Smart Switch Software User Manual GS748T

NETGEAR®

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10331-01
October 2007

Trademarks

October 2007

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Certificate of the Manufacturer/Importer

It is hereby certified that the GS748T Smart Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasGS748T Smart Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Product and Publication Details

Model Number:	GS748T
Publication Date:	October 2007
Product Family:	Smart Switch Series
Product Name:	GS748T Smart Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10331-01
Publication Version Number:	1.0

Contents

About This Manual

The *NETGEAR® Smart Switch Software User Manual GS748T* describes how to install, configure, operate, and troubleshoot the GS748T Smart Switch using its included software. This book describes the software configuration procedures and explains the options available within those procedures.

Who Should Use this Book

The information in this manual is intended for readers with intermediate to advanced system management skills.

This document was created primarily for the system administrator who wishes to install and configure the GS748T switch in a network. It assumes that the reader has a general understanding of switch platforms and a basic knowledge of Ethernet and networking concepts. To install this switch, it is not necessary to understand and use all of its capabilities. Once basic configuration is performed, it will function in a network using its remaining factory default parameters. However, a greater level of configuration—anywhere from the basic up to the maximum possible—will give your network more advantage of its features. The web interface simplifies this configuration at all levels.

How to Use This Book

This document describes configuration commands for the GS748T switch software. The commands can all be accessed from the Web interface.

- Chapter 1, “Switch Management Overview” describes what you can expect from Web management and gives host system requirements.
- Chapter 2, “Using the Smartwizard Discovery Utility” describes how to use the Smartwizard Discovery utility to set up your switch so that you can communicate with it.
- Chapter 4, “Configuring the Switch” describes the features that your switch offers and tells you how to configure and activate them in your network.
- Appendix A, “Specifications and Default Values” gives GS748T switch specifications and lists default feature values.
- Appendix B, “Virtual Local Area Networks (VLANs)” describes some concepts of VLANs

- Appendix C, “Network Cabling” gives cabling requirements and describes some details of port cabling connections.

Note: Refer to the product release notes for the GS748T switch Software application level code. The release notes detail the platform specific functionality of the Switching, SNMP, Config, and Management packages.

Note: Although this document applies to the *NETGEAR*® GS748T Smart Switch, some of the illustrations used may show references to other switch model numbers. Where such model numbers appear, the illustration concerned should be treated as an example. The procedures described with these illustrations apply to each of the family of Smart Switches.

Conventions, Formats and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions.** This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input
`Fixed width`	Screen text, file and server names, extensions, commands, IP addresses

- **Formats.** This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: This is a warning of possible malfunction or damage to the equipment.

Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope.** This manual is written for the GS748T switch according to these specifications:

Product Version	GS748T Smart Switch
Manual Publication Date	October 2007

For more information about network, Internet, firewall, and VPN technologies, use the link to the NETGEAR shown below.

Note: Product updates are available from the NETGEAR, Inc. website at: *http://www.netgear.com/support/GS748T.asp*

HTML Manual Navigation

If an HTML version of this manual is provided, it includes the following:

- Buttons,  and  , for browsing forwards or backwards through the manual one page at a time
- A  button that displays the table of contents and an  button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual, you can choose one of the following options, according to your needs.

- **Printing a Page from HTML**. Each page in the HTML version of the manual is dedicated to a major topic. Select File → Print from the browser menu to print the page contents.
- **Printing from PDF**. Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.
  - **Printing a PDF Chapter.** Use the *PDF of This Chapter* link at the top left of any page.
    - Click the *PDF of This Chapter* link at the top left of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
    - Click the print icon in the upper left of your browser window.
  - **Printing a PDF version of the Complete Manual**. Use the *Complete PDF Manual* link at the top left of any page.
    - Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
    - Click the print icon in the upper left of your browser window.

Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Revision History

Document Part Number	Date	Version Number	Description
202-10233-02	February 2007	1.0	Document created
202-10331-01	October 2007	1.0	GUI update

Chapter 1
Switch Management Overview

Switch Management Interface

This section gives an overview of switch management, including the methods you can use to manage your NETGEAR GS748T Smart Switch.

Your NETGEAR GS748T Smart Switch contains an embedded web server and management software for managing and monitoring switch functions. This switch will function as a simple switch without using the management software but its use enables you to configure more advanced features and consequently improve switch efficiency and the overall performance of your network.

Web-Based Management enables you to monitor, configure, and control your switch remotely using a common web browser, instead of having to use expensive and complicated SNMP software products. Simply by using your web browser, you can monitor the performance of your switch, and optimize its configuration for your network. Using your browser, for example, you can set up VLANs, traffic priority, and configure port trunking.

In addition, NETGEAR provides the Smartwizard Discovery Utility program with this product. This program runs under Microsoft Windows XP or Windows 2000 and provides a “front end” which discovers the switches on your network segment. When you power up your switch for the first time, Smartwizard Discovery enables you to configure its basic network parameters without prior knowledge of IP address or subnet mask. Following such configuration, this program leads you into the Web Management interface.

Table 1-1 shows some features of Smartwizard Discovery and Web Management.

Table 1-1. Switch Management Methods

Management Method	Features
Smartwizard Discovery Utility program	No IP address or subnet mask setup needed Discover all switches on the network User-friendly interface under Microsoft Windows Firmware upgrade capability Password change feature Provides entry to web configuration of switch
Web browser	Password protection Ideal for configuring the switch remotely Compatible with Internet Explorer and Netscape Navigator on any platform Extensive switch configuration possible Configuration backup and restore

For a more detailed discussion of the Smartwizard Discovery Utility Program, see. For a detailed discussion of the Web Browser Interface, see Chapter 3, “Basic Web Management”.

System Requirements

The following hardware and software facilities are required to run the applications described in this manual:

Network facilities:

- Ethernet network with or without DHCP server as appropriate (see Chapter 2, “Using the Smartwizard Discovery Utility”)

For running the Smartwizard Discovery Utility:

- IBM type PC with CD drive; RAM size and disk specification is not critical
- OS software: Microsoft Windows Vista, Windows XP, or Windows 2000
- Ethernet cable: Straight or crossover
- IBM type PC to run web management GUI; RAM and disk requirement is not critical

For running local or remote Web Management

- Desktop computer running Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later, or equivalent.

Chapter 2
Using the Smartwizard Discovery Utility

This section leads you through the steps necessary to begin managing your GS748T Smart Switch. It covers how to install in a network that contains a DHCP server and one without DHCP.

Network with DHCP server

To install the switch in a network with a DHCP server, proceed as follows:

1. Connect the GS748T switch to a DHCP network.
2. Power on the switch by connecting its power cord.
3. Install the Smartwizard Discovery Utility program on your computer.
4. Start the Smartwizard Discovery utility.
5. Click **Discover** for the Smartwizard Discovery to find your GS748T Smart Switch. You should see a screen similar to that shown below.

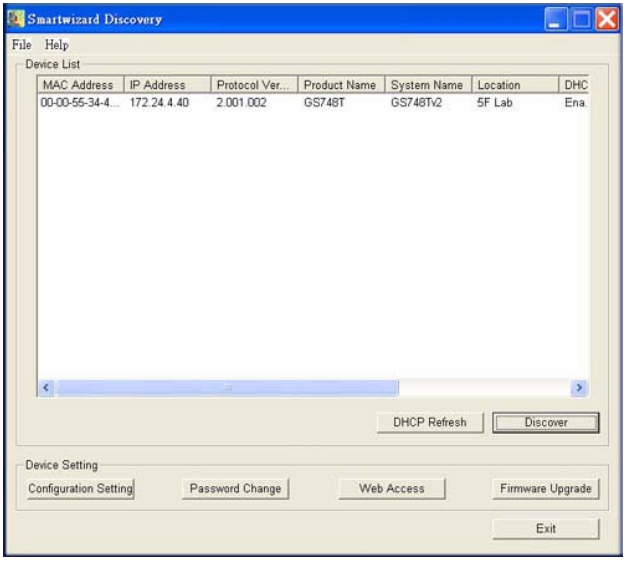

Figure 2-1

6. Make a note of the displayed IP address assigned by the DHCP server. You will need this value to access the switch directly from a web browser (without using Smartwizard Discovery).

7. Select your switch by clicking on the line that displays the switch address. Then click **Web Access**. The discovery utility displays a login window similar to the following:

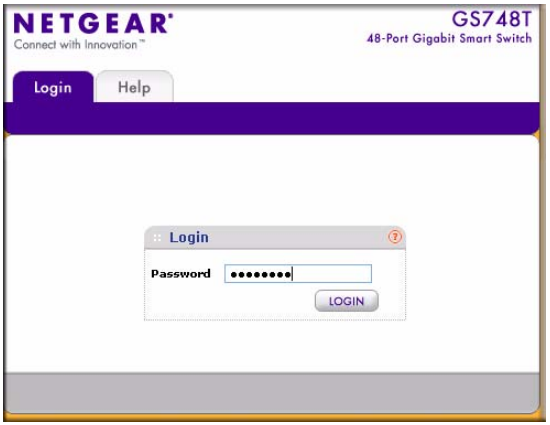

Figure 2-2

8. Enter the default password which is **password.** Then, use your web browser to manage your switch.

Network without DHCP Server

This section describes how to set up your switch in a network without a DHCP server, and is divided into the following tasks:

- Manually assigning network parameters for your switch.
- Configuring the Network Interface Card (NIC) settings on the host PC.
- Logging into the web-based switch management utility.

Manually Assigning Network Parameters

If your network has no DHCP service, you must assign a static IP address to your switch. If you choose, you can assign a static IP address to the switch even if your network has DHCP service.

To manually assign a static IP address to your switch:

1. Connect the GS748T Smart Switch to your existing network.
2. Power on the switch by plugging in the power cord (Default IP is 192.168.0.239).
3. Install the Smartwizard Discovery Utility program on your computer
4. Start the Smartwizard Discovery utility.
5. Click **Discover** for the Smartwizard Discovery Utility to find your GS748T Smart Switch. You should see a screen similar to that shown in Figure 2-1 on page 2-1.
6. Click on **Configuration Setting**. A screen similar to that shown below appears.

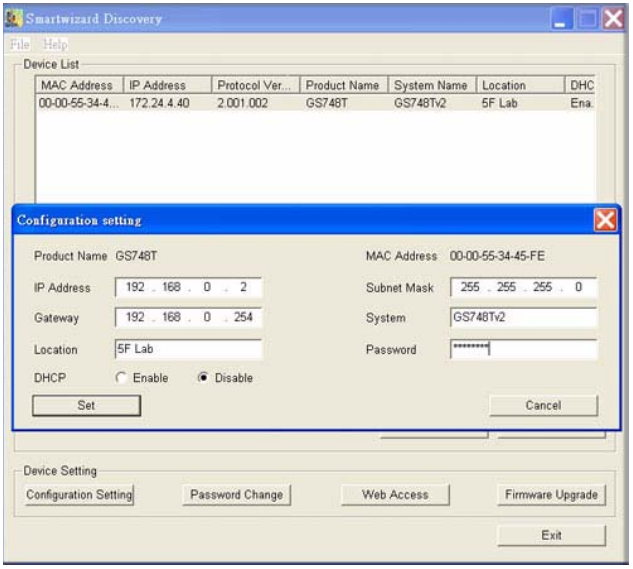

Figure 2-3

7. Choose the **Disable** radio button for DHCP.
8. Enter your chosen switch IP address, gateway IP address and subnet mask, and then type your password and click **Set**. Please ensure that your PC and the GS748T Smart Switch are in the same subnet. Make a note of these settings for later use.

Configuring Your NIC Settings

The settings of your NIC on the host that accesses the GS748T Smart Switch, under MS Windows OS, are made with entries into the Windows screens shown below. For comparison, the settings of the switch are also shown although they do not appear in the Windows view.

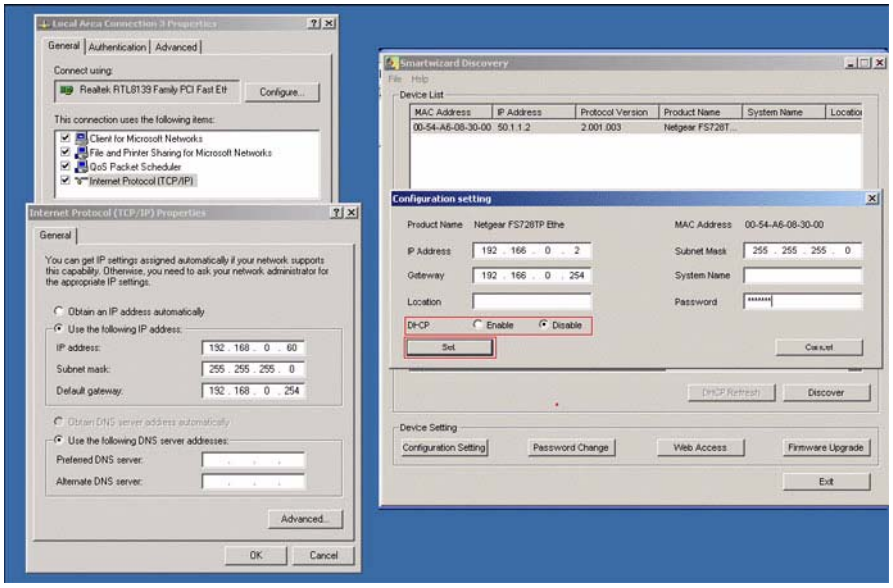

Figure 2-4

To modify your NIC settings (you need Windows Administrator privilege to change these settings):

1. On your PC, access the MS Windows operating system TCP/IP Properties page as shown. In MS Windows XP this is found in **Control Panel** > **Network Connections** > **Local Area Connection** > **General**: Properties.
2. Select Internet Protocol (TCP/IP) and click on **Properties**.
3. Set the appropriate IP address and subnet mask. The subnet mask value should be identical to that set in the switch. The PC IP address must be different from that of the switch but lie in the same subnet.
4. Click **Web Access**. The Login screen will display.
5. Enter the default password **password**. Then, click **Login** to proceed to management of the switch covered in Chapter 3, “Basic Web Management”.

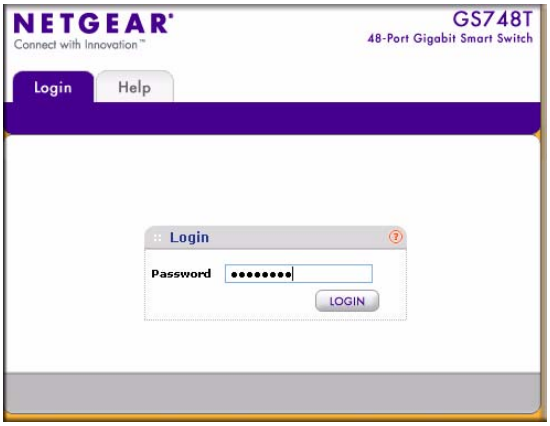

Figure 2-5

Smartwizard Utilities

Alternatively, from the Smartwizard main page of Figure 2-1 you can access the following features:

- Password Change
- Firmware Upgrade

Password Change

You can set a new password of up to 20 ASCII characters.

1. On the Smartwizard Utility screen, click **Password Change**. The Password Change screen. appears. You can set a new password. In this process, you are required to enter the old password and to confirm the new one.
2. Click **Set** to enable the new password.

Firmware Upgrade

The application software for the GS748T switch is upgradeable, enabling your switch to take advantage of improvements and additional features as they become available. The upgrade procedure and the required equipment are described as follows. This procedure assumes that you

have downloaded or otherwise obtained the firmware upgrade and that you have it available as a binary file on your computer. This procedure uses the TFTP protocol to implement the transfer from computer to switch.

To upgrade your firmware:

1. After selecting the switch you want to upgrade, click **Firmware Upgrade** (see Figure 2-1). The following screen will display:

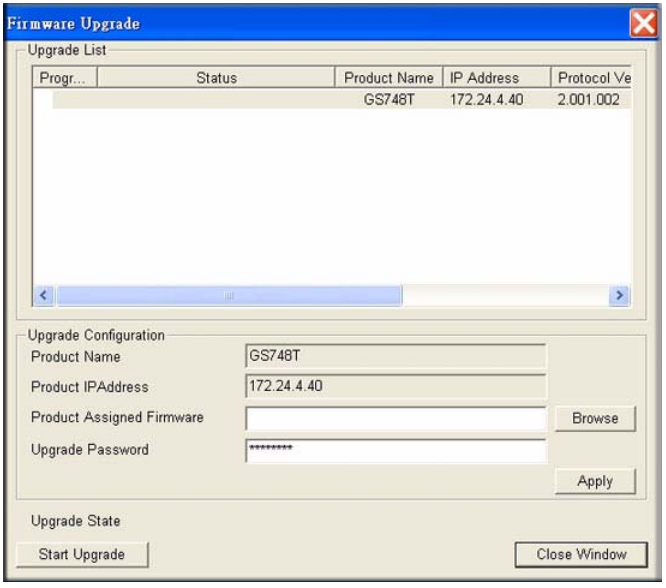

Figure 2-6

2. Enter the following values into the appropriate places in the form
   - **Product Assigned Firmware**: The location of the new firmware file. You can click **Browse** to locate the file. For example:

     `tftp://{tftp address}/{file name}`
   - **Upgrade Password**: Enter your password; the default password is **password**. Click **Apply.**
3. Click **Start Upgrade** to begin loading the upgrade. The system software is automatically loaded to all stacking members. When the process is complete, the switch automatically reboots.

Exit

Click **Exit** from the Switch Setting section to close the Smartwizard Discovery Utility program.

Chapter 3
Basic Web Management

This section contains information for performing basic configuration using your web browser. It also describes how to backup your configuration and how to reboot or reset your router if necessary. The section includes this information under the following headings:

- "Accessing the Switch Management Home Screen"
- "Changing Your Password"
- "Saving and Restoring Your Configuration"
- "Performing a Factory Reset or a Device Reboot"

Your NETGEAR Smart Switch series provides a built-in browser interface that enables you to configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. This interface also allows for system monitoring of the switch. The help page covers many of the basic functions and features of the switch and its web interface.

Web Management requires either Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later

This section describes setting browser interface options and using the home page for the GS748T Smart Switch. This interface is essentially similar to that entered as a result of selecting **Web Access** from the Smartwizard Discovery utility (see Chapter 2, "Using the Smartwizard Discovery Utility"). However, if you want to access the switch directly, without using the Smartwizard Discovery utility, you must work from the same network segment that contains the switch (the subnet mask values of switch and PC host must be the same) and you must point your browser to the switch using the switch IP address. If you used the Smartwizard Discovery utility to set up the IP address and subnet mask, either with or without a DHCP server, use that IP address in your browser window. If you are starting with an "out of the box" switch and are not using the Smartwizard Discovery utility, you must first configure your host PC with a static IP address that is on the same network segment as the default parameters of the switch, which are:

- IP address: 192.168.0.239
- Subnet Mask: 255.255.255.0

From the home page, you can change the network parameters to match those of your network by selecting **Setup**. Your host PC network parameters must then also be set back to match your network.

Accessing the Switch Management Home Screen

You can access the home screen for the GS748T Smart Switch from any PC with a web browser.

To start the application:

1. Open a web browser.
2. Enter the device IP address in the address bar.
3. Press **Enter**. The Login page appears as shown below.

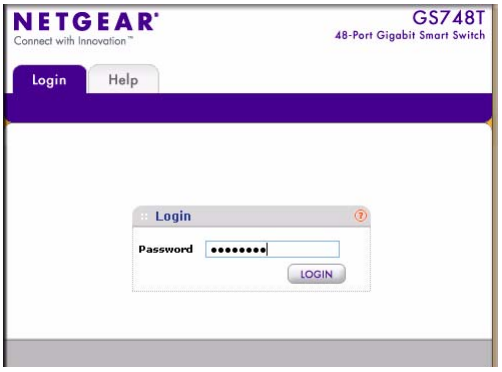

Figure 3-1

4. Enter the password (the factory default is **password**) and click **Login**. The GS748T switch System > Management home page is displayed as shown below.

The home page shows the navigation tabs across the top which provide a menu for access to the various configuration functions of the switch. Under the navigation tab headings are the secondary tabs which allow you to view/change all the components under a specific feature. There are secondary functions available under the subtabs on the left navigation pane.

The main navigation tabs remain displayed as each successive screen is accessed. From the main screen, click **Help** to access customer support.

Within the various browser interface screens, there are several buttons that you can use. Their names and functions are listed below:

- **Refresh**. Refreshes the system data to current values on the system.
- **Apply.** Submits change request to system and refreshes screen data.
- **Add**. Adds new entries to table information and refreshes screen data.
- **Delete**. Deletes selected entries from table and refreshes screen data.

- **Cancel**. Cancels changes made to that screen.

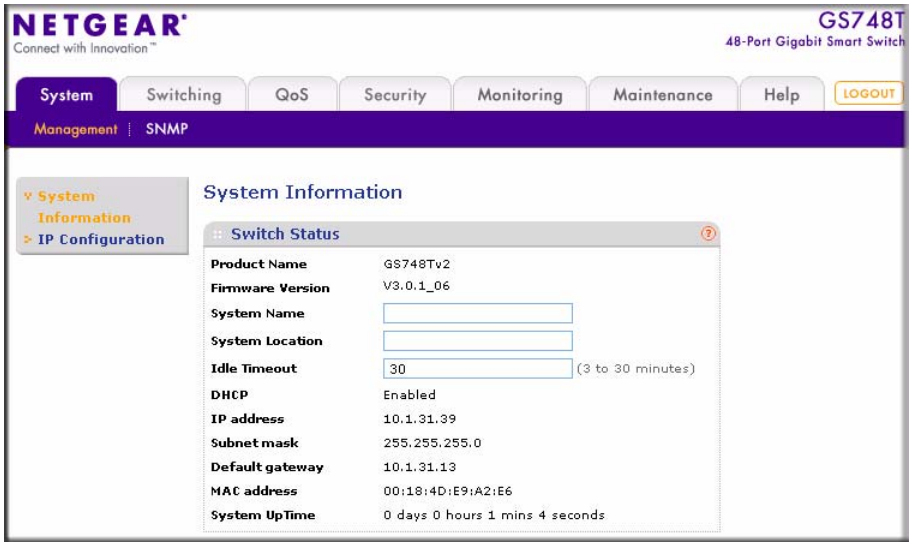

Figure 3-2

System Information Settings

The main screen, **System > Management > System Information,** shows the condition of the functions available in the switch. Click **Refresh** at the bottom of the pane to display updated status information. This information is described briefly as follows:

- **Product Name**. The name of the switch.
- **Firmware Version**. The version of the firmware currently installed on the switch.
- **System Name**. User supplied value (the same as sysName in MIB-2).
- **System Location**. User supplied value (the same as the sysLocation in MIB-2).
- **Idle Timeout**. 3 to 30 minutes. The default is 5 minutes.
- **DHCP**. Shows whether it was enabled.
- **IP Address**. The IP Address assigned to the switch.
- **Subnet Mask**. The subnet of the switch.
- **Default Gateway**. The switch gateway address.
- **MAC address**. The MAC address of the switch.
- **System Up Time**. Indicates how long the switch has been active.

IP Configuration

1. Select the System > Management > IP Configuration screen shown below to set your IP Configuration.

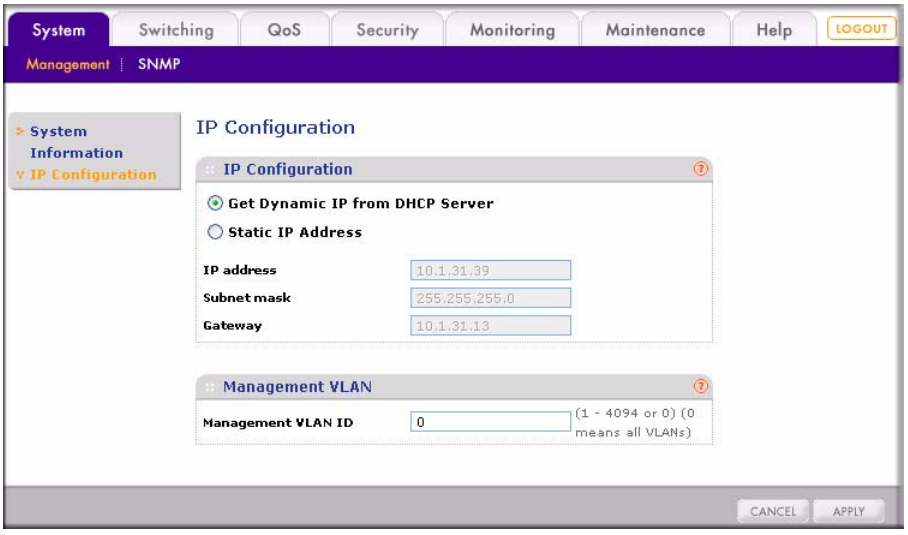

Figure 3-3

2. Select the **Get Dynamic IP from DHCP Server** radio box to enable the DHCP Server, or select the **Static IP Address** to set up a static IP address for the switch. Enter the following fields for a Static IP address:

   - IP Address – Enter a static IP address for you switch (make a note of this address for accessing your switch without using the Smartwizard Discovery utility).
   - Subnet Mask – Enter the subnet mask (make sure that all devices are on the same subnet)
   - Gateway – Enter the gateway address for the switch.

Changing Your Password

It is good practice to secure your system and change the default password. For optimum security, your password should be more than 8 characters long and should be a combination of numbers and letters—names and simple words can be easy to guess. If you forget your password, you can press the Factory Reset button on the front on the device, and the password will return to the default (see “Performing a Factory Reset or a Device Reboot”).

To change password:

1. Select Security > Management Security. The User Configuration > Change Password screen will display.
2. In the **Old Password** field, enter the current password.
3. In the **New Password** field, enter the new password, and then reenter your new password in the **Re-Type New Password** field to confirm the change.
4. Click **Apply** to enable the new password.

Figure 3-4

Managing Your System Configuration

The Maintenance tab on the main menu allows you to access the backup and restore features of the GS748T Smart Switch. These topics are described at this stage of the description because their utility may be needed early in the configuration process.

Saving and Restoring Your Configuration

This facility may be used to protect your system configuration and save a possibly long manual configuration in case of a loss or an accidental manual factory reset. Save Configuration enables you to back up your system configuration settings to your PC.

To save the configuration:

1. Select Maintenance > Save Config from the main menu. The Save Configuration screen will display.
2. Select the **All configuration settings will backup to file** check box.
3. Click **Apply**. A dialog box appears.

4. Click **Save**. When the file location field displays, specify the file name and path for saving the configuration file.

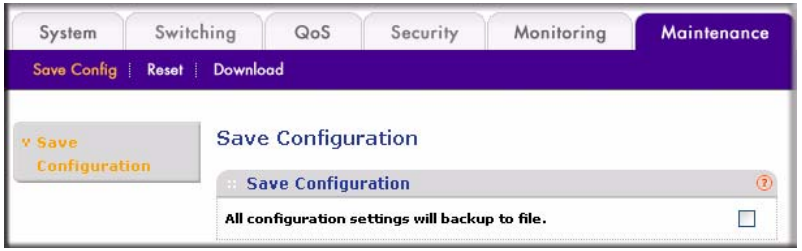

Figure 3-5

File Download enables you to restore the saved configuration file from your PC. To restore your saved configuration file:

1. Select Maintenance > Download. The File Download screen will appear:
2. Click **Browse** and select the configuration file that you want to restore on the switch.
3. Click **Apply** to restore your file.

Figure 3-6

When the saved file has been uploaded, the browser window will close and the switch will reboot.

Performing a Factory Reset or a Device Reboot

Factory Reset restores factory defaults when you want or make a major configuration change or need to regain management access to the switch. Use this feature under the following conditions:

- You have lost your password.
- You are installing your switch into a different network environment for which it is simpler to configure from the factory settings.

- You want to make a major configuration change for another reason.

	**Warning:** Restoring Factory Defaults erases any prior user configuration.

You can perform a Factory Reset using either of the following methods:

- From the main menu, Maintenance > Reset > Factory Default. The Factory Default screen will display.
- Select the **Check this box and click Apply below to reboot and return all configuration settings to default values** check box and then click **Apply,** or
- Press the Factory Defaults button on the right-hand side of the front panel.

The effect of each of these alternatives is identical.

Performing a Device Reboot restarts the system. Your configuration settings remain intact. You can reboot the switch externally by either:

- Power cycle it by disconnecting and reconnecting the power cord, or
- Use the Reset button on the left-hand side of the front panel.

  This operation does not disturb your switch configuration.

To reboot the switch from the switch GUI:

1. Select Maintenance > Reset > Device Reboot. The Device Reboot screen will display.
2. Select the **Check this box and click APPLY below to reboot unit** checkbox.
3. Click **Apply**.

Figure 3-7

Chapter 4
Configuring the Switch

The navigation tabs across the top of the user interface provide access to all of the submenu screens which allow you to manage your GS748T Smart Switch. The features under the following main headings:

- "Configuring Ports"
- "Configuring the Link Aggregation Group (LAG)"
- "Setting Up SNMP"
- "Configuring and Creating VLANs"
- "Enabling Spanning Tree Protocol"
- "Establishing Multicast Groups"
- "Enabling Jumbo Frames"
- "Setting Rate Limits"
- "Setting QoS Global Configuration"
- "Enabling Storm Control"
- "Configuring the IP Access List"
- "Controlling Switch Access by MAC Address and VLAN ID"
- "Setting up Mirroring or "Sniffer Ports""
- "Viewing Packet Statistics"

The description that follows in this chapter covers these features and tells you how to configure them in the GS748T switch.

Configuring Ports

The Port Configuration table displays the port status and contains fields for defining port parameters.

To configure port settings:

1. Select Switching > Ports from the main menu. The Port Configuration screen will display.

2. Select the row of the port that you want to configure. Then, at the top of screen, enter the following information for the selected port:
   - Type a description for the port in the **Port Description** field.
   - From the **Port Speed** pull-down menu, select the rate for the port:
     – 100M (100 Mbps)
     – 10M (10 Mbps)
     – Auto (Auto will set the speed to 1000Mbps)
     – Disable (disable the port)
3. From the **Duplex Mode** pull-down menu, select the duplex mode for the port (this field is available only when auto-negotiation is disabled and the port speed is set to 10M or 100M):
   - Full (Full duplex)
   - Half (Half duplex)
4. From the **Flow Control** pull-down menu, select whether or not to enable or disable Flow Control.
5. From the **Default Priority** pull-down menu, assign a default packet priority for packets without IEEE802.1P tagging. If the packet comes in with a priority tag, the priority is retrieved from priority field of the tag.
6. Click **Apply.**

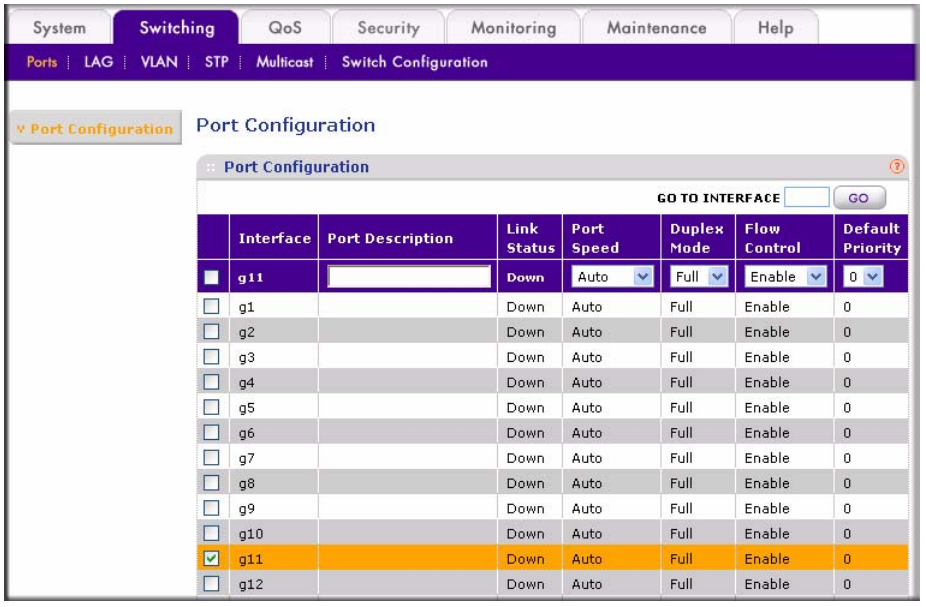

Figure 4-8

Configuring the Link Aggregation Group (LAG)

Link Aggregation Groups (otherwise known as Port Trunking) enables multiple links between switches to work as one virtual link (aggregate link) to provide greater bandwidth than would be available by confining the traffic to a single port. LAGs can be defined for similar port types only. For example, a 10/100 port cannot form a LAG with a gigabit port. Up to 10 LAGs can be operating at the same time.

The LAG table displays the status and administration settings for all the available LAGs, also known as trunks. The GS748T Smart Switch supports 10 static LAGs.

To enable or disable a LAG:

1. Select Switching > LAG > LAG Configuration from the main menu. The LAG Configuration screen will display.
2. Select the row of the LAG ID you want to enable or disable.
3. From the **Admin Mode** pull-down menu, select Enable or Disable.

4. Click **Apply**.

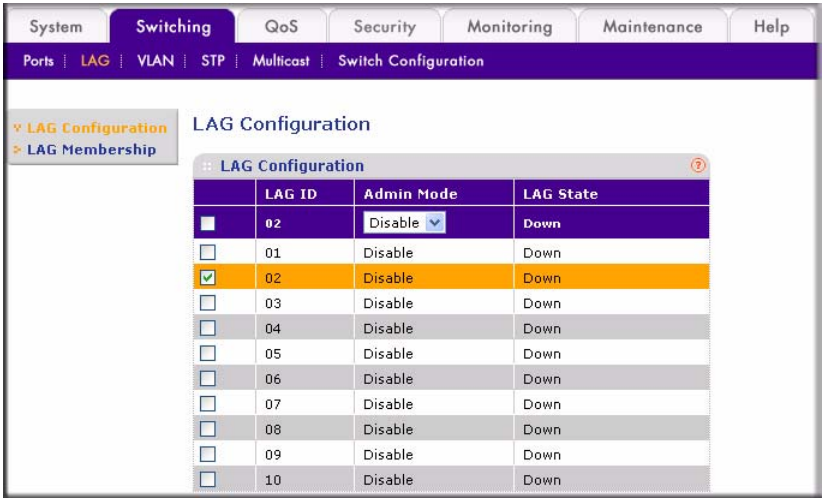

Figure 4-9

The LAG Membership table displays the port members in each LAG. You can also specify port members for LAGs. When specifying LAGs, the following policies apply:

- Each port can belong to only one LAG.
- Each LAG can have up to 8 ports.
- Ports in a LAG must have the same speed and be in the same VLAN group.

To configure port membership of a LAG:

1. Select Switching > LAG > LAG Membership. The LAG Membership screen will display.
2. From the **LAG ID** pull-down menu, select the LAG that you want to modify.
3. Click the **Unit** link next to the check box to display all available ports. (All ports are selected if the **Unit** checkbox is selected. If not selected, no ports are selected.)
4. Select or clear the check box for the ports you want to include or remove.
5. Click **Apply.**

Figure 4-10

Note: The selected LAG ID port must correspond to VLAN group IDs.

Setting Up SNMP

SNMP (Simple Network Management Protocol) is a transport protocol used for network management. The protocol is used in communication between a Manager—the management station—and an agent within the managed device, in this case your switch. The Manager polls the agent which responds by returning data from the Management Information Bases (MIBs) that it maintains on the managed device to indicate its status. An agent can return Traps to the Manager, Traps are messages that alert the manager to conditions that may need attention. Managers and Agents work within Communities which are defined to confine messaging within named groups. An agent only responds to requests from Managers within its community.

The SNMP screen allows you to limit the IP addresses from which the switch MIBs can be accessed and to which IPs the switch sends SNMP traps. The switch only responds to requests from management computers whose IP addresses are carried in the list. This list also holds Privilege information that controls which IPs have read-only or read-write access. You can also select the traps which the switch sends to the hosts from the following trap events. The **Status** field must be set to **Enable** to allow management host communication.

Trap Events are indicated by:

- T1: Authentication fail – The switch generates an SNMP trap when a host tries to gain access to the switch but the host's IP is not in the SNMP host table.
- T2: Device bootup – The switch generates an SNMP trap when it reboots.

- T3: Link Up/Down – The switch generates an SNMP trap when one of its ports changes its link status

You can specify the SNMP management station that can access the MIB of the switch and to which the switch will send the trap. When adding a management station, be aware that:

- You can specify up to four management station IP addresses.
- The switch will respond only to requests from a computer or management station with an IP address that is in the list.
- You can also select the traps that the switch will send to the hosts when the trap events you specify occur.

To add a management station:

1. Select System > SNMP. The SNMP V1/V2 screen will display.
2. In the **Management Station** field, enter the IP address of the management station.
3. In the **Community String** field, specify the community string. The switch processes requests from the management station only if the community string in the request packet matches the community string entered here.
4. From the **Access Mode** pull-down menu, select the access privilege for the management station:
    - Read Only (for GET and GETNEXT requests).
    - Read Write (for GET, GETNEXT, and SET requests).
5. From the **Trap(T2)** pull-down menu, select **Enable** if you want the switch to generate the SNMP cold Start trap when it reboots; otherwise select **Disable.**
6. From the **Trap(T3)** pull-down menu, select **Enable** if you want the switch to generate the SNMP linkUp and linkDown trap when one of its ports changes its link status.
7. From the **Status** pull-down menu, select **Enable** or **Disable** to specify the administration status. A managed station or host is not active until it is set to **Enable**.
8. Click **Add** to add a management station.

To delete a management station:

Select the entry you want to delete and click **Delete.**

To modify an entry:

1. Select the checkbox by the entry you want to modify. The fields available for modifying will appear at the top of the table.

2. Modify the settings in the top row and click **Apply.**

Configuring and Creating VLANs

A Virtual Local Area Network (VLAN) is a means of electronically separating ports on the same switch from a single broadcast domain into separate broadcast domains. By using VLANs, users can group nodes by logical function instead of physical location. For example, Engineering and Accounting department traffic can be separated from one another. VLAN memberships are manipulated by associating switch ports with VLAN IDs (VIDs).

You can choose from two types of VLAN to set up on the switch: IEEE 802.1Q VLAN (Tagged VLAN), or Port-based VLAN. You cannot mix the types on the same switch. In either case, any port can be a member of multiple VLANs.

- **IEEE 802.1Q VLAN**. The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches (Reference: Appendix A and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks). This switch supports the creation of 256 Static-Tag VLAN groups.

  This implementation separates traffic by adding a VLAN tag into the appropriate egress frames (packets) from selected switch ports. A receiving switch associates the tagged frame with the VLAN and forwards it, according to its own VLAN-to-port lookup table, to all ports on the VLAN except the ingress port. In this way, a VLAN structure may be built across a “tree” of switches. You have the option of setting egress frames to be:

  - **Tagged.** This setting adds an 802.1Q tag into the frame leaving the selected port.
  - **Untagged**. This option strips the 802.1Q tags from frame leaving the selected port. The port retains its association with the VLAN. This facility is used when these ports are connected to downstream equipment that does not recognize (and which consequently may be confused by) 802.1Q tags.
  - **Unchanged**. This option is the default and signifies that the port is not associated with a VLAN.

  Every port is a member of VLAN ID 1 by default. You can change the default assignment of any port adjusting the Primary VLAN ID Setting (PVID) table. Use this feature to ensure that untagged frames reach the VLAN that you require.

- **Port-based VLAN**. This implementation confines VLAN members to the ports on the particular switch (for example, the VLANs cannot span multiple switches). VLAN port membership is determined via a lookup table that you set up when you configure the switch. You can create up to 48 port-based VLANS. Every port belongs to VLAN ID 1 by default.

Adding and Configuring IEEE 802.1Q VLAN Groups

Depending on the VLAN type selected in the VLAN Type Configuration table, you can create 256 IEEE 802.1Q-based VLANs or 48 port-based VLANs.

To create a VLAN:

1. Select Switching > VLAN > VLAN Configuration from the main menu. The VLAN Configuration screen will display.
2. Select the **IEEE.802.1Q** radio box and click **Apply.**

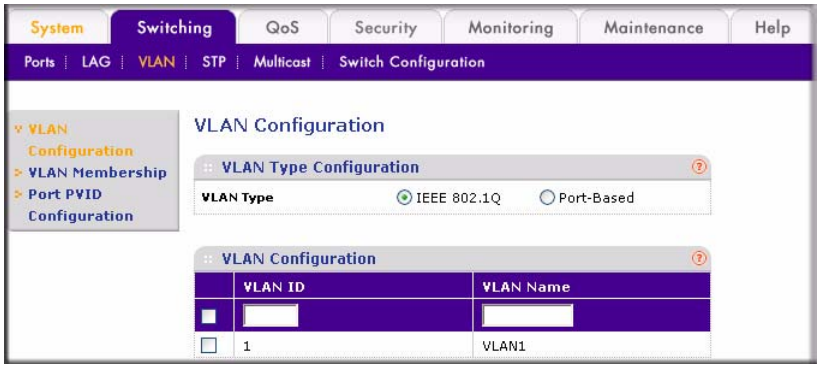

Figure 4-11

3. In the VLAN ID field, specify a VLAN ID from 1 to 4094. This field is available only when the 802.1Q VLAN type is selected. If you have not previously created a VLAN, this window shows VLAN ID 1 (default) with all ports set Untagged
4. In the VLAN Name field, assign a name to help you to identify this VLAN.
5. Click **Add.**

   Use the VLAN Membership table to manage each port's VLAN membership for transmitting packets. These settings determine if packets transmitted from each port are tagged with the VLAN ID and other information. By default, every port is a member of VLAN 1, which has a port VLAN ID (PVID) of 1.

To modify 802.1Q VLAN membership:

1. Select Switching > VLAN > VLAN Membership from the main menu. The VLAN Membership screen will display.
2. In the VLAN Identifier list, select the VLAN that you want to modify. The possible operations are:

   - Untag All: Add all the ports to this VLAN and remove tag on all egress packets)

- Tag All: Add all the ports to this VLAN and tag all egress packets.
- Remove All: Remove all the ports from this VLAN.

3. Click the **Unit** link to display all available ports.
4. Toggle the check box for each port to change its membership and tag setting:
   - An empty check box indicates that the port is not a member of this VLAN.
   - **T** indicates that the egress packet is tagged.
   - **U** indicates that the egress packet is untagged.
5. Click **Apply.**

Figure 4-12

Note: Every port has an initial default VID of 1 (PVID = 1). Whether a port has this VID or has been made a member of another default VID, you cannot remove any port from its prior default VLAN until you have reassigned its PVID to its new value. Use the PVID Setting menu option of VLAN Management to change its PVID before attempting to remove it from its prior default membership.

The PVID Configuration table contains parameters for assigning Port VLAN ID (PVID) values to interfaces. All ports must have a defined PVID. If no other value is specified, the default VLAN PVID is used. If you want to change the port's default PVID, you must first create a VLAN group that includes the port.

To modify a PVID:

1. Select the interface or port that you want to modify.
2. In the PVID field, enter a valid VLAN ID.

3. Click **Apply**.

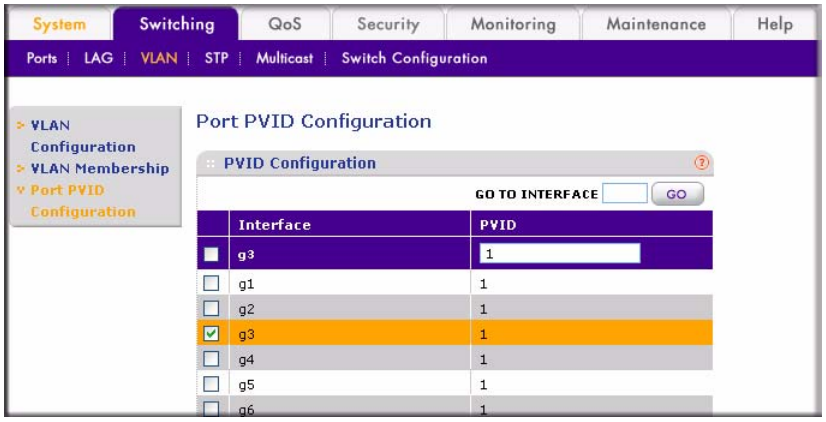

Figure 4-13

Configuring Port-Based VLANs

Unlike 802.1Q based VLAN, an ingress packet with an 802.1Q tag is ignored and preserved.

To modify port-based VLAN membership:

1. Select Switching > VLAN > VLAN Configuration from the main menu. The VLAN Configuration screen will display.

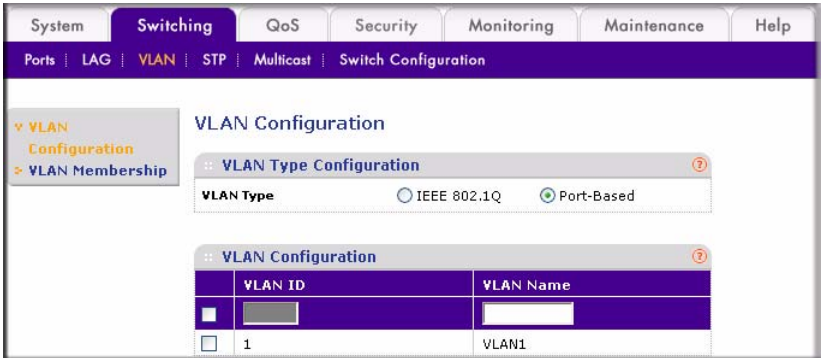

Figure 4-14

2. Ensure that the **Port-Based** radio box has been enabled for **VLAN Type.**
3. In the VLAN Name field, assign a name to help you to identify this VLAN.
4. Click **Add**.

To modify a Port-Based VLAN membership:

1. Select VLAN Membership. The VLAN Membership screen will display all port-based VLAN members.
2. From the **VLAN Identifier** pull-down menu, select the VLAN that you want to modify. You can also click the **Unit** link to display all available ports.
3. Select or clear the check box for the port for the VLAN.
4. Click **Apply**.

To delete a VLAN:

Select the VLAN you want to remove and click **Delete**. all port associations are separated from the VLAN and it is removed.

Selecting a Management VLAN

The Management VLAN allows you to establish an IP connection to the switch from a PC connected to a port in that VLAN. This increases security by allowing only PCs in the management VLAN to configure the switch. Any VLAN can be designated as the management VLAN.

To configure the management VLAN:

1. Select System > Management > IP Configuration. The IP Configuration screen will display.
2. In the **Management VLAN ID** field, enter the ID of the VLAN that you want to use for managing the switch. A zero value means that any PC in any of the VLANs can establish an IP connection to the switch.
3. Click **Apply** to save your settings.

Enabling Spanning Tree Protocol

To achieve reliability in a network, some path redundancy must be provided. However, multiple paths between network nodes can cause loops to exist and result in switching confusion and duplication of traffic. Spanning Tree Protocol (defined by IEE 802.1D) controls the duplicate paths by accounting for statistical weights in the available paths. It blocks the least efficient alternate paths and causes traffic only to be carried over the optimal paths between nodes.

The GS748T switch supports Rapid Spanning Tree Protocol (defined by IEEE 802.1w), which is an improvement (over the 802.1D STP) that shortens connection latency between nodes. The

resultant path between nodes determined by RSTP is the same as that eventually determined by STP. Use the Bridge Settings table to manage attributes related to the Spanning Tree Protocol.

- **Bridge Priority**. The priority value of this switch. After exchanging BPDUs with other STP-enabled devices, the device with the lowest priority value becomes the root bridge.
- **Bridge Max Age.** The maximum age of the current bridge. This is the maximum age of the Spanning Tree Protocol information learned from the network before it is discarded (in seconds).
- **Bridge Hello Time**. Indicates the amount of time (in seconds) that the switch waits before sending configuration PDUs when it is the root of the spanning tree or trying to become the root.
- **Bridge Forward Delay.** Indicates the amount of time, measured in seconds, that the port stays in each of the listening and learning states that precedes the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway.

The IEE 802.1W RSTP Setting page of the GS748T switch contains a set of default values which are optimal for most applications. Adjust these values if you must provide for special conditions.

To set up RSTP:

1. Select Switching > STP > Advanced > RSTP Configuration from the main menu. The RSTP Configuration screen will display.
2. Select the **Enable** radio box for **RSTP Configuration** and click **Apply.**
3. Then select the **Advanced** link to display the Bridge Settings. You can accept the default settings or modify the default settings and click **Apply.**

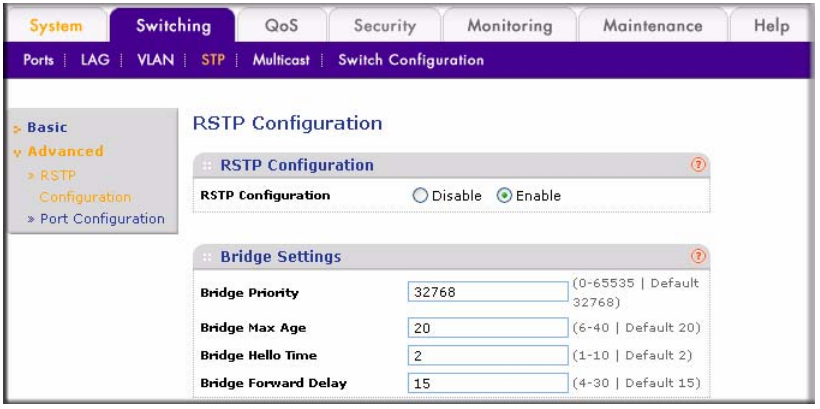

Figure 4-15

The Port Configuration table displays the current status of individual ports. You can also configure ports from this table.

To modify port settings:

1. Select the **Port Configuration** link. The RSTP Port Configuration screen will display.
2. Select the interface or port you want to modify.
3. Modify the settings in the top row:
   - **Path Cos**t. Displays the cost of this port. Cost means the contribution of this port to the cost of paths toward the spanning tree root that include this port. The switch uses this value to determine which port is the forwarding port. If all other factors are equal, the path with the lowest cost to the root bridge is the active path.
   - **Priority**. Displays the priority of this port. This is the value of the priority field contained in the first octet of the port ID. The port with the lowest number has the highest priority.
   - **Edge**. Indicates if this port is the edge port. Once configured as an edge port, the port immediately transitions to the forwarding state.
   - **P2P Forc**e. Indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
4. Click **Apply**.

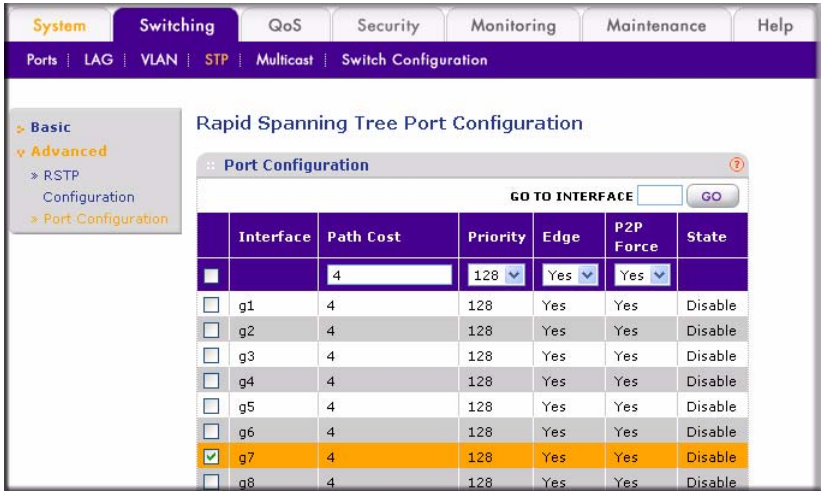

Figure 4-16

Establishing Multicast Groups

You can specify specific ports and VLANs for receiving Multicast packets with specific MAC addresses. The MAC addresses are IPv4 Multicast Addresses (RFC 1112A) formatted as: 01:00:5E-XX-XX-XX. A maximum of 64 groups is supported.

IGMP Snooping

IGMP (Internet Group Management Protocol) specifies how to register a host to a router in order to receive specific multicast traffic. It allows your switch to examine IGMP packets and forward them in ways based on their content.To receive messages, the switch must be configured to use IGMP snooping in subnets that receive IGMP queries from either IGMP groups or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by dynamically configuring Layer 2 LAN ports to forward multicast traffic only to those ports that want to receive the messages. IGMP is a standard defined in RFC 1112 for IGMPv1 and in RFC 2236 for IGMPv2.

Both IGMP Snooping and blocking of unknown multicast addresses (flooding) are disabled by default.

To enable IGMP snooping:

1. Select Switching > Multicast > Basic from the main menu. The IGMP Snooping screen will display.
2. Select the **Enable** radio box to enable the **IGMP Snooping Status** feature.
3. Select the **Enable** radio box for **Block Unknown Multicast Addresses** to allow unknown multicast flooding.
4. Click **Apply**.

Multicast Group Configuration

The Static Multicast table allows you to add and delete static multicast groups. Up to 256 static multicast groups can be supported.

To add a static multicast entry:

1. 1. Select Switching > Multicast > Advanced > Multicast group Configuration. The Multicast Group Configuration screen will display.
2. Enter the following parameters for each field in the top row:

- **VLAN ID**. Specifies the VLAN ID. This field is only applicable if 802.1Q VLAN mode is used.
- **Multicast Entry**. Specifies the multicast group MAC address associated with the VLAN.

3. Click **Add**.

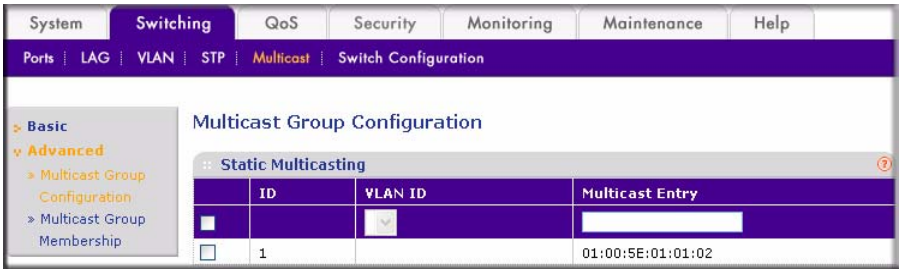

Figure 4-17

To delete a static multicast entry:

1. Select the checkbox adjacent to the multicast group you want to delete.
2. Click **Delete.**

Multicast Group Membership

The Multicast Group Membership table displays the ports associated with each multicast group.

To configure the multicast group membership:

1. Select Switching > Multicast > Advanced > Multicast Group Membership. The Multicast Group Membership screen will display
2. From the ID pull-down menu, select a multicast group that you created in the Multicast Group Configuration screen.
3. Click the **Unit 1** link. All the available ports will display. Select the ports for the Multicast Group (Select the Unit 1 checkbox to select all ports.)
4. Click **Apply.**

Figure 4-18

To remove a multicast group:

1. In the line of the table that specifies the group, check the **Delete** box.
2. Click **Apply** to remove the group.

Enabling Jumbo Frames

Jumbo Frames are not an approved standard Ethernet frame size, so you must ensure that all of your networking equipment can support these nonstandard jumbo frames to prevent them from being dropped. The Jumbo Frame screen allows you to enable or disable jumbo frame support. The maximum default frame size is 1,518 bytes. When jumbo frame support is enabled, the frame size can vary from 64 bytes to 9,216 bytes. Jumbo frames is disabled by default.

To configure a jumbo frame:

1. Select Switching > Switch Configuration from the main menu. The Jumbo Frame Configuration will display.
2. In the **Jumbo** Frame radio box, select **Enable**.
3. Click **Apply.**

Setting Rate Limits

Rate Limiting determines the bandwidth of ingress and egress traffic for a specific port.[1] There are 11 data rate options in the range 512K bps to 1000M bps, including a disable option that applies no limit to the data rate. Ingress and egress rates are separately configurable.

To configure the rate limit for a specific port:

1. Select QoS > Basic > Rate Limit. The Rate Limit | Rate Control Setting screen will display.
2. Select the checkbox adjacent to the port you want to configure.
3. In the top row, select the rate limitations from the pull-down menus:
   - In the **Ingress Rate** list, select the rate limitation of incoming traffic in this port.
   - In the **Egress Rate** list, select the rate limitation of outgoing traffic in this port.
4. Click **Apply**.

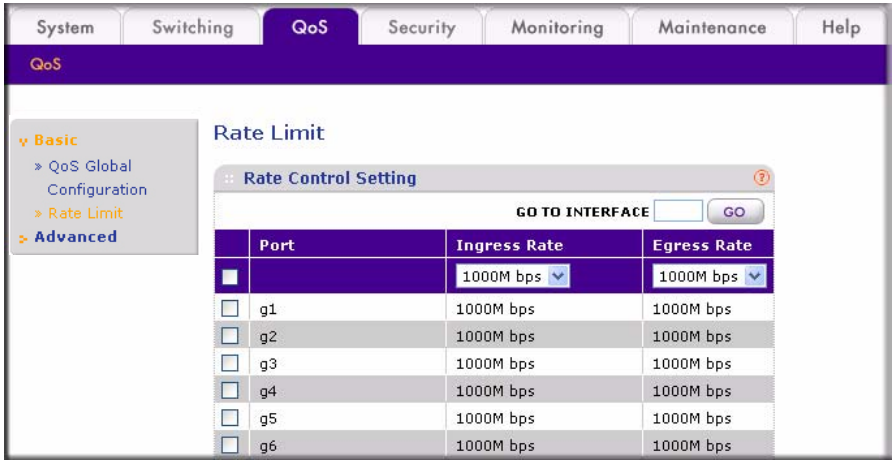

Figure 4-19

Setting QoS Global Configuration

Quality of Service (QoS) is used to manage traffic in a network by treating different types of traffic with different levels of priority. Higher priority traffic receives preferential treatment during times of switch congestion.

1. Egress rate limiting is available only with v3 hardware.

Two possible system mode implementations of QoS are supported:

- **IEEE 802.1p-based QoS.**
- **DSCP-based (Differentiated Services Code Point) QoS.**

To specify the QoS Global system mode:

1. Select QoS > Basic > QoS Global Configuration from the main menu. The QoS Global Configuration screen will display.
2. Select either the **802.1p Based** radio box or the **DSCP Based** radio box.
3. Click **Apply.**

IEEE 802.1p-Based QoS

IEEE 802.1p-based QoS enables the user to map each of the eight priority levels specified in IEEE 802.1p (p0 to p7) to one of four internal hardware priority queues: **High**, **Normal**, **Low**, and **Lowest**. The eight priority levels specified in IEEE 802.1p (p0 to p7) are implemented by a three-bit priority field in the VLAN tag. The switch empties the four hardware priority queues in order, from High to Lowest. Packets are transferred to empty the buffers of each higher hardware priority queue in turn before the next lower hardware priority queue can begin to transfer its received packets through the switch.

The 802.1p to Queue Mapping table contains fields for mapping 802.1p priority values to the four hardware traffic queues

To map 802.1p priorities to queues:

1. Select QoS > Advanced > 802.1p Queue Mapping. The 802.1p to Queue Mapping screen will display.

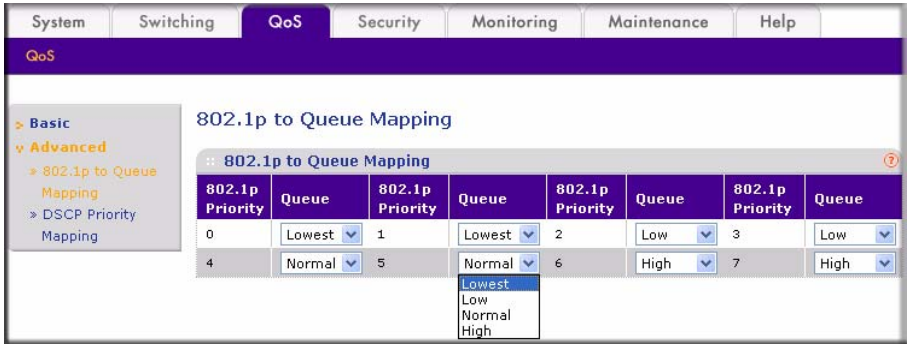

Figure 4-20

2. From each 802.1p priority value pull-down menu, select one of the four hardware priority queues.
3. Click **Apply.**

Differentiated Services Code Point (DSCP)-based QoS

The DSCP 6-bit field in an IP packet header enables levels of service to be assigned to network traffic according to the field's binary value. This 6-bit field comprises three IP Precedence MSBs with a least-significant 3-bit expansion field as defined in RFC 2474. The IP Precedence bits in the DSCP field are compatible with routers that only support IP Precedence. DSCPs specifically tailored to be backward compatible with routers that only support IP precedence lack the 3-bit expansion field and are called Class-selector DSCPs.

The DSCP to Priority Mapping table contains fields for mapping DSCP values to the eight 802.1p priority values. For the DSCP QoS to work properly, make sure that the priority values are correctly mapped to the appropriate hardware queues.

To map DSCP values to 802.1p priorities:

1. Select QoS > Advanced > DSCP Priority Mapping from the main menu. The DSCP to Priority Mapping screen will display.
2. Select one of the eight priority values for each DSCP value.
   - Match these DHCP values to set "Per Hop Behavior" (PHB) priorities by selecting a QoS service-class value of between 0 and 7. Packets within these service classes are treated with equal priority.
   - RFC 2597 defines the assured forwarding (AF) PHB. It guarantees a certain amount of bandwidth to an AF class.
   - The Expedited Forwarding (EF) PHB is defined in RFC 2598 and uses Codepoint 101110. The EF PHB is used to build a low loss, low latency, low jitter, assured bandwidth service. This premium service can appear to the user be a point to point connection.
3. Click **Apply**.

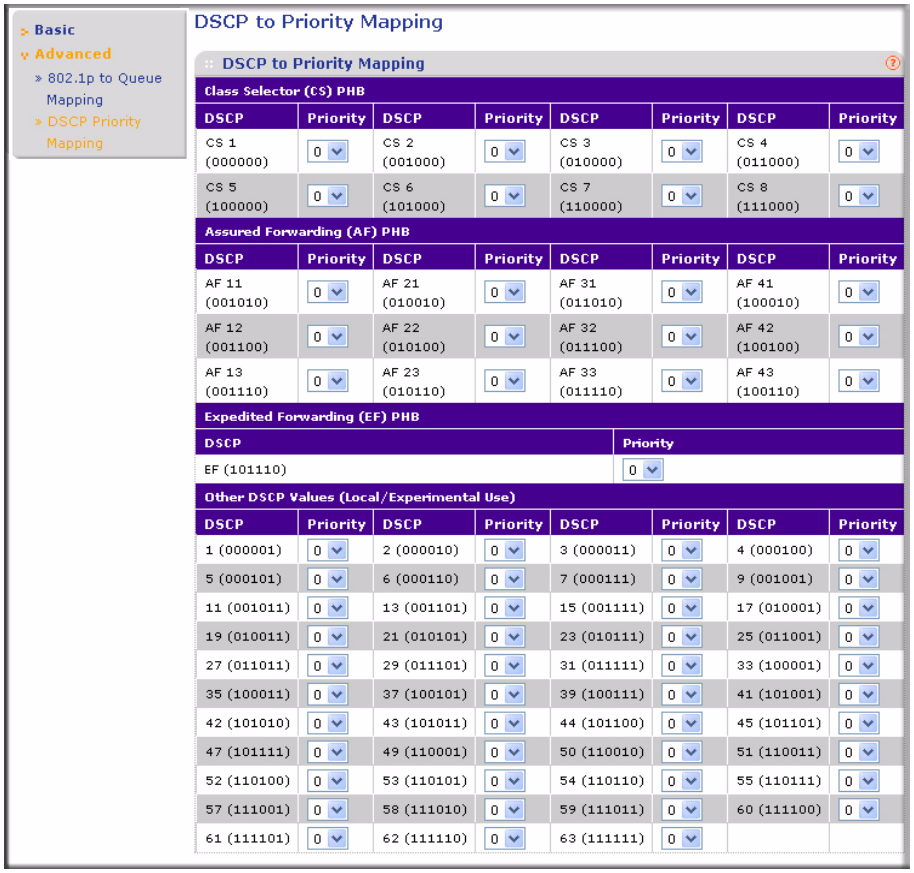

Figure 4-21

Enabling Storm Control

The Storm Control feature enables you to prevent network performance from being disrupted by specifying the threshold of ingress broadcast or multicast and broadcast packets on each port. The traffic source may be Multicast and Broadcast; Broadcast only; or Unknown Unicast, Multicast or Broadcast—or it may be disabled. A selected received threshold rate of between 1000 and 65535 packets per second may be specified in each case. If Multicast and Broadcast is selected as the source of the traffic, then the threshold value is the combined rate of both types of packet. If the incoming traffic rate of the specified packet types is above the specified value, the packets are discarded.

The Storm Control Settings table contains system-wide configuration parameters for storm control.

To configure storm control:

1. Select Security > Traffic Control. The Storm Control screen will display.

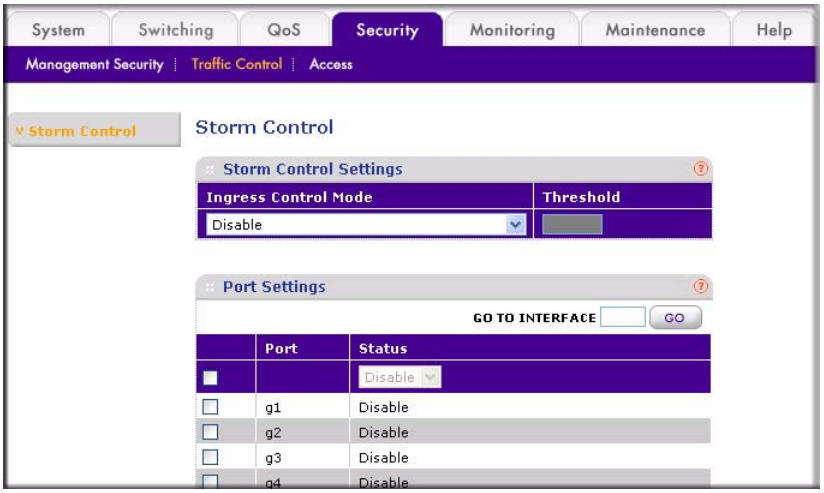

Figure 4-22

2. From the **Ingress Control Mode** pull-down menu, select the type of the packet storm:
   - Disable (to turn off storm control)
   - Unknown Unicast, Multicast and Broadcast
   - Multicast and Broadcast
   - Broadcast Only
3. In the Threshold field, specify the threshold rate limit (packets per seconds) for storm control. The valid range is from 1000 to 65535.
4. Click **Apply**.

You must enable the Storm Control feature on each port individually from the Port Settings table. Storm Control is disabled on every port by default.

To enable Storm Control:

1. Select Security > Traffic Control. The Storm Control screen will display.
2. Select the checkbox adjacent to the port that you want to change.

3. In the top row, from the **Status** pull-down menu, select either **Enable** or **Disable**.
4. Click **Apply**.

Configuring the IP Access List

The IP Access List table allows you to limit and specify the IP addresses that can access the management portion of the switch. An empty list means that all IP addresses are allowed to access the switch. Otherwise, the switch will respond only to requests from computers with an IP address in the list. So make sure that you include the IP address of your PC if you are setting this feature. The list can have a maximum of 10 IP addresses.

To add an entry to the IP Access list:

1. Select Security > Access > IP Access List from the main menu. The IP Access List will display.
2. In the IP Address field of the configuration row, enter the IP address of the PC that you want to manage the switch from.
3. Click **Add.**

To delete an entry from the IP Access list:

1. Select the checkbox adjacent to the entry of the IP address you want to remove.
2. Click **Delete**.

Controlling Switch Access by MAC Address and VLAN ID

The Trusted MAC table shows all the Trusted MAC addresses that you can specify to allow forwarded traffic to the switch. The maximum number of trusted MAC addresses is 256 per system. All source MACs are trusted when the Trusted MAC list is empty. If the list includes MAC addresses, any incoming traffic with a source MAC address that is not included in the trusted MAC table is dropped.

If the VLAN mode for the switch is set up as Port-based, you enter a MAC address and port number that you want to permit access this switch. If the VLAN is set up in 802.1Q mode, you enter a MAC address and VLAN ID to permit access

To add a trusted MAC address:

1. Select Security > Access > Trusted MAC. The Trusted MAC screen will display.

2. Specify the trusted MAC address parameters in the configuration row:
   - **Interface**. From the **Interface** pull-down menu, select the interface or port that you want to have this feature.
   - **MAC Address**. Specify the trusted source MAC address.
   - **VLAN ID.** Enter a VLAN ID that the interface belongs to if the 802.1Q VLAN mode is enabled.
3. Click **Add**.

To delete a trusted MAC address:

1. Select the checkbox adjacent to the trusted MAC entry that you want to delete from the list.
2. Click **Apply**.

Setting up Mirroring or "Sniffer Ports"

Port Mirroring allows you to configure traffic from any number of ports to be copied (mirrored) to your selected "sniffer" port, which may be any port that is not a source port. This traffic may be selected from transmitted or outgoing (egress) frames, received or incoming (ingress) frames or all frames. A port cannot be both a mirrored and a destination port at the same time. Sniffing may be disabled globally.

To configure port mirroring:

1. Select Monitoring > Mirroring. The Port Mirroring screen will display.
2. From the Destination Port pull-down menu, select a port to be the destination port. All mirrored traffic will be routed to this port.
3. From the **Mirroring** pull-down menu, select the mirroring mode. The possible settings are:
   - **Tx and Rx**. Mirrors both incoming and outgoing traffic on the designated source ports.
   - **Rx Only**. Mirrors only the incoming traffic to the designated source ports.
   - **Tx Only**. Mirrors only the outgoing traffic to the designated source ports.
   - **Disable**. Disables port mirroring globally.
4. Select the Source Port check boxes for the ports to be mirrored. Clear the check boxes for the ports you do not want to be mirrored.
5. Click **Add**.

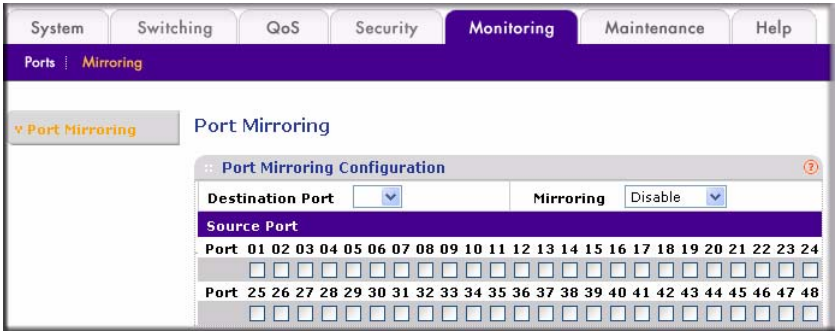

Figure 4-23

Viewing Packet Statistics

The Port Statistics screen shows reports of packet traffic and packet errors formatted as follows:

- **Port Selection**: The port number on the switch—selected from the Port pull-down menu.
- **Statistics**: Detailed Tx and Rx statistical information, by port.
- **Summary Statistics**: All ports Tx and Rx statistics summarized. Presents the information from each port's internal counters.

To view statistics for a single port:

1. From the **Port** pull-down menu, select the port number.
2. Click **Apply.**

To retrieve summary statistics.

1. Click **Refresh** to retrieve the current count from the device and update the tables.
2. Click **Clear Counters** to reset all counters to zero.

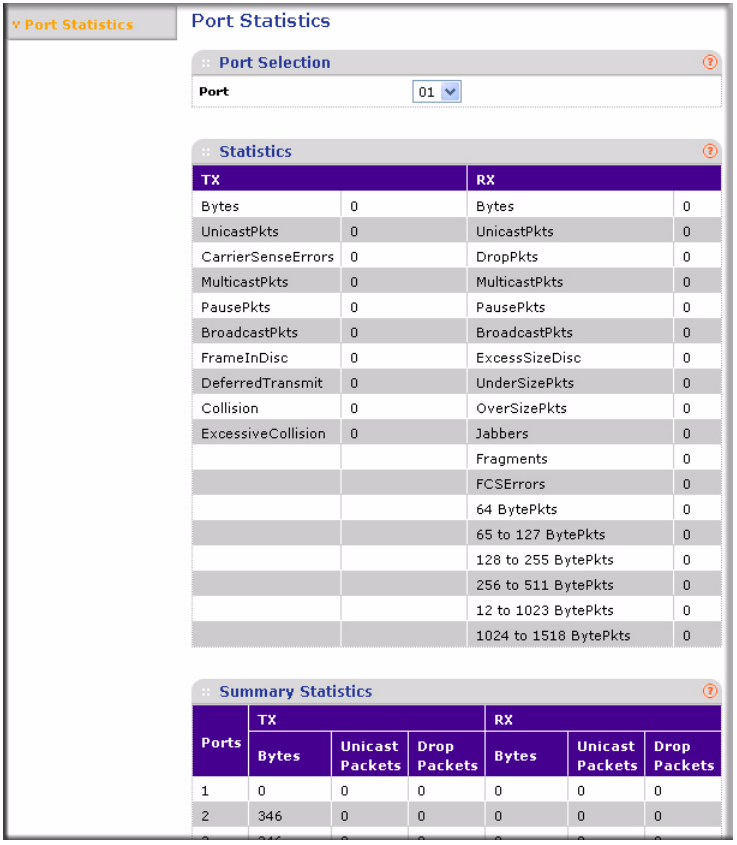
Port Statistics
Port Statistics
Port Selection
Port
01
Statistics
TX
Bytes 0
UnicastPkts 0
CarrierSenseErrors 0
MulticastPkts 0
PausePkts 0
BroadcastPkts 0
FrameInDisc 0
DeferredTransmit 0
Collision 0
ExcessiveCollision 0
RX
Bytes 0
UnicastPkts 0
DropPkts 0
MulticastPkts 0
PausePkts 0
BroadcastPkts 0
ExcessSizeDisc 0
UnderSizePkts 0
OverSizePkts 0
Jabbers 0
Fragments 0
FCSErrors 0
64 BytePkts 0
65 to 127 BytePkts 0
128 to 255 BytePkts 0
256 to 511 BytePkts 0
12 to 1023 BytePkts 0
1024 to 1518 BytePkts 0
Summary Statistics
Ports
TX
Bytes
Unicast Packets
Drop Packets
RX
Bytes
Unicast Packets
Drop Packets
1 0 0 0 0 0 0
2 346 0 0 0 0 0

Figure 4-24

Appendix A
Specifications and Default Values

GS748T Smart Switch Specifications

The GS748T Smart Switch conforms to the TCP/IP, UDP, HTTP, ICMP, TFTP, DHCP, 802.1D, 802.1p, and 802.1Q standards.

Table A-1. GS748T Smart Switch Specifications

Feature	Value
Interfaces	48G (P01 - P48)
Fiber Optic	4 Mini-GBIC Combo (P45f - P48f)
PoE	N/A
Flash Memory Size	2MB
SRAM Size and Type	16MB DDR

Table A-2. Switch Performance

Feature	Value
Switching Capacity	48 x 1Gbps
Forwarding Method	Store and Forward
Packet Forwarding Rate	10M:14,880 pps / 100M:148,809 pps / 1G:1,488,095 pps
MAC addresses	8K
Packet RAM buffer capacity	512K-bytes

GS748T Smart Switch Features and Defaults

Table A-3. Port Characteristics

Feature	Sets Supported	Default
Auto-Negotiation / Static Speed / Duplex	48 (per-port)	Auto-Negotiation
Auto MDI/MDIX	N/A	Enabled
802.3x flow control / Back Pressure	48 (per-port)	Enabled
Port Mirroring	1	Disabled
Port Trunking (Aggregation)	10	Disabled
802.1D Spanning Tree	1	Disabled
802.1w RSTP	1	Disabled
IGMP Snooping	1	Disabled
Static 802.1Q Tagging	256	VID = 1 Member Ports = [1-48]
Port Based Private VLAN	48X1	MemberPorts[1] = [1-48]
Learning Process	N/A	N/A

Table A-4. Quality Of Service

Feature	Sets Supported	Default
Number of Queues	N/A	N/A
Port Based	48 (per port)	Normal for all ports
802.1p	1	Disabled
DSCP	1	Disabled

Table A-5. Security

Feature	Sets Supported	Default
ACL	10	All IP addresses allowed
Password Control Access	1	Login Time Out = 5 mins. Password = “password”

Table A-5. Security (continued)

Feature	Sets Supported	Default
Trust Matadors Filter	256	Disabled
Port -MAC lock down	48 (per port)	Disabled
Management VLAN	1	0

Table A-6. Traffic Control

Feature	Sets Supported	Default
Rate control	48 (per port)	Disabled
Storm control	1 (per switch)	Disabled
Jumbo frame	48 (per port)	Disabled

Table A-7. System Setup

Feature	Sets Supported	Default
DHCP\Manual IP	1	192.168.0.239
System Name Configuration	1	NULL
Configuration Save/Restore	1	N/A
Firmware Upgrade	1	N/A
Factory Reset	1	N/A

Table A-8. Other Features

Feature	Sets Supported	Default
Static Multicast Entry	64	Disabled
Filter Multicast Control	1	Disabled

Table A-9. Management

Feature	Sets Supported	Default
SNMPv1/V2c	4	Disabled
MIB Support	1	Disabled

Table A-9. Management

Feature	Sets Supported	Default
Smartwizard	N/A	Enabled
Statistics	48 (per port)	N/A

Appendix B
Virtual Local Area Networks (VLANs)

A Local Area Network (LAN) can generally be defined as a broadcast domain. Hubs, bridges or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local-area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application). To communicate between VLANs, traffic must go through a router, just as if they were on two separate LANs.

A VLAN is a group of PCs, servers and other network resources that behave as if they were connected to a single, network segment—even though they may not be. For example, all marketing personnel may be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

The Advantages of VLANs:

- Easy to do network segmentation: Users that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is largely contained within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- Easy to manage: The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- Increased performance: VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- Enhanced network security: VLANs create virtual boundaries that can only be crossed through a router. So standard, router-based security measures can be used to restrict access to each VLAN

IEEE 802.1Q VLANs

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user-configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the PVID Setting page.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID Setting. The packet proceeds to the VLAN specified by its VLAN ID (VID) tag number.
- If the port in which the packet entered does not have membership with the VLAN specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet is able to be sent to other ports with the same VLAN ID.
- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A "U" for a given port means that packets leaving the switch from that port are Untagged. Inversely, a "T" for a given port means that packets leaving the switch from that port are tagged with the VLAN ID associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

802.1Q Example

This example demonstrates several scenarios of VLAN use and describes how the switch handles Tagged and Untagged traffic.

1. Setup the following VLANs: VLAN 10, 20.

2. Configure the VLAN membership. Be sure to set all of them as follows.

- Setting up first VLAN group, VLAN ID = 10:
- Setting up second VLAN group, VLAN ID = 20:

3. Modify PVID Setting to apply previous two VLAN groups: Modify Default VLAN group (VLAN ID = 1) to apply two new VLAN groups:

The specific ports above have the following Port VLAN ID settings:

- Default VLAN: Port 7 – Port 26 (all U), VID = 1
- VLAN 1: Port 1 (U), Port 2 (U), Port 3 (T), VID = 10
- VLAN 2: Port 4 (U), Port 5 (T), Port 6 (U), VID = 20.

4. The following situations produce results as described:

- If an untagged packet enters Port 1, the switch tags it with a VLAN tag value 10. The packet has access to Port 2 and Port 3. The outgoing packet is stripped of its tag to leaves Port 2 as an untagged packet. For Port 3, the outgoing packet leaves as a tagged packet with a VLAN tag value of 10.
- If a tagged packet with a VLAN tag value 10 enters Port 3, the packet has access to Port 1 and Port 2. If the packet leaves Port 1 and/or Port 2, it is stripped of its tag to leave the switch as an untagged packet.
- If an untagged packet enters Port 4, the switch tags it with a VLAN tag value 20. The packet will have access to Port 5 and Port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves Port 6. For Port 5, the outgoing packet leaves as a tagged packet with a VLAN tag value of 20.

Port-based VLANs

Port-based VLANs help to confine broadcast traffic to the switch ports. This switch allows up to 26 port-based VLAN group, Any one port can belong to different VLAN groups. The default VLAN group is a port-based VLAN that has all ports belonging to VLAN 1.

Packets received by the switch are treated in the following way:

- When a packet enters a port, it can only proceed to ports with the same VLAN membership as that ingress port.
- If a port on the switch does not have a common VLAN membership with the source port, the packet is dropped.

Port-based VLAN Example Configuration

This example basically demonstrates how the port-based VLANs work to meet your needs.

Setup the following VLANs, each with defined descriptions:

- VLAN 1 (IT department)
- VLAN 2 (Sales department)
- VLAN 3 (Marketing department)
- VLAN 4 (Accounting department).
- Configure the VLAN membership. Be sure to set all of them as follows.
- Setting up second VLAN group (Sales), VLAN ID = 02, with membership of ports 1~8, 25.

- Setting up third VLAN group (Marketing), VLAN ID = 03, with membership of ports 7~14, 25.
- Setting up fourth VLAN group (Accounting), VLAN ID = 04, with membership of ports 19~20, 25.
- Setting up first VLAN group (IT), VLAN ID = 01, with membership of all ports.
- Since VLAN ID 01 has been setup by default, you will have to remove the ports that belong to all other VLAN groups except port 25.
- Ports 7 and 8 are kept for connected file server and printer server use. Sales and Marketing departments can share file archives and printing services.
- Port 25 provides Gigabit speed for e-mail server and Internet connection.

The specific ports above have the following functions:

- VLAN 1: Port 15 – Port 18, Port 21 – Port 24, Port 26, for IT department to monitor and control activities on all other VLANs
- VLAN 2: Port 1 – Port 8, for Sales department, port 7 and 8 connect to file archives and printer server.
- VLAN 3: Port 7 – Port 14, for Marketing department, port 7 and 8 connect to file archives and printer server.
- VLAN 4: Port 19 – Port 20, for Accounting department, its work is kept secret from other departments except IT.

VLAN Configuration Results

If a packet comes in on port 2, it can go to ports 1, 3, 4, 5, 6, 7, 8, and 25, as those are the only ports in that VLAN. A Sales person on Port 2 can get to the Internet, send and receive e-mail, but cannot access the marketing department print server or file archives.

If a Marketing user sends out a broadcast message, the Sales and Accounting departments are not affected by the message, because it does not go out on their ports. Only the Marketing department and the IT group will receive the broadcast message.

If an IT user sends out a broadcast message, everyone receives it.

Appendix C
Network Cabling

This appendix provides specifications for cables used with a NETGEAR GS748T Smart Switch.

Fast Ethernet Cable Guidelines

Fast Ethernet uses UTP cable, as specified in the IEEE 802.3u standard for 100BASE-TX.The specification requires Category 5 UTP cable consisting of either two-pair or four-pair twisted, insulated copper conductors bound in a single plastic sheath. Category 5 cable is certified up to 100 MHz bandwidth. 100BASE-TX operation uses one pair of wires for transmission and the other pair for receiving and for collision detection.

When installing Category 5 UTP cabling, use the following guidelines to ensure that your cables perform to the following specifications:

- Certification: Ensure that your Category 5 UTP cable has completed the Underwriters' Laboratories (UL) or Electronic Testing Laboratories (ETL) certification process.
- Termination method: To minimize cross-talk noise, maintain the twist ratio of the cable up to the point of termination; untwist at any RJ-45 plug or patch panel should not exceed 0.5 inch (1.5 cm).

Category 5 Cable

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

Category 5 Cable Specifications

Ensure that the fiber cable is crossed over to guarantee link.

Table C-1 lists the electrical requirements of Category 5 UTP cable.

Table C-1. Electrical Requirements of Category 5 Cable

Specifications	Category 5 Cable Requirements
Number of pairs	Four
Impedance	100 ± 15%
Mutual capacitance at 1 KHz	5.6 nF per 100 m
Maximum attenuation (dB per 100 m, at 20° C)	at 4 MHz: 8.2 at 31 MHz: 11.7 at 100 MHz: 22.0
NEXT loss (dB minimum)	at 16 MHz: 44 at 31 MHz: 39 at 100 MHz: 32

Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

Figure C-1 illustrates straight-through twisted pair cable.

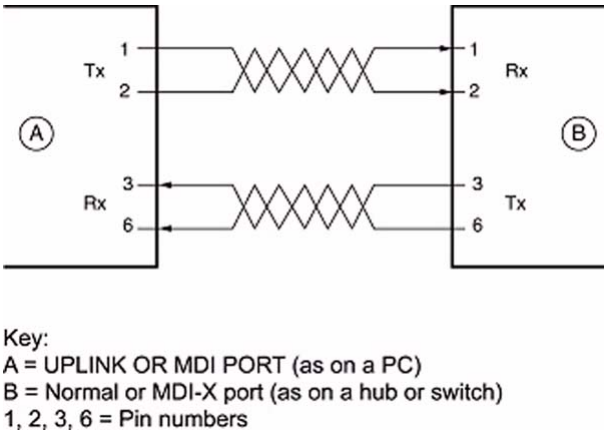

Figure C-1

Figure C-2 illustrates crossover twisted pair cable.

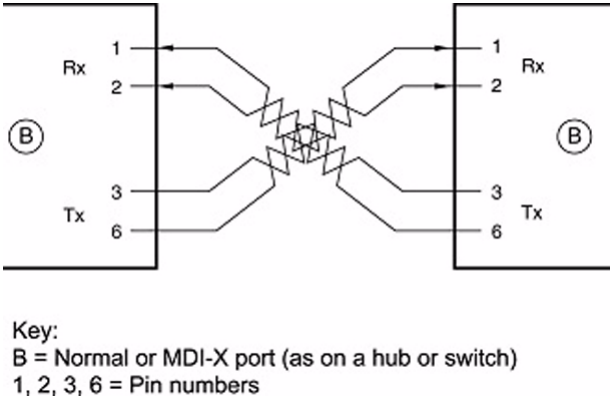

Figure C-2

Patch Panels and Cables

If you are using patch panels, make sure that they meet the 100BASE-TX requirements. Use Category 5 UTP cable for all patch cables and work area cables to ensure that your UTP patch cable rating meets or exceeds the distribution cable rating.

To wire patch panels, you need two Category 5 UTP cables with an RJ-45 plug at each end, as shown in Figure C-3.

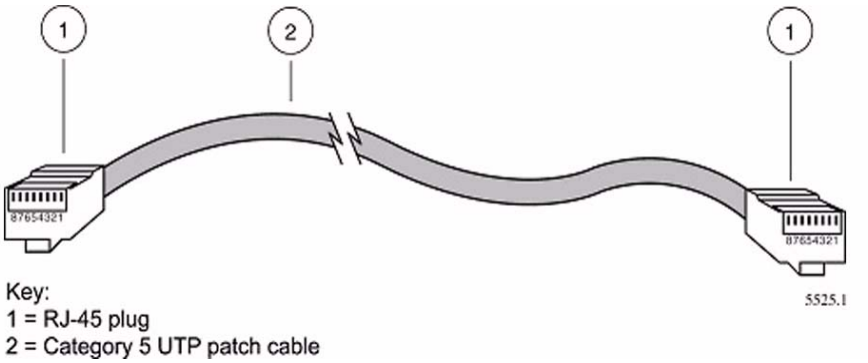

Figure C-3

	Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Using 1000BASE-T Gigabit Ethernet over Category 5 Cable

When using the new 1000BASE-T standard, the limitations of cable installations and the steps necessary to ensure optimum performance must be considered. The most important components in your cabling system are patch panel connections, twists of the pairs at connector transition points, the jacket around the twisted-pair cable, bundling of multiple pairs on horizontal runs and punch down blocks. All of these factors affect the performance of 1000BASE-T technology if not correctly implemented. The following sections are designed to act as a guide to correct cabling for 1000BASE-T.

Cabling

The 1000BASE-T product is designed to operate over Category 5 cabling. To further enhance the operation, the cabling standards have been amended. The latest standard is Category 5e, which defines a higher level of link performance than is available with Category 5 cable.

If installing new cable, we recommend using Category 5e cable, since it costs about the same as Category 5 cable. If using the existing cable, be sure to have the cable plant tested by a professional who can verify that it meets or exceeds either ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications.

Length

The maximum distance limitation between two pieces of equipment is 100 m, as per the original Ethernet specification. The end-to-end link is called the “channel.”

TSB-67 defines the “Basic Link” which is the portion of the link that is part of the building infrastructure. This excludes patch and equipment cords. The maximum basic link length is 295 feet (90 m).

Return Loss

Return loss measures the amount of reflected signal energy resulting from impedance changes in the cabling link. The nature of 1000BASE-T renders this measurement very important; if too much energy is reflected back on to the receiver, the device does not perform optimally.

Unlike 10BASE-T and 100BASE-TX, which use only two of the four pairs of wires within the Category 5, 1000BASE-T uses all four pairs of the twisted pair. Make sure all wires are tested — this is important.

Factors that affect the return loss are:

The number of transition points, as there is a connection via an RJ-45 to another connector, a patch panel, or device at each transition point.

Removing the jacket that surrounds the four pairs of twisted cable. It is highly recommended that, when RJ-45 connections are made, this is minimized to 1-1/4 inch (32 mm).

Untwisting any pair of the twisted-pair cabling. It is important that any untwisting be minimized to 3/8 inch (10 mm) for RJ-45 connections.

Cabling or bundling of multiple Category 5 cables. This is regulated by ANSI/EIA/TIA-568A-3. If not correctly implemented, this can adversely affect all cabling parameters.

Near End Cross Talk (NEXT)

This is a measure of the signal coupling from one wire to another, within a cable assembly, or among cables within a bundle. NEXT measures the amount of cross-talk disturbance energy that is detected at the near end of the link — the end where the transmitter is located. NEXT measures the amount of energy that is “returned” to the sender end. The factors that affect NEXT and cross talk are exactly the same as outlined in the Return Loss section. The cross-talk performance is directly related to the quality of the cable installation.

Patch Cables

When installing your equipment, replace old patch panel cables that do not meet Category 5e specifications. As pointed out in the NEXT section, this near end piece of cable is critical for successful operation.

RJ-45 Plug and RJ-45 Connectors

In a Fast Ethernet network, it is important that all 100BASE-T certified Category 5 cabling use RJ-45 plugs. The RJ-45 plug accepts 4-pair UTP or shielded twisted-pair (STP) 100-ohm cable and connects into the RJ-45 connector. The RJ-45 connector is used to connect stations, hubs, and switches through UTP cable; it supports 10 Mbps, 100 Mbps, or 1000 Mbps data transmission.

Figure C-4 shows an RJ-45 plug and RJ-45 connection with built-in LEDs.

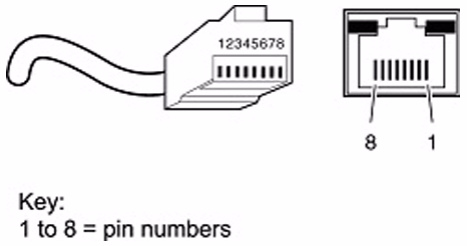

Figure C-4

Table C-2 lists the pin assignments for the 10/100 Mbps RJ-45 plug and the RJ-45 connector.

Table C-2. 0/100 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

Pin	Normal Assignment on Ports 1 to 8	Uplink Assignment on Port 8
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data –	Output Transmit Data –
3	Output Transmit Data +	Input Receive Data +
6	Output Transmit Data –	Input Receive Data –
4, 5, 7, 8	Internal termination, not used for data transmission	

Table C-2 lists the pin assignments for the 100/1000 Mbps RJ-45 plug and the RJ-45 connector.

Table C-3. 100/1000 Mbps RJ-45 Plug and RJ-45 Connector Pin Assignments

Pin	Channel	Description
1 2	A	Rx/Tx Data + Rx/Tx Data
3 6	B	Rx/Tx Data + Rx/Tx Data
4 5	C	Rx/Tx Data + Rx/Tx Data
7 8	D	Rx/Tx Data + Rx/Tx Data

Conclusion

For optimum performance of your 1000BASE-T product, it is important to fully qualify your cable installation and ensure that it meets or exceeds ANSI/EIA/TIA-568-A:1995 or ISO/IEC 11801:1995 Category 5 specifications. Install Category 5e cable where possible, including patch panel cables. Minimize transition points, jacket removal, and untwisted lengths. Cable bundles must be properly installed to meet the requirements in ANSI/EIA/TIA-568A-3.