Smart Switch Series Software Manual

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA
Phone 1-888-NETGEAR

July 2005

Trademarks

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.

Customer Support

For assistance with installing and configuring your NETGEAR system or with questions or problems following installation:

- Check the NETGEAR Web page at http://www.NETGEAR.com.
- Call Technical Support in North America at 1-888-NETGEAR. If you are outside North America, please refer to the phone numbers listed on the Support Information Card that shipped with your switch.
- Email Technical Support at support@NETGEAR.com.

Defective or damaged merchandise can be returned to your point-of-purchase representative.

NETGEAR maintains a World Wide Web home page that you can access at the uniform resource locator (URL) http://www.NETGEAR.com. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.

Contents

Chapter 1
About This Guide

Thank you for purchasing the NETGEAR™ Smart Switch Series Switch.

Audience

This reference manual assumes that the reader has basic-to-intermediate computer and Internet skills. However, basic computer network, Internet, and wireless technology tutorial information is provided in the Appendices.

This document describes configuration commands for the Smart Switch Series Switch software. The commands can be accessed from the CLI, telnet, and Web interfaces.

Why the Document was Created

This document was created primarily for system administrators configuring and operating a system using Smart Switch Series Switch software. It is intended to provide an understanding of the configuration options of Smart Switch Series Switch software.

It is assumed that the reader has an understanding of the relevant switch platforms. It is also assumed that the reader has a basic knowledge of Ethernet and networking concepts.

How to Use This Document

This document describes configuration commands for the Smart Switch Series Switch software. The commands can be accessed from the CLI, telnet (CMI), and Web interfaces.

- Chapter 4, “Administration Console Telnet Interface” describes the CMI.
- Chapter 4, “Web-Based Management Interface” describes the Web interface.
- Chapter 5, “Software Upgrade” describes the CLI, which can be reached through the telnet (CMI) interface.

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

Typographical Conventions

This guide uses the following typographical conventions:

Table 1. Typographical conventions

italics	Emphasis.
bold times roman	User input.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
SMALL CAPS	DOS file and directory names.

Special Message Formats

This guide uses the following formats to highlight special messages:

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

This manual is written for the Smart Switch Series Switch according to these specifications:

Table 1-1. Manual Specifications

Product Version	Smart Switch Series Switch
Manual Publication Date	July 2005

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://www.netgear.com/support/main.asp*.

Chapter 2
Switch Management Overview

This chapter gives an overview of switch management, including the methods you can use to manage your NETGEAR Smart Switch Series Switch. Topics include:

- Management Access Overview
- SNMP Access
- Protocols

Management Access Overview

Your NETGEAR Smart Switch contains software for viewing, changing, and monitoring the way it works. This management software is not required for the switch to work. You can use the 10/100 Mbps ports and the built-in Gigabit ports without using the management software. However, the management software allows you configure ports, VLAN and Trunking features and also improve the efficiency of the switch and, as a result, improve the overall performance of your network. The Switch gives you the flexibility to access and manage the switch using any of the following methods:

- Smartwizard Discovery Utility program
- Web browser interface

After you power-up the switch for the first time, you can configure it using a utility program called Smartwizard Discovery or a Web browser. Please refer to the screenshots in following pages for Smartwizard Discovery Utility and Web Management GUI. Each of these management methods has advantages. The table below compares the two management methods.

Table 2-1. Comparing Switch Management Methods

Management Method	Advantages	Disadvantages
SmartWizard Discovery Utility	• No IP address or subnet needed Show all switches on the network • User-friendly interface • Firmware upgradeable	• Not convenient for remote access
Web browser	• Can be accessed from any location via the switch's IP address • Password protected • Ideal for configuring the switch remotely • Compatible with Internet Explorer and Netscape Navigator Web browsers • Intuitive browser interface • Most visually appealing • Extensive switch configuration allowed • Configuration backup for duplicating settings to other switches	• Security can be compromised (hackers can attack if they know IP address) • May encounter lag times on poor connections • Displaying graphical objects over a browser interface may slow navigation
SNMP Agent	• Communicates with switch functions at the Management Information Base (MIB) level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Limited amount of information available • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Chapter 3
Getting Started

This chapter will walk you through the steps to start managing your switch. This chapter will cover how to get started in a network with a DHCP server (most common) as well as if you do not have a DHCP server.

For a Network with a DHCP Server

1. Connect the Smart Switch to a DHCP network.
2. Power on the Smart Switch by plugging in power cord.
3. Install the Smartwizard Discovery program on your computer
4. Start the Smartwizard Discovery utility. (Chapter 4 has detailed instructions on the Smartwizard Discovery utility)
5. Click Discover of the Smartwizard Discovery utility to find your switch. You should see a something similar to Figure 2-1.
6. Select your switch by clicking on it. Then click on Web Access, as highlighted in Figure 2-2.

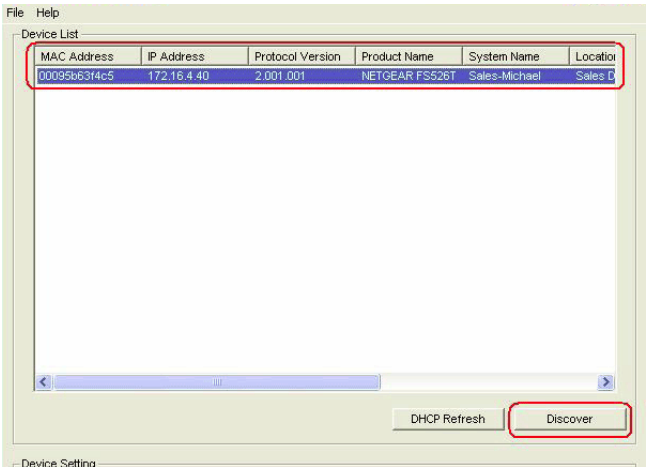


Figure 3-1: Smartwizard Discovery Utility > Discover

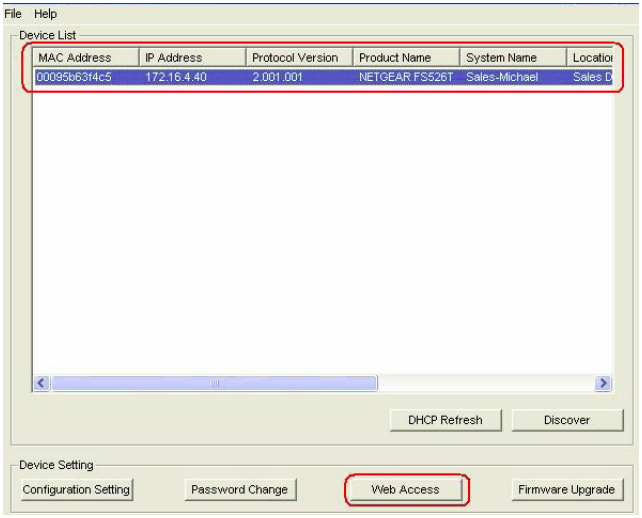


Figure 3-2: Smartwizard Discovery > Web Access

7. To manage your switch via your web browser, click **Web Access**. The main page below will display. The default password is **password**.

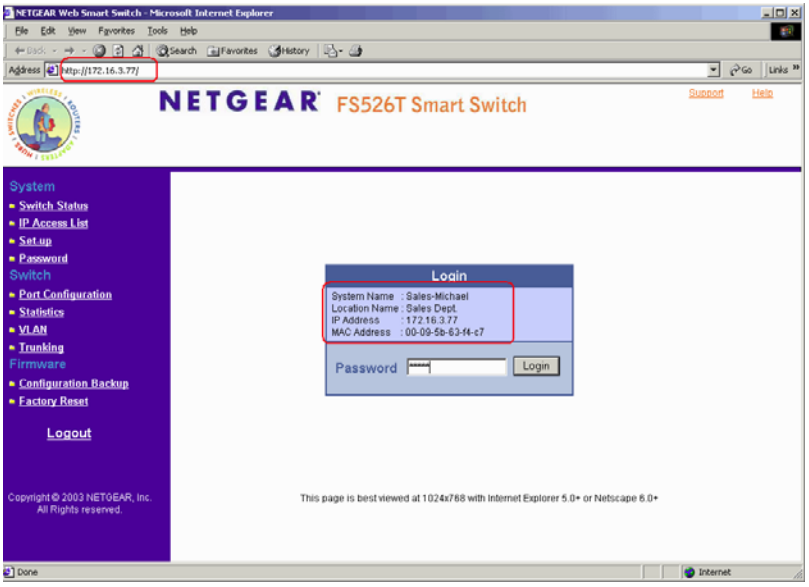


Figure 3-3: Web Management main page

For a Network without a DHCP Server

1. Connect your switch to your existing network.
2. Power on your switch by plugging in the power cord.
3. The default IP is 192.168.0.239.
4. Install the Smartwizard Discovery program on your PC.
5. Start the Smartwizard Discovery utility.
6. Click **Discover** to find your switch.
7. Click **Configuration Setting**.

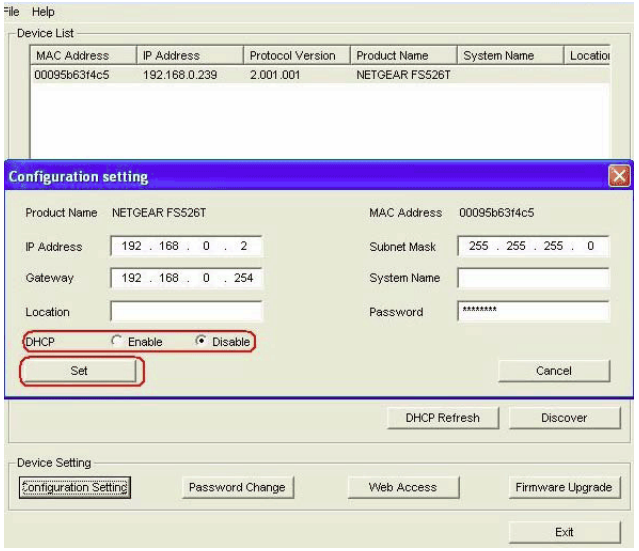


Figure 3-4: Assigning the switch a static IP address

8. Choose **Disable** on DHCP.
9. Enter your IP address, Gateway and Subnet. Then, type your password and click **Set**. Make sure your PC and your switch are in the same subnet.

Note: You can always assign a Static IP address to your switch no matter if your network has a DHCP server or not.

10. Select your switch by clicking on it. Then click **Web Access**.

11. To manage your switch via your web browser, click **Web Access**. The main page below will display. The default password is **password**.

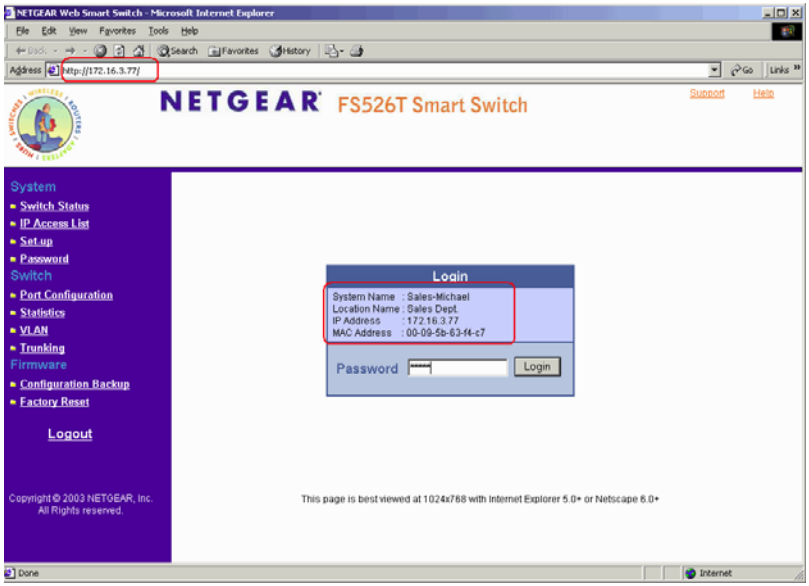
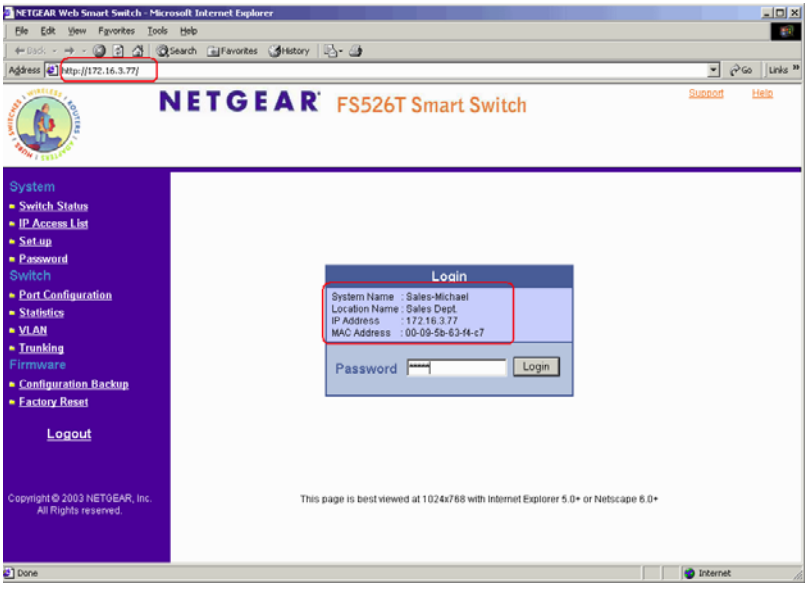


Figure 3-5: Web Management main page

Chapter 4
Web-Based Management Interface

Your NETGEAR Smart Switch series provides a built-in browser interface that lets you 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 will cover 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.



Note: Only one user can be logged in at any time.

There are 3 menu options available:

- System
- Switch
- Firmware

There is a Help Menu in the top of right side of screen. Click the help to read the full Help Menu. On some pages, there is a Help button. If you click that button, you will go to the part of the Help Menu that discusses that page.

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

Browse:	Locates a certain path for a desired file.
Refresh:	Pulls that screen's data from current values on the system
Apply:	Submits change request to system and refreshes screen data
Add:	Add new entries to table information and refreshes screen data
Delete:	Deletes selected entries from table and refreshes screen data
Factory Reset:	Restore the system factory default value.
Help:	Goes to relevant section of Help Menu

System Menu

There are 4 options available in the system menu:

- Switch Status
- IP Access List
- Setup
- Password

System> Switch Status Page

The Switch Status page displays the port settings for both 10/100 Mbps and 10/100/1000 Mbps ports. To configure the ports, go to the Switch> Port Configuration page.

- ID: The port number on the switch
- Speed: Indicates the communication mode set for the port. The default setting for all ports is Auto-negotiation (Auto). The possible entries are Auto-negotiation (Auto), 10 Mbps half duplex (10M Half), 10 Mbps full duplex (10M Full), 100 Mbps half duplex (100M Half), 100 Mbps full duplex (100M Full), or Disable.

- Flow Control: Indicates whether Flow Control support is set for on (Enabled) or off (Disabled). The default setting for all ports is enabled.
- Link Status: Indicates the current speed and duplex for the port. DOWN means no link.

The next part of the Switch Status page shows the Virtual Local Area Network (VLAN) status. A VLAN is a way to electronically separate specified ports on the same switch into separate broadcast domains. By using VLAN, users can group by logical function instead of physical location.

This page displays the port-based IEEE 802.1Q VLAN settings. The default VLAN setting is all ports belong to port-based VLAN 1. To configure user-defined VLAN groups, go to the Switch> VLAN page.

Port Trunking is a feature that allows multiple links between switches to work as one virtual link (aggregate link). Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, trunks can only be formed within the same bank.

This page displays the Trunk status. The default Trunk setting is all groups disabled. To configure user-defined TURNK groups, go to the Switch> Trunking page.

If the IEEE802.1Q VLAN is enabled, this page will display the Tagged VLAN status. To know more about Tag VLAN, see Switch> VLAN for details.

System> IP Access List Page

This page displays an IP access list, which lists switches that are allowed to login this Switch. The switch will only respond to requests from computers with the IP address in the list, so make sure you include your IP address if you are using this feature. This is a powerful way to limit remote access to your switch. The default setting is all host IP addresses allowed.

Note: Once this new IP access is enabled, you can only access the switch via this IP. Make sure that your new IP is the same of current PC.

System> Set-up Page

This page will allow access to the system information parameters.

- Enter Login Timeout. The default duration is 5 minutes.
- Enter System Name and Location Name

- The DHCP function is enabled by default. Click Static IP Address to disable the DHCP function.
- Enter site-specific IP address, Subnet mask and Gateway in the appropriate boxes
- Click Apply to activate the setting

System> Password Page

The password entered is encrypted on the screen and will display as a sequence of asterisks (*). The default password is 'password' and can be changed here.

- Type the old password in the Old Password field
- Type the new password in the New Password field
- Re-type the new password in the Re-type New Password field
- Click Apply to activate the new password

Note: The password is case sensitive and with a maximum length of 20.

Switch Menu

There are 4 options available:

- Port Configuration
- Statistics
- VLAN
- Trunking

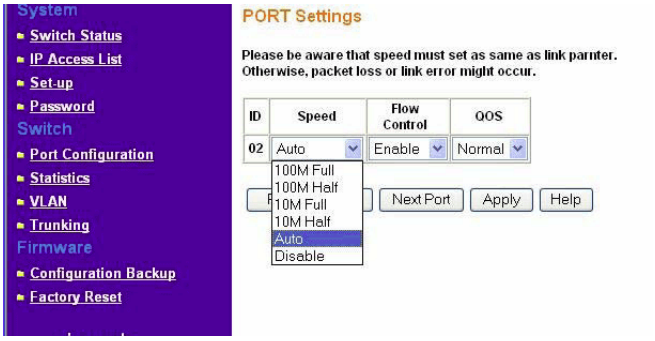
Switch> Port Configuration Page

You can configure the status per port by clicking a port ID at the port setting menu.

- ID: The port number on the switch. Click this number to configure the port.
- Speed: Indicates the communication mode set for the port. The default setting for all ports is Auto-negotiation (Auto). The possible entries are Auto-negotiation (Auto), 10 Mbps half duplex (10M Half), 10 Mbps full duplex (10M Full), 100 Mbps half duplex (100M Half), 100 Mbps full duplex (100M Full), or Disable.

- Flow Control: Indicates whether Flow Control support is set for on (Enabled) or off (Disabled). The default setting for all ports is enabled.
- Link Status: Indicates the current speed and duplex for the port. DOWN means no link.

Switch> Port Configuration: Set speed



- Click a port ID.
- Click to select a speed from the pull-down menu under Speed.
- Click Apply to activate the new speed.

Note: Please be aware that speed must set as same as link partner. Otherwise, packet loss or link error might occur.

Switch> Port Configuration: Set flow control

- Click a port ID.
- Click to select Enable or Disable from the pull-down menu under Flow Control.
- Click Apply to activate the new setting.

Switch> Statistics Page

The Statistics Table shows the statistics types for one port over time.

- ID: The port number on the switch
- Tx: Transmitted packet/s.
- Rx: Received packet/s.

- Tx Error: Transmitted packet/s with error.
- Rx Error: Received packet/s with error. Packets are counted as TX Error if they:
- Had a late collision detected during the transmission (512 bit-times into the transmission).
- Experienced 16 failed transmission attempts due to collision.
- Were dropped due to lack of resources. Packets are counted as RX Error if they:
- Were less than 64 bytes or greater than 1522 bytes?
- Had a bad FCS.
- Were dropped due to lack of resources.

Switch> Statistics> Refresh

Click Refresh to obtain current statistics data.

Switch> Statistics> Clear Counter

Click Clear Counter to start new statistics over time.

Switch> Statistics>Q0S Page

Indicate the priority for the port. Quality of Service (QoS) is a way of managing traffic in a network, by treating different types of traffic with different levels of priority. Higher priority traffic gets faster treatment during times of switch congestion.

The QoS page supports two types of QoS:

- Port-based QoS is the defualt option and the default setting for all ports is normal.
- IEEE802.1p-based QoS allows user to map different IEEE801.1p traffic to different levels of priority.

Switch> VLAN Page

A Virtual Local Area Network (VLAN) is a means to electronically separate ports on the same switch from a single broadcast domain into separate broadcast domains. By using VLAN, users can group by logical function instead of physical location.

The VLAN Table shows two types of VLAN and other information:

- IEEE 802.1Q VLAN (Tagged VLAN)
- Port-based VLAN
- ID: The port number on the switch
- Description: User-definable
- Member: Indicates which port/s belong to a VLAN group

Switch> VLAN> Port-based VLAN

Multiple port-based VLAN groups are supported on the switch, and any one port can belong to different VLAN groups. The number of supported port-based VLAN groups varies according to the switch model.

The default VLAN group port-based VLAN that have all ports belonging to VLAN 1.

Change members

- Click a VLAN ID
- Click to select port/s for VLAN members
- Click Apply to activate the new setting

Add VLAN

- Click Add VLAN.
- Enter a description for this VLAN
- Click to select port/s for VLAN members or click Set all to select all ports
- Click Clear all to unselect all ports
- Click Apply to activate the new setting

Delete VLAN

- Click Delete VLAN
- Click to select a VLAN ID
- Click Apply to confirm delete this VLAN

Switch> VLAN> IEEE802.1Q Tag VLAN

Depending on your model switch there are up to 64 static Tag VLAN groups supported on your switch. 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).

Click to select IEEE802.1Q VLAN. A screen pops up to confirm this change.

All ports are set belonging to VLAN 1 by default, all untagged.

From the page, you can create a new VLAN, add new ports to an existing VLAN, remove ports from an existing VLAN or, delete a VLAN.

Add a port to a VLAN Group

- Under the VLAN ID drop down menu, select the VLAN you want to edit.
- Click the box below the port number so that a ‘T’ (tagged) or ‘U’ (untagged) appears.
- Click Apply.

Remove a port from a VLAN Group

- Click the box again until a blank box appears. This will remove VLAN membership from the port.
- Click Apply.

Note: The default PVID of all ports is 1; therefore, you cannot remove any ports for the default Tag VLAN. It means that before removing any desired port from default Tag VLAN, changes PVID of such desired port to the PVID other than 1.

Create a new VLAN Group

- Under the VLAN ID drop down menu, select Add new VLAN.
- Enter the VLAN ID “2” in the provided fields. VLAN ID must be set within 2 ~ 4094.
- Add VLAN members if so desired; click the box below the port number so that a ‘T’ (tagged) or ‘U’ (untagged) appears.
- Click Apply.

Note: To allow untagged packets to participate in VLAN 2, make sure to change the Port VLAN Ids (PVID) for the relevant ports. Access the PVID Settings by using the VLAN ID drop down menu.

Delete a VLAN Group

- Under the VLAN ID drop down menu, select the VLAN you want to remove.
- Click to select Remove VLAN.
- Click Apply.

PVID Setting

All untagged packets entering the switch will by default be tagged with the port's Primary VLAN Identification (PVID). This screen allows you to specify the PVID for each port.

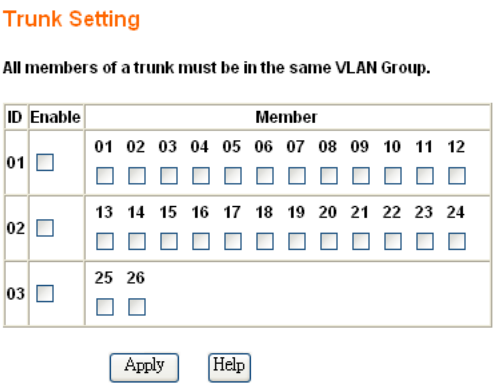
Take VLAN 2 for example: ports 5, 6, 7, and 8 have been checked as tagged ports for this VLAN. You must change the PVID value from "1" to "2" for those ports to avoid losing untagged packets when they are received.

Under the VLAN ID drop down menu, select PVID Setting. See below for an example of setting PVID for VLAN 2.

Change the PVID value of ports 5, 6, 7, and 8.

Click Apply.

Switch> Trunking Page



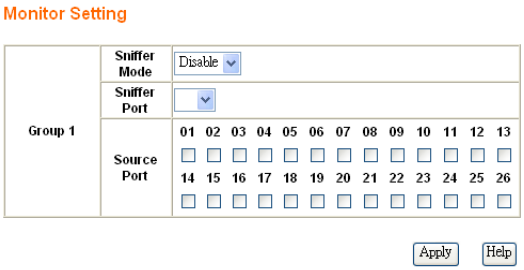
Port Trunking is a feature that allows multiple links between switches to work as one virtual link (aggregate link). Trunks can be defined for similar port types only. For example, a 10/100 port cannot form a Port Trunk with a gigabit port. For 10/100 ports, trunks can only be formed within the same bank. A bank is a set of eight ports, such as ports 1 to 8, ports 9 to 16, ports 17 to 24, or port 25 and port 26, on the same switch unit. Up to four trunks can be operating at the same time.

The Trunk Table shows all four trunking groups are set disabled by default. For each trunk group, trunk members are pre-set for selection.

To select Trunk members for a Trunk group, click Apply to activate the new setting

Note: The selected trunk port setting must set to the same VLAN group.

Switch> Monitor Page



The Monitor feature allows you to configure any port's incoming and/or outgoing traffic to be mirrored to a pre-defined sniffer port.

Sniffer Mode:

- .Disable - disable port mirroring globally.
- .RX - mirroring only the ingress traffic to the designated source ports.
- .TX - mirroring only the egress traffic to the designated source ports.
- Both - mirroring both incoming and outgoing traffic on the designated source ports.
- Sniffer Port: Select one from a pull-down menu.
- Source Ports: Select any number of ports to be monitored (mirrored). The ports can not be the Sniffer port

Switch> Advanced> Jumbo Frame

This page allows you to enable or disable the Jumbo Frame support. Jumbo Frames are not an approved standard Ethernet frame size, so you will need to ensure that all of your networking gear can support these non-standard Jumbo Frames to prevent them from being dropped. By clicking 'Help' button on this page, you can see the maximum frame size the switch can carry.

Switch> Advanced> Spanning Tree Page

- Fast Link: When a port running the standard Spanning Tree Protocol (STP) is connected, it will go through the STP negotiation (listening -> learning -> forwarding or blocking) before it will be fully available. If a server is trying to access a client through the switch running the STP negotiation, it will not be able to connect to it immediately. This can be a problem for some networks. Fastlink mode solves this problem by setting the port directly to forwarding mode, thus allowing any server access request to be forwarded. Fastlink mode can cause temporary loops in your network, but the STP will eliminate them. Fastlink is best used on end node ports, i.e. ports connected to PCs or servers, to avoid network loops.
- Bridge Priority: Priority setting of this switch in the Spanning Tree.
- Bridge Max Age: Amount of time before a configuration message is discarded by the system.
- Bridge Hello Time: Interval between configuration messages sent by the Spanning Tree algorithm.
- Bridge Forward Delay: Amount of time system spends in 'learning' and 'listening' states.
- Path Cost: The switch uses this to determine which port is the forwarding port. All other factors equal, the path with the lowest cost to the root bridge will be the active path.
- Path Priority: STP bases on this to determine the port to use for forwarding. The port with the lowest number has the highest priority.

Switch> Advanced> SNMP

SNMP page allows you to limit the IP address which can access the MIB of the switch and which the switch will send trap to. The switch will only respond to requests from computers with the IP address in the list. You can also select the traps which the switch will send to the hosts in the following trap events. The setting of a host will not be active until it is set to “Enable” in the Admin field.

Trap Events :

- Device bootup - The switch generates an SNMP trap when it reboots.
- 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.
- Link Up/Down - The switch generates an SNMP trap when one of its ports changes its link status.

Firmware Menu

There are 2 options available:

- Configuration Backup
- Factory Reset

Firmware> Configuration Backup Page

You can backup the system and switch settings to your workstation. This can help you to reconfigure the switch quickly if you have to re-set to factory defaults. Additionally, if you want to try out different configurations on the switch, this feature will enable you to quickly return to a previous configuration.

If you own several switches and you want them to have the same configuration, you can use this feature to duplicate the settings to each switch.

Saving your Backup file:

- Click Backup to store the current setting to a file in your PC.
- Follow the instructions on the screen to select where you want to store your Backup file. Restoring your Backup file (or using a duplicate configuration):
- Click Restore to recover the Backup file from your PC to the current switch. If you do not want to type in the path name, click Browse to find the Backup file.
- Click OK in the File Download dialog box.
- When download process is finished, click OK to confirm disconnection of current browser connection.

Note: Please be aware that the switch will reboot after a successful restore.
Note: The Backup file does not affect the password and MAC address of the switch

Firmware> Factory Reset Page

You can always reset the switch to default values by using this function.

- Click Factory Reset to enable this function
- When reset process is finished, click OK to confirm disconnection of current browser connection as shown in Figure 5-34.

Note: Please be aware that the switch will reboot after a successful reset.

Logout

When finished with all configuration and settings, click Logout to disconnect the current browser connection. The login page will pop up.

Chapter 5
Software Upgrade

The application software for the Smart 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 in the following section. The upgrade procedure is as follows:

1. Save the new firmware to your computer.
2. Start the Smartwizard Discovery utility program.
3. Select your switch by clicking on it.
4. Then click **Firmware Upgrade**.
5. Enter the location of the new firmware in the Firmware path below Firmware setting. Alternatively, you can click Browse to locate the file.
6. Click **Start** to download the new firmware file in non-volatile memory.

Note: Once the system finishes firmware upgrade process, the switch will automatically reboot. The Smartwizard Discovery utility will determine success of upgrade process based on the success of the system reboot.

Appendix B
IEEE 802.1Q Virtual Local Area Network (VLAN)

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 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 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 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 will be treated in the following way:

- When an untagged packet enters a port, it will be 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 PVID Setting page.
- When a tagged packet enters a port, the tag for that packet will be unaffected by the default VLAN ID Setting.
- The packet will now proceed to the VLAN specified by its VLAN ID 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 will be dropped.
- If the port has membership to the VLAN specified by the packet's VLAN ID, the packet will be able to be sent to other ports with the same VLAN ID membership.
- Packets leaving the switch will be 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 will be Untagged. Inversely, a 'T' for a given port means that packets leaving the switch from that port will be tagged with the respective VLAN ID in which it participated in.

The example given in this section will step through a more elaborate setup illustrating all possible scenarios for a comprehensive understanding of tagged VLANs.

Example

This example demonstrates several scenarios of VLAN use and how the switch will handle 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 scenarios will produce results as described below:

   (1). If an untagged packet enters Port 1, the switch will tag it with a VLAN tag value 10. The packet will have access to Port 2 and Port 3. The outgoing packet will be stripped away its tag becoming an untagged packet as it leaves Port 2. For Port 3, the outgoing packet will leave as a tagged packet with a VLAN tag value 10.

   (2). If a tagged packet with a VLAN tag value 10 enters Port 3, the packet will have access to Port 1 and Port 2. If the packet leaves Port 1 and/or Port 2, it will be stripped away its tag becoming an untagged packet as it leaves switch.

   (3). If an untagged packet enters Port 4, switch will tag it with a VLAN tag value 20. The packet will have access to Port 5 and Port 6. The outgoing packet will be stripped away its tag becoming an untagged packet as it leaves Port 6. For Port 5, the outgoing packet will leave as a tagged packet with a VLAN tag value 20.

Appendix C
Port-Based VLAN

Port-based VLAN will help efficiently confine the broadcast traffic to the switch ports. This switch allows up to 26 port-based VLAN groups, any one port can belong to different VLAN groups. The default VLAN group port-based VLAN that have all ports belonging to VLAN 1.

Port-based VLANs

Packets received by the switch will be treated in the following way:

- When a packet enters a port, it only can proceed to the VLAN which the port belongs to. The packet will be able to be sent to other ports with the same VLAN ID membership.
- If the port in which the packet entered does not have membership with the same VLAN as the source port does, the packet will be dropped.

Example

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 group except port 25.

- Ports 7 and 8 are kept for the usage of connecting file server and printer server. Sales and Marketing departments can share file archives and printing services.
- Port 25 provides Gigabit speed for email 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.

Scenarios:

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 email, 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 will not be affected by the message, as it will not go out on their ports. Only the Marketing department and the IT group will get the broadcast message.

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

Appendix D
Cabling Guidelines

This appendix provides specifications for cables used with a NETGEAR Smart Switch Series 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
Make sure 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 F-1 lists the electrical requirements of Category 5 UTP cable.

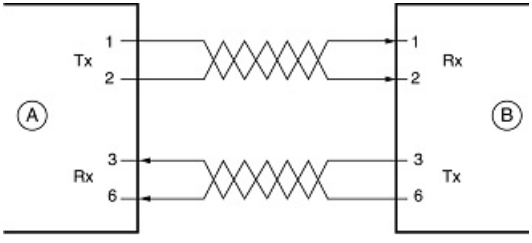
Table-D-1. Electrical Requirements of Category 5 Cable

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 D-1 illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure D-1: Straight-Through Twisted-Pair Cable

Figure D-2 illustrates crossover twisted pair cable.

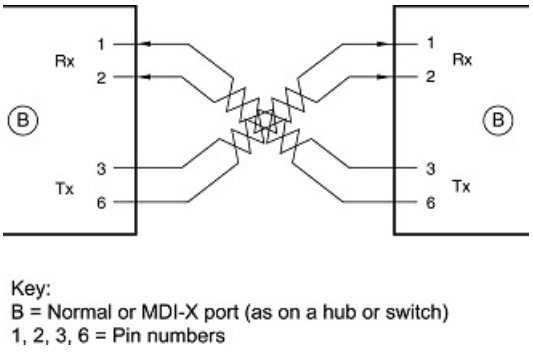


Figure D-2: Crossover Twisted-Pair Cable

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 here.

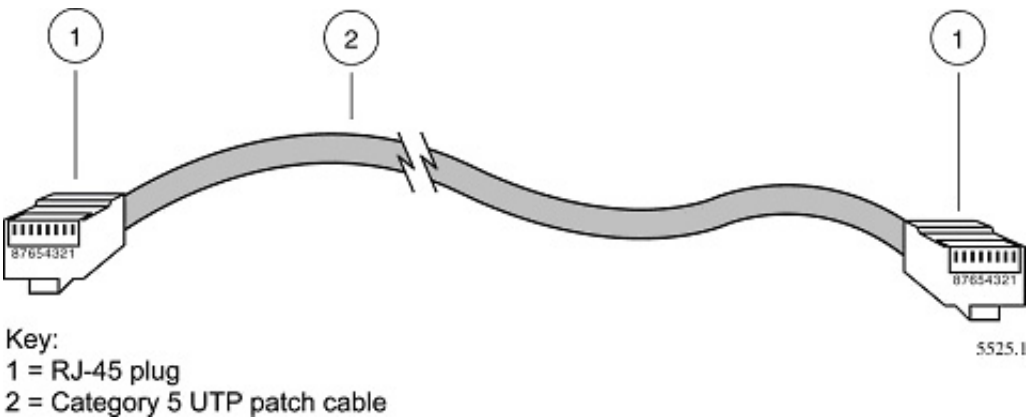


Figure D-3: Category 5 UTP Cable with Male RJ-45 Plug at Each End

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 D-4 shows the RJ-45 plug and RJ-45 connector.

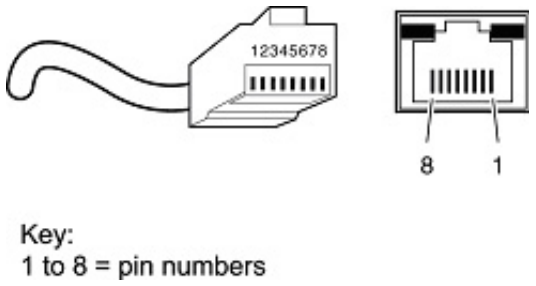


Figure D-4: RJ-45 Plug and RJ-45 Connector with Built-in LEDs

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

Table-D-2. 10/100 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 E-2 lists the pin assignments for the 100/1000 Mbps RJ-45 plug and the RJ-45 connector.

Table-D-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 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 untwist lengths. Bundling of cables must be properly installed to meet the requirements in ANSI/EIA/TIA-568A-3.

Appendix A
Default Settings

This appendix provides default settings for the NETGEAR Smart Switches. You can always configure the switch to default settings by using the Factory Reset function from a Web browser.

Table A-1. Default Settings

FEATURE	DEFAULT SETTING
Port Speed	Auto-negotiation
Port Duplex	Auto-negotiation
Flow Control (half duplex)	Enabled
Flow Control (full duplex)	Enabled
IP Configuration	DHCP enabled
Password	password
VLAN	Port-Based VLAN
Link Aggregation (Trunk)	Disabled
Traffic Prioritization (QoS)	Optimized for flow control, all ports set normal priority

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

V

W

Z