GS1510-16/GS1510-24

16-port / 24-port Managed Gigabit Ethernet Switch

User's Guide

Default Login Details

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

Firmware Version 1.00
Edition 1, 9/2010

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the Switch using the Web Configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Supporting 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.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.

- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

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. See http://www.zyxel.com/web/contact_us.php for contact information. 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.

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.

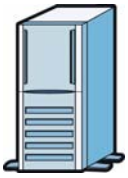
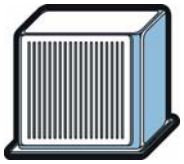
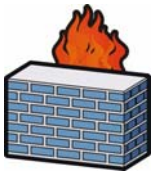
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The GS1510-16/GS1510-24 may be referred to as the "Switch", the "device", or the "system" in this User's Guide.
- 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.
- 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.
- 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

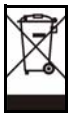
Figures in this User's Guide may use the following generic icons. The Switch icon is not an exact representation of your device.

Switch 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 
Switch 		

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.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

This product is recyclable. Dispose of it properly.



Contents Overview

Table of Contents

PART I
Introduction and Hardware Overview

1

Getting to Know Your Switch

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

1.1 Introduction

Your Switch is an intelligent layer 2 switch with 1000BASE-T RJ-45 ports and mini-GBIC slots (GS1510-24 only) for fiber-optic transceivers.

- The GS1510-16 has 16 1000BASE-T RJ-45 ports.
- The GS1510-24 has 24 1000BASE-T RJ-45 ports, and two SFP open slots.

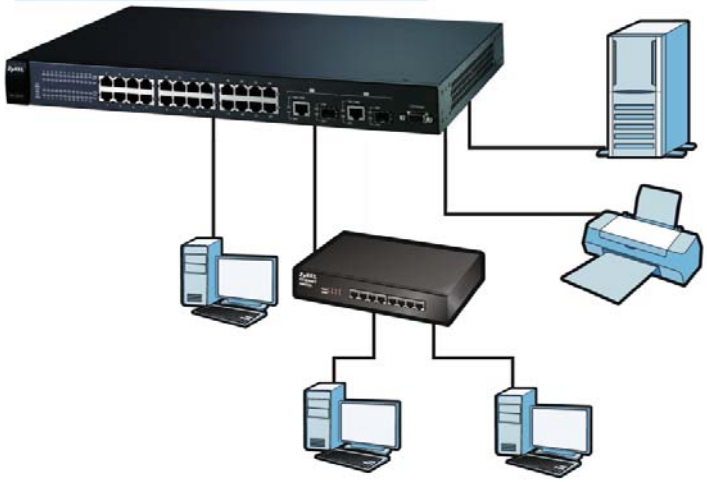
With its built-in Web Configurator, managing and configuring the Switch is easy. The Switch can operate in low power idle mode in compliance with IEEE 802.3az Energy Efficient Ethernet (EEE). See Chapter 25 on page 151 for a full list of software features available on the Switch.

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

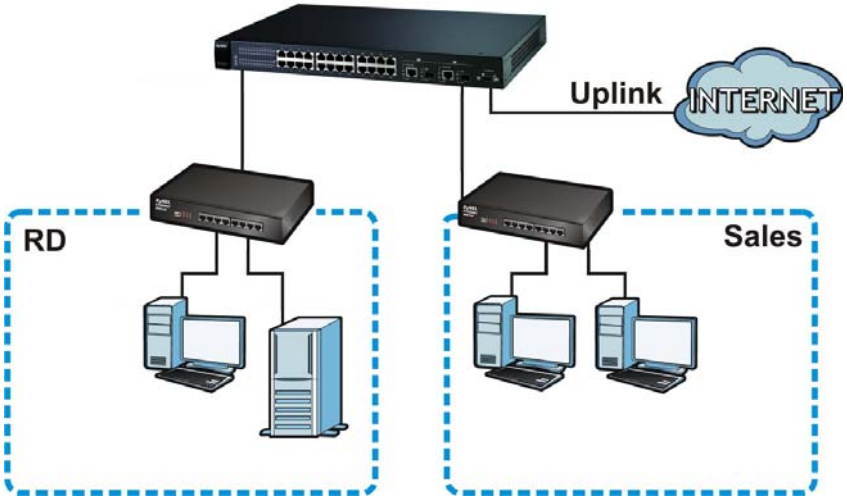


1.1.2 Bridging Example

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

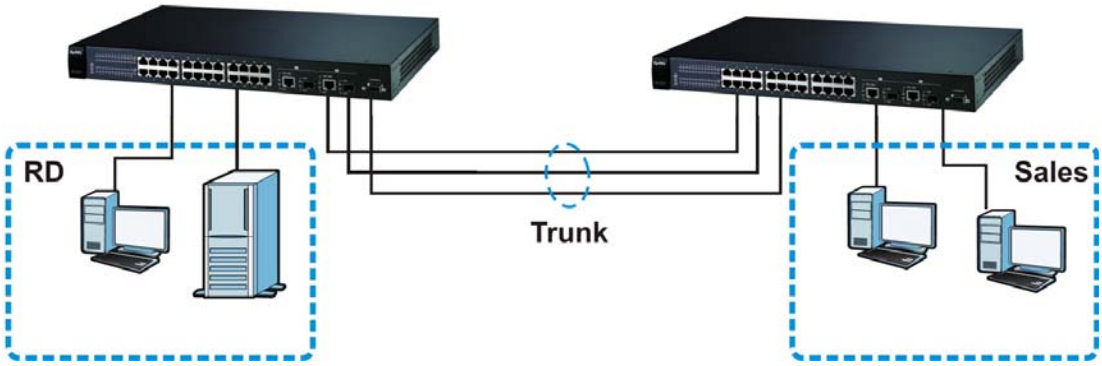


1.1.3 High Performance Switching Example

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.

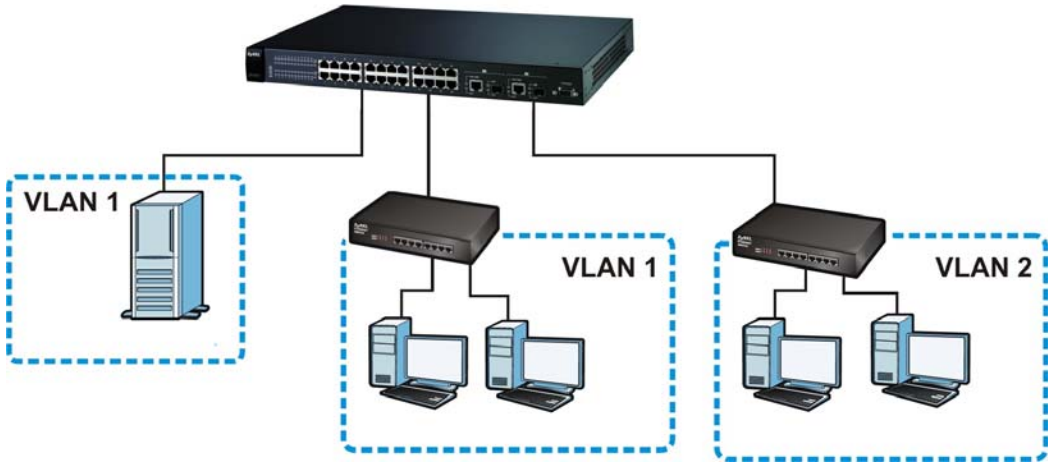
For more information on VLANs, refer to Chapter 10 on page 63.

1.1.4.1 Tag-based VLAN Example

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

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 on the Switch can belong to other VLAN groups too.

Figure 4 Shared Server Using VLAN Example



1.2 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

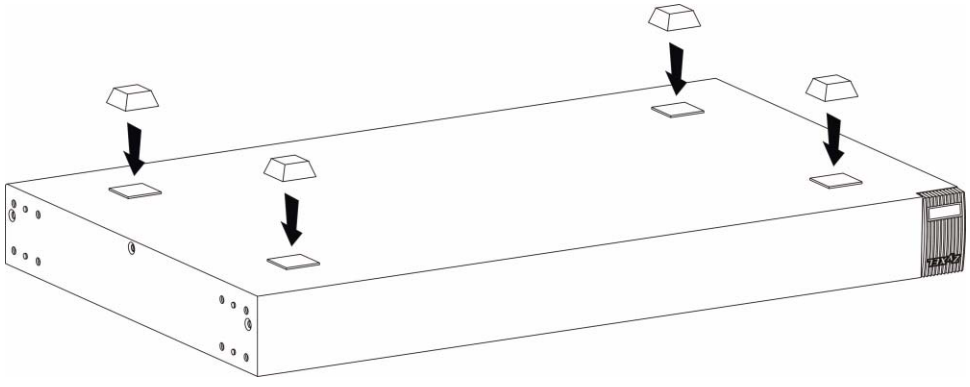
Hardware Installation and Connection

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.

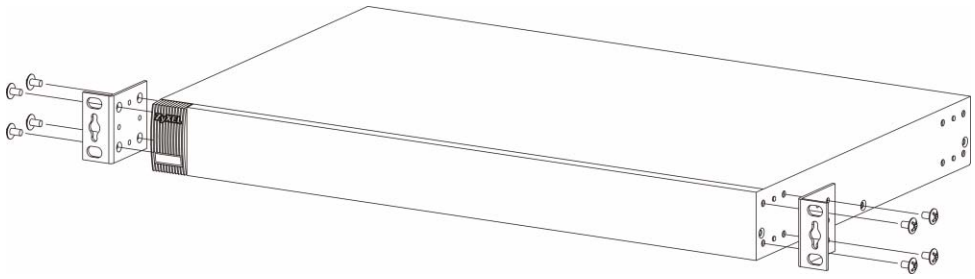
2.2.1.1 Precautions

- 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.

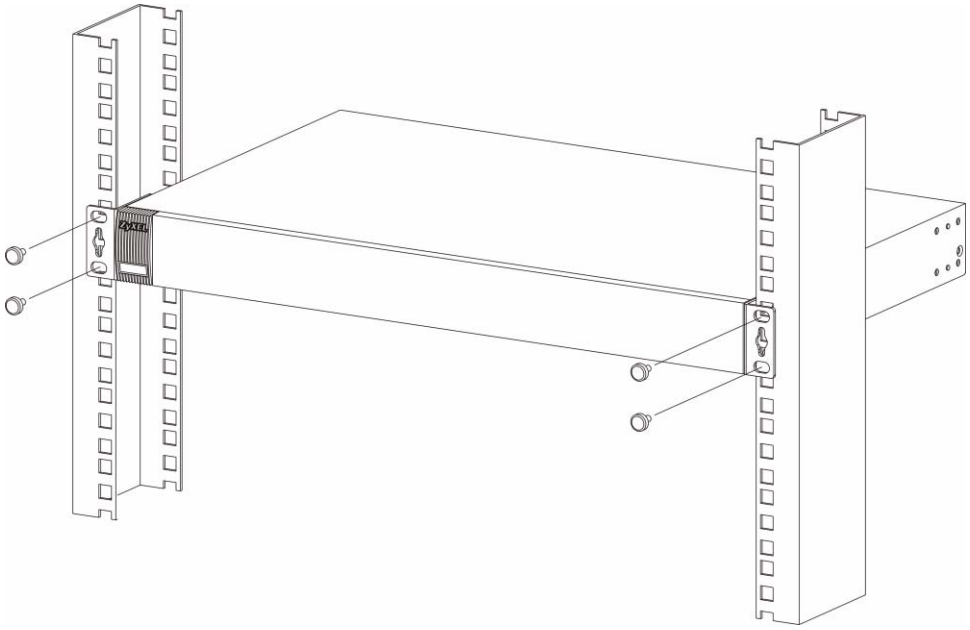
3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.

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

The figures below show the front panel of the Switch.

Figure 8 GS1510-16 Front Panel

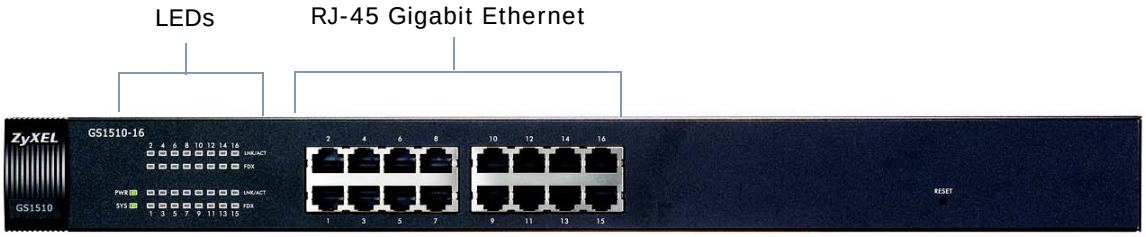
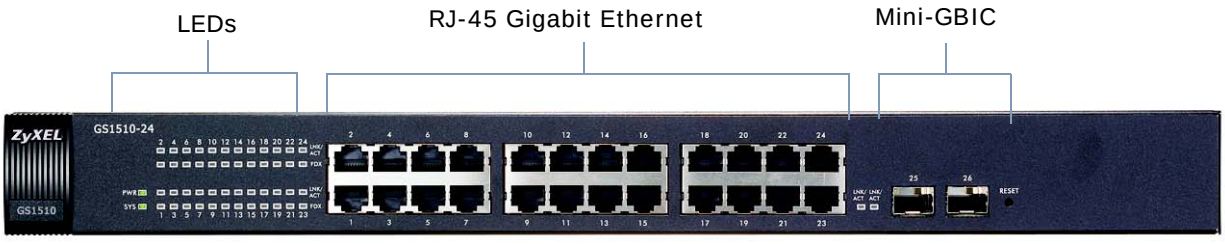


Figure 9 GS1510-24 Front Panel



The following table describes the ports on the panels.

Table 1 Panel Connections

CONNECTOR	DESCRIPTION
RJ-45 Gigabit Ethernet Ports	Connect these Gigabit Ethernet ports to high-bandwidth backbone network Ethernet switches or use them to daisy-chain other switches.
Mini-GBIC Slots (GS1510-24 only)	Use mini-GBIC transceivers in these slots for fiber-optic connections to backbone Ethernet switches.

3.1.1 Ethernet Ports

The GS1510-16 has 16 auto-negotiating, auto-crossover RJ-45 Gigabit Ethernet ports.

The GS1510-24 has 24 auto-negotiating, auto-crossover RJ-45 Gigabit Ethernet ports.

The speed of the Gigabit Ethernet ports can be 10 Mbps, 100Mbps or 1000Mbps and the duplex mode can be half duplex (at 100 Mbps) or full duplex.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100/1000Mpbs) and duplex mode (full duplex or half duplex) of the connected device.7

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

3.1.1.1 Default Ethernet Settings

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

- Speed: Auto
- Duplex: Auto
- Flow control: Off

3.1.2 Mini-GBIC Slots

There are two mini-GBIC (Gigabit Interface Converter) slots for mini-GBIC transceivers on GS1510-24. 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.

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)

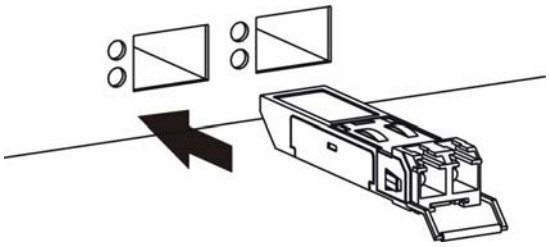
Note: To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.2.1 Transceiver Installation

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

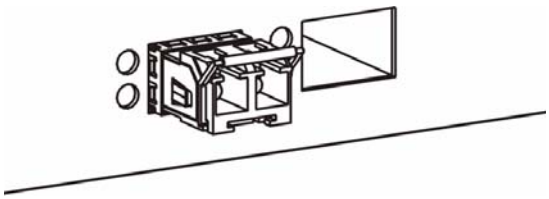
1. Insert the transceiver into the slot with the exposed section of PCB board facing down.

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

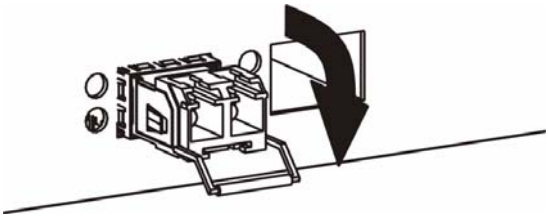


3.1.2.2 Transceiver Removal

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

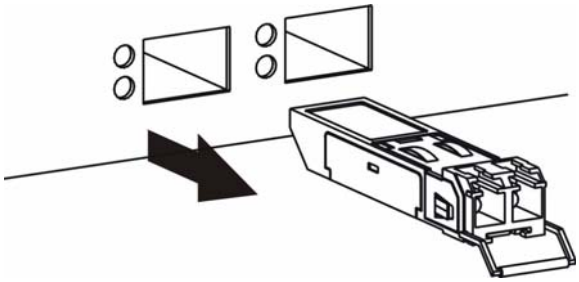
1 Open the transceiver's latch (latch styles vary).

Figure 12 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

Figure 13 Transceiver Removal Example



3.1.3 The RESET Button

Reset the Switch to its factory default configuration via the **RESET** button. Press the **RESET** button for at least five seconds and then release. The Switch automatically reboots and reloads its factory default configuration file. The **RESET** button is on the front panel of the Switch.

Note: When you use the RESET button all of your configuration settings will be lost. Use the default IP address (192.168.1.1) and user name (admin) and password (1234) to log back into the Switch. It may take up to 2 minutes for the Switch to restart when you reload the default configuration file.

3.2 LEDs

The following table describes the LEDs.

Table 2 LEDs

LED	STATUS		DESCRIPTION
PWR	Green	On	The system is turned on.
	Off		The system is off.
SYS	Green	On	The system is on and functioning properly.
	Off		The system is off or is malfunctioning.

Table 2 LEDs (continued)

LED	STATUS		DESCRIPTION
Gigabit Ethernet Ports			
LINK/ACT	Green	On	The link to a 10/1000 Mbps Ethernet network is up.
	Amber	On	The link to a 100 Mbps Ethernet network is up.
	Blinking		The port is transmitting/receiving data.
	Off		The link to an Ethernet network is down.
FDX	Amber	On	The port is negotiating in full-duplex mode.
	Off		The port is negotiating in half-duplex mode and no collisions are occurring.
Mini-GBIC Slots (GS1510-24 ONLY)			
LNK/ACT	Green	On	The port has a successful connection.
	Blinking		The port is receiving or transmitting data.
	Off		No Ethernet device is connected to this port or the link to an Ethernet network is down.

3.3 Rear Panel

The following figures show the rear panels of the AC power input model Switch. The rear panel contains a receptacle for the power cord.

Figure 14 GS1510-16 Rear Panel

Figure 15 GS1510-24 Rear Panel

3.3.1 Power Connector

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

To connect the power to the Switch, insert the female end of the power cord into the power receptacle on the rear panel. Connect the other end of the supplied power cord to a 100~240V AC, 50/60 Hz power outlet capable of supplying at least 0.3A.

PART II
Basic Settings

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 setup and management of the Switch via an Internet browser. Use Internet Explorer 6.0 or later to access the web configurator. 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).

Note: This User's Guide shows screens from the GS1510 Series, unless otherwise specified.

4.2 Device Auto Discovery Utility

To access the web configurator, you will need to know the IP address of the Switch. If the default IP address (192.168.1.1) has been changed, use the ZyXEL device discovery utility to easily locate the Switch on your network. The utility can be found on the CD that came with the Switch, see Appendix A on page 159 for installation and usage details.

4.3 System Login

1 Start your web browser.

2 Type “http://” and the IP address of the Switch (for example, the default is 192.168.1.1) in the Location or Address field. Press [ENTER].

3 The login screen appears. The default username is **admin** and the associated default password is **1234**.

Figure 16 Web Configurator: Login

4 Click **Login** to view the first Web Configurator screen.

4.3.1 Smart Mode

The **Smart** mode screens enable you to quickly set up important options such as basic IP settings, Energy Efficient Ethernet, Web Authentication, DHCP Snooping and Spanning Tree Protocol (STP).

To go directly to the Advance mode settings, see Section 4.3.2 on page 40.

4.3.1.1 IP Setting

The **Smart** > **IP Setting** screen is the first screen that displays when you access the Web Configurator. Use this screen to configure the IP address and subnet mask for the Switch. Click **Apply** to save the changes.

Figure 17 Web Configurator Smart Screen - IP Setting

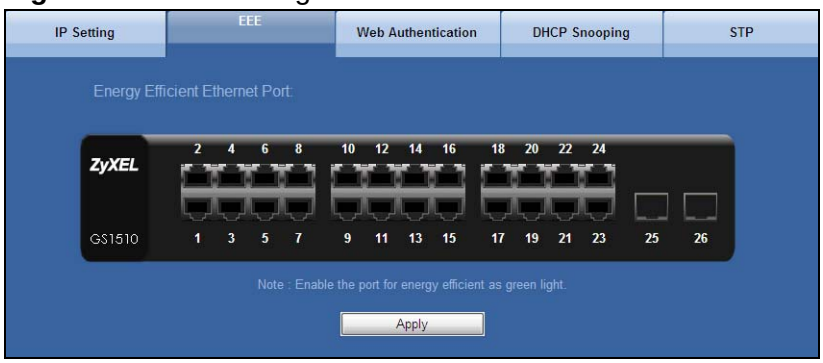
4.3.1.2 EEE (Energy Efficient Ethernet)

Use this screen to reduce energy consumption over RJ-45 Ethernet Ports during idle periods. Click the **EEE** tab (Energy Efficient Ethernet) to display the screen as shown next.

You can enable IEEE 802.3az Energy Efficient Ethernet on a port by clicking on it in the Switch graphic.

Click **Apply** to save any changes.

Figure 18 Web Configurator Smart Screen - EEE



4.3.1.3 Web Authentication

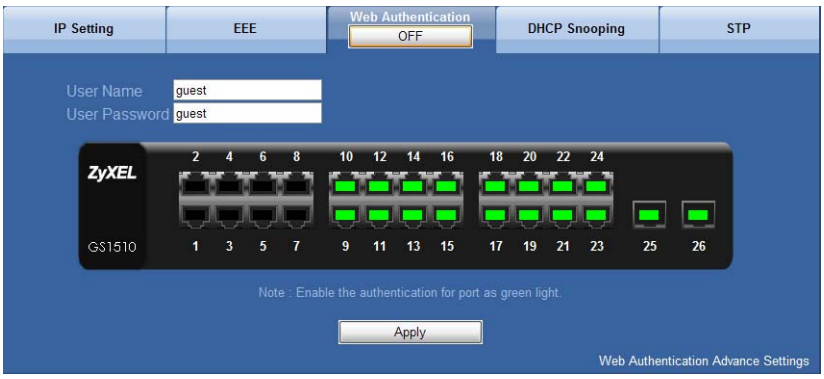
Click the **Web Authentication** tab to open the screen as shown next. This feature is used to authenticate users before they access a website on the Internet. Use the **ON** or **OFF** button on this screen to globally enable/disable web authentication across all ports.

You can enable or disable web authentication on a specific port by clicking on it. When a port is green, it means authentication is enabled on the port. The default user name and password for web authentication is guest/guest. You can change the password on this screen.

The **Management > User Account** screen (Section 23.2 on page 143) allows you to create more user accounts for web authentication.

Click **Apply** to save any changes.

Figure 19 Web Authentication Smart Screen - Web Authentication



4.3.1.4 DHCP Snooping

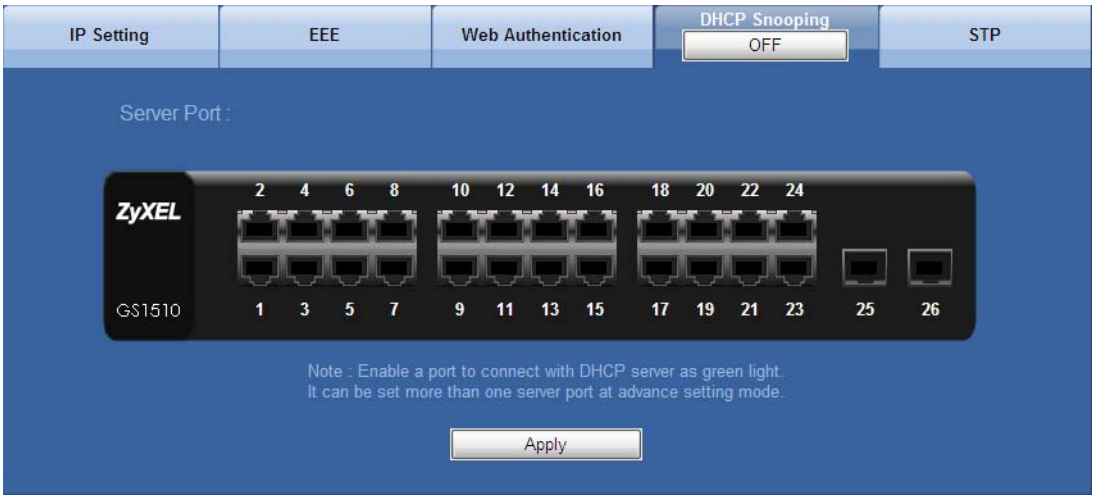
Use this screen to enable or disable the DHCP Snooping feature which filters unauthorized DHCP packets on the network.

Click the **DHCP Snooping** tab to open the screen as shown next. Use the **ON** or **OFF** button on this screen to enable or disable DHCP Snooping. You can set a specific port to act as a server port by clicking on it to make it green. A server port is a port that is connected to a DHCP server.

Note: You can only enable one port as a server port on this screen, to enable more than one port, use the advanced DHCP snooping screen (Section 18.4 on page 107).

Click **Apply** to save any changes.

Figure 20 Web Configuration Smart Screen - DHCP Snooping

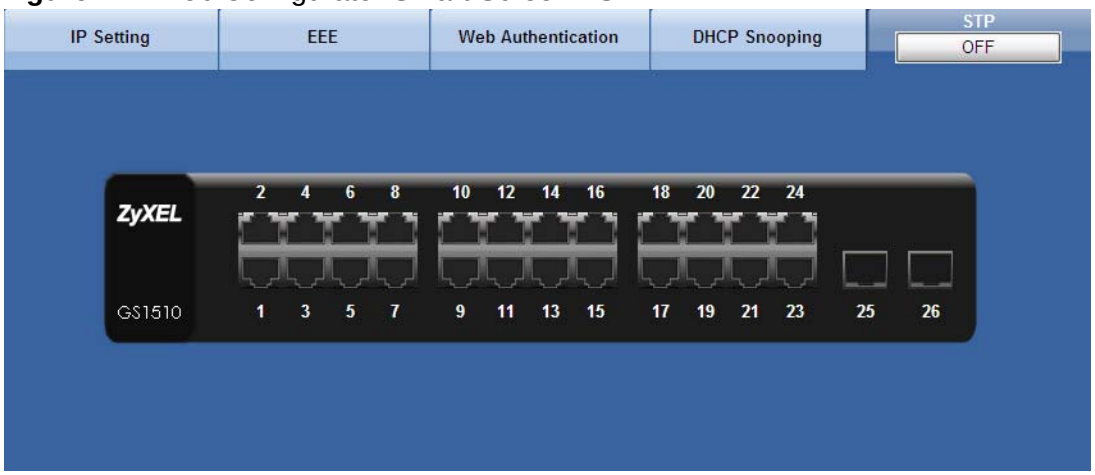


4.3.1.5 STP (Spanning Tree Protocol)

Use this screen to activate the Spanning Tree Protocol (STP) feature which is used to prevent loops in the core of your network.

Click the **STP** tab to open the screen as shown next. Use the **OFF** or **ON** button to globally enable or disable Spanning Tree Protocol for the Switch.

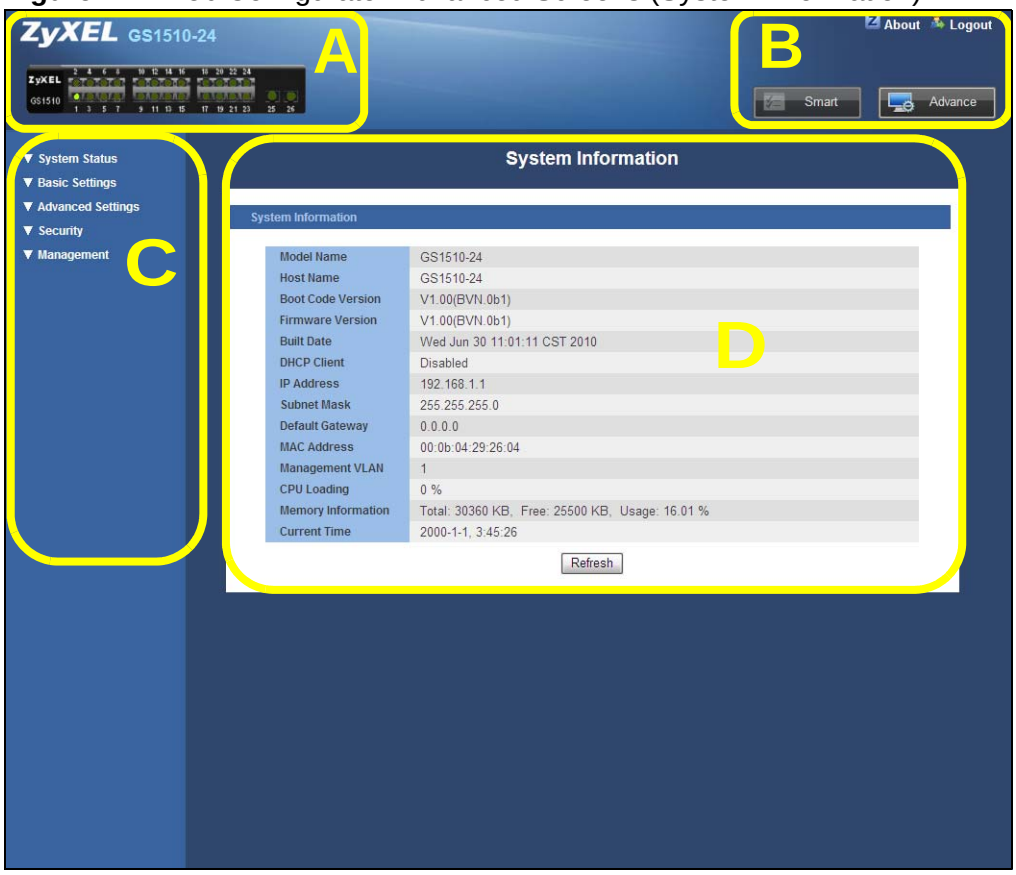
Figure 21 Web Configurator Smart Screen - STP



4.3.2 The Advanced Main Screen

Click **Advance** to display the following screen that shows the main navigating components of the Web Configurator screen.

Figure 22 Web Configurator Advanced Screens (System Information)



A - The device graphic displays the status of the ports.

B - Use the **About** link to view more information about the device's vendor. Use the **Logout** link to exit the Web Configurator. Use the **Smart** button to go to the smart screens where you can quickly set up some main functions. Use the **Advanced** button to go to the advanced configuration screens.

C - The navigation panel has links to screens that let you configure the Switch's features.

D - The function frame allows you to view and edit individual feature settings.

4.3.3 The Navigation Panel

Navigate to individual feature configuration screens from the navigation panel.

The following table describes the links in the navigation panel.

Table 3 Navigation Panel Links

LINK	DESCRIPTION
System Status	
System Information	Use these screens to view general system information such as firmware version, IP address and so on.
Basic Settings	
General Settings	Use these screens to configure the system name, IP address, maximum frame size, and system time settings.
MAC Management	Use these screens to configure static MAC address settings and view the MAC table.
Port Mirroring	Use this screen to copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Port Settings	Use this screen to enable/disable a port, configure the port speed and duplex and flow control, and view the current connection status.
Advanced Settings	
VLAN	
Port Isolation	Use this screen to isolate each port from communicating with each other. Each port can only communicate with the CPU management port.
VLAN	Use these screens to create new IEEE 802.1Q VLANs as well as configuring Port VLAN ID (PVID), tag/untag, and acceptable frame settings.
EEE	Use this screen to enable/disable Energy Efficient Ethernet on each port.
IGMP Snooping	Use this screen to configure multicast related settings such as IGMP Snooping, IGMP Snooping VLAN, unknown multicast packet handling, and immediate leave ports.
Link Aggregation	Uses these screens to logically aggregate physical links to form one logical, higher-bandwidth link.
Loop Guard	Use this screen to configure protection against network loops that occur on the edge of your network.
QoS	Use these screens to configure 802.1p priority, IP Diffserv (DSCP), queuing method with associated queue weights and priority/queue mapping for the Switch.
Storm Control	Use this screen to cap the rate of broadcast, multicast and destination lookup failure (DLF) packets the Switch will allow on individual ports.
STP	Use these screens to configure the STP/RSTP to prevent network loops.
Security	
IP Source Guard	
DHCP Snooping	Use these screens to configure filtering of unauthorized DHCP packets in your network.
ARP Inspection	Use these screens to configure filtering of unauthorized ARP packets in your network.
Binding Table	Use this screen to view the information of any hosts which successfully connected to an IP address through the DHCP server.

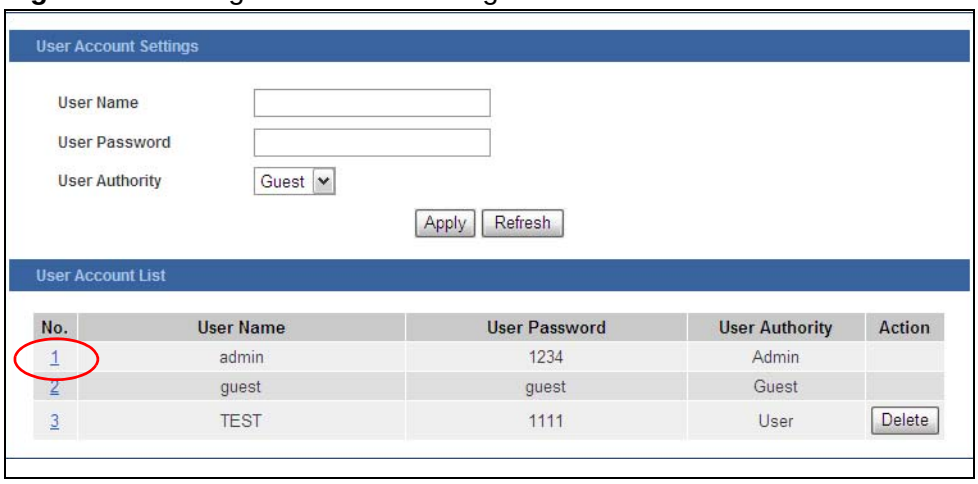
Table 3 Navigation Panel Links (continued)

LINK	DESCRIPTION
802.1x	Use this screen to configure 802.1x authentication method. This method uses an authentication server (RADIUS server) to validate access to a port based on a username and password provided by the user.
Web Authentication	Use this screen to configure settings that define when notifications are sent to an external management station.
Management	
Maintenance	Use this screen to perform firmware upgrades, configuration backup and restore.
SNMP	Use this screen to reboot the Switch or to restore the default configuration of the Switch. Use this screen to define security parameters for SNMP v1 and SNMP v2c. Use this screen to configure settings that define when notifications are sent to an external management station.
User Account	Use this screen to create users and assign them to pre-defined SNMP groups.

4.3.4 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **User Account** to display the next screen. Click **1** in the **No.** field to change the admin password.

Figure 23 Change Administrator Login Password



4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the Switch.

4.5 Switch Lockout

You could block yourself (and all others) from using the Web Configurator if you:

1. Remove all the ports from the default VLAN (default is VLAN 1) when no other VLANs exist.
2. Disable all ports.
3. Forget the password and/or IP address.
4. Enable Dynamic ARP without entering the proper MAC to IP address binding.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reset the Switch back to the factory defaults.

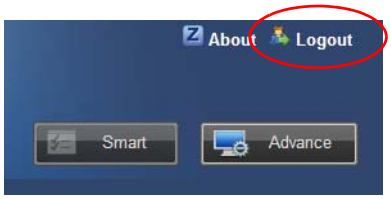
Use the **RESET** button to reset the Switch back to factory defaults. Press and hold the **RESET** button for five seconds. The Switch will reload its factory defaults.

The Switch is now reinitialized with a default configuration file including the default administrator username (admin) and password (1234). The IP address of the Switch also reverts to the default 192.168.1.1.

4.7 Logging Out of the Web Configurator

Click **Logout** on the top right corner of the 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 24 Web Configurator: Logout Link



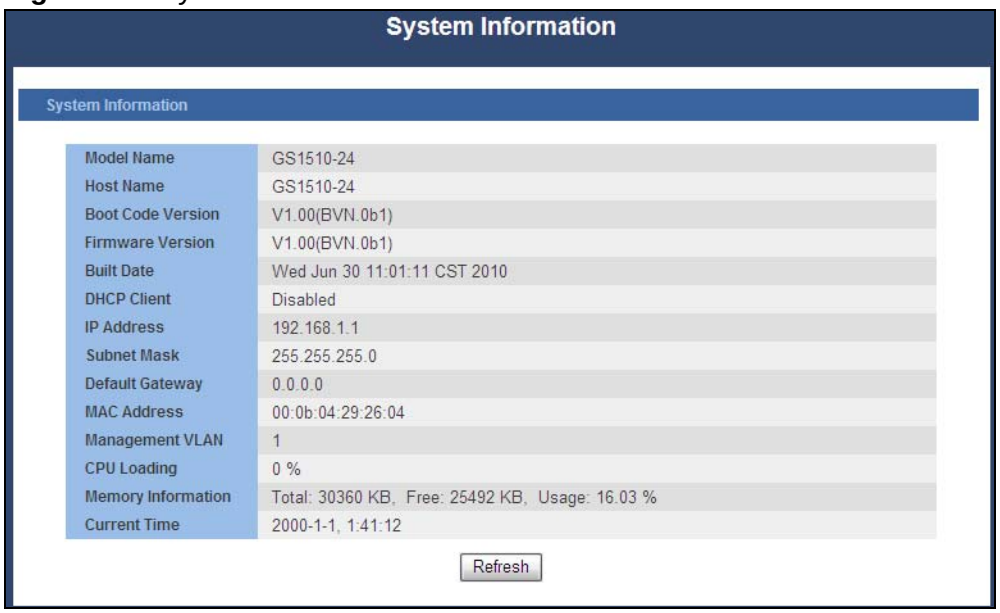
5 System

This chapter describes the system screens.

5.1 System Screen

The home screen of the Web Configurator displays general system information. Click **System Status** > **System Information** in the navigation panel to view device specific information such as host name, firmware version and so on.

Figure 25 System



The following table describes the labels in this screen.

Table 4 System

LABEL	DESCRIPTION
Model Name	This field displays the model name of your Switch.
Host Name	This field displays the name of your Switch.
Boot Code Version	This field displays the boot code version.

Table 4 System (continued)

LABEL	DESCRIPTION
Firmware Version	This field displays the version number of the Switch's current firmware. Click **Upgrade** to go to the firmware upgrade screen. See Section 21.3.2 on page 131.
Built Date	This field displays the date of the currently installed firmware.
DHCP Client	This field displays whether the DHCP client feature is enabled or disabled.
IP Address	This field indicates the IP address of the Switch. You can click the existing IP address to change it. See Section 6.2 on page 47.
Subnet Mask	This field indicates the subnet mask of the Switch.
Default Gateway	This field indicates the IP address of the default gateway.
MAC Address	This field displays the MAC (Media Access Control) address of the Switch.
Management VLAN	This field displays the VLAN ID that is used for the Switch management purposes.
CPU Loading	This field displays the percentage of your Switch's system load.
Memory Information	This field displays the total memory the Switch has and the memory which is currently available (**Free**) and occupied (**Usage**).
Current Time	This field displays current date (yyyy-mm-dd) and time (hh:mm:ss).
Refresh	Click this to update the information in this screen.

6

General Settings

This chapter describes the General Settings screens in the Basic Settings menu.

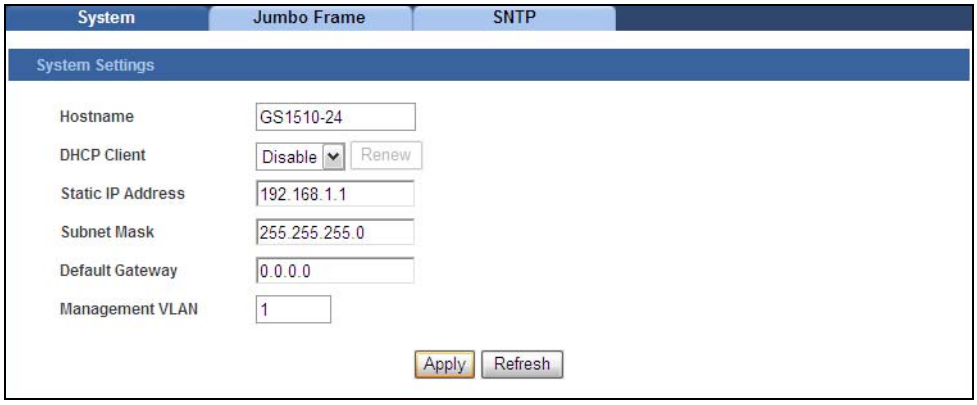
6.1 What You Can Do

- Use the **System** screen (Section 6.2 on page 47) to configure the basic IP address settings for the Switch.
- Use the **Jumbo Frame** screen (Section 6.3 on page 48) to configure the jumbo frame size the Switch accepts.
- Use the **SNTP** screen (Section 6.4 on page 49) to configure the date and time of the Switch.

6.2 System

Use the **System** Settings screen under Basic Settings > General Settings to set up the IP address for the Switch. You can enable DHCP or set up a static IP address. The following screen appears when you click **Basic Settings** > **General Settings** > **System**.

Figure 26 System Settings



The following table describes the labels in this screen.

Table 5 System Settings

LABEL	DESCRIPTION
Hostname	Enter up to 16 alphanumeric characters for the name of your Switch. Hyphens (-) and underscores (_) are also allowed.
DHCP Client	Select **Enable** to allow the Switch to automatically get an IP address from a DHCP server. Click **Renew** to have the Switch reget an IP address from the DHCP server. Select **Disable** if you want to configure the Switch's IP address manually.
Static IP Address	Enter the IP address of your Switch in dotted decimal notation. For example, 192.168.1.1.
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 192.168.1.5.
Management VLAN	Enter a VLAN ID used for Switch management purposes.
Apply	Click **Apply** to save your changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

6.3 Jumbo Frame

Jumbo frames are Ethernet frames with a payload greater than 1500 bytes. Jumbo frames can enhance data transmission efficiency in a Gigabit network.

Use this screen to configure the jumbo frame size the Switch accepts. Click **Basic Settings** > **General Settings** > **Jumbo Frame** to display the screen as shown.

Figure 27 Basic Settings > General Settings > Jumbo Frame

The following table describes the labels in this screen.

Table 6 Basic Settings > General Settings > Jumbo Frame

LABEL	DESCRIPTION
Frame Size	Select the maximum number of bytes (1522, 1536, 1552 or 9216) of a jumbo frame. The bigger the frame size, the better the performance.

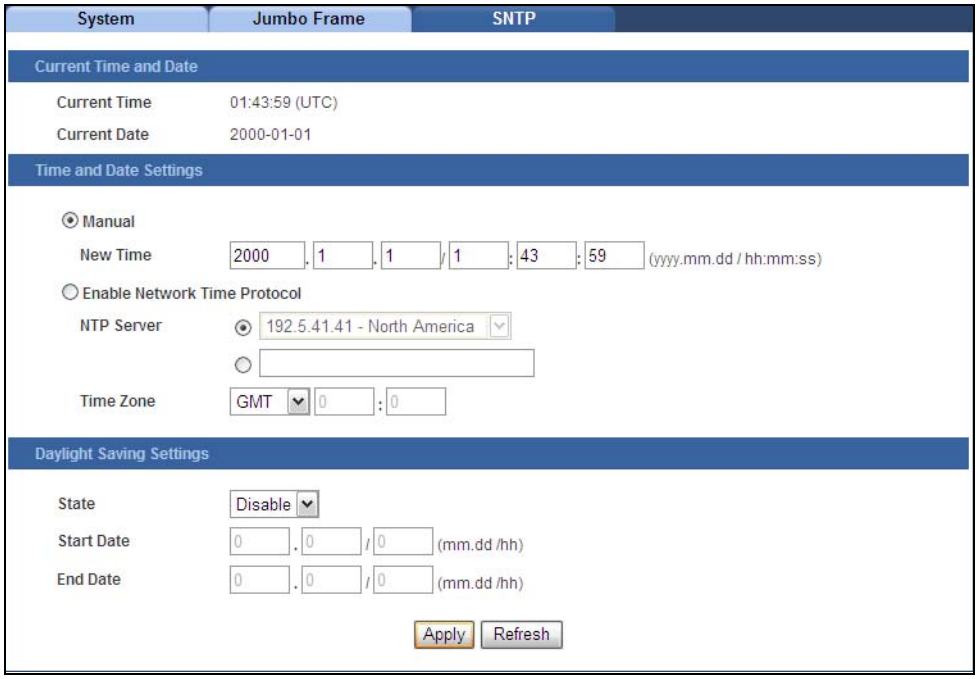
Table 6 Basic Settings > General Settings > Jumbo Frame (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

6.4 SNTP

Use this screen to configure system date and time. Click **Basic Settings** > **General Settings** > **SNTP** to display the screen as shown.

Figure 28 Basic Settings > General Settings > SNTP



The following table describes the labels in this screen.

Table 7 Basic Settings > General Settings > SNTP

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time you open this menu (or refresh the menu).
Current Date	This field displays the date you open this menu.
Time and Date Settings	
Manual	Select this option if you want to enter the system date and time manually.
New Time	Enter the new date in year, month and day format and time in hour, minute and second format. The new date and time then appear in the **Current Date** and **Current Time** fields after you click **Apply**.

Table 7 Basic Settings > General Settings > SNTP (continued)

LABEL	DESCRIPTION
Enable Network Time Protocol	Select this option to use Network Time Protocol (NTP) for the time service.
NTP Server	Select a pre-designated time server or type the IP address of your time server. The Switch searches for the timeserver for up to 60 seconds.
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 Settings 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.	
State	Select **Enable** if you want to use Daylight Saving Time. Otherwise, select **Disable** to turn it off.
Start Date	Configure the day and time when Daylight Saving Time starts if you enabled 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).
End Date	Configure the day and time when Daylight Saving Time ends if you enabled 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 last Sunday of October. 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 back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

7

MAC Management

7.1 Overview

Use these screens to add, delete and view entries in the MAC address table.

The **MAC Table** (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's MAC Table. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered).

7.2 What You Can Do

- Use the **Static MAC Settings** screen (Section 7.4 on page 52) to manually add a static MAC address to the table.
- Use the **MAC Table** screen (Section 7.5 on page 53) to view the static and dynamic MAC address entries.

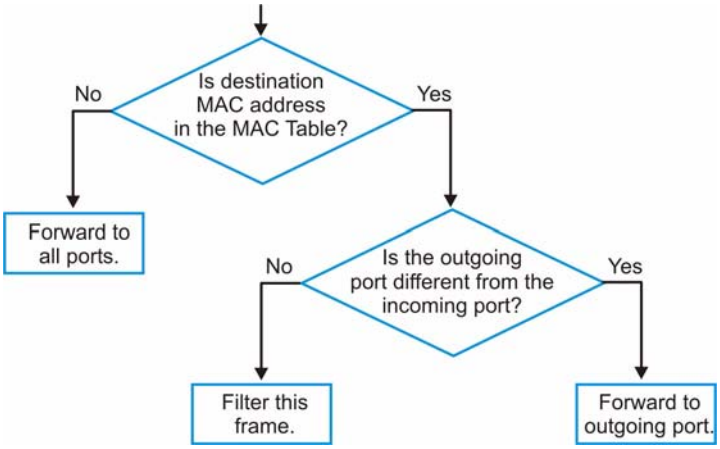
7.3 What You Need to Know

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 from 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 29 MAC Table Flowchart

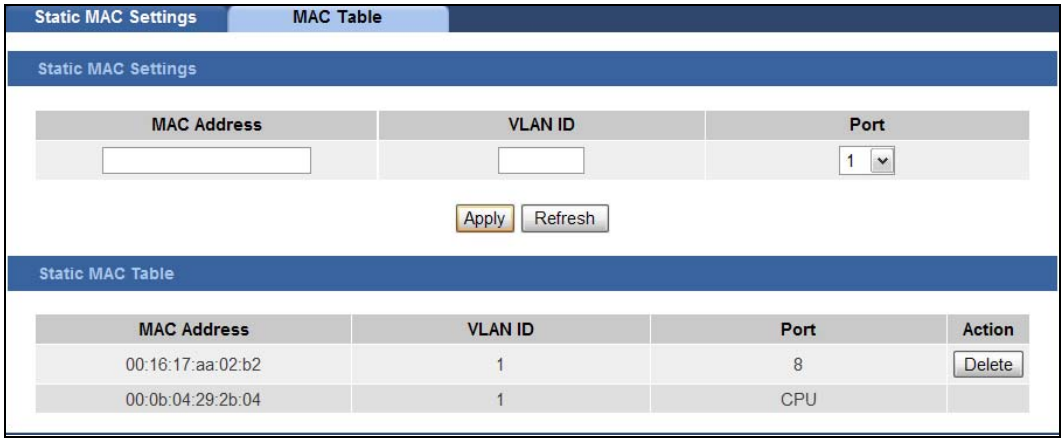


7.4 Static MAC Settings

A static Media Access Control (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.

Click **Basic Settings > MAC Management > Static MAC Settings** in the navigation panel to display the configuration screen as shown.

Figure 30 Static MAC Settings



The following table describes the labels in this screen.

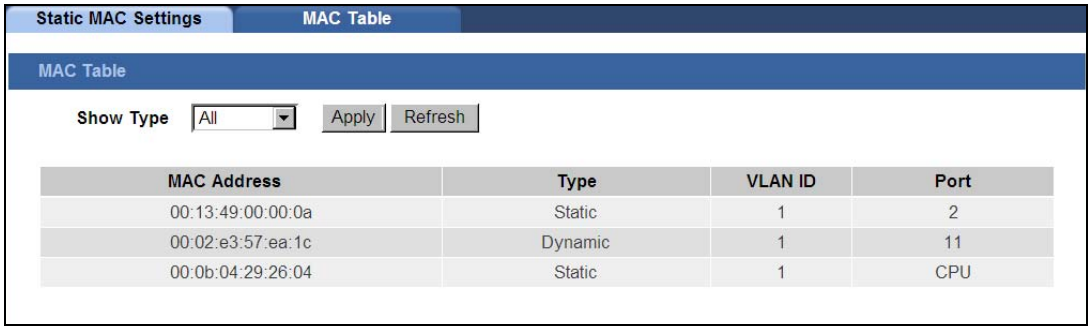
Table 8 Static MAC Settings

LABEL	DESCRIPTION
Static MAC Settings	
MAC Address	Enter the MAC address of a computer or device that you want to add to the MAC address table.
VLAN ID	Enter the VLAN ID to apply to the computer or device.
Port	Enter the port number to which the computer or device is connected.
Apply	Click **Apply** to add the MAC address entry to the MAC address table.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Static MAC Table	
MAC Address	This field displays the MAC address of a manually entered MAC address entry.
VLAN ID	This field displays the VID of a manually entered MAC address entry.
Port	This field displays the port number of a manually entered MAC address entry. The MAC address with the port listed as **CPU** is the Switch's MAC address.
Action	Click **Delete** to remove this manually entered MAC address entry from the MAC address table. You cannot delete the Switch's MAC address from the static MAC address table.

7.5 MAC Table

Use the **MAC Table** screen to view entries in the MAC address table. Click **Basic Settings > MAC Management > MAC Table** in the navigation panel to display the screen as shown.

Figure 31 MAC Table



The following table describes the labels in this screen.

Table 9 MAC Table

LABEL	DESCRIPTION
Show Type Apply	Select **Static**, **Dynamic**, or **All** and then click **Apply** to display the corresponding MAC address entries on this screen.
Refresh	Click this to update the information in the MAC table.
MAC Address	This field displays a MAC address.
Type	This field displays whether this entry was entered manually (**Static**) or whether it was learned by the Switch (**Dynamic**).
VLAN ID	This field displays the VLAN ID of the MAC address entry.
Port	This field displays the port number the MAC address entry is associated. It displays **CPU** if it is the entry for the Switch itself.

8

Port Mirroring

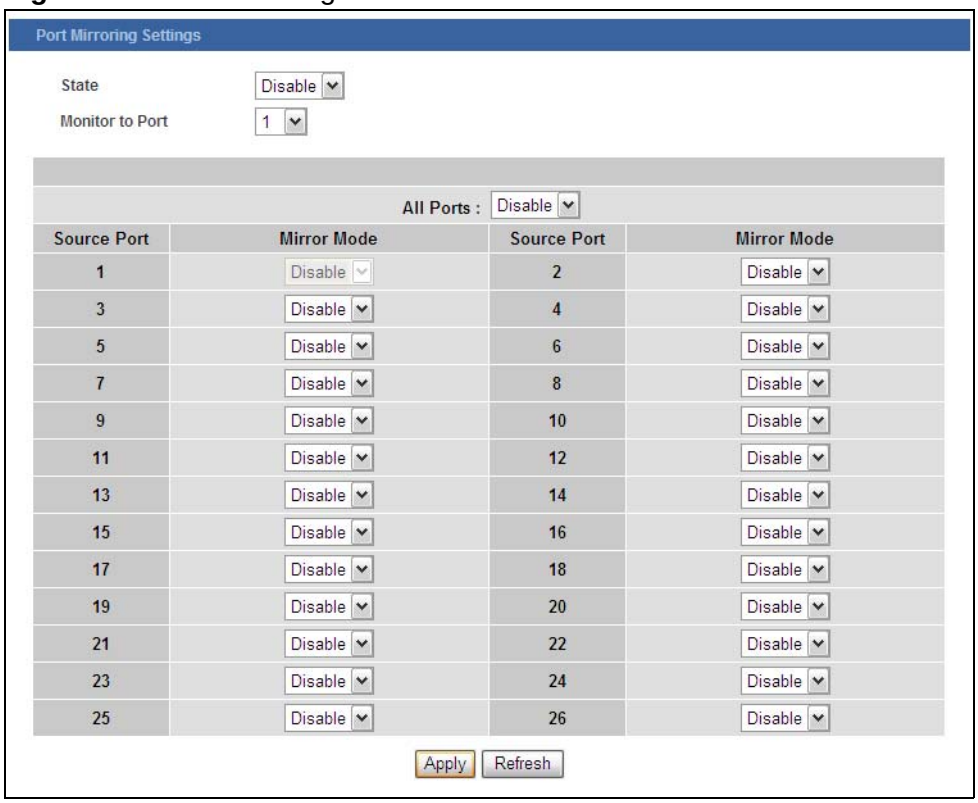
This chapter discusses port mirroring.

8.1 Port Mirroring Settings

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

Click **Basic Settings > Port Mirroring** to display the following screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 32 Port Mirroring



The following table describes the labels in this screen.

Table 10 Port Mirroring

LABEL	DESCRIPTION
State	Select **Enabled** to turn on port mirroring or select **Disabled** to turn it off.
Monitor to Port	Select the ports for which you want to monitor the traffic.
All Ports	Settings in this field apply to all ports. Use this field only if you want to make some settings the same for all ports. Use this field first to set the common settings and then make adjustments on a port-by-port basis.
Source Port	This field displays the number of a port.
Mirror Mode	Select **Ingress**, **Egress** or **Both** to only copy the ingress (incoming), egress (outgoing) or both (incoming and outgoing) traffic from the source ports to the port specified in the **Monitor to Port** field. Select **Disable** to not copy any traffic from the source ports to the port specified in the **Monitor to Port** field.
Apply	Click **Apply** to save your changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

9

Port Settings

This chapter describes how to view and configure the port settings on the Switch.

9.1 Port Settings

Use this screen to configure and view Switch port settings. Click **Basic Settings > Port Settings** to display the following screen.

9.1.1 Auto Negotiation

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.

9.1.2 Flow Control

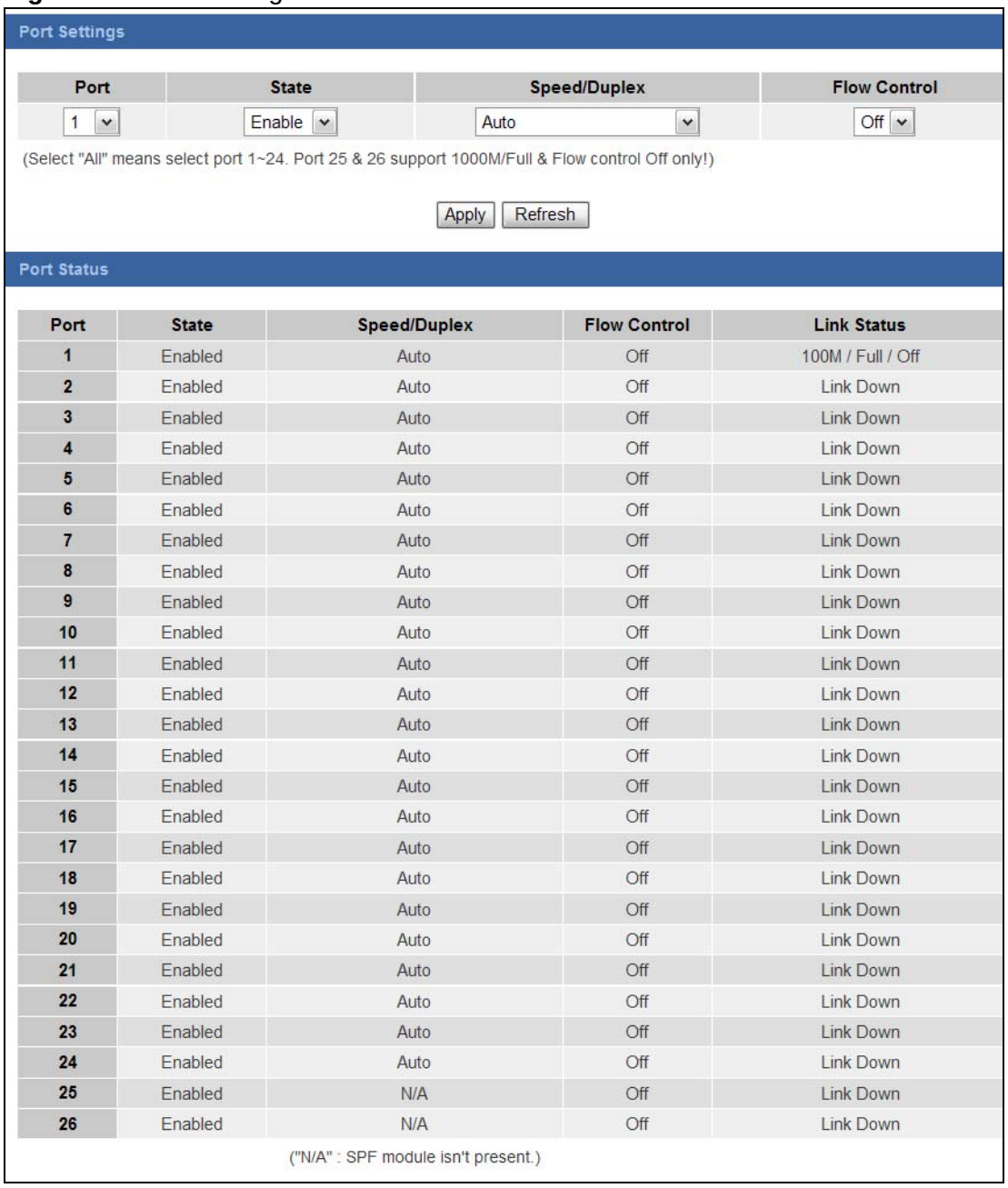
A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port.

The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.

IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.

Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Figure 33 Port Settings



The following table describes the labels in this screen.

Table 11 Port Settings

LABEL	DESCRIPTION
Port Settings	
Port	Select a port number you want to configure on this screen.
State	Select **Enable** to activate the port or **Disable** to deactivate the port.
Speed/Duplex	Select the speed and duplex mode of the port. The choices are: • **Auto** • **10 Mbps / Full Duplex** • **10 Mbps / Half Duplex** • **100 Mbps / Full Duplex** • **100 Mbps / Half Duplex** • **1000 Mbps / Full Duplex** • **1000 Mbps / Half Duplex**
Flow Control	Select **On** to enable access to buffering resources for the port thus ensuring lossless operation across network switches. Otherwise, select **Off** to disable it.
Apply	Click **Apply** to save the changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Port Status	
Port	This field displays the port number.
State	This field displays whether the port is enabled or disabled.
Speed/Duplex	This field displays the speed either **10M**, **100M** or **1000M** and the duplex mode **Full** or **Half**.
Flow Control	This field displays whether the port's flow control is **On** or **Off**.
Link Status	This field displays the link status of the port. If the port is up, it displays the port's speed, duplex and flow control setting. Otherwise, it displays **Link Down** if the port is disabled or not connected to any device.

PART III
Advanced Settings

10 VLAN

10.1 Overview

This chapter shows you how to configure IEEE 802.1Q tagged VLANs and port-based VLANs.

10.2 What You Can Do

- Use the **Port Isolation** screen (Section 10.4 on page 64) to specify which ports can communicate with each other.
- Use the **VLAN Settings** screen (Section 10.5 on page 67) to configure a VLAN and assign member ports.
- Use the **Tag Settings** screen (Section 10.6 on page 68) to add a VLAN ID tag to all outgoing frames on a member port.
- Use the **Port Settings** screen (Section 10.7 on page 69) to configure the VLAN port settings.

10.3 What You Need to Know

10.3.1 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

10.3.2 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.

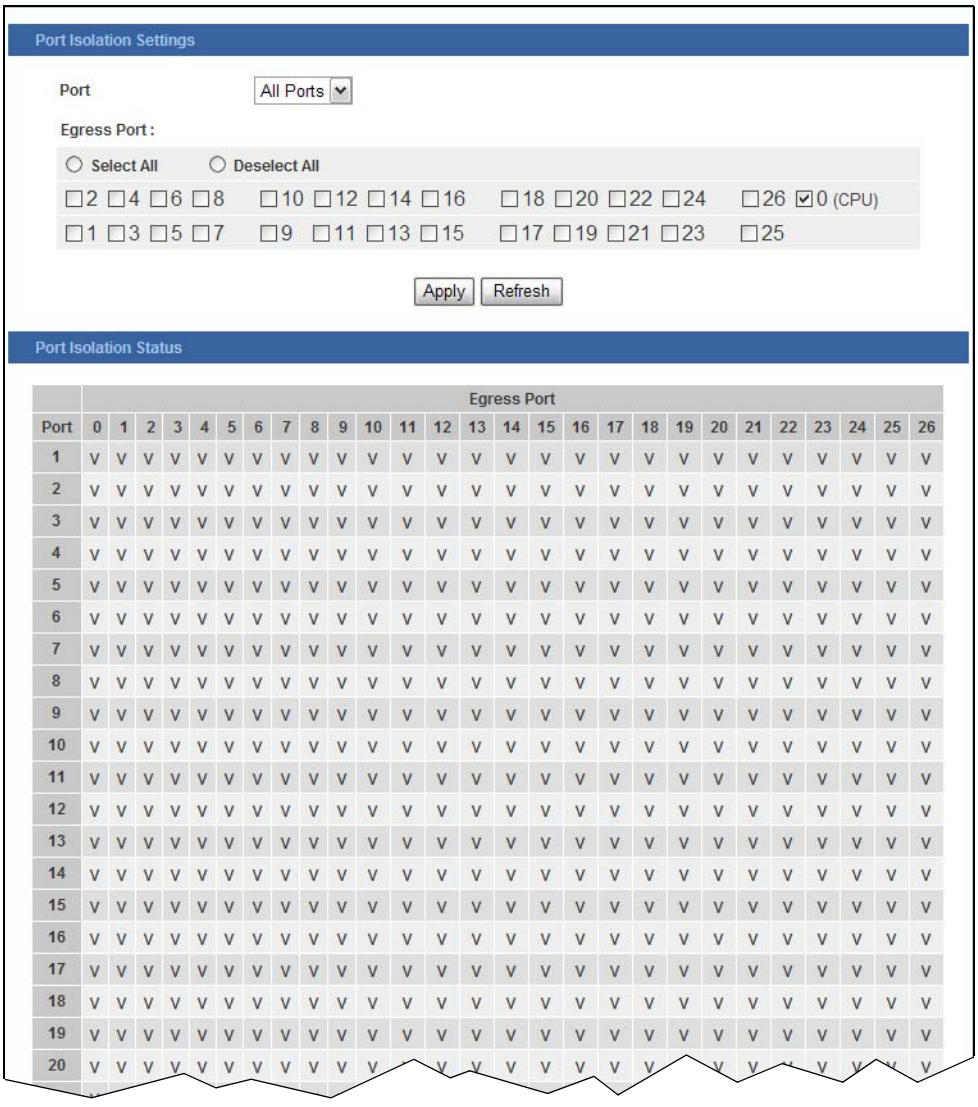
A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

10.4 Port Isolation

Use this screen to restrict specific ports on the Switch from communicating with each other. This screen can also be used to specify which ports will forward received packets to other ports on the Switch.

Click **Advanced Settings > VLAN** > **Port Isolation** to display the following screen.

Figure 34 Port Isolation



The following table describes the labels in this screen.

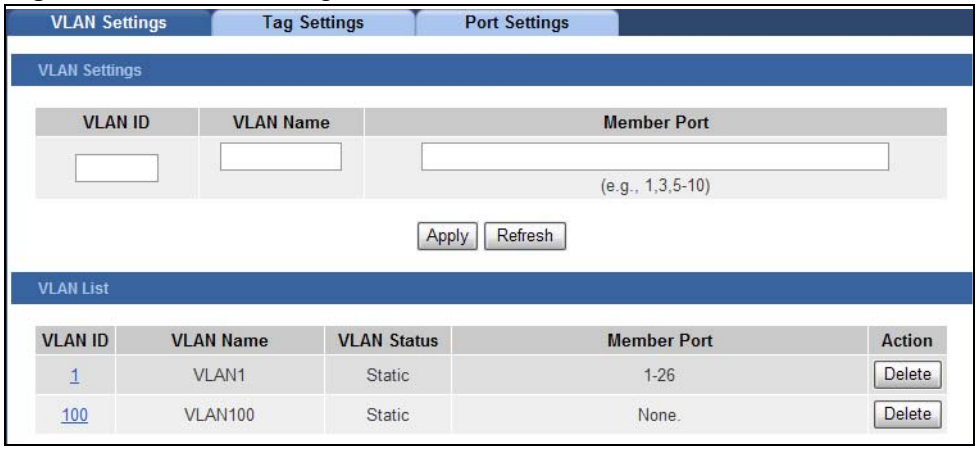
Table 12 Port Isolation

LABEL	DESCRIPTION
Port	Select a port number to configure its port isolation settings. Select **All Ports** to configure the port isolation settings for all ports on the Switch.
Egress Port	An egress port is an outgoing port, that is, a port through which a data packet leaves. Selecting a port as an outgoing port means it will communicate with the port currently being configured. 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.
Select All/ Deselect All	Click **Select All** to mark all ports as egress ports and permit traffic. Click **Deselect All** to unmark all ports and isolate them. Deselecting all ports means the port being configured cannot communicate with any other port. This will also deselect the CPU outgoing port which will disable Switch management for that port. This option is the most limiting but also the most secure.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
Port Isolation Status	“V” indicates the port’s packets can be sent to that port. “-” indicates the port’s packets cannot be sent to that port.

10.5 VLAN Settings

Use this screen to configure a static VLAN and assign member ports to it. Click **Advanced Settings > VLAN** > **VLAN** > **VLAN Settings** to display the following screen.

Figure 35 VLAN Settings



The following table describes the labels in this screen.

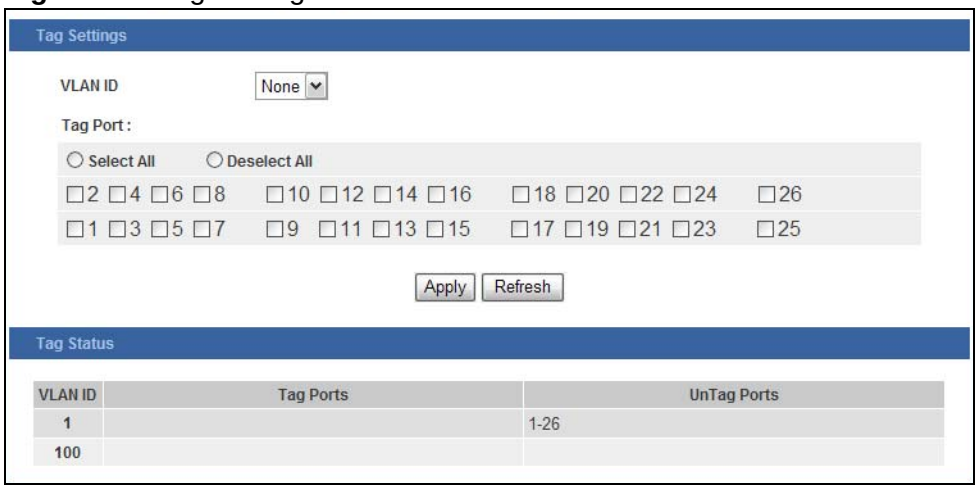
Table 13 VLAN Settings

LABEL	DESCRIPTION
VLAN ID	Enter the VLAN ID for this entry; the valid range is between 1 and 4094.
VLAN Name	Enter a descriptive name for the VLAN for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Member Port	Enter the port numbers you want the Switch to assign to the VLAN as members. You can designate multiple port numbers individually by using a comma (,) and by range with a hyphen (-).
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
VLAN List	
VLAN ID	This field displays the index number of the VLAN entry. Click the number to modify the VLAN.
VLAN Name	This field displays the name of the VLAN.
VLAN Status	This field displays the status of the VLAN. **Static** or **Dynamic** (802.1Q VLAN).
Member Port	This field displays which ports have been assigned as members of the VLAN. This will display **None** if no ports have been assigned.
Action	Click **Delete** to remove the VLAN.

10.6 Tag Settings

Use this screen to tag any outgoing frames from a port with its assigned VLAN ID. You must first configure a VLAN (Section 10.5 on page 67) before using this screen. Click **Advanced Settings > VLAN** > **VLAN** > **Tag Settings** to display the following screen.

Figure 36 Tag Settings



The following table describes the labels in this screen.

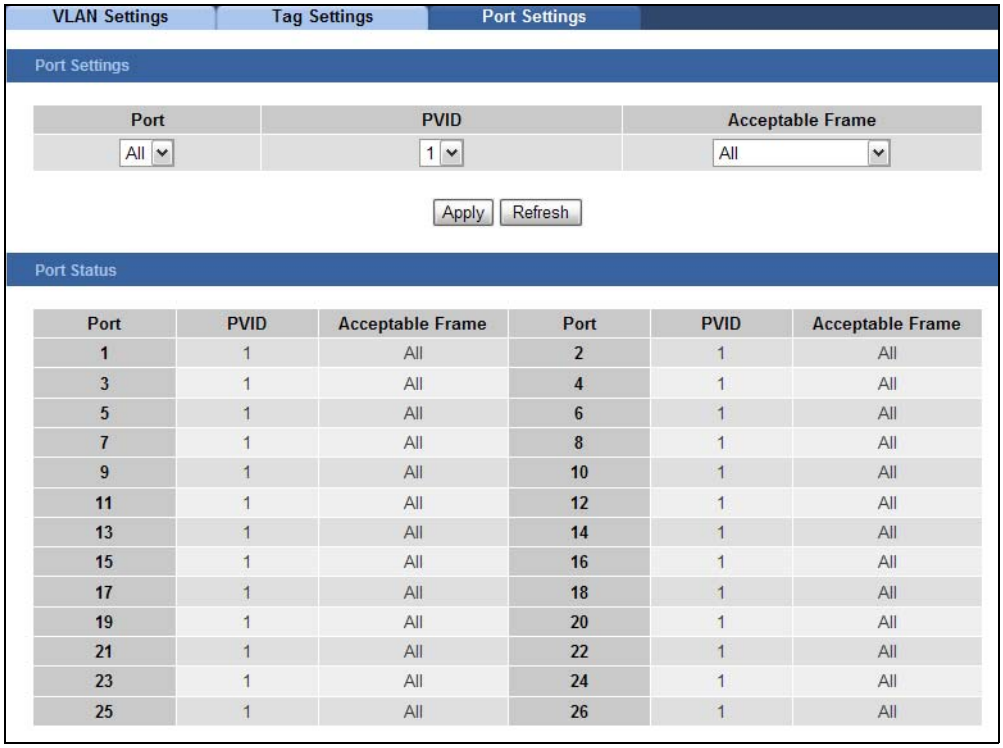
Table 14 Tag Settings

LABEL	DESCRIPTION
VLAN ID	Select a VLAN ID to configure its port tagging settings.
Tag Port	Selecting a port which is a member of the selected VLAN ID will make it a tag port. This means the port will tag all outgoing frames transmitted with the VLAN ID.
Select All	Click **Select All** to mark all member ports as tag ports.
Deselect All	Click **Deselect All** to mark all member ports as untag ports.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
Tag Status	
VLAN ID	This field displays the VLAN ID.
Tag Ports	This field displays the ports that have been assigned as tag ports.
UnTag Ports	This field displays the ports that have been assigned as untag ports.

10.7 Port Settings

Use this screen to configure the VLAN port settings. Click **Advanced Settings > VLAN** > **VLAN** > **Port Settings** to display the following screen.

Figure 37 Port Settings



The following table describes the labels in this screen.

Table 15 Port Settings

LABEL	DESCRIPTION
Port	Select a port number to configure from the drop-down box. Select **All** to configure all ports at the same time.
PVID	Select a **PVID** (Port VLAN ID number) from the drop-down box.
Acceptable Frame	Specify the type of frames allowed on a port. Choices are **All**, **VLAN Untagged Only** or **VLAN Tagged 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 **VLAN Untagged Only** to accept only untagged frames on this port. All tagged frames will be dropped. Select **VLAN Tagged Only** to accept only tagged frames on this port. All untagged frames will be dropped.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
Port Status	

Table 15 Port Settings (continued)

LABEL	DESCRIPTION
Port	This field displays the port number.
PVID	This field displays the Port VLAN ID number.
Acceptable Frame	This field displays the type of frames allowed on the port. This will either display **All** or **Tag Only**.

11 EEE

11.1 Overview

This chapter explains the **EEE (Energy Efficient Ethernet)** screen.

Use this screen to reduce energy consumption over RJ-45 Ethernet Ports during idle periods.

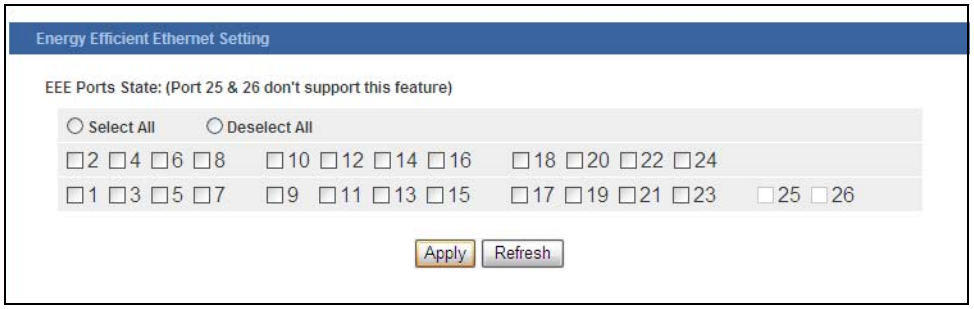
The hardware devices connected to the ports must also support EEE for this function to work.

Note: A similar version of this screen appears in **Smart Mode**. See Section 4.3.1.2 on page 37.

11.1.1 EEE Screen

Click **Advanced Settings** > **EEE** to view the screen as shown.

Figure 38 EEE



The following table describes the labels in this screen.

Table 16 EEE

LABEL	DESCRIPTION
EEE Port State	Click a port to enable IEEE 802.3az Energy Efficient Ethernet on that port.
Select All	Click this to enable IEEE 802.3az Energy Efficient Ethernet across all ports.
Deselect All	Click this to disable IEEE 802.3az Energy Efficient Ethernet across all ports.

Table 16 EEE (continued)

LABEL	DESCRIPTION
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.

12

IGMP Snooping

12.1 Overview

This chapter shows you how to configure IGMP snooping for multicast traffic. 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. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

12.2 What You Can Do

- Use the **General Settings** screen (Section 12.4 on page 74) to enable IGMP snooping.
- Use the **Port Settings** screen (Section 12.5 on page 75) to enable or disable immediate leave on ports.

12.3 What You Need to Know

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.

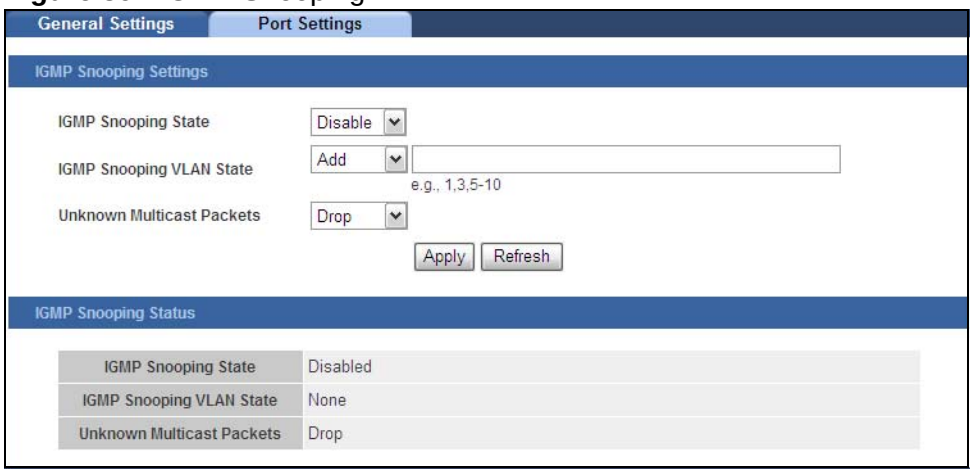
12.3.1 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 4094 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 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.

12.4 General Settings

Click **Advanced Settings > IGMP Snooping** to display the screen as shown.

Figure 39 IGMP Snooping



The following table describes the labels in this screen.

Table 17 IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping State	Select **Enable** to activate IGMP Snooping to forward group multicast traffic only to ports that are members of that group. Select **Disable** to disactivate the feature.
IGMP Snooping VLAN State	Select **Add** and enter VLANs upon which the Switch is to perform IGMP snooping. The valid range of VLAN IDs is between 1 and 4094. Use a comma (,) or hyphen (-) to specify more than one VLANs. Select **Delete** and enter VLANs on which to have the Switch not perform IGMP snooping.
Unknown Multicast Packets	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.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

Table 17 IGMP Snooping (continued)

LABEL	DESCRIPTION
IGMP Snooping State	This field displays whether IGMP snooping is globally enabled or disabled.
IGMP Snooping VLAN State	This field displays VLANs on which the Switch is to perform IGMP snooping. None displays if you have not enabled IGMP snooping on any port yet.
Unknown Mulitcast Packets	This field displays whether the Switch is set to discard or flood unknown mulicast packets.

12.5 Port Settings

Click **Advanced Applications > IGMP Snooping > Port Settings** to open the following screen. Use this screen to enable or disable immediate leave on ports. When immediate leave is enabled on a port, the Switch removes a port from the multicast table immediately when an IGMP leave report is received on that port.

Figure 40 IGMP Snooping Port Setting

The following table describes the labels in this screen.

Table 18 IGMP Snooping Port Setting

LABEL	DESCRIPTION
Immediate Leave Ports	Select individual ports on which to enable immediate leave. Use **Select All** or **Deselect All** to enable or disable immediate leave for all ports.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

13

Link Aggregation

13.1 Overview

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

13.2 What You Can Do

- Use the **Static Trunk** screen (Section 13.4 on page 78) to aggregate groups of physical ports into one higher capacity link.
- Use the **LACP** screen (Section 13.5 on page 79) to enable Link Aggregation Control Protocol (LACP).

13.3 What You Need to Know

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 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.

13.3.1 Dynamic Link Aggregation

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

The IEEE 802.3ad standard describes the Link Aggregation Control Protocol (LACP) for dynamically creating and managing trunk groups.

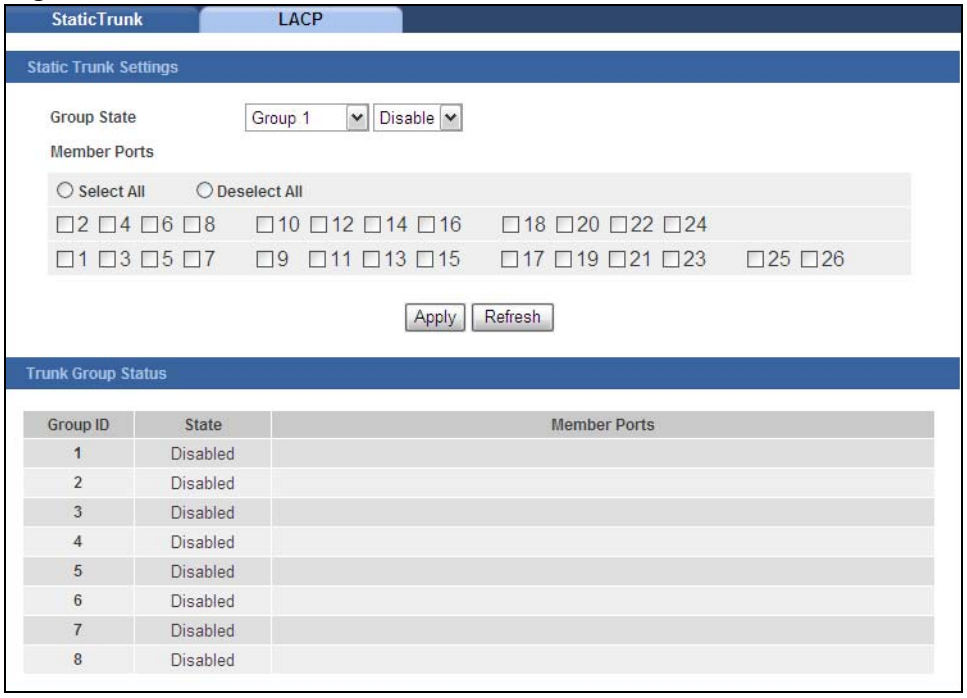
When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. 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.

13.4 Static Trunk

Use this screen to aggregate groups of physical ports into one higher capacity link. Click **Advanced Settings > Link Aggregation** > **Static Trunk** to display the following screen.

Figure 41 Static Trunk



The following table describes the labels in this screen.

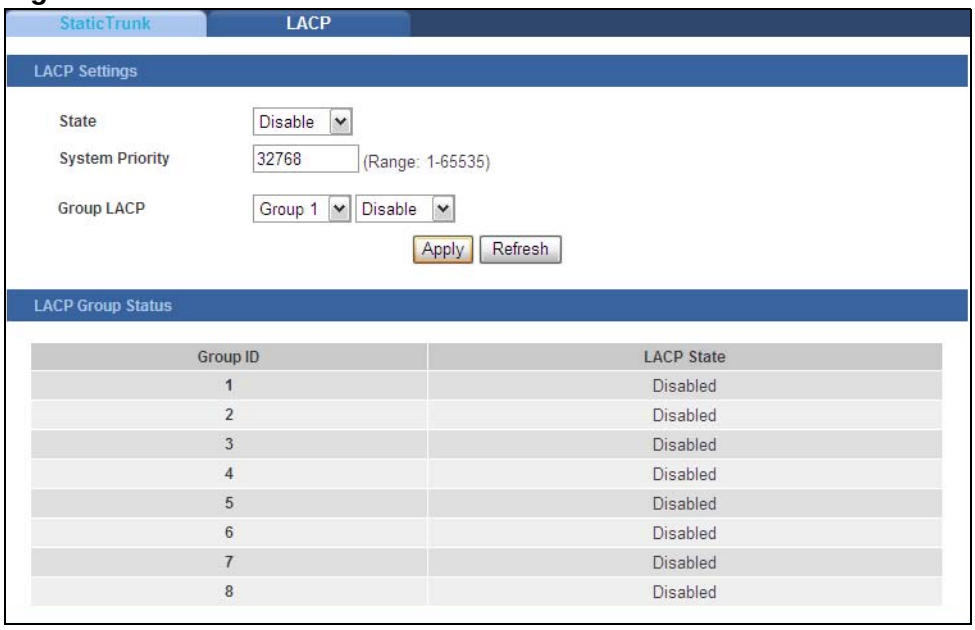
Table 19 Static Trunk

LABEL	DESCRIPTION
Group State	Select the group ID to use for this trunk group, that is, one logical link containing multiple ports. Select **Enable** to use this static trunk group.
Member Ports	Select the ports to be added to the static trunk group.
Select All	Click this to select all ports as members of the static trunk group.
Deselect All	Click this to deselect all ports as members of the trunk gorup.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
State	This field displays if the trunk group is enabled or disabled.
Member Ports	This field displays the assigned ports that comprise the static trunk group.

13.5 LACP

Click **Advanced Settings > Link Aggregation** > **LACP** to display the following screen. See Section 13.3.1 on page 77 for more information on dynamic link aggregation.

Figure 42 LACP



The following table describes the labels in this screen.

Table 20 LACP

LABEL	DESCRIPTION
State	Select **Enable** from the drop down box to enable Link Aggregation Control Protocol (LACP). Select **Disable** to not use LACP.
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group LACP	Select a trunk group ID and then select whether to **Enable** or **Disable** Group Link Aggregation Control Protocol for that trunk group.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP State	This field displays if the group has LACP enabled.

14

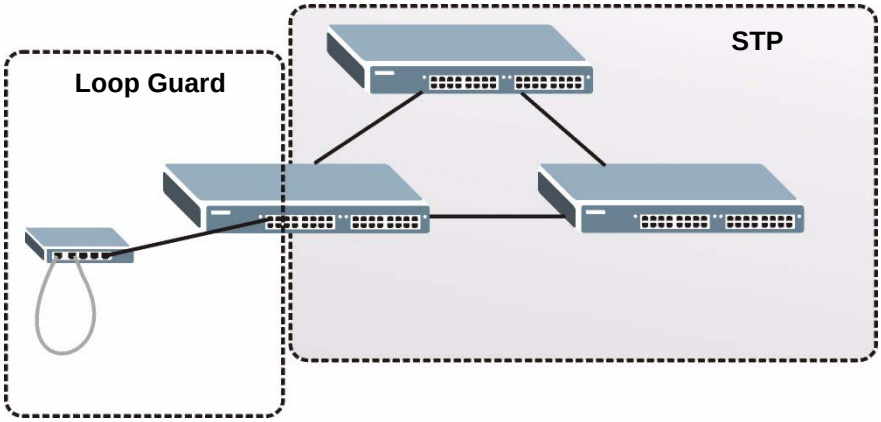
Loop Guard

14.1 Overview

Use the Loop Guard screen (Section 14.3 on page 83) to configure the Switch to guard against loops on the edge of your network.

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 43 Loop Guard vs STP



14.2 What You Need to Know

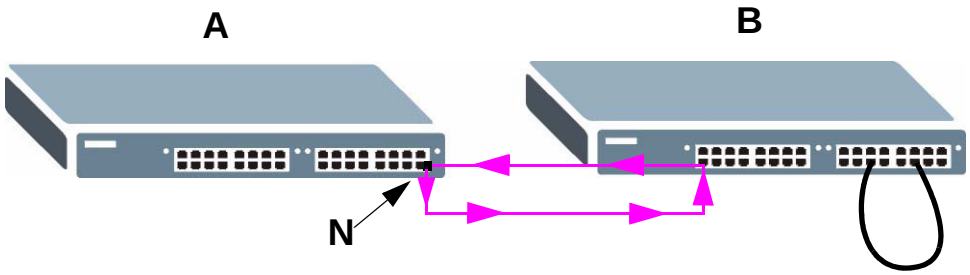
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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**.

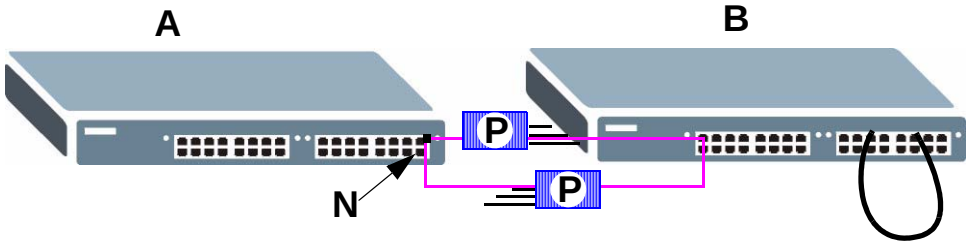
Figure 44 Switch in Loop State



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 45 Loop Guard - Probe Packet

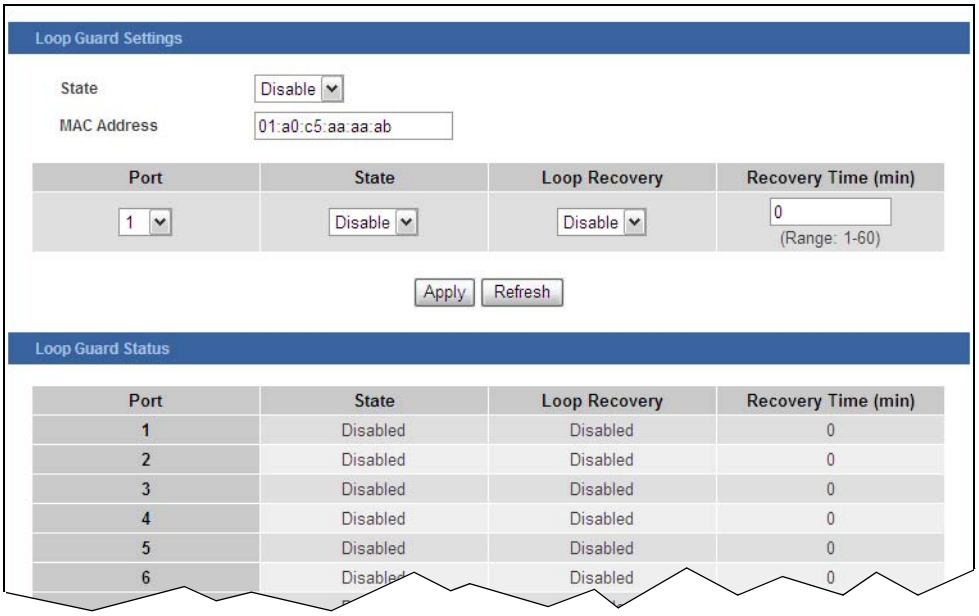


The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops.

14.3 Loop Guard

Use this screen to enable the loop guard feature and to configure the port recovery time for when a port goes down. Click **Advanced Settings** > **Loop Guard** to display the screen as shown.

Figure 46 Loop Guard



The following table describes the labels in this screen.

Table 21 Loop Guard

LABEL	DESCRIPTION
State	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.
MAC Address	Enter the destination MAC address the probe packets will be sent to. If the port receives these same packets the port will be shut down.
Port	Select a port on which to configure loop guard protection.
State	Select **Enable** to use the loop guard feature on the Switch.
Loop Recovery	Select **Enable** to reactivate the port automatically after the designated recovery time has passed.
Recovery Time	Specify the recovery time in minutes that the Switch will wait before reactivating the port. This can be between 1 to 60 minutes.
Apply	Click **Apply** to save your changes to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Port	This field displays a port number.
State	This field displays if the loop guard feature is enabled.

Table 21 Loop Guard (continued)

LABEL	DESCRIPTION
Loop Recovery	This field displays if the loop recovery feature is enabled.
Recovery Time (min)	This field displays the recovery time for the loop recovery feature.

15

QoS

15.1 Overview

This chapter introduces the quality of service (QoS) parameters you can configure on the Switch.

QoS is used to help solve performance degradation when there is network congestion. The Switch allows you to use IEEE 802.1p priority tags or Differentiated Services Code Points (DSCPs) tags to prioritize traffic.

15.2 What You Can Do

- Use the **Port Priority** screen (Section 15.4 on page 86) to specify IEEE 802.1p priority for each port.
- Use the **IP DiffServ (DSCP)** screen (Section 15.5 on page 87) to configure DSCP-based QoS settings.
- Use the **Priority / Queue Mapping** screen (Section 15.6 on page 89) to configure IEEE 802.1p priority and queue mappings for the Switch.
- Use the **Queuing Method** screen (Section 15.7 on page 90) to configure the weight value of each queue.

15.3 What You Need to Know

15.3.1 Queuing algorithms

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

15.3.1.1 Weighted Round Robin (WRR)

Round Robin scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin (WRR) scheduling 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.

15.3.2 QoS Enhancement

You can configure the Switch to prioritize traffic even if the incoming packets are not marked with IEEE 802.1p priority tags or change the existing priority tags based on the criteria you select. The Switch allows you to choose one of the following methods for assigning priority to incoming packets on the Switch:

Port Based QoS - Assign priority to packets based on the incoming port on the Switch. See Section 15.4 on page 86.

DSCP Based QoS - Assign priority to packets based on their Differentiated Services Code Points (DSCPs). See Section 15.5.1 on page 88.

Note: Advanced QoS methods only affect the internal priority queue mapping for the Switch. The Switch does not modify the IEEE 802.1p value for the egress frames.

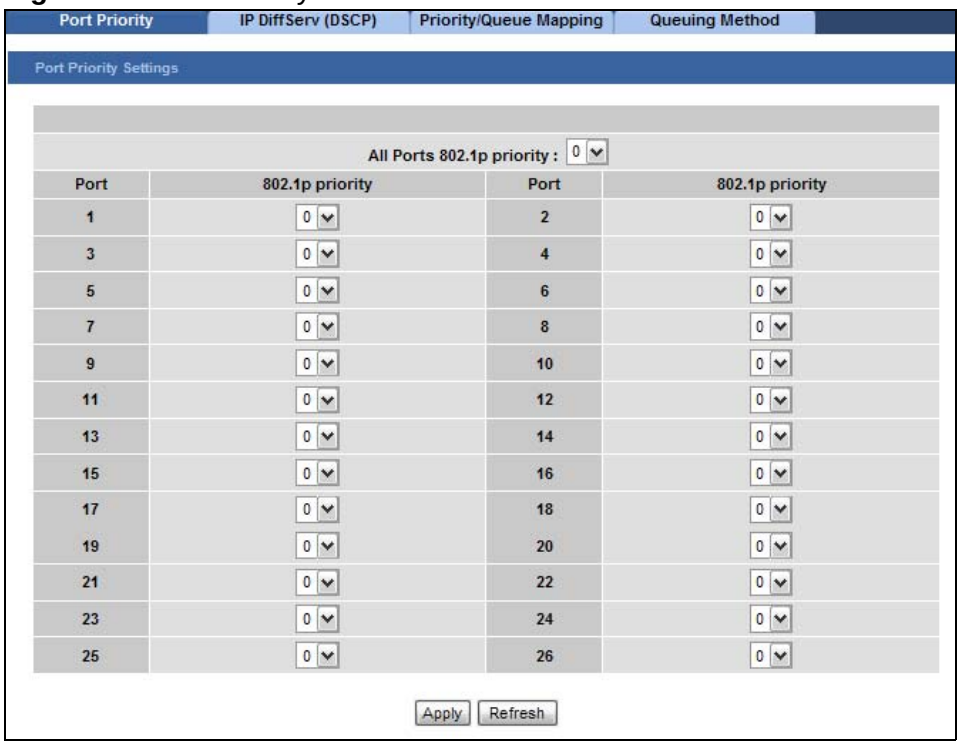
You can choose one of these ways to alter the way incoming packets are prioritized or you can choose not to use any QoS enhancement setting on the Switch.

15.4 Port Priority

Use the **Port Priority** screen to specify IEEE 802.1p priority for each port. Packets without 802.1p priority tags will be applied the priority settings according to the

received port of the Switch. Click **Advanced Settings > QoS > Port Priority** to open the following screen.

Figure 47 Port Priority



The following table describes the labels in this screen.

Table 22 Port Priority

LABEL	DESCRIPTION
All Ports 802.1p priority	Use this field to set a priority for all ports. The value indicates packet priority and is added to the priority tag field of incoming packets. The values range from 0 (lowest priority) to 7 (highest priority).
Port	This field displays the number of a port.
Priority	Select a priority for packets received by the port. Only packets without a 802.1p priority tagged will be applied the priority you set here.
Apply	Click **Apply** to save your changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

15.5 IP DiffServ (DSCP)

Use this screen to configure DSCP-based QoS settings. You can also use this screen to decide whether to use Switch IEEE 802.1p priority or DSCPs for the

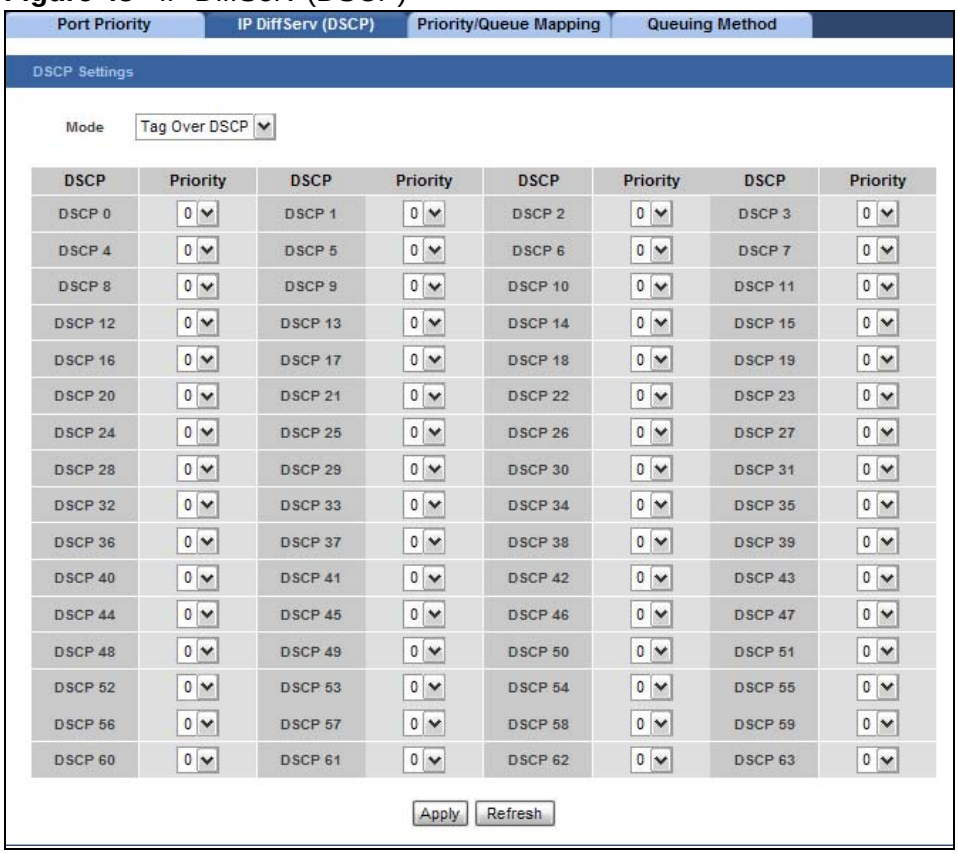
Switch to prioritize all incoming traffic. Click **Advanced Settings > QoS > IP DiffServ (DSCP)** to open the screen.

15.5.1 Differentiated Services Code Point (DSCP)

Differentiated Services (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.

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

Figure 48 IP DiffServ (DSCP)



The following table describes the labels in this screen.

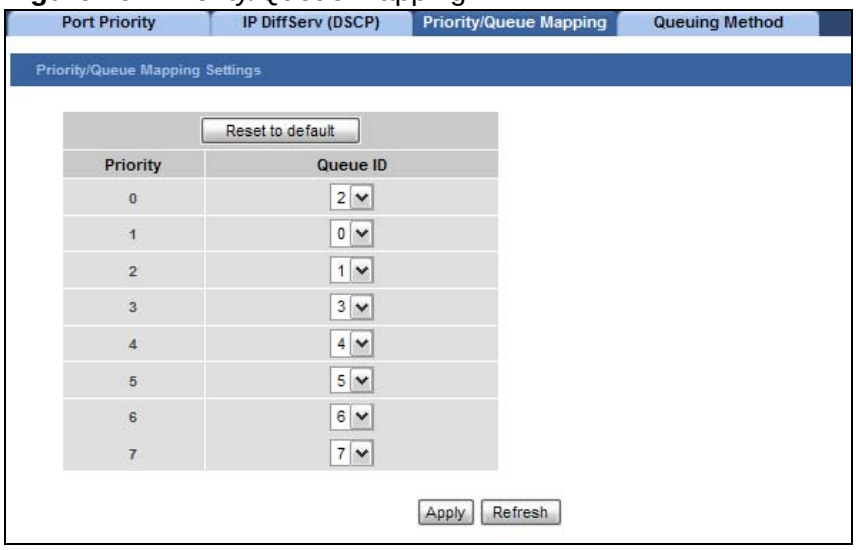
Table 23 IP DiffServ (DSCP)

LABEL	DESCRIPTION
Mode	Select **Tag Over DSCP** if you want to use 802.1p Priority in packets to prioritize traffic. Select **DSCP Over Tag** if you want to use DSCP priority to prioritize traffic, even if the packet has an IEEE 802.1p priority tag.
DSCP	This field displays the number of each DSCP service level.
Priority	Select the IEEE 802.1p priority you want to assign to the packets with the DSCP service level. Note: The changes are not applied until you click **Apply**.
Apply	Click **Apply** to save the changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

15.6 Priority/Queue Mapping

Use the **Priority / Queue Mapping Settings** screen to configure IEEE 802.1p priority and queue mappings for the Switch. Click **Advanced Settings > QoS > Priority / Queue Mapping** to open the following screen.

Figure 49 Priority/Queue Mapping



The following table describes the labels in this screen.

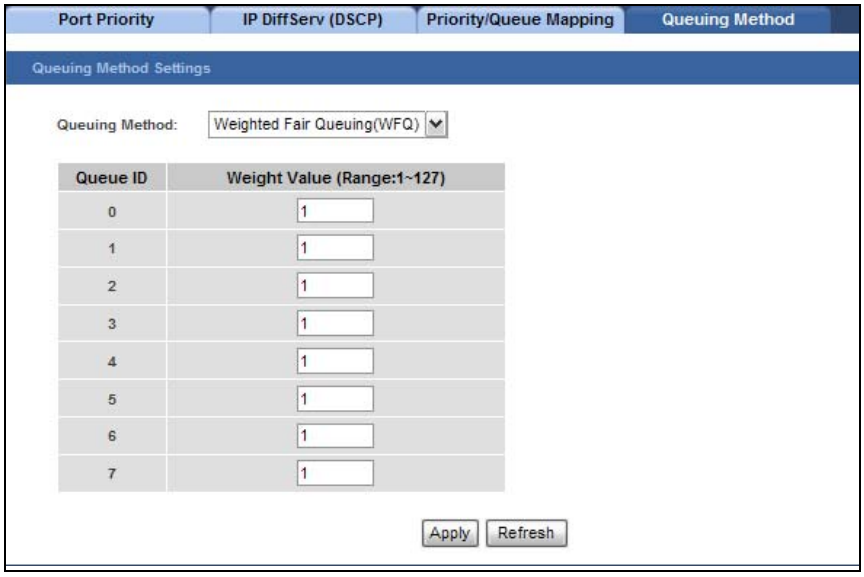
Table 24 Priority/Queue Mapping

LABEL	DESCRIPTION
Reset to default	Click this button to reset the priority to queue mappings to the defaults.
Priority	This field displays each priority level. The values range from 0 (lowest priority) to 7 (highest priority).
Queue ID	Select the number of a queue for packets with the priority level.
Apply	Click **Apply** to save your changes.
Refresh	Click **Refresh** to begin configuring the screen afresh.

15.7 Queuing Method

Use the **Queuing Method** screen to configure the weight value of each queue. Click **Advanced Settings > QoS > Queuing Method** to open the following screen.

Figure 50 Queuing Method



The following table describes the labels in this screen.

Table 25 Queuing Method

LABEL	DESCRIPTION
QoS Method	Select **Weighted Fair Queuing** (**WFQ**), **Strict Priority** (SP) or **Weighted Round Robin** (**WRR**). Note: Queue weights can only be changed when **Weighted Round Robin** is selected. **Weighted Round Robin** scheduling 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.
Queue ID	This field indicates which Queue (0 to 7) you are configuring. Queue 0 has the lowest priority and Queue 7 the highest priority.
Weight Value	You can only configure the queue weights when **Weighted Round Robin** is selected. Bandwidth is divided across the different traffic queues according to their weights. Note: If you want to use **Strict Priority** but want to change the weights for the queues, configure them with **Weighted Round Robin** selected first and then change the scheduling method to **Strict Priority**.
Apply	Click **Apply** to save the changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.

16

Storm Control

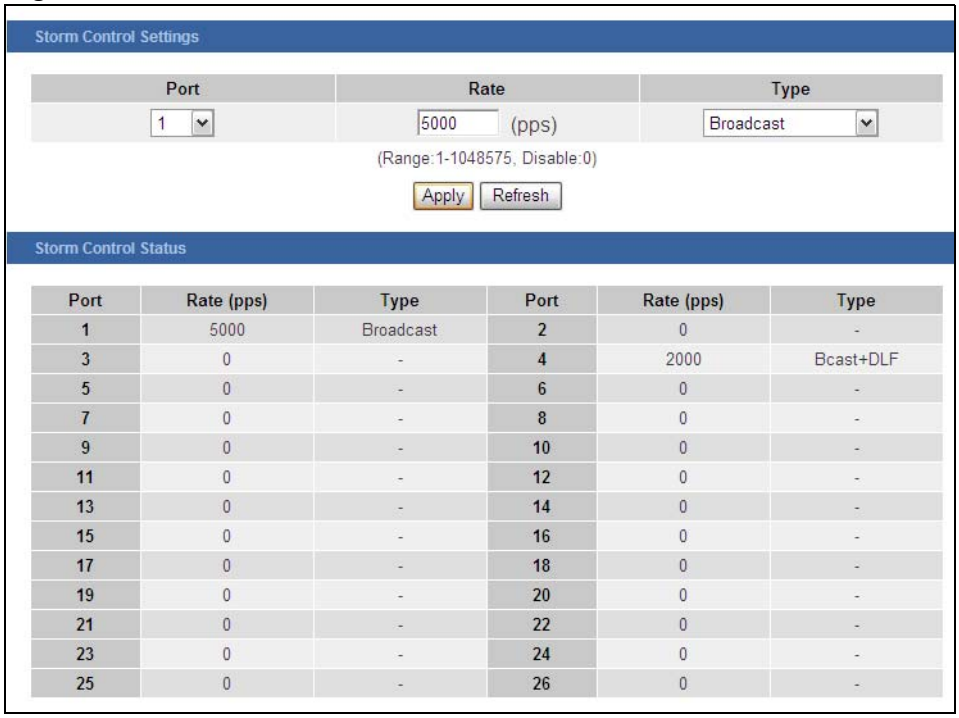
This chapter shows you how you can manage bandwidth on each port and set up broadcast storm control settings using the **Storm Control** screen.

16.0.1 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and unknown unicast (also referred to as Destination Lookup Failure or DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and unknown unicast packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and unknown unicast packets in your network.

Click **Advanced Settings > Bandwidth Management > Storm Control** to display the screen as shown next.

Figure 51 Broadcast Storm Control



Port	Rate (pps)	Type	Port	Rate (pps)	Type
1	5000	Broadcast	2	0	-
3	0	-	4	2000	Bcast+DLF
5	0	-	6	0	-
7	0	-	8	0	-
9	0	-	10	0	-
11	0	-	12	0	-
13	0	-	14	0	-
15	0	-	16	0	-
17	0	-	18	0	-
19	0	-	20	0	-
21	0	-	22	0	-
23	0	-	24	0	-
25	0	-	26	0	-

The following table describes the labels in this screen.

Table 26 Broadcast Storm Control

LABEL	DESCRIPTION
Storm Control Settings	
Port	Select the port number for which you want to configure storm control settings.
Rate	Select the number of packets (of the type specified in the **Type** field) per second the Switch can receive per second.
Type	Select **Broadcast** - to only specify a limit for the amount of broadcast packets received per second. **Multicast** - to only specify a limit for the amount of multicast packets received per second. **DLF** - to only specify a limit for the amount of DLF packets received per second. **Bcast+Mcast** - to specify a limit for the amount of broadcast and multicast packets received per second. **Mcast+DLF** - to specify a limit for the amount of multicast and DLF packets received per second. **Bcast+DLF** - to specify a limit for the amount of broadcast and DLF packets received per second. **Bcast+Mcast+DLF** - to specify a limit for the amount of broadcast, multicast and DLF (Destination Lookup Failure) packets received per second.
Apply	Click **Apply** to save your changes.
Refresh	Click **Refresh** to begin configuring this screen afresh.
Storm Control Status	
Port	This field displays the number of a port.
Rate (pps)	This field displays the number of packets (of the type displayed in the **Type** field) per second the Switch can receive per second.
Type	This field displays the packet types that the limit (of the rate displayed in the **Rate** field) is applied on the Switch.

17

Spanning Tree Protocol

17.1 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 supports Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) as defined in the following standards.

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

17.2 What You Can DO

- Use the **General Settings** screen (Section 17.4 on page 97) to enable and configure STP.
- Use the **STP Status** screen (Section 17.5 on page 98) to check the STP current status.

17.3 What You Need to Know

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 and then the root bridge 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.

17.3.1 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 27 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 bridge communicates with the root through the root port. The root port 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.

17.3.2 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.

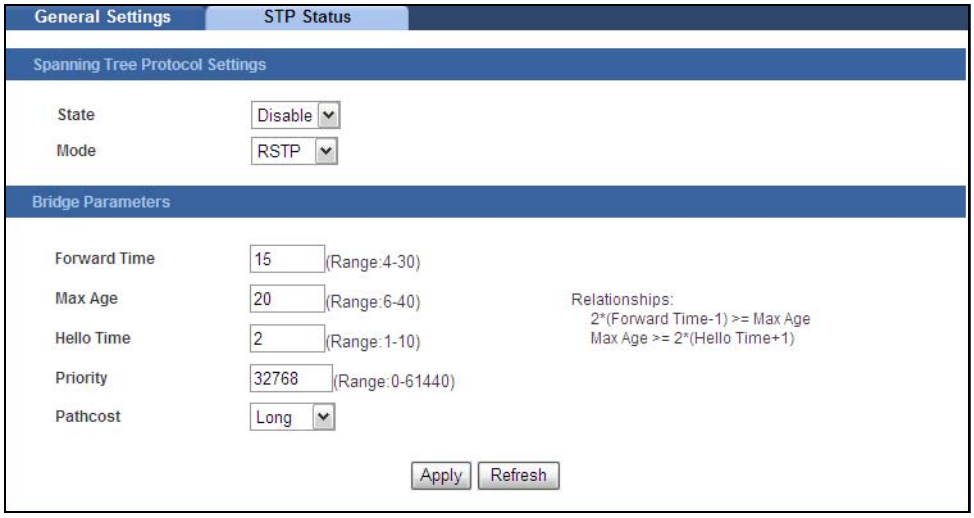
STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

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.

17.4 General Settings

Use this screen to enable and configure the STP settings. Click **Advanced Settings** > **STP > General Settings** to see the screen as shown.

Figure 52 General Settings



The following table describes the labels in this screen.

Table 28 General Settings

LABEL	DESCRIPTION
Spanning Tree Protocol Settings	
State	Select **Enabled** to use Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP).
Mode	Select to use either Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). See Section 17.1 on page 95 for background information on STP.
Bridge Parameters	
Forward Time	This is the maximum time (in seconds) the 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.
Max Age	This is the maximum time (in seconds) the 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.
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.

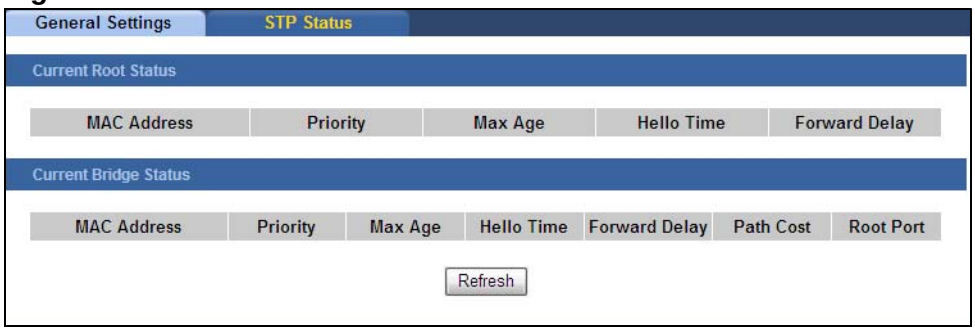
Table 28 General Settings (continued)

LABEL	DESCRIPTION
Priority	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. Enter a value from 0~61440. The lower the numeric value you assign, the higher the priority for this bridge. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
Pathcost	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.
Apply	Click **Apply** to save your changes.
Refresh	Click **Refresh** to begin configuring this screen afresh.

17.5 STP Status Screen

Use this screen to check the current status of the STP feature. Click **Advanced Settings** > **STP > STP Status** to display the screen as shown.

Figure 53 STP Status



The following table describes the labels in this screen.

Table 29 STP Status

LABEL	DESCRIPTION
Current Root Status	
MAC Address	This is the MAC address of the root bridge.
Priority	**Root** refers to the base of the spanning tree (the root bridge). This field displays the root bridge's priority. This Switch may also be the root bridge.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.

Table 29 STP Status (continued)

LABEL	DESCRIPTION
Hello Time	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.
Forward Delay	This is the time (in seconds) the root switch will wait before changing states.
Current Bridge Status	
MAC Address	This is the MAC address of the current bridge.
Priority	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. Priority determines the root bridge, which in turn determines the Root Hello Time, Root Maximum Age and Root Forwarding Delay.
Max Age	This is the maximum time (in seconds) the 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.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch.
Forward Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.
Path Cost	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.
Root Port	This is the number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Refresh	Click this to update the status screen.

PART IV
Security and Management

18

IP Source Guard

18.1 Overview

Use the IP source guard screens to filter unauthorized DHCP and ARP packets in your network. IP source guard uses a binding table to distinguish between the authorized and unauthorized DHCP and ARP packets in your network.

18.2 What You Can Do

- Use the **DHCP Snooping** screens (Section 18.4 on page 107) to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- Use the **ARP Inspection** screens (Section 18.6 on page 110) to filter unauthorized ARP packets on the network.
- Use the **Binding Table** screens (Section 18.7 on page 112) to manually enter static bindings and to convert dynamic bindings to static.

18.3 What You Need To Know

A binding in the IP source guard binding table 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 the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

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

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

18.3.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

18.3.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection.

Trusted ports are connected to DHCP servers or other switches. The Switch learns dynamic bindings from trusted ports.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

18.3.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again.

18.3.1.3 Configuring DHCP Snooping

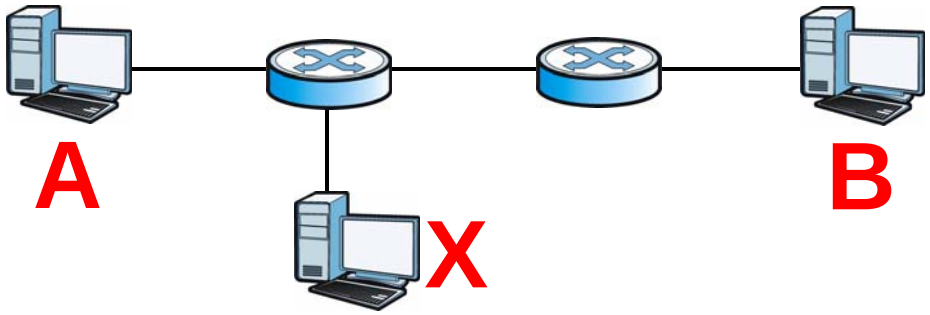
Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN.
3. Configure trusted and untrusted ports.
4. Configure static bindings.

18.3.2 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 54 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.

18.3.2.1 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.

- 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.

18.3.2.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

18.3.2.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 21 on page 133) 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.

18.3.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping. See Section 18.3.1.3 on page 105.

   Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

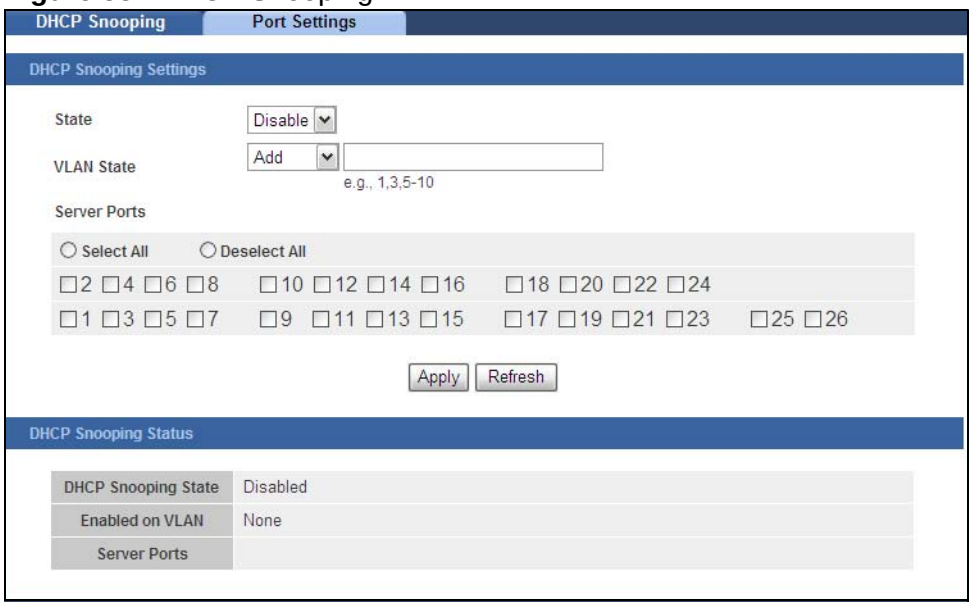
2. Enable ARP inspection on each VLAN.

3. Configure trusted and untrusted ports.

18.4 DHCP Snooping

Use this screen to enable and configure the settings for **DHCP Snooping** which is used to filter unauthorized DHCP packets on the network. To open this screen, click **Security > IP Source Guard > DHCP Snooping > DHCP Snooping**.

Figure 55 DHCP Snooping



The following table describes the labels in this screen.

Table 30 DHCP Snooping

LABEL	DESCRIPTION
State	Select **Enable** to use DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLANs and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports. Select **Disable** to not use DHCP snooping.
VLAN State	Select **Add** and enter the VLAN IDs you want the Switch to enable DHCP snooping on. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-). Select **Delete** and enter the VLAN IDs you no longer want the Switch to use DHCP snooping on.

Table 30 DHCP Snooping (continued)

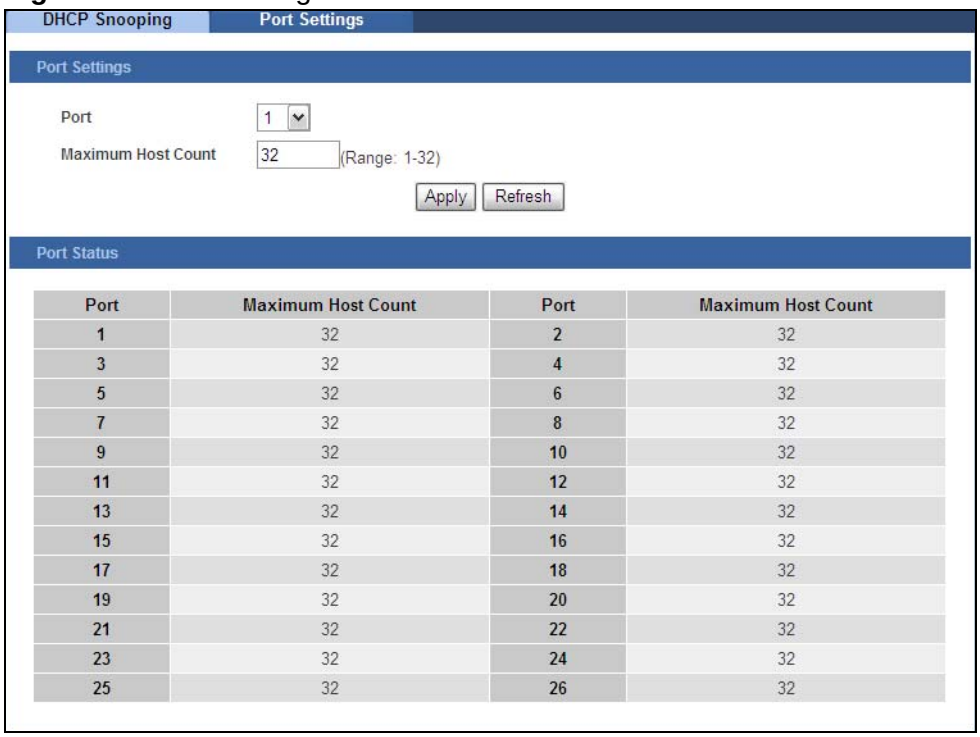
LABEL	DESCRIPTION
Server Ports	Select the ports that are connected to DHCP servers or other Switches and deselect the ports which are not. Server ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from these ports in the following situations: • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Select All	Click this to set all ports as server ports.
Deselect All	Click this to deselect all ports that are set as server ports.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
DHCP Snooping State	This field displays the current status of the DHCP snooping feature, **Enabled** or **Disabled**.
Enabled on VLAN	This field displays the VLAN IDs that have DHCP snooping enabled on them. This will display **None** if no VLANs have been set.
Server Ports	This field displays the ports which have been set as server ports. This will display **None** if no ports have been set

18.5 Port Settings

Use this screen to define the maximum number of hosts allowed to simultaneously connect to each port. Each host that successfully acquires an IP address from a

DHCP server on the port is recorded in the dynamic binding table. To open this screen, click **Security > IP Source Guard > DHCP Snooping > Port Settings**.

Figure 56 Port Settings



The following table describes the labels in this screen.

Table 31 Port Settings

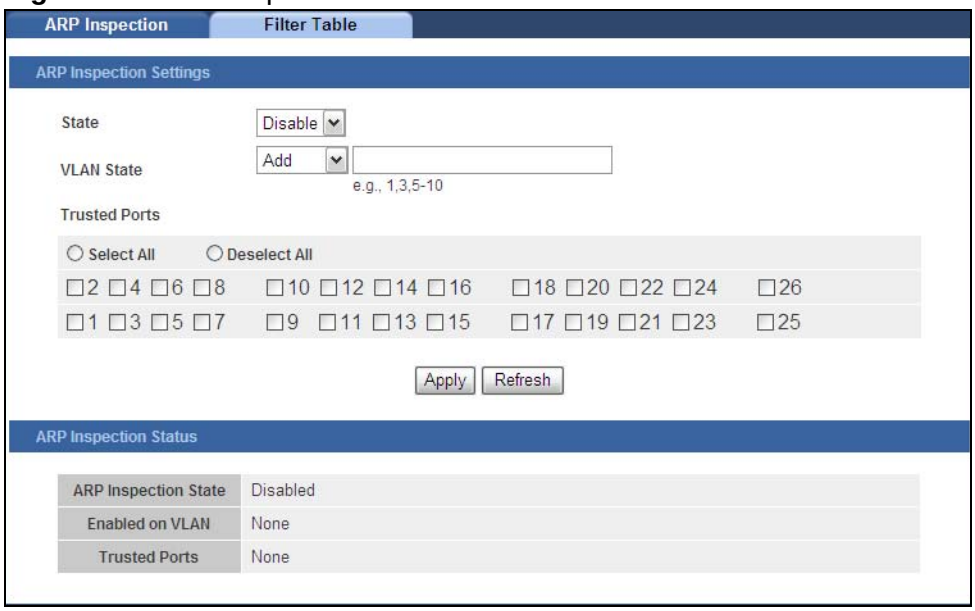
LABEL	DESCRIPTION
Port Settings	
Port	Select a port number (1-16 for GS1510-16, 1-26 for GS1510-24) to modify its maximum host count.
Maximum Host Count	Enter the maximum number of hosts (1-32) that are permitted to simultaneously connect to a port.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
Port Status	
Port	This field displays the port number.
Maximum Host Count	This field displays the maximum host count for each port on the Switch.

18.6 ARP Inspection

Use this screen to enable/disable **ARP Inspection**. You can also use this screen to specify whether ports are trusted or untrusted and which VLANs are enabled for ARP inspection.

To open this screen, click **Security > IP Source Guard > ARP Inspection > ARP Inspection**.

Figure 57 ARP Inspection



The following table describes the labels in this screen.

Table 32 ARP Inspection

LABEL	DESCRIPTION
State	Use this to **Enable** or **Disable** ARP inspection on the Switch.
VLAN State	Enter the VLAN IDs you want the Switch to enable ARP Inspection for. You can designate multiple VLANs individually by using a comma (,) and by range with a hyphen (-).
Trusted Ports	Select the ports which are trusted and deselect the ports which are untrusted. The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Select All	Click this to set all ports to trusted.

Table 32 ARP Inspection (continued)

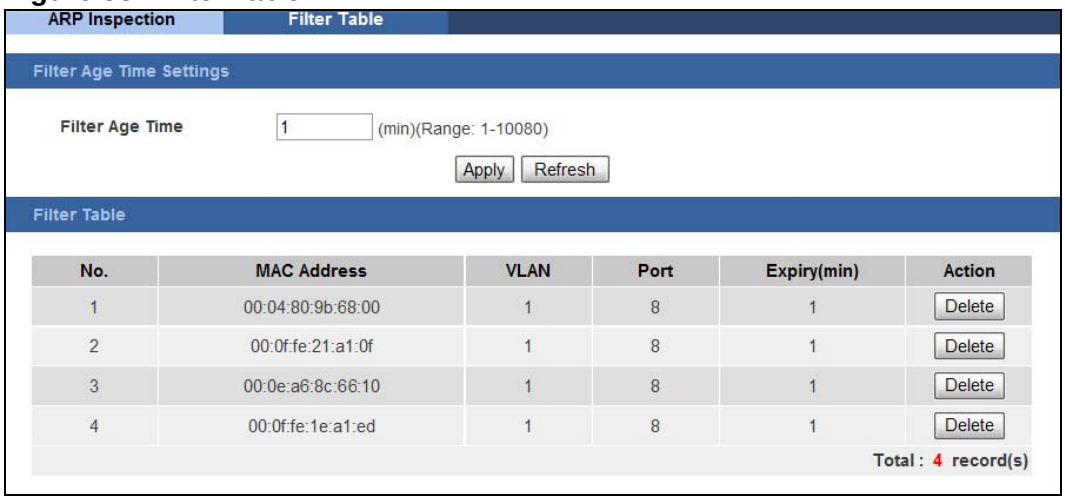
LABEL	DESCRIPTION
Deselect All	Click this to set all ports to untrusted.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reload the screen and reset any changes that were just made.
ARP Inspection Status	
ARP Inspection State	This field displays the current status of the ARP Inspection feature, **Enabled** or **Disabled**.
Enabled on VLAN	This field displays the VLAN IDs that have ARP Inspection enabled on them. This will display **None** if no VLANs have been set.
Trusted Ports	This field displays the ports which are trusted. This will display **None** if no ports are trusted.

18.6.1 Filter Table

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 **Security > IP Source Guard > ARP Inspection > Filter Table**.

Figure 58 Filter Table



The following table describes the labels in this screen.

Table 33 Filter Table

LABEL	DESCRIPTION
Filter Age Time	This setting has no effect on existing MAC address filters. Enter how long (1-10080 minutes) 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.
Apply	Click this to save any changes.
Refresh	Click this to reload the screen and reset any changes that were just made.
Filter Table	
No.	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.
VLAN	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 (min)	This field displays how long (in minutes) the MAC address filter remains in the Switch.
Action	Click **Delete** to remove the record manually.
Total	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.

18.7 Binding Table

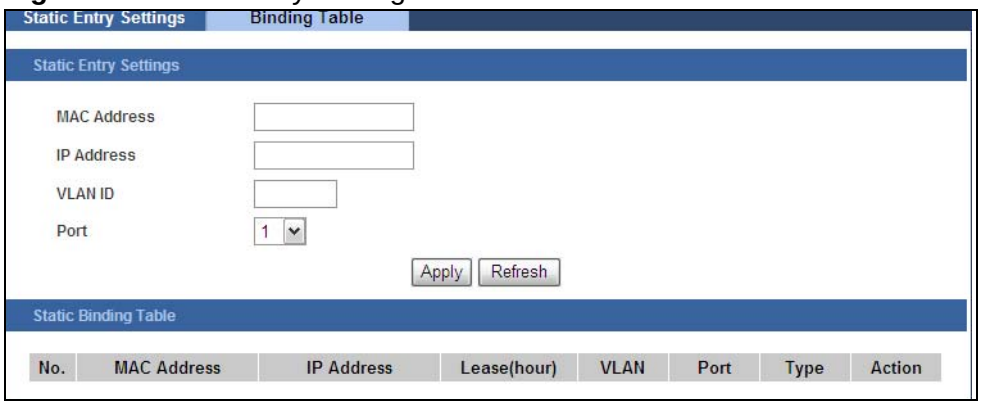
Use these screens to manage both the static and dynamic binding entries.

18.7.1 Static Entry Settings

Use this screen to manage static bindings for DHCP snooping and 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 **Security > IP Source Guard > Binding Table** > **Static Entry Settings**.

Figure 59 Static Entry Settings



The following table describes the labels in this screen.

Table 34 Static Entry Settings

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 ID	Enter the source VLAN ID in the binding.
Port	Specify the port in the binding.
Apply	Click this to create the specified static binding or to update an existing one.
Refresh	Click this to reload the screen and reset any changes that were just made.
No.	This field displays a sequential number for each binding. Click it to update an existing entry.
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(hour)	This field displays how long the binding is valid.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding.
Type	This field displays how the Switch learned the binding. **Static**: This binding was learned from information provided manually by an administrator. **Dynamic**: This binding was learned by snooping DHCP packets.
Action	Click **Delete** to remove the specified entry.

18.7.2 Binding Table

Use this screen to look at the current bindings. You can also use this screen to convert dynamic binding entries to static entries by selecting the entries and clicking **Apply**.

Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the dynamic bindings by snooping DHCP packets and from information provided manually in the **Static Entry Settings** screen.

To open this screen, click **Security > IP Source Guard > Binding Table** > **Binding Table**.

Figure 60 Binding Table

The following table describes the labels in this screen.

Table 35 Binding Table

LABEL	DESCRIPTION
Show Type	Select **All** to display both dynamic and static binding entries. Select **Dynamic** to display dynamic binding entries only. Select **Static** to display static binding entries only.
Show	Click this to refresh the screen and display the binding entries for the currently selected type.
All	Click this to highlight all binding entries. By clicking the **Apply** button, the Switch will convert the dynamic binding entries to static entries.
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 (hour)	This field displays how long the binding is valid.
VLAN	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.

Table 35 Binding Table (continued)

LABEL	DESCRIPTION
Type	This field displays how the Switch learned the binding. **Static**: This binding was learned from information provided manually by an administrator. **Dynamic**: This binding was learned by snooping DHCP packets.
Apply	Click **Apply** and the Switch will convert any selected dynamic binding entries to static entries.
Refresh	Click this to reload the screen and to display any recently added bindings.

19

802.1x

This chapter describes the IEEE 802.1x screens.

19.1 Overview

Port authentication is a way to validate access to ports on the Switch to clients based on a local or external server (authentication server). The Switch supports the following method for port authentication:

- **IEEE 802.1x**[1] - An authentication server validates access to a port based on a username and password provided by the user.

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. This external method of authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 19.3 on page 118 for more information on configuring your RADIUS server settings.

19.2 What You Can Do

- Use the **Global Settings** screen (Section 19.4 on page 118) to activate IEEE 802.1x security and configure the local or RADIUS server settings.
- Use the **Port Setting** screen (Section 19.5 on page 120) to configure IEEE 802.1x port authentication settings.

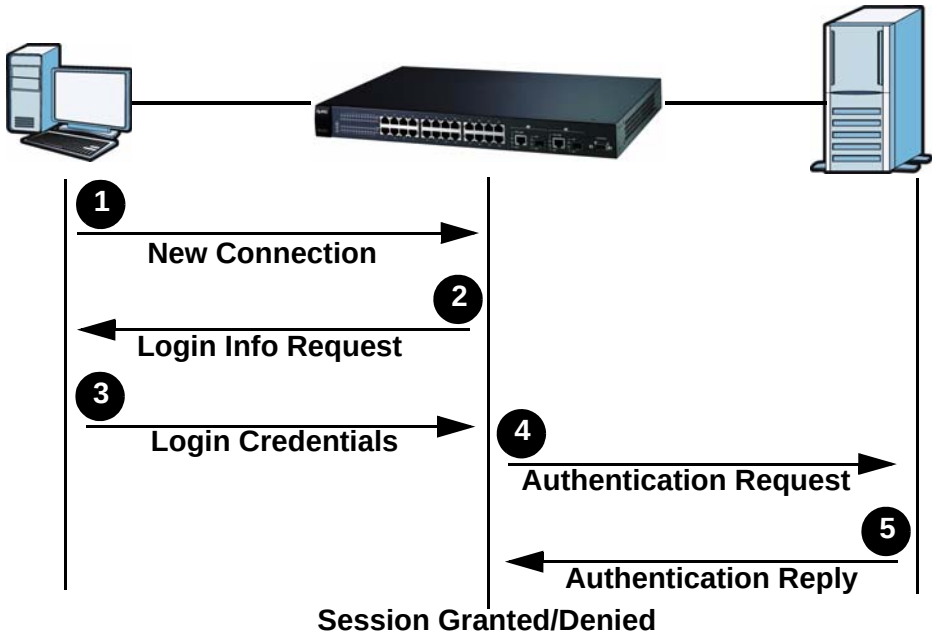
1. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

19.3 What You Need to Know

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

Figure 61 IEEE 802.1x Authentication Process



19.3.2 Local User Accounts

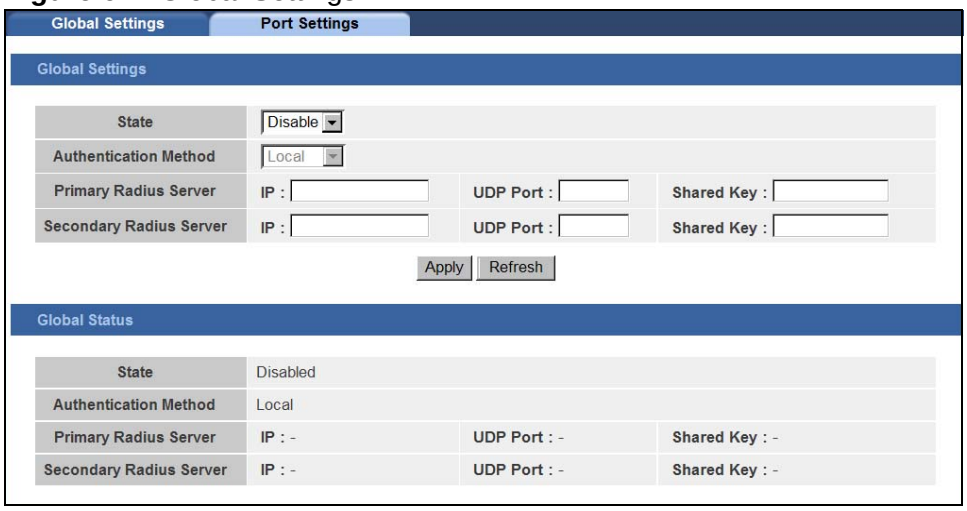
By storing user profiles locally on the Switch, your Switch is able to authenticate users without interacting with a network authentication server. However, there is a limit on the number of users you may authenticate in this way.

19.4 Global Settings

Use this screen to enable 802.1x authentication and configure the method of authentication.

To open the screen as shown, click **Security > 802.1x > Global Settings**.

Figure 62 Global Settings



The following table describes the labels in this screen.

Table 36 Global Settings

LABEL	DESCRIPTION
State	Select **Enable** 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.
Authentication Method	Select whether to use **Local** or **RADIUS** as the authentication method. The **Local** method of authentication uses the "guest" and "user" user groups of the user account database on the Switch itself to authenticate. However, only a certain number of accounts can exist at one time. **RADIUS** is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.
Primary Radius Server	When **RADIUS** is selected as the 802.1x authentication method, the **Primary Radius Server** will be used for all authentication attempts.
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**.
Shared Key	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.
Second Radius Server	This is the backup server used only when the **Primary Radius Server** is down.
Apply	Click this to save any changes.
Refresh	Click this to reload the screen and reset any changes that were just made.

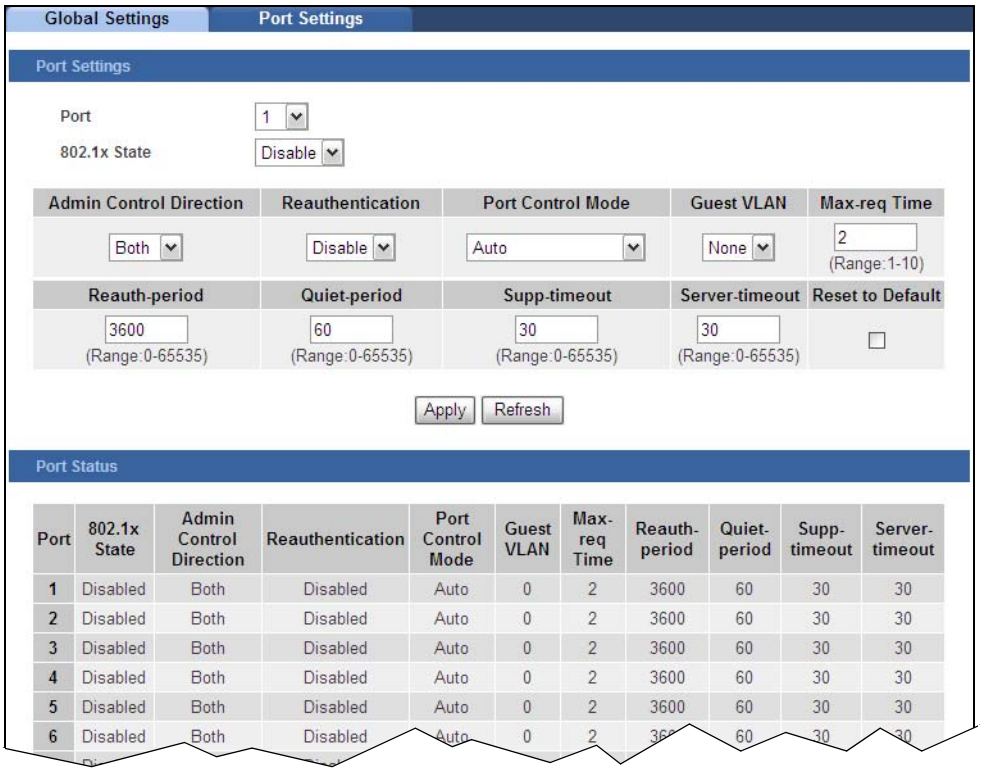
Table 36 Global Settings (continued)

LABEL	DESCRIPTION
Global Status	
State	This field displays if 802.1x authentication is **Enabled** or **Disabled**.
Authentication Method	This field displays if the authentication method is **Local** or **RADIUS**.
Primary Radius Server	This field displays the IP address, UDP port and shared key for the **Primary Radius Server**. This will be blank if nothing has been set.
Second Radius Server	This is the backup server used only when the **Primary Radius Server** is down.

19.5 Port Settings

Use this screen to activate IEEE 802.1x security on specific ports according to customized settings. Click **Security > 802.1x > Port Settings** to display the configuration screen as shown.

Figure 63 Port Settings



The following table describes the labels in this screen.

Table 37 Port Settings

LABEL	DESCRIPTION
Port	Select a port number to configure.
802.1x State	Select **Enable** to permit 802.1x authentication on the port. You must first enable 802.1x authentication on the Switch before configuring it on each port.
Admin Control Direction	Select **Both** to drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. Select **In** to drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Reauthenticati on	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	Select **Auto** to require authentication on the port. Select **Force Authorized** to always force this port to be authorized. Select **Force Unauthorized** to always force this port to be unauthorized. No packets can pass through this port.
Guest VLAN	Select **None** to disable Guest VLAN. Select **1** to use VLAN 1 for traffic from hosts that have not passed authentication. Use this to limit the permissions of hosts which have not passed authentication.
Max-req Time	Specify the amount of times the Switch will try to connect to the authentication server before determining the server is down. The acceptable range for this field is 1 to 10 times.
Reauth period	Specify how often a client has to re-enter his or her username and password to stay connected to the port. The acceptable range for this field is 0 to 65535 seconds.
Quiet period	Specify a period of the time the client has to wait before the next reauthentication attempt. This will prevent the Switch from becoming overloaded with continous reauthentication attempts from the client. The acceptable range for this field is 0 to 65535 seconds.
Supp timeout	Specify how long the Switch will wait before communicating with the client. The acceptable range for this field is 0 to 65535 seconds.
Server timeout	Specify how long the Switch will wait before communicating with the server. The acceptable range for this field is 0 to 65535 seconds.
Reset to Default	Select this and click **Apply** to reset the custom 802.1x port authentication settings back to default.
Apply	Click this to save any changes.
Refresh	Click this to reload the screen and reset any changes that were just made.
Port Status	
Port	This field displays the port number.
802.1x State	This field displays if 802.1x authentication is **Enabled** or **Disabled** on the port.

Table 37 Port Settings (continued)

LABEL	DESCRIPTION
Admin Control Direction	This field displays the Admin Control Direction. **Both** will drop incoming and outgoing packets on the port when a user has not passed 802.1x port authentication. **In** will drop only incoming packets on the port when a user has not passed 802.1x port authentication.
Reauthenticati on	This field displays if the subscriber must periodically re-enter his or her username and password to stay connected to the port.
Port Control Mode	This field displays the port control mode. **Auto** requires authentication on the port. **Force Authorized** forces the port to be authorized. **Force Unauthorized** forces the port to be unauthorized. No packets can pass through the port.
Guest VLAN	This field displays the Guest VLAN setting for hosts that have not passed authentication. **None** or **1**.
Max-req Time	This field displays the amount of times the Switch will try to connect to the authentication server before determining the server is down.
Reauth period	This field displays how often a client has to re-enter his or her username and password to stay connected to the port.
Quiet period	This field displays the period of the time the client has to wait before the next reauthentication attempt.
Supp timeout	This field displays how long the Switch will wait before communicating with the client.
Server timeout	This field displays how long the Switch will wait before communicating with the server.

20

Web Authentication

20.1 Overview

This feature is used to authenticate users before they can access a website on the Internet.

The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself (see Section 23.2 on page 143). The Switch can also use an external authentication server to authenticate a larger number of users. This external method of authentication uses the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users.

When a user on an enabled port accesses the Internet, a customized web login page will display. User accounts with “User” or “Guest” privileges can login past this screen and access the Internet.

20.2 What You Can Do

- Use the **Configuration** screen (Section 20.4 on page 125) to configure the authentication method and port settings.
- Use the **Customization** screen (Section 20.5 on page 126) to configure the appearance of the web login screen that users will see.

20.3 What You Need to Know

Web authentication allows the network administrator to set a username and password for Internet access on a particular port.

This feature could be used on a guest terminal, for example in a company meeting room, where guests are allowed to connect to the Internet but not the local network (which is thereby kept secure).

When a device using that port attempts to connect to the Internet, the web browser will request a username and password before allowing access. If a port is not successfully authenticated, all IP packets from that device will be filtered.

Note: The URL entered by the user should be a domain such as http://news.zyxel.com, it cannot be in one of the formats listed below:

- A specific IP address (example: http://172.20.1.111)
- A domain with a full address (example: http://news.zyxel.com/article/100826.html)

20.3.1 User Authentication Experience

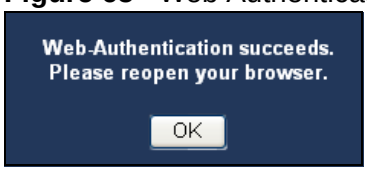
When the user attempts to access the Internet through a port which is secured with Web Authentication, the following screen will display and request them to enter a username and password.

Note: The appearance of this login page can be modified in the **Customization** screen (Section 20.5 on page 126).

Figure 64 Web Authentication - Login

After successfully logging in the following message will display. At this point, users should close the browser and relaunch it to access the Internet.

Figure 65 Web Authentication - Login Success



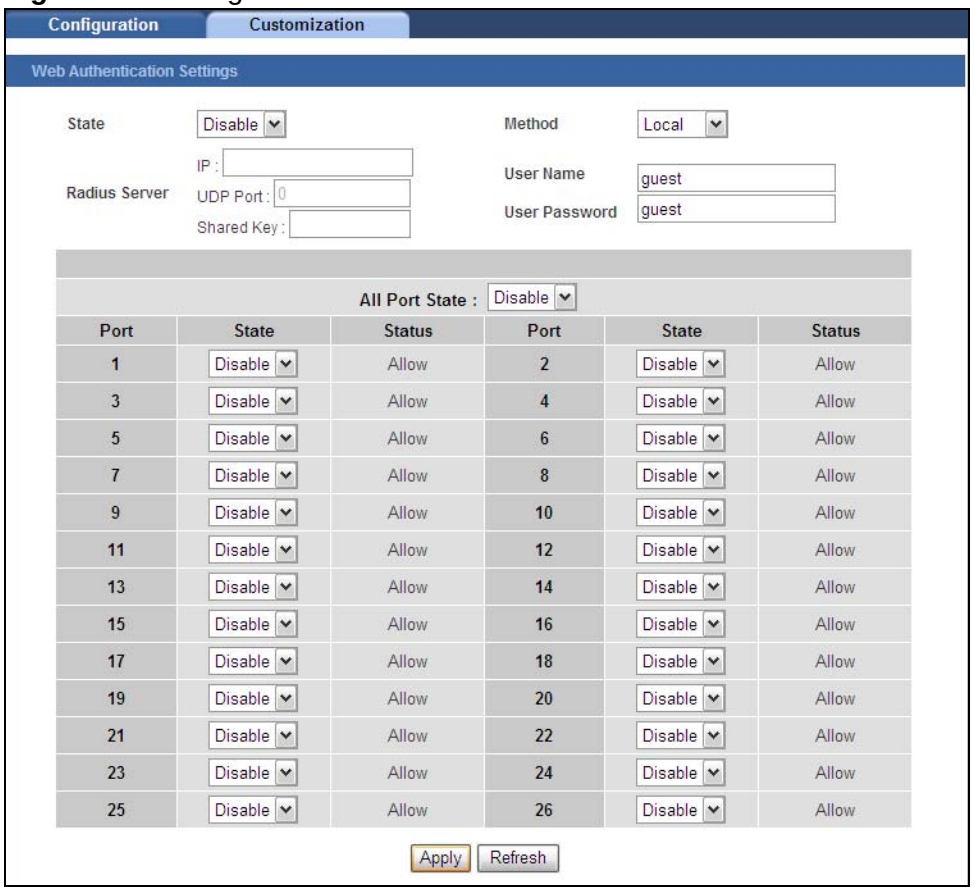
20.4 Configuration

Use the Configuration screen to enable or disable the **Web Authentication** feature. You can also use this screen to configure the authentication method.

Note: Another version of this screen can be accessed in Smart Mode. See Section 4.3.1.3 on page 38 for more details.

Click **Security > Web Authentication > Configuration** to open the following screen.

Figure 66 Configuration



The following table describes the labels in this screen.

Table 38 Configuration

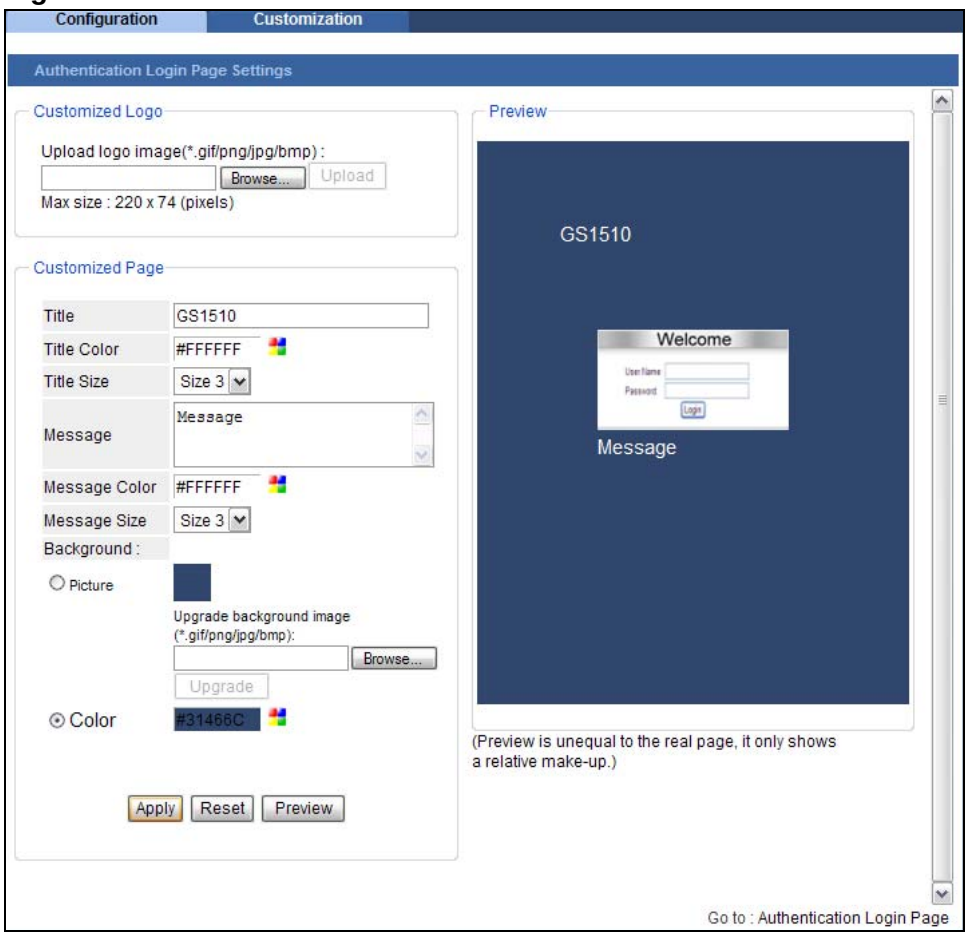
LABEL	DESCRIPTION
State	Select **Enable** to use the web authentication feature.
Method	Select whether to use **Local** or **RADIUS** as the authentication method. The **Local** method of authentication uses the user and guest user groups of the user account database on the Switch to authenticate. However, only a certain number of accounts can exist at one time. **RADIUS** is a security protocol used to authenticate users by means of an external server instead of an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS allows you to validate an unlimited number of users from a central location.
Radius Server	When **RADIUS** is selected as the authentication method, this **Radius Server** will be used for all web authentication attempts.
IP	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	Enter the UDP port of the RADIUS server. The default port of a RADIUS server for authentication is **1812**.
Shared Key	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.
User Name	Specify a username for the main guest account. This will only be used when the **Local** method of authentication has been selected.
User Password	Specify a password for the main guest account. This will only be used when the **Local** method of authentication has been selected.
All Port State	Use this to **Enable** or **Disable** web authentication globally across all ports.
Port	This field displays the port number.
State	Use this to **Enable** or **Disable** web authentication on a specific port.
Status	This field displays the current web authentication status of a specific port.
Apply	Click this to save any changes.
Refresh	Click this to reload the screen and reset any changes that were just made.

20.5 Customization

Use this screen to customize the appearance of the web login page that users will see before accessing the Internet.

Click **Security > Web Authentication > Customization** to open the following screen.

Figure 67 Customization



The following table describes the labels in this screen.

Table 39 Customization

LABEL	DESCRIPTION
Upload Logo File	Enter or browse to the location of a suitable image file (GIF/PNG/JPG/BMP) of no greater size than 220 x 74 pixels and click **Upload**. This will appear as the logo.
Title	Enter a text title to display on the login page.
Title Color	Enter the HTML code for the color of the **Title** or pick one from the swatch palette icon.
Title Size	Select the size of the title from the drop-down box.
Message	Enter a message to display on the login page.
Message Color	Enter the HTML code for the color of the **Message** or pick one from the swatch palette icon.
Message Size	Select the size of the message from the drop-down box.
Picture	Enter or browse to the location of a suitable image file (GIF/PNG/JPG/BMP) and click **Upload**. This will appear as the background.

Table 39 Customization (continued)

LABEL	DESCRIPTION
Color	Enter the HTML code for the color of the **Background** or pick one from the swatch palette icon.
Apply	Click this to save any changes.
Reset	Click this to reset any changes that were made.
Preview	Click this to update the demonstration of the login page.

21 Maintenance

21.1 Overview

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

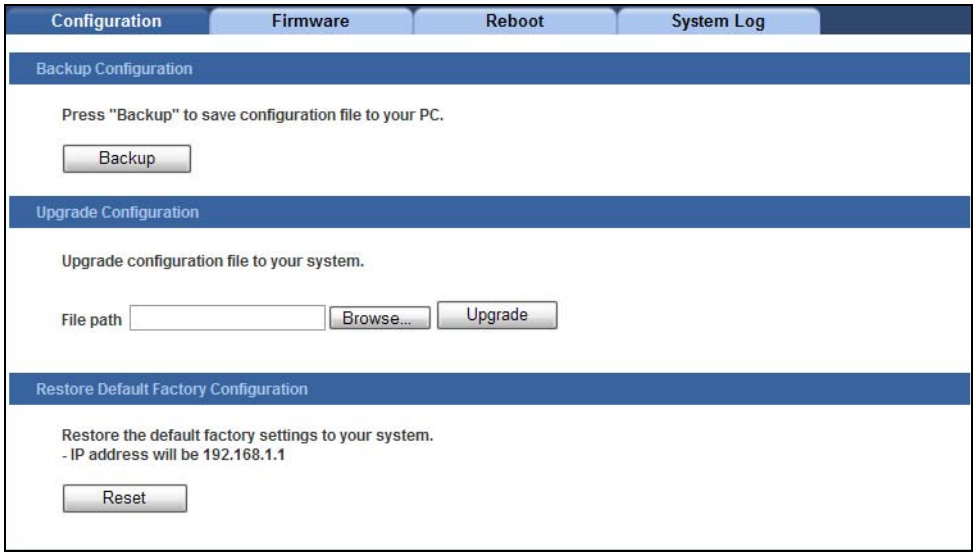
21.2 What You Can Do

- Use the **Configuration** screen (Section 21.3 on page 130) to manage the configuration settings.
- Use the **Firmware screen** (Section 21.4 on page 132) to upgrade the firmware of the Switch.
- Use the **Reboot screen** (Section 21.5 on page 132) to reboot the Switch without resetting any settings.
- Use the **System Log** screen (Section 21.6 on page 133) to look at the log entries generated by the Switch.

21.3 Configuration

Use this screen to manage configuration files. Click **Management** > **Maintenance > Configuration** to open the following screen.

Figure 68 Configuration



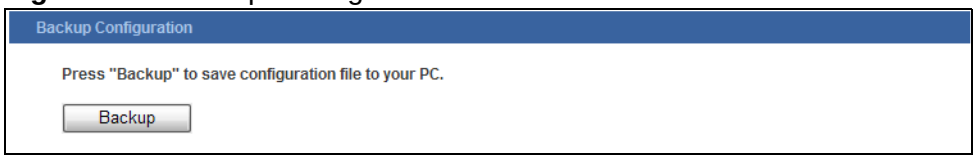
21.3.1 Backup Settings

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

Follow the steps below to back up the current Switch configuration.

1 Click **Backup**.

Figure 69 Backup Settings



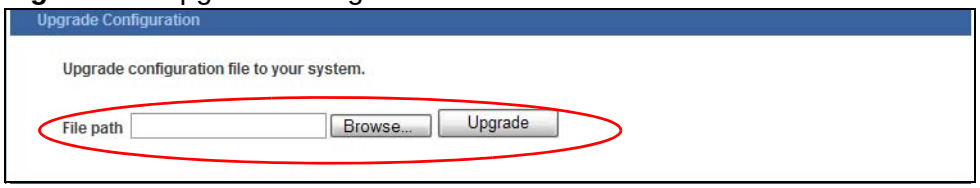
2 Click **Save** to display the **Save As** screen.

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

21.3.2 Upgrade Configuration

Restore a previously saved configuration from your computer to the Switch.

Figure 70 Upgrade Configuration



Type the path and file name of the configuration file you wish to restore in the **File path** text box or click **Browse** to display the **Choose file** screen from which you can locate it. After you have specified the file, click **Upgrade**.

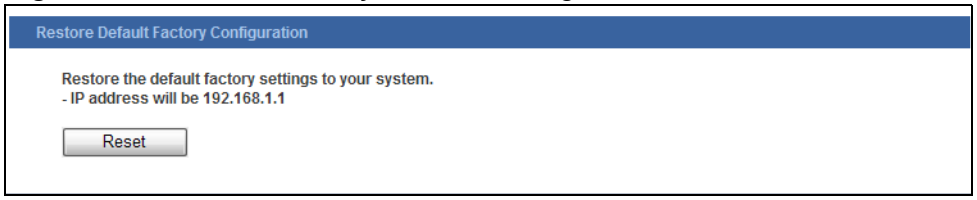
Make sure you are using the proper configuration when you are restoring your configuration. The file name extension should be ".rom" or ".cfg".The following table describes the labels in this screen.

21.3.3 Restore Factory Default Settings

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

1 In the **Configuration** screen, click the **Reset** button to clear all Switch configuration information you configured and return to the factory defaults.

Figure 71 Restore Factory Default Settings



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

Figure 72 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).

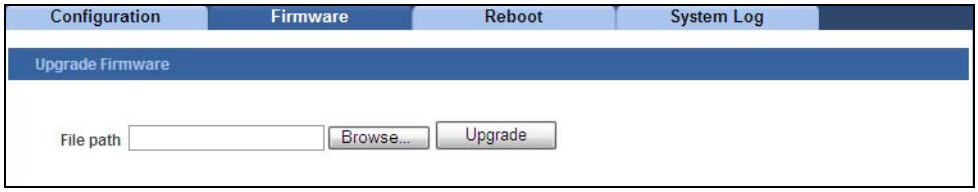
21.4 Firmware

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.

Click **Management > Maintenance > Firmware** to display the screen as shown next.

Figure 73 Firmware



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. Click **Upgrade** to load the new firmware.

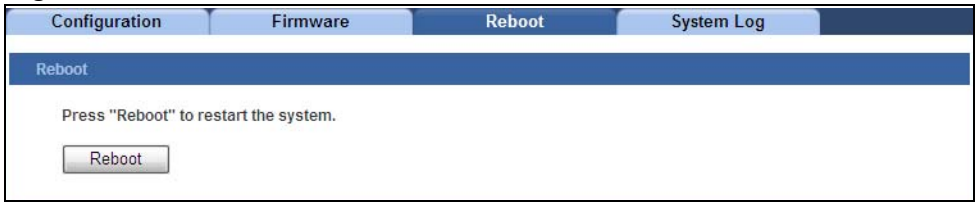
After the firmware upgrade process is complete, see the **System Status > System Information** screen to verify your current firmware version number.

21.5 Reboot

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

Click **Management > Maintenance > Reboot** screen as shown next.

Figure 74 Reboot



1 In the **Reboot** screen, click the **Reboot** button. The following screen displays.

Figure 75 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.

21.6 System Log

Use this screen to view the system logs and to configure an external syslog server.

21.6.1 Syslog

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

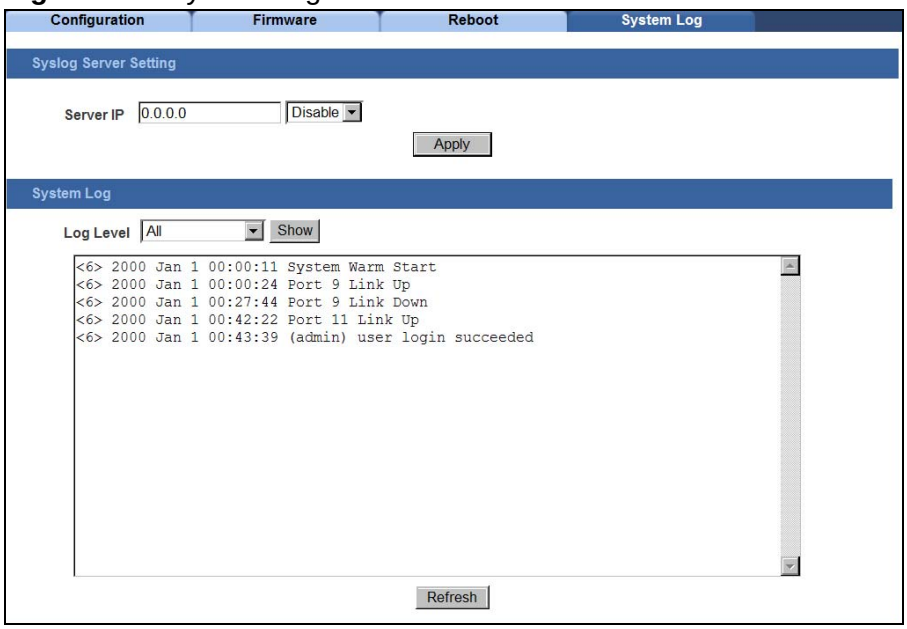
Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details.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

Table 40 Syslog Severity Levels

CODE	SEVERITY
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.

Click **Management > Maintenance > System Log** to display the screen as shown next. Click **Refresh** to update the log and see any available new entires.

Figure 76 System Log



The following table describes the labels in this screen.

Table 41 System Log

LABEL	DESCRIPTION
Server IP	Enter the IP address of an external syslog server in dotted decimal notation. Select **Enable** to use the external syslog server or **Disable** to not use it.
Apply	Click this to save any changes.
Log Level	Select the severity level of the logs to be displayed. For more information, refer to the **Syslog Severity Level** table above. Select **All** to display all levels.
Show	Click this to update the system log with log events of the selected severity level.
Refresh	Click this to update the log and see any available new entires.

22 SNMP

22.1 Overview

This chapter describes how to configure the SNMP options of the Switch.

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices.

22.2 What You Can Do

- Use the **SNMP Settings** screen (Section 22.4 on page 137) to configure the basic SNMP settings for the Switch.
- Use the **Community Name** screen (Section 22.5 on page 138) to create SNMP communities.
- Use the **Trap Receiver** screen (Section 22.6 on page 140) to configure the sending of SNMP traps to remote SNMP management stations.

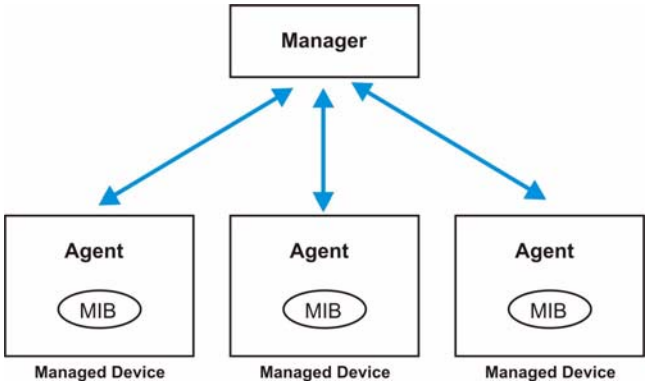
22.3 What You Need to Know

22.3.1 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) or SNMP version 2c. The

next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 77 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 network device (the Switch). An agent translates the local management information from the managed device 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 the device. 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 42 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.

22.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- RFC 1157 SNMP
- RFC 1213 SNMP MIB II
  - MIB II - System
  - MIB II - Interface
- RFC 1643 Ethernet MIB
- RFC 1493 - Bridge MIB
- RFC 1757 RMON
  - Group 1 (Statistics)
  - Group 2 (History)
  - Group 3 (Alarm)
  - Group 9 (Event)

22.3.3 SNMP Traps

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

Table 43 SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
SNMPv1/SNMPv2 Trap/Inform Requests:		
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.
RFC2819 Traps (alarmEntry)	1.3.6.1.2.1.16.3.1.1	A RMON event has been triggered.

22.4 SNMP Settings

Use this screen to configure the basic SNMP settings.

Click **Management > SNMP > SNMP Settings** to open the screen as shown.

Figure 78 SNMP Settings

The following table describes the labels in this screen.

Table 44 SNMP Settings

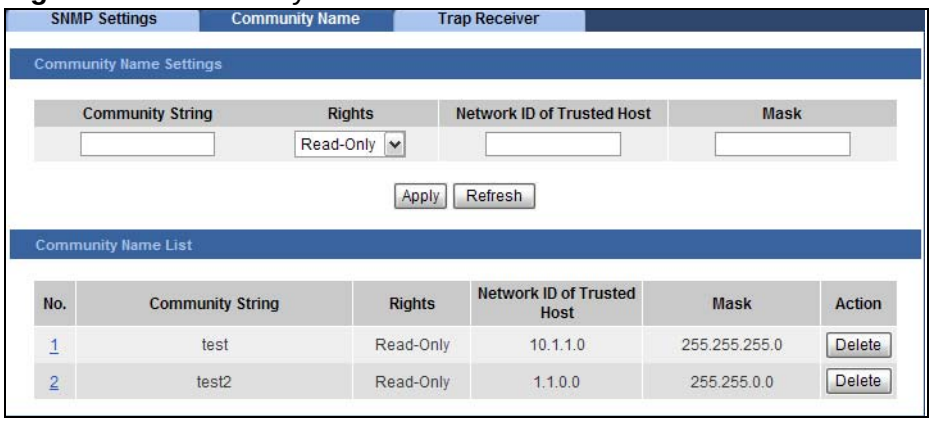
LABEL	DESCRIPTION
SNMP State	Select **Enable** to activate SNMP on the Switch. Select **Disable** to not use SNMP on the Switch.
System Name	Type a System Name for the Switch.
System Location	Type a System Location for the Switch.
System Contact	Type a System Contact for the Switch.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reset the fields to the last saved setting.

22.5 Community Name

Use the **Community Name** screen to create SNMP communities and associate rights to them. Click **Management > SNMP > Community Name** to view the screen as shown.

SNMP communities act like passwords and are used to define the security parameters of SNMP clients in an SNMP v1 and SNMP v2c environments. The default SNMP community is “public” for both SNMP v1 and SNMP v2c.

Figure 79 Community Name



The following table describes the labels in this screen.

Table 45 Community Name

LABEL	DESCRIPTION
Community Name Settings	
Community String	Enter a Community string, this will act as a password for requests from the management station. An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
Rights	Select Read-Only to allow the SNMP manager using this string to collect information from the Switch. Select Read-Write to allow the SNMP manager using this string to create or edit MIBs (configure settings on the Switch).
Network ID of Trusted Host	Type the IP address of the remote SNMP management station in dotted decimal notation, for example 192.168.1.1.
Mask	Type the subnet mask for the IP address of the remote SNMP management station in dotted decimal notation, for example 255.255.255.0.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reset the contents of the text boxes.
Community Name List	
No.	This field indicates the community number. It is used for identification only. Click on the individual community number to edit the community settings.
Community String	This field displays the SNMP community string. An SNMP community string is a text string that acts as a password.

Table 45 Community Name (continued)

LABEL	DESCRIPTION
Rights	This field displays the community string's rights. This will be **Read Only** or **Read Write**.
Network ID of Trusted Host	This field displays the IP address of the remote SNMP management station after it has been modified by the subnet mask.
Subnet Mask	This field displays the subnet mask for the IP address of the remote SNMP management station.
Action	Click **Delete** to remove a specific Community String.

22.6 Trap Receiver

Use the **Trap Receiver** screen to enable the sending of SNMP traps to a remote SNMP management station(s). Click **Management** > **SNMP > Trap Receiver** to view the screen as shown.

SNMP traps are used to send out SNMP notifications of urgent or normal events in the system to external management stations.

Figure 80 Trap Receiver

The following table describes the labels in this screen.

Table 46 Trap Receiver

LABEL	DESCRIPTION
IP Address	Enter the IP address of the remote trap station in dotted decimal notation.
Version	Select the version of the Simple Network Management Protocol to use. **v1** or **v2c**.
Community String	Specify the community string used with this remote trap station.
Apply	Click this to save any changes to the Switch.
Refresh	Click this to reset the contents of the text boxes.
Trap Receiver List	

Table 46 Trap Receiver (continued)

LABEL	DESCRIPTION
No.	This field displays the index number of the trap receiver entry. Click the number to modify the entry.
IP Address	This field displays the IP address of the remote trap station.
Version	This field displays the version of Simple Network Management Protocol in use. **v1** or **v2c**.
Community String	This field displays the community string used with this remote trap station.
Action	Click **Delete** to remove a configured trap receiver station.

23

User Account

23.1 Overview

This chapter describes the User Account screen.

There are three types of user accounts on the Switch. **Admin**, **User** and **Guest**.

- The **Admin** account is used for administrating the Switch using the web configurator.
- The **User** and **Guest** accounts are used for IEEE 802.1x Authentication (Chapter 19 on page 117) and Web Authentication (Chapter 20 on page 123).

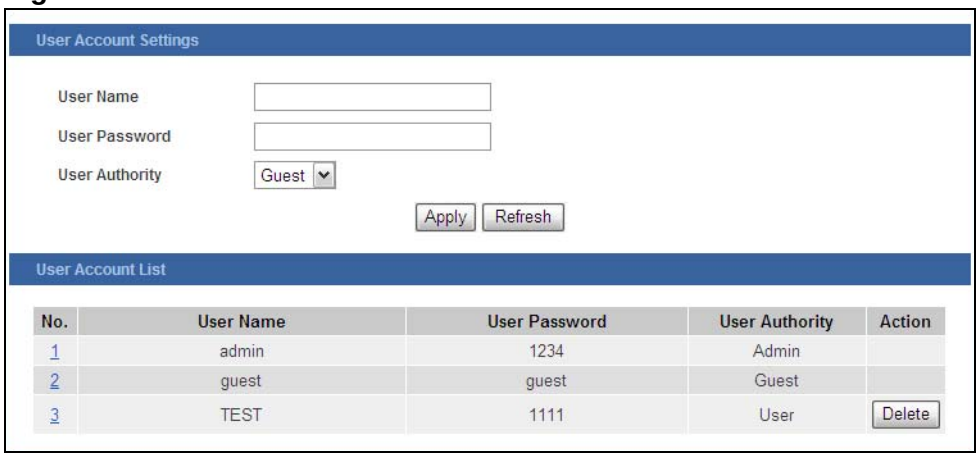
23.2 User Account Screen

Use this screen to configure the admin, user and guest accounts on the Switch. To access the screen, click **Management > User Account**.

To create a new account, type a username, password and set a user authority for the account and then click **Apply**. To modify an existing account, click the index number for that account and click **Apply** after modifying any details.

Note: You cannot delete the default **Admin** and **Guest** accounts. However, you can modify the **Guest** username and password.

Figure 81 User Account



The following table describes the labels in this screen.

Table 47 User Account

LABEL	DESCRIPTION
User Name	Type a new username or modify an existing one.
User Password	Type a new password or modify an existing one. Enter up to 15 alpha-numeric characters; spaces are allowed.
User Authority	Select with which group the user associates.
Apply	Click **Apply** to save the changes back to the Switch.
Refresh	Click **Refresh** to begin configuring this screen afresh.
No.	This field displays the index number of an entry.
User Name	This field displays the name of a user account.
User Password	This field displays the password.
User Authority	This field displays the associated group.
Action	Click the **Delete** button to remove the user account. Note: You cannot delete the default admin and guest accounts.

PART V
Troubleshooting & Product Specifications

24

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Switch Access and Login

24.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the Switch.
2. Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the Switch.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 3.2 on page 30.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power cord to the Switch.

5 If the problem continues, contact the vendor.

24.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default IP address is **192.168.1.1**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 3.3 on page 31.

I forgot the username and/or password.

1 The default username is **admin** and the default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 3.3 on page 31.

I cannot see or access the **Login** screen in the Web Configurator.

1 Make sure you are using the correct IP address.

- The default IP address is **192.168.1.1**.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See your Quick Start Guide and Section 3.2 on page 30.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 3.3 on page 31.

6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

I can see the **Login** screen, but I cannot log in to the Switch.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.

3 Disconnect and re-connect the cord to the Switch.

4 If this does not work, you have to reset the device to its factory defaults. See Section 3.3 on page 31.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the Web Configurator you need to allow:

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

25

Product Specifications

This chapter gives details about your Switch's hardware and firmware features.

25.1 General Switch Specifications

The following tables list the product specifications.

Table 48 Physical and Environmental Specifications

LEDs	Per Switch: PWR, SYS Per Gigabit port: LNK/ACT, FDX Per mini-GBIC port: LNK/ACT
Dimensions	Standard 19" rack mountable GS1510-16/GS1510-24: 440 (W) x 170 (D) x 44 mm (H)
Device Weight	GS1510-16: 2.3 Kg GS1510-24: 2.4 Kg
Temperature	Operating: 0º C ~ 50º C (32º F ~ 122º F) Storage: -40º C ~ 70º C (-40º F ~ 158º F)
Humidity	10 ~ 95% (non-condensing)
Power Supply	GS1510-16: AC: 100 - 240V 50/60Hz 0.3A max internal universal power supply GS1510-24: AC: 100 - 240V 50/60Hz 0.4A max internal universal power supply
Power Consumption	GS1510-16: 18W (maximum) GS1510-24: 21W (maximum)
Safety	UL 60950-1 CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

Table 49 General Product Specifications

Interface		GS1510-16: 16 1000BASE-T RJ-45 Gigabit Ethernet ports GS1510-24: 24 1000BASE-T RJ-45 Gigabit Ethernet ports For GS1510-24, 2 Mini-GBIC (Small Form-Factor Pluggable (SFP)) slot. Auto-negotiation Auto-MDIX Compliant with IEEE 802.3ad/u/x Back pressure flow control for half duplex Flow control for full duplex (IEEE 802.3x)
Layer 2 Features	Bridging	16K MAC addresses Static MAC address forwarding by destination Broadcast storm control Static MAC address forwarding
	Switching	Switching fabric: GS1510-16: 32Gbps, non-blocking GS1510-24: 52Gbps, non-blocking Max. Frame size: 1522 bytes
	QoS	IEEE 802.1p 8 priority queues per port Port-based egress traffic shaping DSCP to IEEE 802.1p mapping
Layer 2 Features	VLAN	Port-based VLAN setting Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 4K, 256 static maximum Guest VLAN
	Port Aggregation	Supports static port trunking Eight groups (up to 8 ports each)
	Port mirroring	All ports support port mirroring
Security		802.1x port authentication (MD5, PEAP) IP Source Guard Web authentication (MD5, PEAP) MAC filtering (dynamic)

Table 50 Management Specifications

System Control	LED indication for power status Performance monitoring Line speed Four RMON groups (history, statistics, alarms, and events) Port mirroring and aggregation Firmware upgrade and download through HTTP Reset to default button
Network Management	Web-based management SNMP v1, v2c RMON groups (history, statistics, alarms and events) 1 Logging server supported
MIB	RFC 1157 - SNMP RFC 1213 MIB II RFC 1643 Ethernet MIB RFC 1493 - Bridge MIB RFC 1757 RMON Group 1, 2, 3, 9 (history, statistics, alarms and events)

This section describes the general software features of the Switch.

Table 51 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Administrator User Name	admin
Default Password	1234
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 Management	Forward traffic based on the destination MAC address and VLAN group (ID).
QoS	Queuing is used to help solve performance degradation when there is network congestion. Two scheduling services are supported: Strict Priority (SP) 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 51 Firmware Features

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.
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.
STP (Spanning Tree Protocol)	STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.
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 DHCP and ARP packets in your network.
Authentication	The Switch supports authentication services via RADIUS servers.
Device Management	Use the Web Configurator to easily configure the rich range of features on the Switch.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the Web Configurator to put it on the Switch. Note: Only upload firmware for your specific model!
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.
Logging	The Switch allows you to specify what information should be logged and where it should be stored. It supports internal logging as well as external logging via a syslog server.

The following lists, which are not exhaustive, illustrate the standards supported in the Switch.

Table 52 Standards Supported (IEEE)

STANDARD	DESCRIPTION
IEEE 802.3	Packet Format
IEEE 802.3u	100Base-TX Ethernet
IEEE 802.3ab	Link Layer Discovery Protocol (LLDP)
IEEE 802.3z	1000Base-SX/LX/LHX
IEEE 802.3	Packet Format
IEEE 802.3x	Flow Control
IEEE 802.1D	MAC Bridges
IEEE 802.1w	Rapid Spanning Tree protocol

Table 52 Standards Supported (continued)(IEEE)

STANDARD	DESCRIPTION
IEEE 802.1p	Class of Service, Priority protocols
IEEE 802.1Q	Tagged VLAN
IEEE 802.1X	Port Authentication
IEEE 802.3ad	LACP Aggregation

Table 53 Standards Supported (RFC)

STANDARD	DESCRIPTION
RFC 826	Address Resolution Protocol (ARP)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1213	SNMP MIB II
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1493	Bridge MIBs
RFC 1643	Ethernet MIBs
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 2236	Internet Group Management Protocol, Version 2.
RFC 2865	RADIUS - Vendor Specific Attribute
RFC 3164	Syslog
RFC 3376	Internet Group Management Protocol, Version 3
RFC 3580	RADIUS - Tunnel Protocol Attribute

PART VI
Appendices and Index

A

Device Auto Discovery

This appendix introduces the ZyXEL device discovery utility.

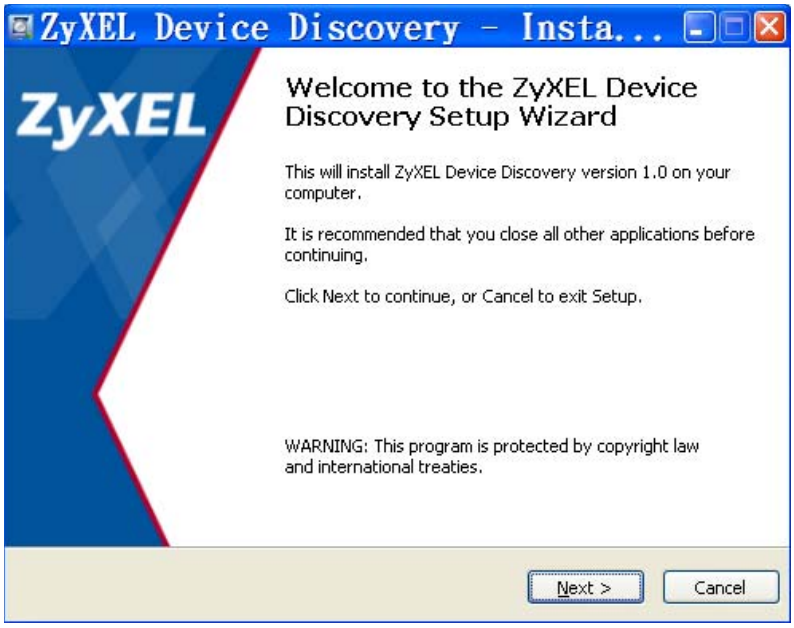
This utility helps the network administrator find the IP address of a device on the network by performing a scan. This function is useful if the default IP address has been changed and the device can not be located on the network, this utility is even more useful if the Switch does not have a console port.

The program ZyXEL_device_discovery.exe can be found on the CD that accompanies the Switch. The software is compatible with Windows XP, Vista and 7.

Installing the Software

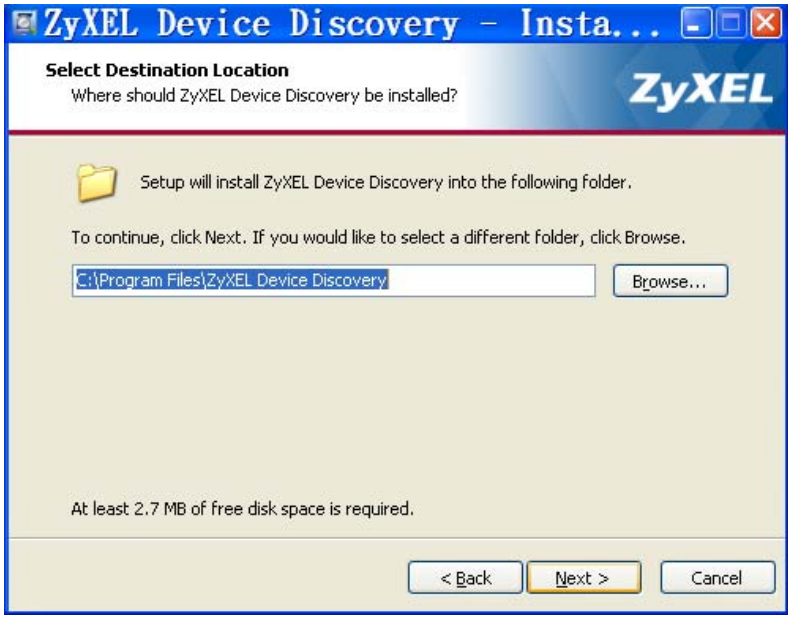
1 Double-click the file **zyxel_device_discovery_setup.exe** located on the CD that came with the Switch.

2 The following screen will display, click **Next.**

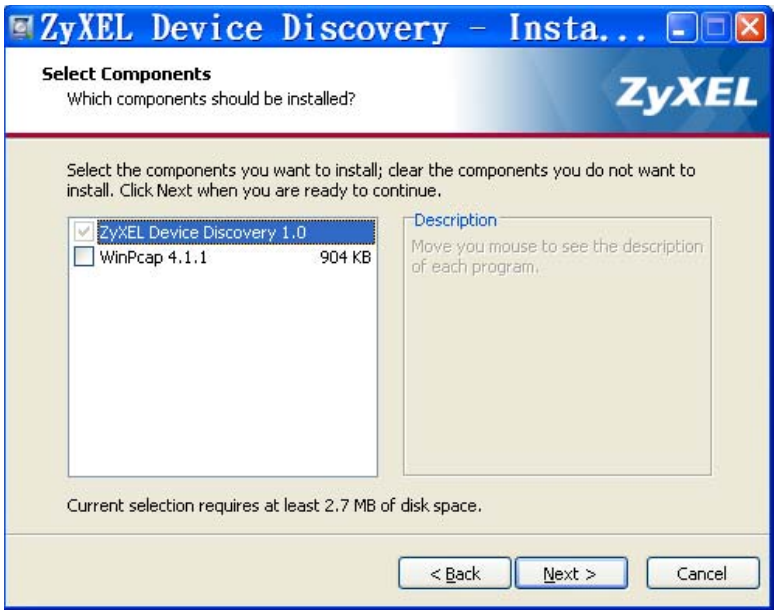


3 After reading the license agreement, select **I accept the agreement** and click **Next**.

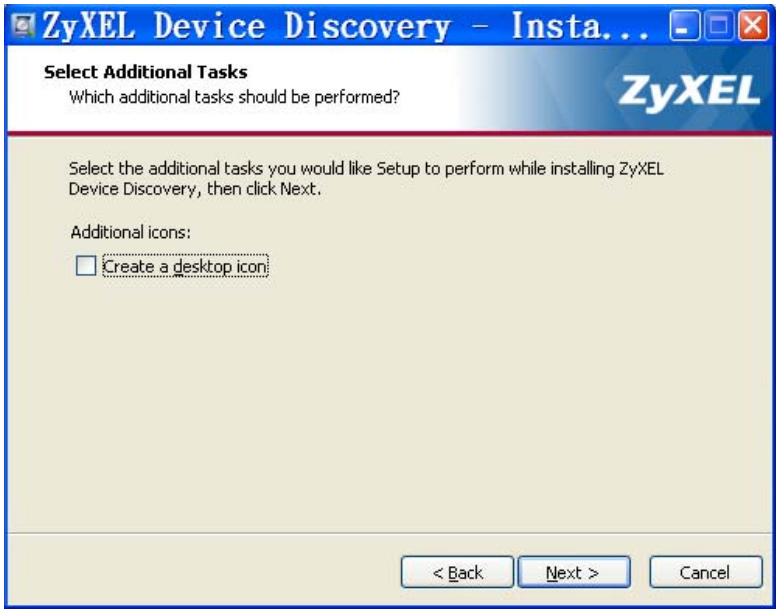
4 Choose the location in which to install the program files to. The default location is C:\Program Files\ZyXEL Device Discovery. Click **Next** to continue the installation.



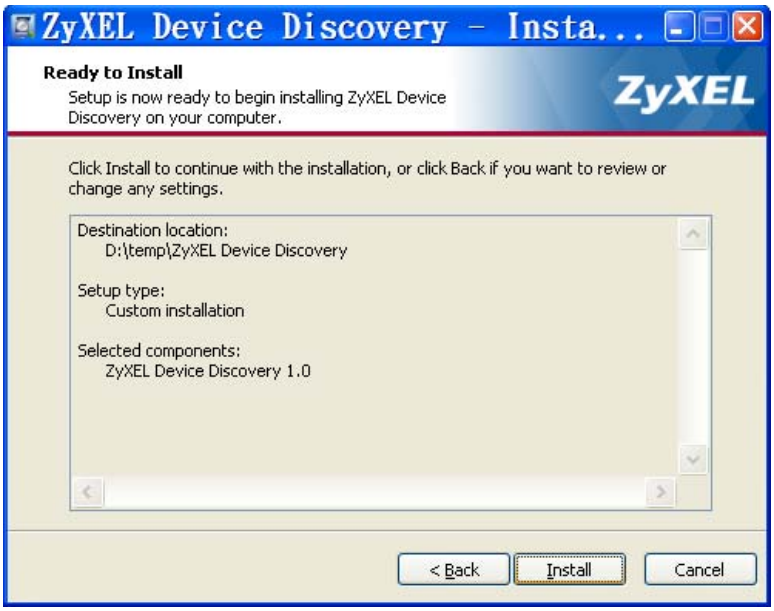
5 Select the components to install, **ZyXEL Device Discovery 1.0** is mandatory. **WinPCap 4.1.1** is optional. Click **Next** to continue the installation.



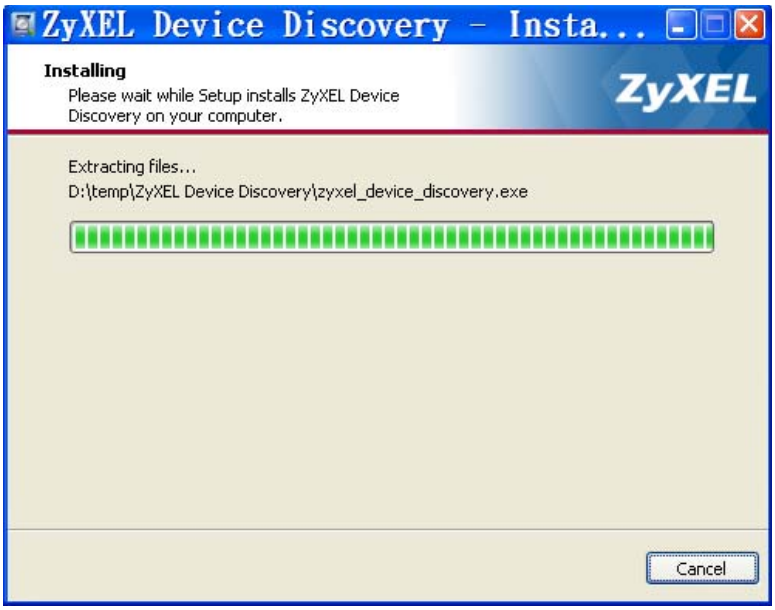
6 Select if you want to create an icon for the program on your desktop and click **Next** to continue the installation.



7 Confirm the installation settings you have just configured and click **Install** to start the installation. To change an installation setting, click **Back**.



8 A progress bar will display as the software is being installed.

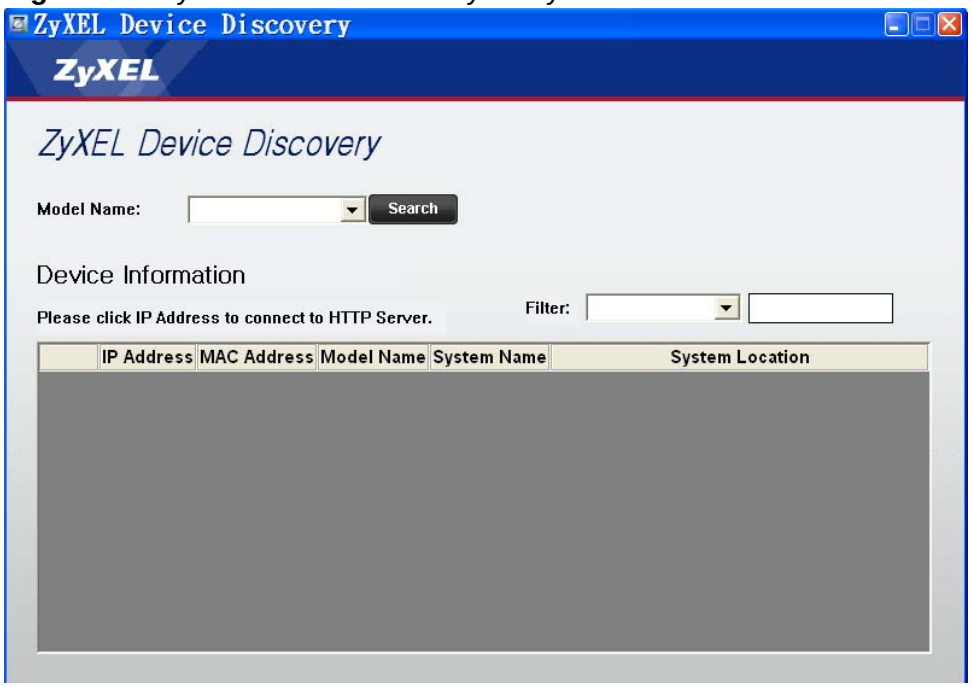


9 After the installation has finished, select whether to launch the utility now or later and click **Finish** to complete the setup process.

Using the Software

After launching the utility, the following screen will display. To begin scanning for devices on the network you are currently connected to, click the **Search** button. You can also configure a more specific search by selecting to search only for devices with a specific model name. To do this, use the **Model Name** drop-down box. If no model name is entered, all devices will be scanned.

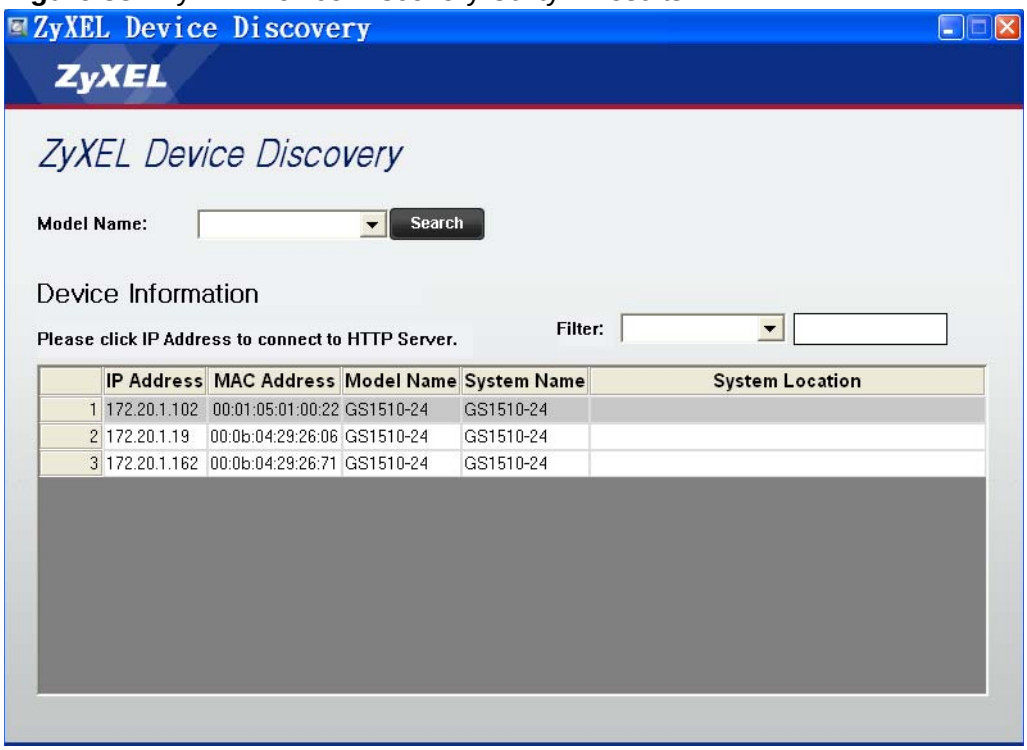
Figure 82 ZyXEL Device Discovery Utility



After performing a search on the network, some results will display in the table. When you have located the device you are looking for, double-click anywhere within the row to launch the device's web configurator in your browser.

If there are too many devices on the network, you can use the **Filter** drop-down box to narrow down the results. With this function you can filter the results by Model Name, MAC Address and IP Address.

Figure 83 ZyXEL Device Discovery Utility - Results



B

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.

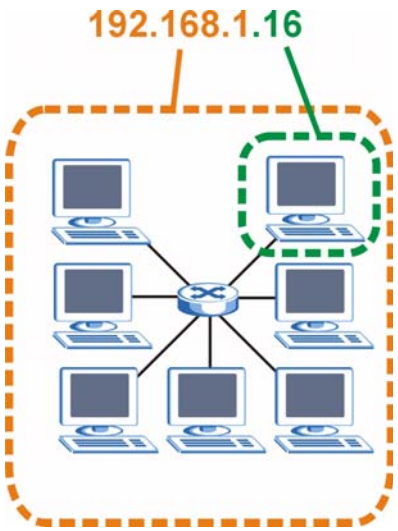
Structure

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 84 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 54 Subnet Mask 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

Table 54 Subnet Mask Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
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 55 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 56 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 57 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

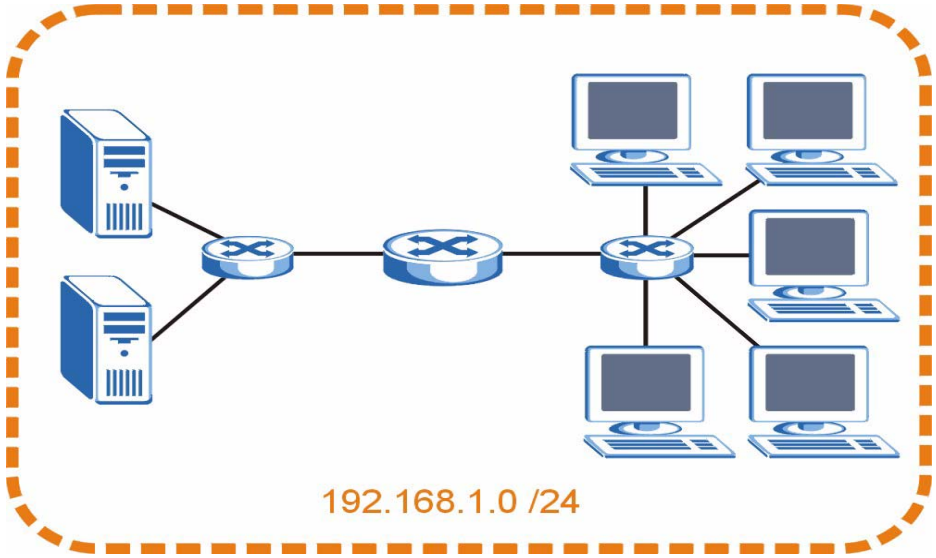
Subnetting

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 85 Subnetting Example: Before Subnetting

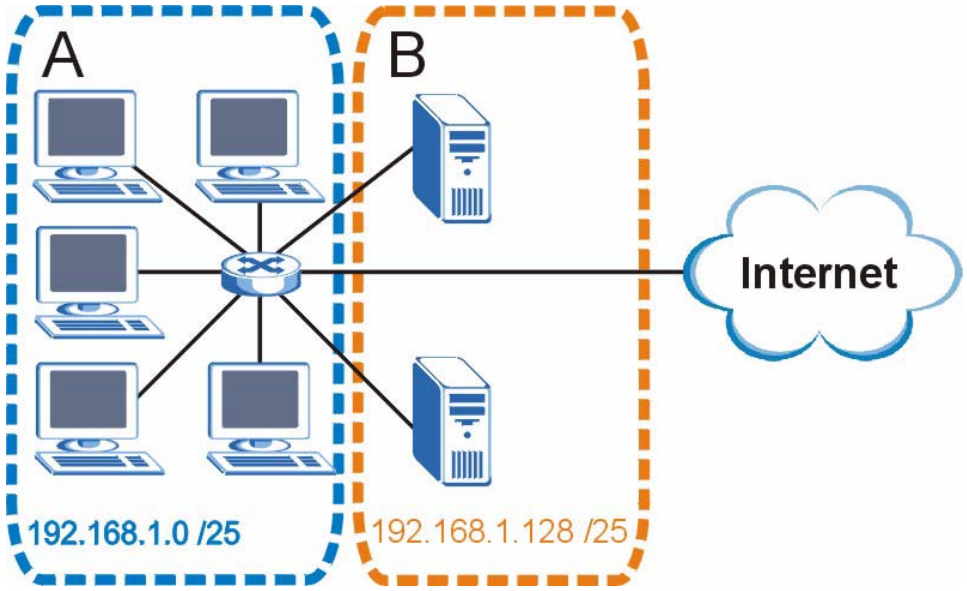


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

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 86 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 58 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 59 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 60 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 61 Subnet 4

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

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

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

Table 62 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 63 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 64 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

Table 64 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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

Federal Communications Commission (FCC) Interference Statement

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

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

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

CE Mark Warning:

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

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

警告使用者
這是甲類的資訊產品, 在居住的環境使用時,
可能造成射頻干擾, 在這種情況下,
使用者會被要求採取某些適當的對策.

Notices

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

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

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

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

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

Note

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

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

Registration

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

Index

G

H

I

L

M

N

P

Q

R

S

T

U

V

W