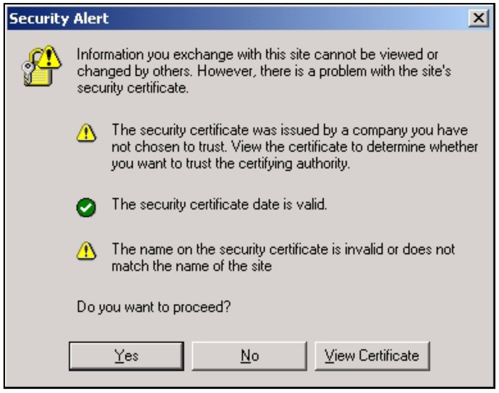
If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

29.8.1 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 134 Security Alert Dialog Box (Internet Explorer)



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

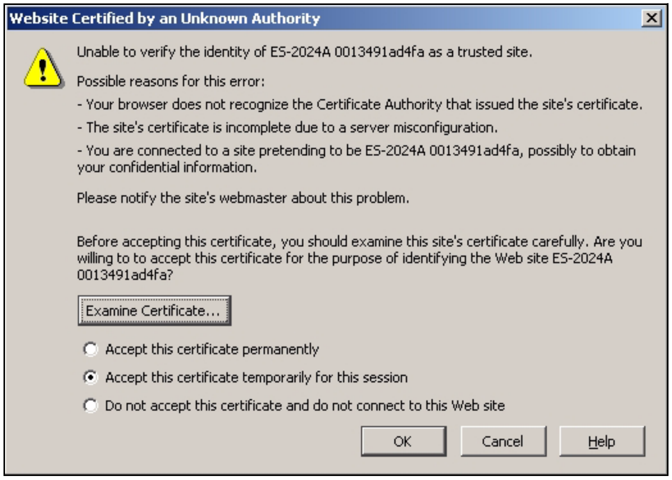
29.8.2 Netscape Navigator Warning Messages

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 135 Security Certificate 1 (Netscape)



Unable to verify the identity of ES-2024A 0013491ad4fa as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

- You are connected to a site pretending to be ES-2024A 0013491ad4fa, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

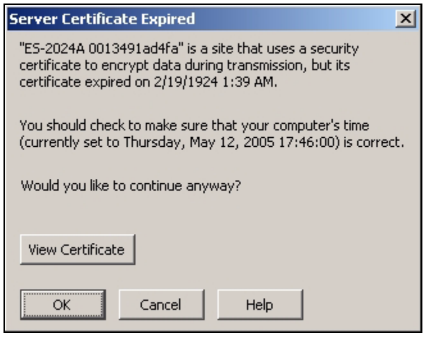
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site ES-2024A 0013491ad4fa?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this Web site

Figure 136 Security Certificate 2 (Netscape)



"ES-2024A 0013491ad4fa" is a site that uses a security certificate to encrypt data during transmission, but its certificate expired on 2/19/1924 1:39 AM.

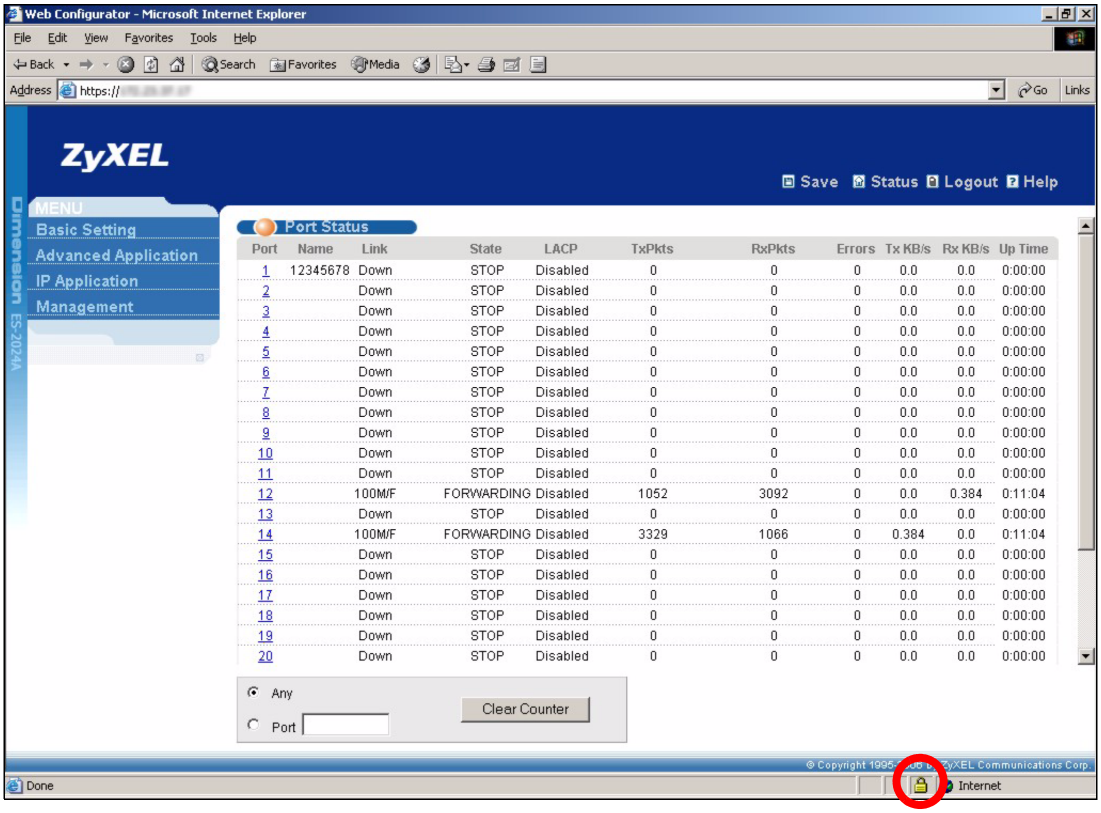
You should check to make sure that your computer's time (currently set to Thursday, May 12, 2005 17:46:00) is correct.

Would you like to continue anyway?

29.8.3 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 137 Example: Lock Denoting a Secure Connection


Web Configurator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://
Go Links
ZyXEL
Save Status Logout Help
Dimension ES-2024A
MENU
Basic Setting
Advanced Application
IP Application
Management
Port Status
© Copyright 1995-2006 by ZyXEL Communications Corp.
Done
Internet

Port	Name	Link	State	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1	12345678	Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
12		100M/F	FORWARDING	Disabled	1052	3092	0	0.0	0.384	0:11:04
13		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
14		100M/F	FORWARDING	Disabled	3329	1066	0	0.384	0.0	0:11:04
15		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
16		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
17		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
18		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
19		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00
20		Down	STOP	Disabled	0	0	0	0.0	0.0	0:00:00

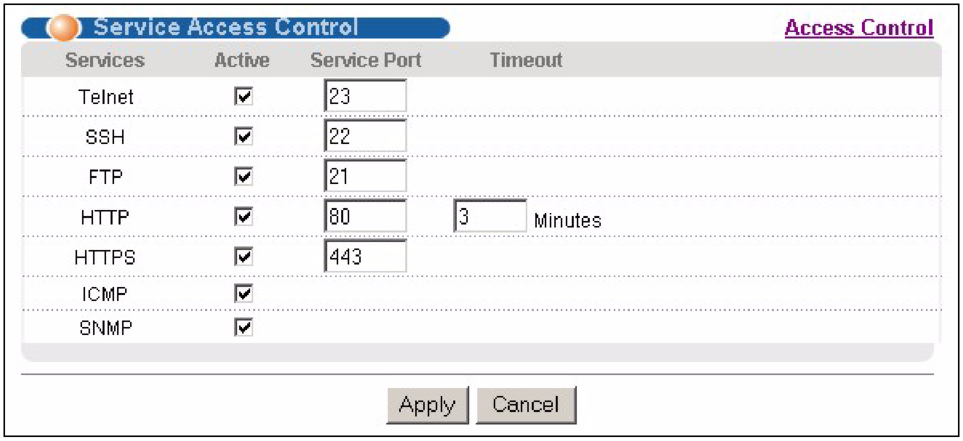
● Any
○ Port

Clear Counter

29.9 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 138 Management > Access Control > Service Access Control



Service Access Control

Access Control

Services	Active	Service Port	Timeout
Telnet	☑	23	
SSH	☑	22	
FTP	☑	21	
HTTP	☑	80	3 Minutes
HTTPS	☑	443	
ICMP	☑		
SNMP	☑		

The following table describes the fields in this screen.

Table 87 Management > Access Control > Service Access Control

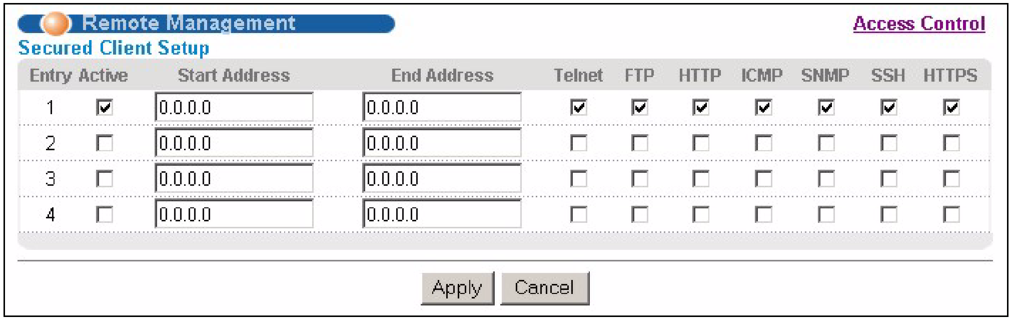
LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the 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 (1-255) 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.

29.10 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 139 Management > Access Control > Remote Management



Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☑	0.0.0.0	0.0.0.0	☑	☑	☑	☑	☑	☑	☑
2	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
3	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□
4	□	0.0.0.0	0.0.0.0	□	□	□	□	□	□	□

The following table describes the labels in this screen.

Table 88 Management > 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.

30

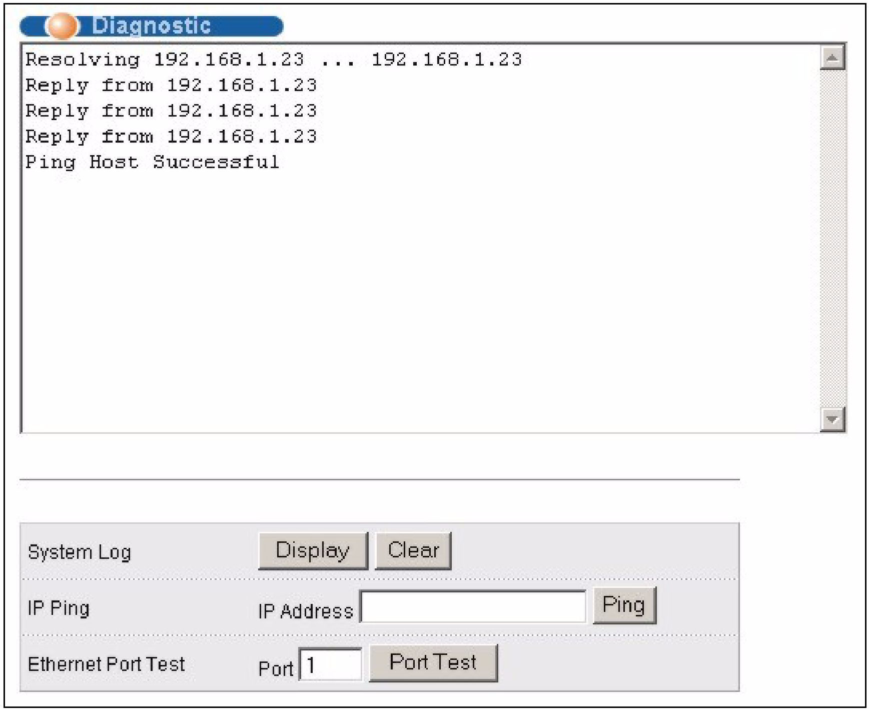
Diagnostic

This chapter explains the **Diagnostic** screen.

30.1 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 140 Management > Diagnostic



```
Resolving 192.168.1.23 ... 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Reply from 192.168.1.23
Ping Host Successful
```

System Log	Display Clear
IP Ping	IP Address ____ Ping
Ethernet Port Test	Port 1 Port Test

The following table describes the labels in this screen.

Table 89 Management > 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 an internal loopback test.

31

Syslog

This chapter explains the syslog screens.

31.1 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.

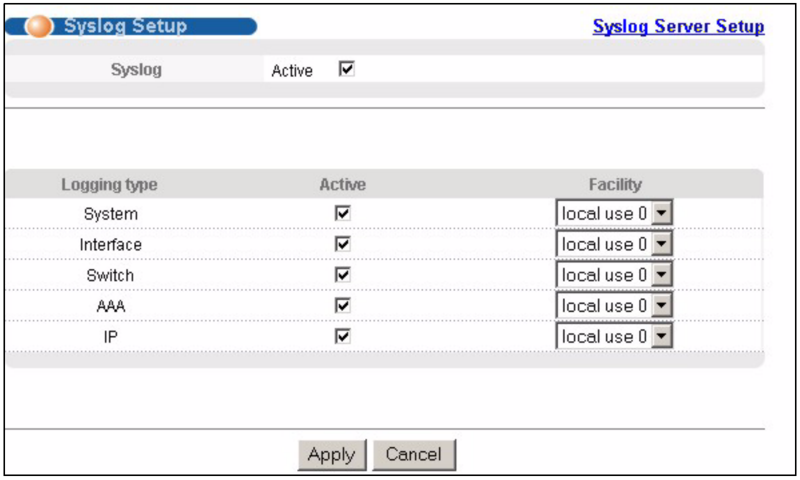
Table 90 Syslog Severity Levels

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.

31.2 Syslog Setup

Click **Management** > **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 141 Management > Syslog



Syslog	Active ☑

Logging type	Active	Facility
System	☑	local use 0
Interface	☑	local use 0
Switch	☑	local use 0
AAA	☑	local use 0
IP	☑	local use 0

The following table describes the labels in this screen.

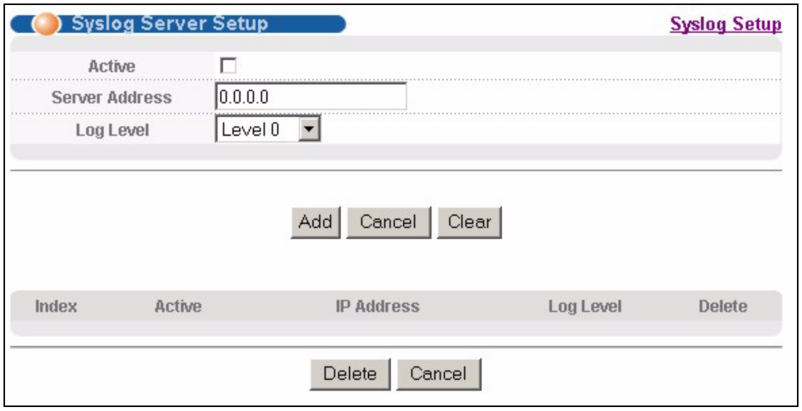
Table 91 Management > Syslog

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 begin configuring this screen afresh.

31.3 Syslog Server Setup

Click **Management** > **Syslog** > **Syslog Server Setup** to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 142 Management > Syslog > Server Setup



Syslog Server Setup

Active	□
Server Address	0.0.0.0
Log Level	Level 0

Index	Active	IP Address	Log Level	Delete

The following table describes the labels in this screen.

Table 92 Management > 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 begin configuring this screen afresh.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32

Cluster Management

This chapter introduces cluster management.

32.1 Clustering Management Status Overview

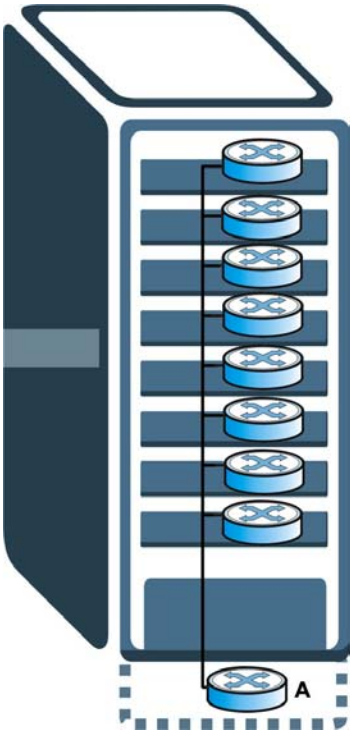
Cluster Management allows you to manage switches through one switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 93 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 143 Clustering Application Example

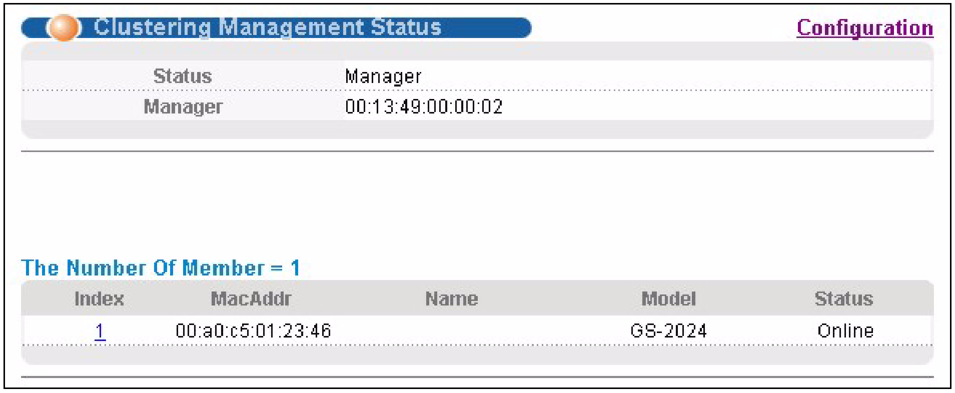


32.2 Cluster Management Status

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

Note: A cluster can only have one manager.

Figure 144 Management > Cluster Management



Status	Manager
Manager	00:13:49:00:00:02

The Number Of Member = 1

Index	MacAddr	Name	Model	Status
1	00:a0:c5:01:23:46		GS-2024	Online

The following table describes the labels in this screen.

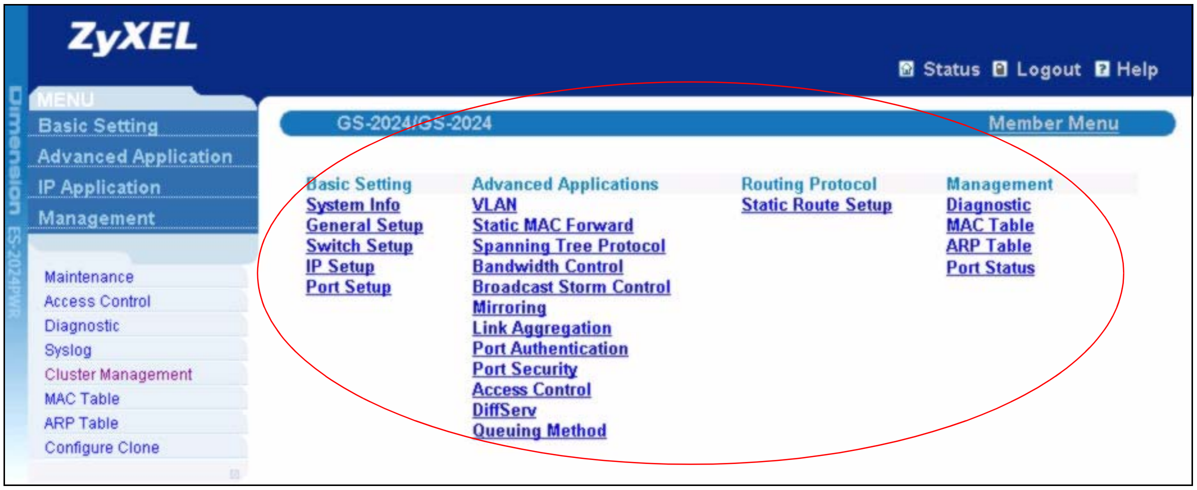
Table 94 Management > Cluster Management

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 145 on page 264).
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)

32.2.1 Cluster Member Switch Management

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

Figure 145 Cluster Management: Cluster Member Web Configurator Screen



32.2.1.1 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 146 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 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        3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group         393216 Jul 01 12:00 config
--w--w--w-   1 owner    group              0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group              0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 370lt0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

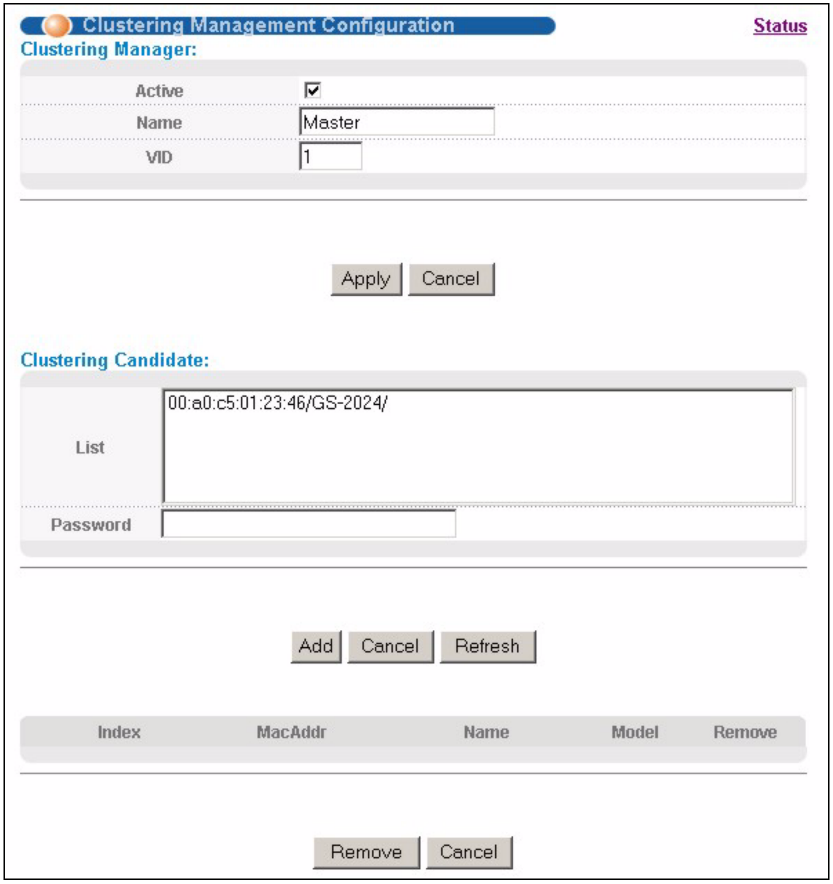
Table 95 FTP Upload to Cluster Member Example

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.
`360lt0.bin`	This is the name of the firmware file you want to upload to the cluster member switch.
`fw-00-a0-c5-01-23-46`	This is the cluster member switch’s firmware name as seen in the cluster manager switch.
`config-00-a0-c5-01-23-46`	This is the cluster member switch’s configuration file name as seen in the cluster manager switch.

32.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 147 Management > Clustering Management > Configuration



Clustering Management Configuration

Clustering Manager:

Active	☑
Name	Master
VID	1

Clustering Candidate:

List	00:a0:c5:01:23:46/GS-2024/
Password	

Index	MacAddr	Name	Model	Remove

The following table describes the labels in this screen.

Table 96 Management > 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 screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen and a warning icon (⚠) appears in the member summary list below. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
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 begin configuring this screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.

Table 96 Management > Clustering Management > Configuration (continued)

LABEL	DESCRIPTION
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 screen afresh.

33

MAC Table

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

33.1 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.

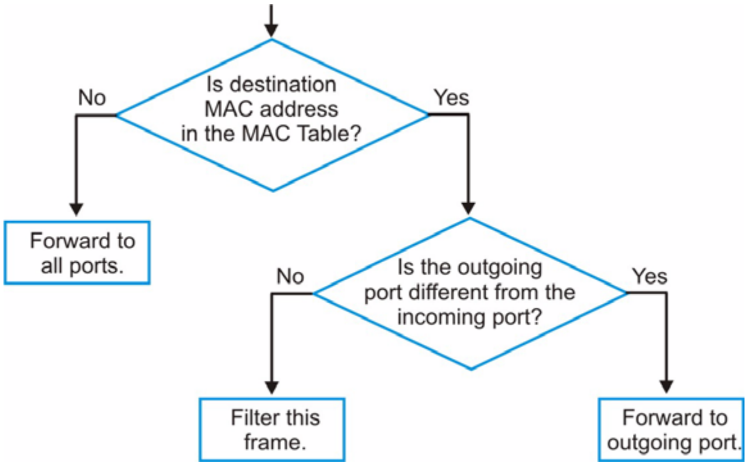
1 The Switch examines a received frame and learns the port on which this source MAC address came.

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.

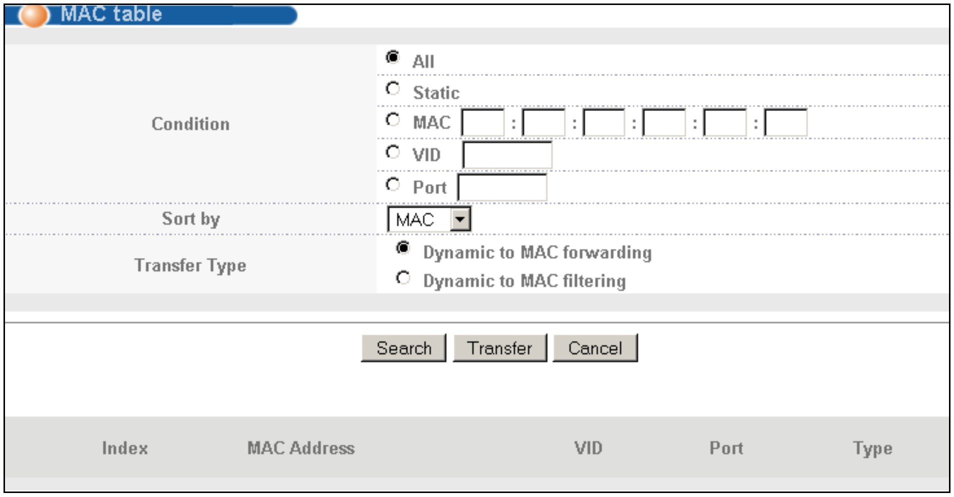
Figure 148 MAC Table Flowchart


Is destination MAC address in the MAC Table?
No
Yes
Forward to all ports.
Is the outgoing port different from the incoming port?
No
Yes
Filter this frame.
Forward to outgoing port.

33.2 Viewing the MAC Table

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

Figure 149 Management > MAC Table



MAC table

Condition	● All ○ Static ○ MAC [ ] : [ ] : [ ] : [ ] : [ ] : [ ] ○ VID [ ] ○ Port [ ]
Sort by	MAC ▾
Transfer Type	● Dynamic to MAC forwarding ○ Dynamic to MAC filtering

Search | Transfer | Cancel

Index	MAC Address	VID	Port	Type

The following table describes the labels in this screen.

Table 97 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the buttons and click **Search** to only display the data which matches the criteria you specified. Select **All** to display any entry in the MAC table of the Switch. Select **Static** to display the MAC entries manually configured on the Switch. Select **MAC** and enter a MAC address in the field provided to display a specified MAC entry. Select **VID** and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select **Port** and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port.
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
MAC	Click this button to display and arrange the data according to MAC address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).

34

ARP Table

This chapter introduces ARP Table.

34.1 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.

34.1.1 How ARP Works

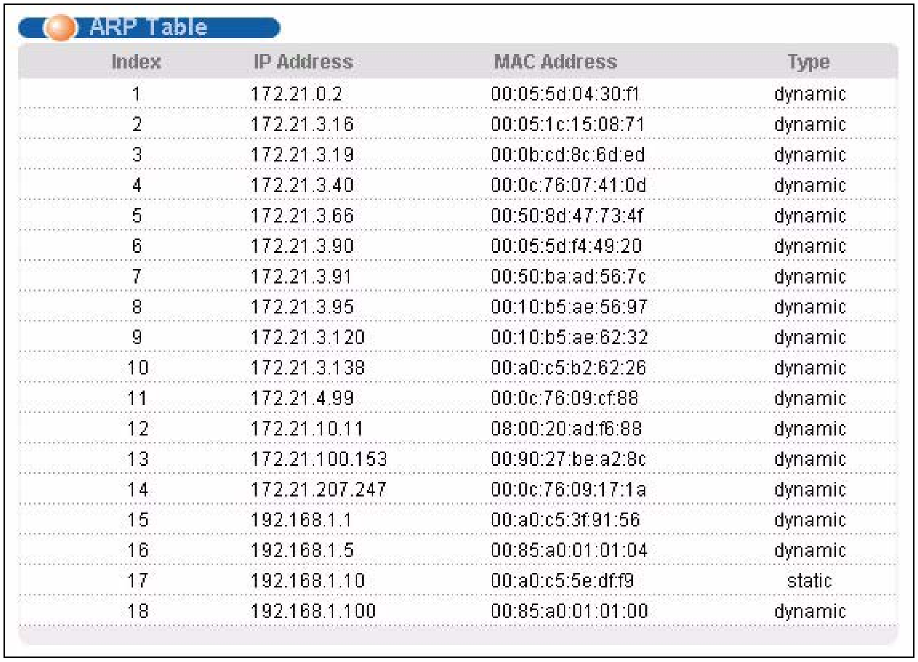
When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

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.

34.2 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 150 Management > ARP Table



ARP Table

Index	IP Address	MAC Address	Type
1	172.21.0.2	00:05:5d:04:30:f1	dynamic
2	172.21.3.16	00:05:1c:15:08:71	dynamic
3	172.21.3.19	00:0b:cd:8c:6d:ed	dynamic
4	172.21.3.40	00:0c:76:07:41:0d	dynamic
5	172.21.3.66	00:50:8d:47:73:4f	dynamic
6	172.21.3.90	00:05:5d:f4:49:20	dynamic
7	172.21.3.91	00:50:ba:ad:56:7c	dynamic
8	172.21.3.95	00:10:b5:ae:56:97	dynamic
9	172.21.3.120	00:10:b5:ae:62:32	dynamic
10	172.21.3.138	00:a0:c5:b2:62:26	dynamic
11	172.21.4.99	00:0c:76:09:cf:88	dynamic
12	172.21.10.11	08:00:20:ad:f6:88	dynamic
13	172.21.100.153	00:90:27:be:a2:8c	dynamic
14	172.21.207.247	00:0c:76:09:17:1a	dynamic
15	192.168.1.1	00:a0:c5:3f:91:56	dynamic
16	192.168.1.5	00:85:a0:01:01:04	dynamic
17	192.168.1.10	00:a0:c5:5e:df:f9	static
18	192.168.1.100	00:85:a0:01:01:00	dynamic

The following table describes the labels in this screen.

Table 98 Management > 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).

35

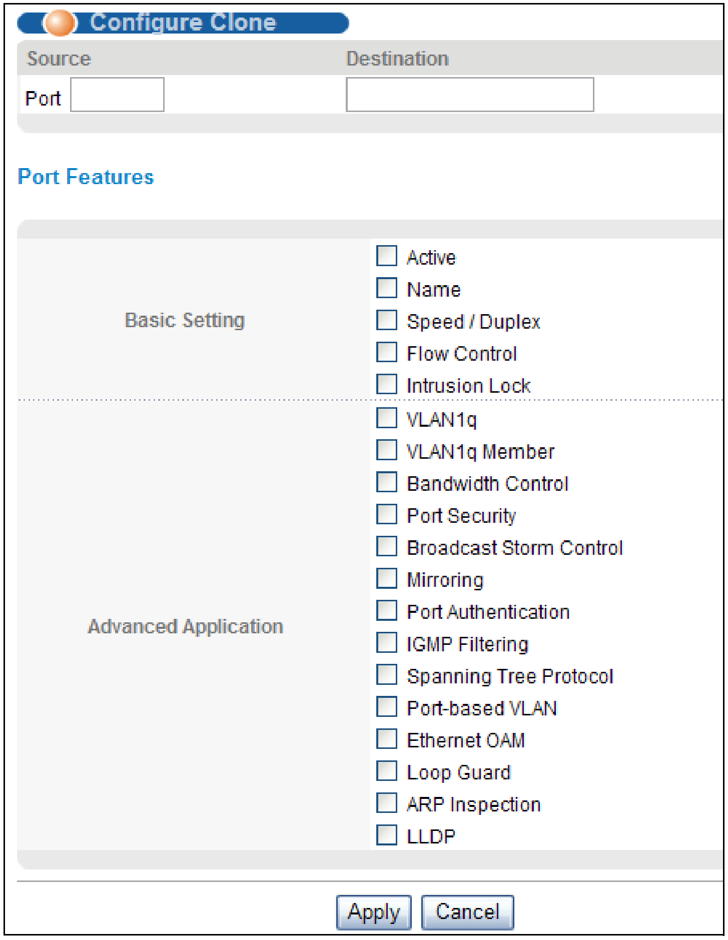
Configure Clone

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

35.1 Configure Clone

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

Figure 151 Management > Configure Clone



Configure Clone

Source		Destination
Port		

Port Features

Basic Setting	□ Active □ Name □ Speed / Duplex □ Flow Control □ Intrusion Lock
Advanced Application	□ VLAN1q □ VLAN1q Member □ Bandwidth Control □ Port Security □ Broadcast Storm Control □ Mirroring □ Port Authentication □ IGMP Filtering □ Spanning Tree Protocol □ Port-based VLAN □ Ethernet OAM □ Loop Guard □ ARP Inspection □ LLDP

The following table describes the labels in this screen.

Table 99 Management > 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** menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (you configured in the **Advanced Application** menus) 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 begin configuring this screen afresh.

Part VI
Appendices and Index

A

Product Specifications

The following tables summarize the Switch’s hardware and firmware features.

Table 100 Hardware Specifications

SPECIFICATION	DESCRIPTION
Dimensions	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)
Weight	ES-2024A: 2.2 kg ES-2024PWR: 4.0 kg
AC Model Power Consumption	ES-2024A: 24 W ES-2024PWR: 200 W
AC Model Power Supply	100-240 VAC, 50/60 Hz ES-2024A: 0.4 A ES-2024PWR: 2 A
DC Model Power Consumption	ES-2024A: 16.8 W

Table 100 Hardware Specifications (continued)

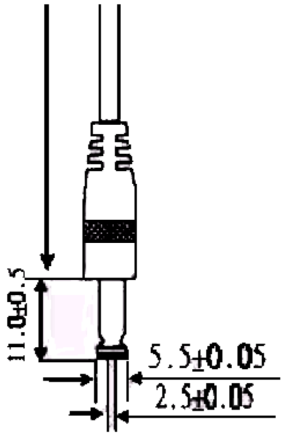
SPECIFICATION	DESCRIPTION
DC Model Power Specification	Overload protection 12 V DC 1.4 A maximum. The power wires should be at least 18 AWG (American Wire Gauge). AWG is a measurement system that specifies the thickness of wire. The thicker the wire, the smaller the AWG number. Use a standard 2.5 mm jack plug. The DC power plug should match the following specifications (the measurements are in millimeters). **Figure 152** DC Power Plug 
Operating Environment	Temperature: 0º C ~ 45º C (32º F ~ 113º F) Humidity: 10 ~ 90% (non-condensing)
Storage Environment	Temperature: -25º C ~ 70º C (13º F ~ 158º F) Humidity: 10 ~ 90% (non-condensing)
Fast Ethernet Ports	24 100Base-Tx ports RJ-45 Ethernet cable connector Auto-negotiation Auto-MDI/MDI-X Compliant with 802.3/802.3u Back-pressure flow control in half duplex mode 802.3x flow control in full duplex mode (ES-2024PWR only) Power over Ethernet to 24 PoE ports (max. 15.4 Watt/port, 185Watt/system) Power budget management

Table 100 Hardware Specifications (continued)

SPECIFICATION	DESCRIPTION
Gigabit Ethernet Ports	2 Dual Personality interfaces(1000Base-T and SFP redundant) Supports 100/1000 full duplex mode only Compliant with 802.3z/802.3ab Copper/fiber interface auto-selection by signal detection (Fiber first)
Console Port	D-Sub 9 pin Female (DCE)
System Monitoring	Voltage: 1.25 V: +/- 6% 1.8 V: +/- 6% 3.3 V: +/- 6% 2.5 V: +/- 6% Temperature: CPU: 60 degrees C MAC: 60 degrees C Fan Speed: 3500~8000 rpm

Table 101 Feature Descriptions

FEATURE	DESCRIPTION
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.
MAC Address Filter	Filter traffic based on the source and/or destination MAC address and VLAN group (ID).
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the relay DHCP requests to DHCP servers on your network.
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.
Differentiated Services (DiffServ)	With DiffServ, the Switch marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
Queuing	Queuing is used to help solve performance degradation when there is network congestion. Three 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.

Table 101 Feature Descriptions (continued)

FEATURE	DESCRIPTION
Port Mirroring	Port mirroring allows you to copy traffic going from one or all ports to another or all ports in order that you can examine the traffic from the mirror port (the port you copy the traffic to) without interference.
Static Route	Static routes tell the Switch how to forward IP traffic when you configure the TCP/IP parameters manually.
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) / MSTP (Multiple 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. The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.
Loop Guard	Use the loop guard feature to protect against network loops on the edge of your network.
IP Source Guard	Use IP source guard to filter unauthorized ARP packets in your network.
Link Aggregation	Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.
Port Authentication and Security	For security, the Switch allows authentication using IEEE 802.1x with an external RADIUS server and port security that allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch.
Authentication, Authorization and Accounting	The Switch supports authentication, authorization and accounting services via RADIUS and TACACS+ AAA servers.
Device Management	Use the web configurator or commands to easily configure the rich range of features on the Switch.
Port Cloning	Use the port cloning feature to copy the settings you configure on one port to another port or ports.
Syslog	The Switch can generate syslog messages and send it to a syslog server.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, CLI or an FTP/TFTP tool to put it on the Switch. Note: Only upload firmware for your specific model!

Table 101 Feature Descriptions (continued)

FEATURE	DESCRIPTION
Configuration Backup & Restoration	Make a copy of the Switch's configuration and put it back on the Switch later if you decide you want to revert back to an earlier configuration.
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.
LLDP (Link Layer Discovery Protocol)	The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.
OAM (Operations, Administration and Maintenance)	Ethernet OAM as described in IEEE 802.3ah is a link monitoring protocol. It utilizes OAM Protocol Data Units or OAM PDU's to transmit link status information between directly connected Ethernet devices. Both devices must support IEEE 802.3ah. Because link layer Ethernet OAM operates at layer two of the OSI (Open Systems Interconnection Basic Reference) model, neither IP or SNMP are necessary to monitor or troubleshoot network connection problems.

Table 102 Firmware Specifications

FEATURE	SPECIFICATION
Default IP Address	192.168.1.1
Number of IP Addresses Configurable	64
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
Number of Login Accounts Configurable on the Switch	4 management accounts configured on the Switch. Authentication via RADIUS and TACACS+ also available.
Bridging	8K MAC addresses (2 way set associative) Static MAC address forwarding 256 entries Broadcast storm control per port Automatic address learning and aging Aging time from 10 to 3000 sec default 300 sec

Table 102 Firmware Specifications (continued)

FEATURE	SPECIFICATION
Switching	8.8 Gbps, non-blocking Maximum frame size: 1522 bytes including tag/CRC Store and forward
QoS	802.1p 4 priority queue with SP/WRR Port-based rate control in 64Kbps for both ingress and egress IGMP snooping DSCP to 802.1p priority mapping
Multicasting	IGMP snooping per VLAN (IGMPv1/v2/v3 up to 16 VLAN, user configurable), up to 256 groups IGMP filtering MVR Configurable IGMP snooping timer and priority. IGMP throttling Static multicast IGMP snooping fast-leave IGMP snooping statistics
IP service	DHCP relay
Spanning Tree	802.1w rapid spanning tree protocol 802.1s MSTP
VLAN	Port based VLAN 802.1Q VLAN Maximum number of VLAN: 4K, 256 static VLAN GVRP for dynamic group registration VLAN ingress filtering Acceptable frame type for tagged only and all frames

Table 102 Firmware Specifications (continued)

FEATURE	SPECIFICATION
Security	Static MAC address forward Static MAC address filtering Block unresolved address forwarding/Port security Limiting number of dynamic address per port. 802.1x port authentication by RADIUS Management login by RADIUS authentication. SSHv1/v2 SSL MAC freeze Intrusion lock Multiple RADIUS servers Multiple TACACS+ servers 802.1X VLAN and bandwidth assignment. Login authentication by RADIUS Login authentication by TACACS+ IP source guard Static IP/MAC binding ARP Inspection
AAA	Support RADIUS and TACACS+
Port aggregation	2 groups for fast Ethernet, 1 group for gigabit Ethernet 4 ports per group randomly selected (100BaseTX) Supports 802.3ad static and LACP dynamic aggregation
Port mirroring	Port-based mirroring to a monitor port
Bandwidth Control	Ingress rate limiting in 64-Kbps steps Egress shaping in 64-Kbps steps

Table 102 Firmware Specifications (continued)

FEATURE	SPECIFICATION
Clustering	Act as clustering slave or master 24 slaves can be managed in a cluster at most
System management	Configuration by console/Telnet/web Firmware upgrade by FTP/web/console Configuration backup and restore by FTP/web/console System management access control System clock by manual setup or NTP SNMP v2c / v3 Telnet (up to 9 concurrent sessions) RMON group 1,2,3,9 ICMP echo/echo reply Cisco-like CLI commands Text based configuration file Administration user management Syslog Daylight saving time support 802.3ah OAM Loop guard

The following list, which is not exhaustive, illustrates the standards supported in the Switch.

Table 103 Standards Supported

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 894	Ethernet II Encapsulation
RFC 1112	Internet Group Management Protocol v1
RFC 1155	SMI
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs

Table 103 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1757	RMON
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2131, RFC 2132	Dynamic Host Configuration Protocol (DHCP)
RFC 2138	RADIUS (Remote Authentication Dial In User Service)
RFC 2139	RADIUS Accounting
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2475	DSCP to IEEE 802.1p priority mapping
RFC 2674	SNMP v2, v2c P-BRIDGE-MIB, Q-BRIDGE-MIB
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 3046	DHCP Relay
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP v3)
RFC 3580	RADIUS - Tunnel Protocol Attribute
IEEE 802.1x	Port Based Network Access Control
IEEE 802.1ab	Link Layer Discovery Protocol
IEEE 802.1d	MAC Bridges
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1q	Tagged VLAN
IEEE 802.1w	Rapid Spanning Tree Protocol (RSTP)
IEEE 802.1s	Multiple Spanning Tree Protocol (MSTP)
IEEE 802.3	Packet Format
IEEE 802.3ad	Link Aggregation
IEEE 802.3af	Power over Ethernet
IEEE 802.3ah	Ethernet OAM (Operations, Administration and Maintenance)
IEEE 802.3u	Fast Ethernet
IEEE 802.3x	Flow Control
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

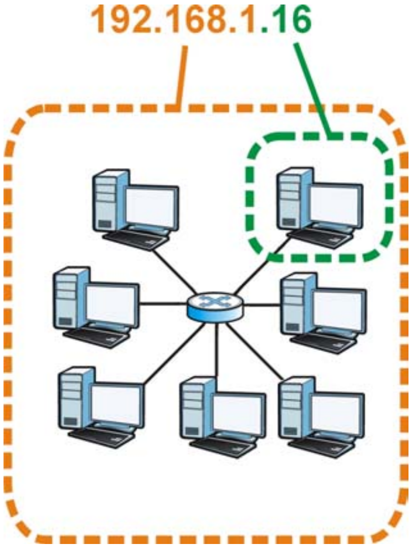
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 153 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

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). The term “subnet” is short for “sub-network”.

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.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 104 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

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.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 105 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 106 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

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 subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 107 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (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
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

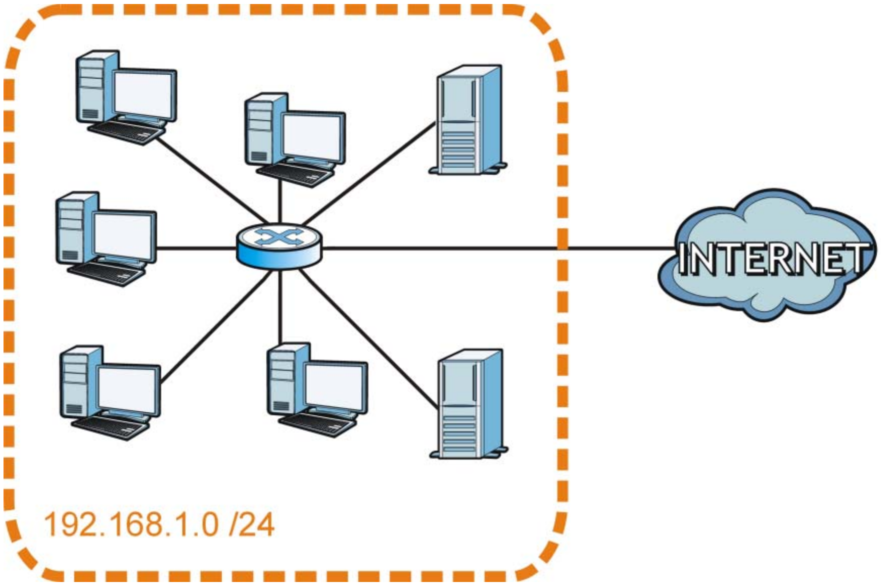
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 154 Subnetting Example: Before Subnetting

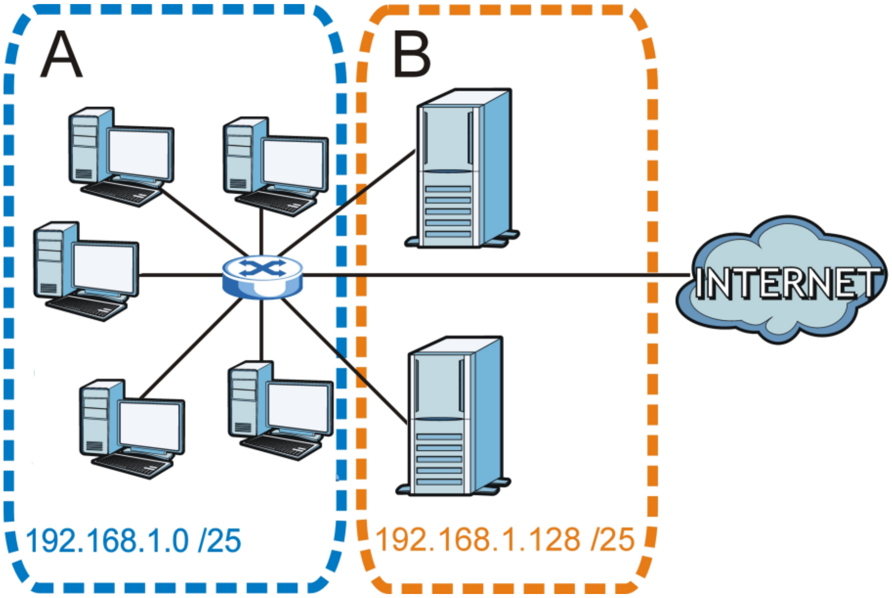


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 155 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit 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 (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 108 Subnet 1

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

Table 109 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 110 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 111 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

Table 111 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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 IP address last octet values for each subnet.

Table 112 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

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 113 24-bit Network Number 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

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 114 16-bit Network Number 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

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the Switch.

Once you have decided on the network number, pick an IP address for your Switch that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Switch will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Switch unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

C

Legal Information

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 (Class B)

Federal Communications Commission (FCC) Interference Statement

The 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.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Notices

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

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France. (for IEEE 802.11b/g wireless devices)

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

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

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

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

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 five 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 your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

- 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index