

NETGEAR[®]

26 PORT

10/100Mbps

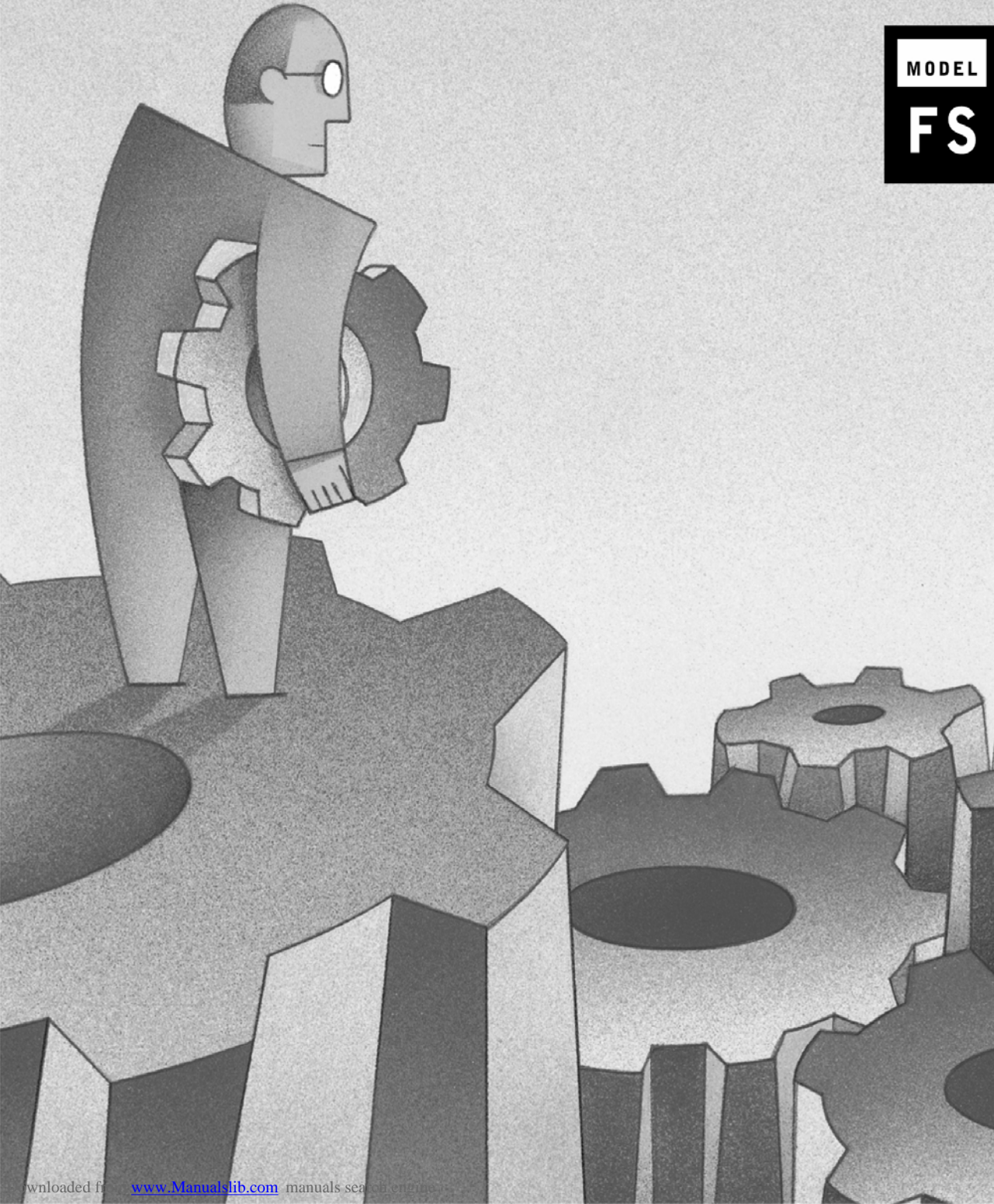
Smart Fast Ethernet Switch

User's Manual

MODEL

FS

526^T



Trademarks

@2003 NETGEAR, Inc. NETGEAR, the Netgear logo, The Gear Guy and Everybody's connecting are trademarks of Netgear, Inc. in the United States and/or other countries. Other brand and product names are trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

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 NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports has been suppressed in accordance with the conditions set out in the BMPT-AmtsbVfg 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.

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.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the first category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

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

This device may not cause harmful interference.

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

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

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

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

EN 55 022 Declaration of Conformance

This is to certify that the NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55024 Class A (CISPR 22).

EN 55 022 and EN 55 024 Statements

This is to certify that the NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22) and EN 55 024.



Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take appropriate measures.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports) do not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

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.

Internet/World Wide Web

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: SWITCH MANAGEMENT OVERVIEW	7
<i>Management Access Overview</i>	<i>7</i>
CHAPTER 2: GETTING STARTED	8
NETWORK WITH DHCP SERVER:	8
<i>GearDiscovery > Discover</i>	<i>8</i>
<i>GearDiscovery > Web Access</i>	<i>9</i>
<i>Web Management</i>	<i>10</i>
NETWORK WITHOUT DHCP SERVER	11
<i>GearDiscovery > Configuration Setting > Default</i>	<i>11</i>
<i>GearDiscovery > Configuration Setting > Assign Static IP</i>	<i>12</i>
<i>NIC setting on the PC that accesses FS526T</i>	<i>13</i>
<i>Web Management</i>	<i>14</i>
CHAPTER 3: SOFTWARE UPGRADE PROCEDURE	15
CHAPTER 4: GEARDISCOVERY UTILITY PROGRAM	17
<i>Main Screen</i>	<i>17</i>
<i>Main Screen> Device List> Discover</i>	<i>18</i>
<i>Main Screen> Switch Setting> Configuration Setting</i>	<i>19</i>
<i>Main Screen> Switch Setting> Password Change</i>	<i>19</i>
<i>Main Screen> Switch Setting> Web Access</i>	<i>20</i>
<i>Main Screen> Switch Setting> Firmware Upgrade</i>	<i>21</i>
<i>Main Screen> Switch Setting> Exit</i>	<i>21</i>
CHAPTER 5: WEB MANAGEMENT ACCESS	22
<i>System</i>	<i>23</i>
<i>System> Switch Status</i>	<i>23</i>
<i>System> IP Access List</i>	<i>28</i>
<i>System> Set-up</i>	<i>30</i>
<i>System> Password</i>	<i>31</i>
<i>Switch</i>	<i>32</i>
<i>Switch> Port Configuration</i>	<i>32</i>
<i>Switch> Statistics</i>	<i>36</i>
<i>Switch> VLAN</i>	<i>37</i>
<i>Switch> VLAN> Port-based VLAN</i>	<i>37</i>
<i>Switch> VLAN> IEEE802.1Q Tag VLAN</i>	<i>40</i>
<i>Switch> Trunking</i>	<i>45</i>
<i>Firmware</i>	<i>47</i>
<i>Firmware> Configuration Backup</i>	<i>47</i>
<i>Firmware> Factory Reset</i>	<i>49</i>
<i>Logout</i>	<i>50</i>
APPENDIX A: DEFAULT SETTINGS	51
APPENDIX B: VIRTUAL LOCAL AREA NETWORK (VLAN) IEEE 802.1Q	52
APPENDIX C: VIRTUAL LOCAL AREA NETWORK (VLAN): PORT-BASED VLAN	57

Figures

FIGURE 2-1. GEARDISCOVERY UTILITY MAIN SCREEN.....	8
FIGURE 2-2. WEB ACCESS.....	9
FIGURE 2-3. WEB MANAGEMENT FRONT PAGE AFTER CLICK “WEB ACCESS” ON GEARDISCOVERY UTILITY.....	10
FIGURE 2-4. CONFIGURATION SETTING.....	11
FIGURE 2-5. MANUALLY SETTING IP ADDRESS.....	12
FIGURE 2-6. SETTING IP ADDRESS AND SUBNET MASK.....	13
FIGURE 2-7. WEB MANAGEMENT FRONT PAGE AFTER CLICK “WEB ACCESS” ON GEARDISCOVERY UTILITY.....	14
FIGURE 3-1. SELECT THE SWITCH YOU WANT TO UPGRADE AND CLICK FIRMWARE UPGRADE.....	15
FIGURE 3-2. LOCATE NEW FIRMWARE.....	16
FIGURE 3-3. ENTER PASSWORD AND CLICK START.....	16
FIGURE 4-1. GEARDISCOVERY UTILITY MAIN SCREEN.....	17
FIGURE 4-2. MAIN SCREEN: DEVICE LIST> DISCOVER.....	18
FIGURE 4-3. MAIN SCREEN: SWITCH SETTING> CONFIGURATION SETTING.....	19
FIGURE 4-4. MAIN SCREEN: SWITCH SETTING> PASSWORD CHANGE.....	19
FIGURE 4-5. WEB MANAGEMENT LOGIN PAGE.....	20
FIGURE 4-6. MAIN SCREEN: SWITCH SETTING> FIRMWARE UPGRADE.....	21
FIGURE 5-1. WEB MANAGEMENT LOGIN PAGE.....	22
FIGURE 5-2. SYSTEM> SWITCH STATUS: SWITCH STATUS.....	23
FIGURE 5-3. SYSTEM> SWITCH STATUS: PORT STATUS.....	24
FIGURE 5-4. SYSTEM> SWITCH STATUS: PORT-BASED VLAN & TRUNK.....	25
FIGURE 5-5. SYSTEM> SWITCH STATUS: TAG VLAN PVID TABLE.....	26
FIGURE 5-6. SYSTEM> SWITCH STATUS: TAG VLAN SETTINGS.....	27
FIGURE 5-7. SYSTEM> IP ACCESS LIST.....	28
FIGURE 5-8. SYSTEM> IP ACCESS LIST> ADD NEW IP.....	29
FIGURE 5-9. SYSTEM> SET-UP> SYSTEM SETTING.....	30
FIGURE 5-10. SYSTEM> PASSWORD> PASSWORD SETTING.....	31
FIGURE 5-11. SWITCH> PORT CONFIGURATION> PORT SETTING MENU.....	32
FIGURE 5-12. SWITCH> PORT CONFIGURATION> PORT SETTINGS: SPEED.....	33
FIGURE 5-13. SWITCH> PORT CONFIGURATION> PORT SETTINGS: FLOW CONTROL.....	34
FIGURE 5-14. SWITCH> PORT CONFIGURATION> PORT SETTINGS: QOS.....	35
FIGURE 5-15. SWITCH> STATISTICS.....	36
FIGURE 5-16. SWITCH> VLAN.....	37
FIGURE 5-17. SWITCH> VLAN SETTING> PORT-BASED VLAN: ADD GROUP.....	38
FIGURE 5-18. SWITCH> VLAN SETTING> PORT-BASED VLAN: DELETE GROUP.....	39
FIGURE 5-19. SWITCH> VLAN SETTING> TAG VLAN.....	40
FIGURE 5-20. SWITCH> VLAN SETTING> TAG VLAN: DEFAULT.....	40
FIGURE 5-21. SWITCH> VLAN SETTING> TAG VLAN MENU.....	41
FIGURE 5-22. SWITCH> VLAN SETTING> TAG VLAN: ADD NEW VLAN.....	42
FIGURE 5-23. SWITCH> VLAN SETTING> TAG VLAN: DELETE A VLAN.....	43
FIGURE 5-24. SWITCH> VLAN SETTING> TAG VLAN: PVID SETTING.....	44
FIGURE 5-25. SWITCH> TRUNK SETTING.....	45
FIGURE 5-26. SWITCH> TRUNK SETTING: TRUNK GROUP 01.....	46
FIGURE 5-30. FIRMWARE> CONFIGURATION BACKUP> BACKUP SETTING: BACKUP.....	47
FIGURE 5-31. FIRMWARE> CONFIGURATION BACKUP> BACKUP SETTING: RESTORE.....	48
FIGURE 5-32. FIRMWARE> CONFIGURATION BACKUP> BACKUP SETTING: REBOOT.....	48
FIGURE 5-33. FIRMWARE> FACTORY RESET.....	49
FIGURE 5-34. FIRMWARE> FACTORY RESET: REBOOT.....	50

Tables

TABLE 1-1. COMPARING SWITCH MANAGEMENT METHODS.....	7
TABLE A-1. DEFAULT SETTINGS.....	51

CHAPTER 1: SWITCH MANAGEMENT OVERVIEW

This chapter gives an overview of switch management, including the methods you can use to manage your NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports. Topics include:

Management Access Overview

Management Access Overview

Your NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports 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:

GearDiscovery Utility program

Web browser interface

After you power-up the switch for the first time, you can configure it using a utility program called GearDiscovery or a Web browser. Please refer to the screenshots in following pages for GearDiscovery Utility and Web Management GUI. Each of these management methods has advantages. Table 1-1 compares the three management methods.

Table 1-1. Comparing Switch Management Methods

Management Method	Advantages
GearDiscovery Utility program	<ul style="list-style-type: none">■ No IP address or subnet needed■ Show all switches on the network■ User-friendly interface■ Firmware upgradeable
Web browser	<ul style="list-style-type: none">■ 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■ More visually appealing■ Extensive switch configuration allowed■ Configuration backup for duplicating settings to other switches

For a more detailed discussion of the GearDiscovery Utility Program, see chapter 4. For a more detailed discussion of the Web Browser Interface, see chapter 5.

CHAPTER 2: Getting Started

This chapter will walk you through the steps to start managing your FS526T 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.

Network with DHCP server:

1. Connect FS526T to a DHCP network.
2. Power on FS526T by plugging in power cord.
3. Install GearDiscovery Utility program on your computer
4. Start GearDiscovery utility. (Chapter 4 has detailed instructions on the GearDiscovery utility)
5. Click Discover for the GearDiscovery to find your FS526T switch. You should see a something similar to Figure 2-1.

GearDiscovery > Discover

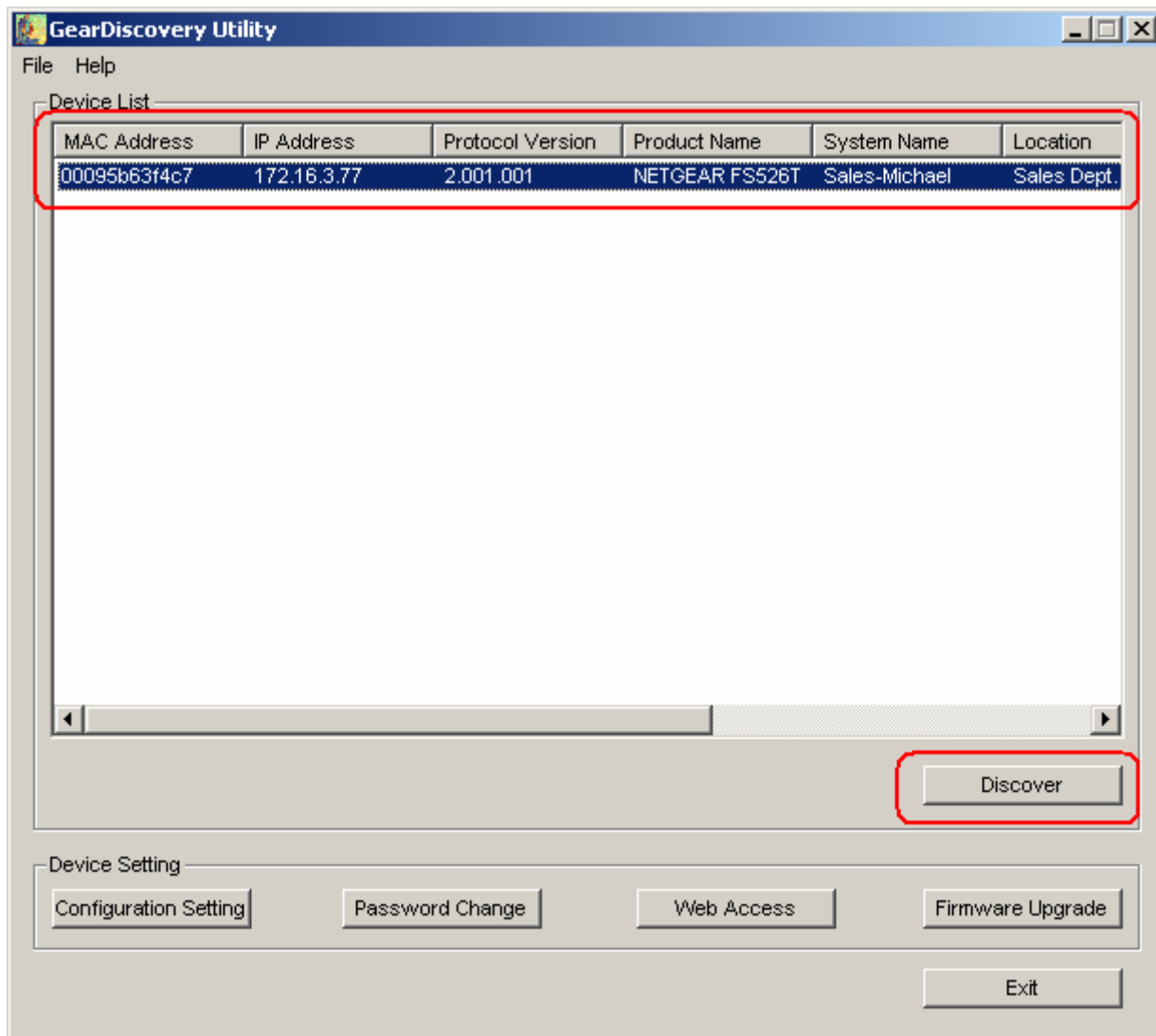


Figure 2-1. GearDiscovery Utility Main Screen

6. Select your switch by clicking on it. Then click on Web Access, as highlighted in Figure 2-2.

Note: Your PC must be in the same subnet as the switch to use a web browser to manage the switch.

GearDiscovery > Web Access

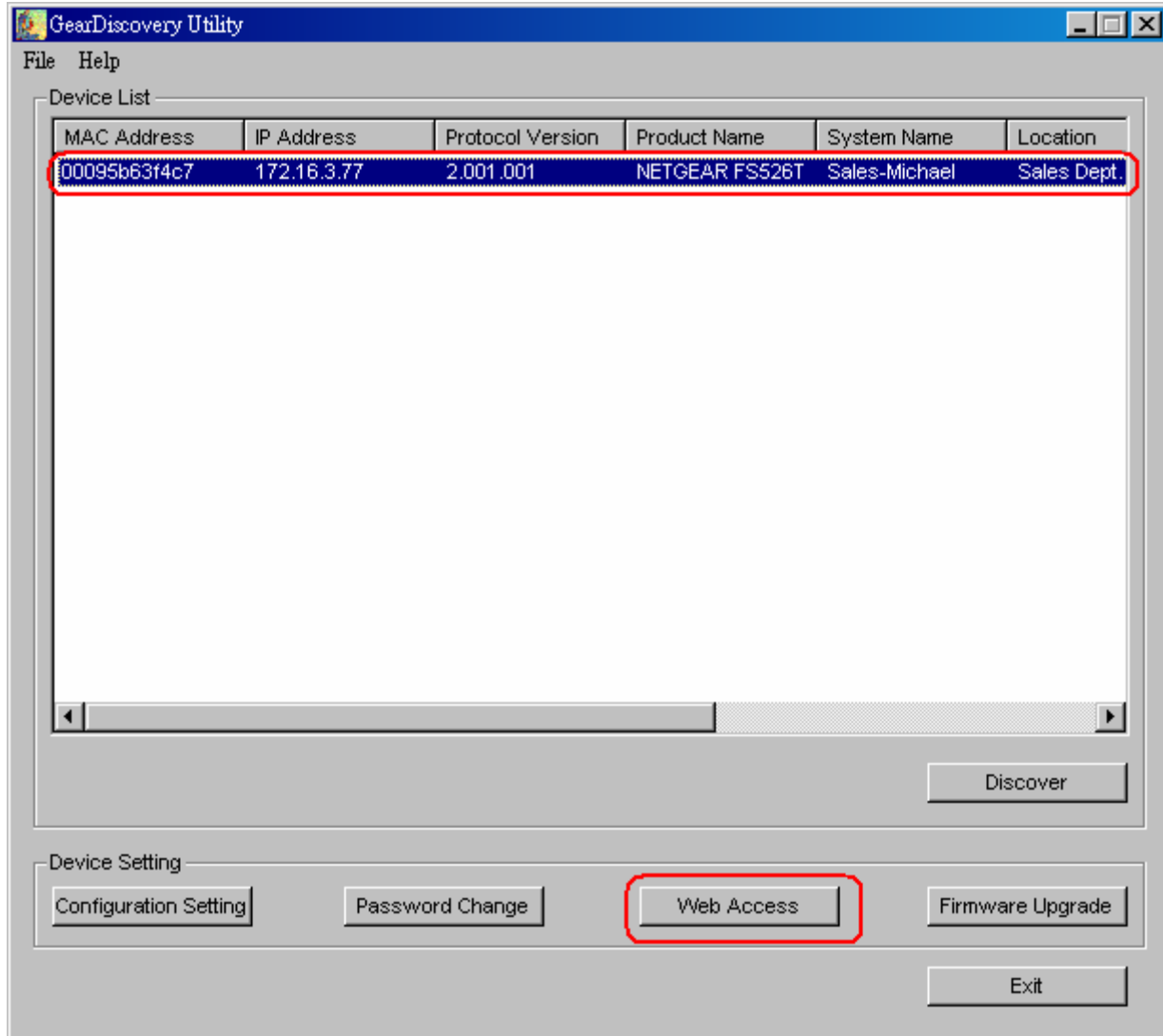


Figure 2-2. Web Access

7. Start managing your switch via your web browser. The default password is 'password'. For a detailed description on web management, please refer to Chapter 5.

Web Management

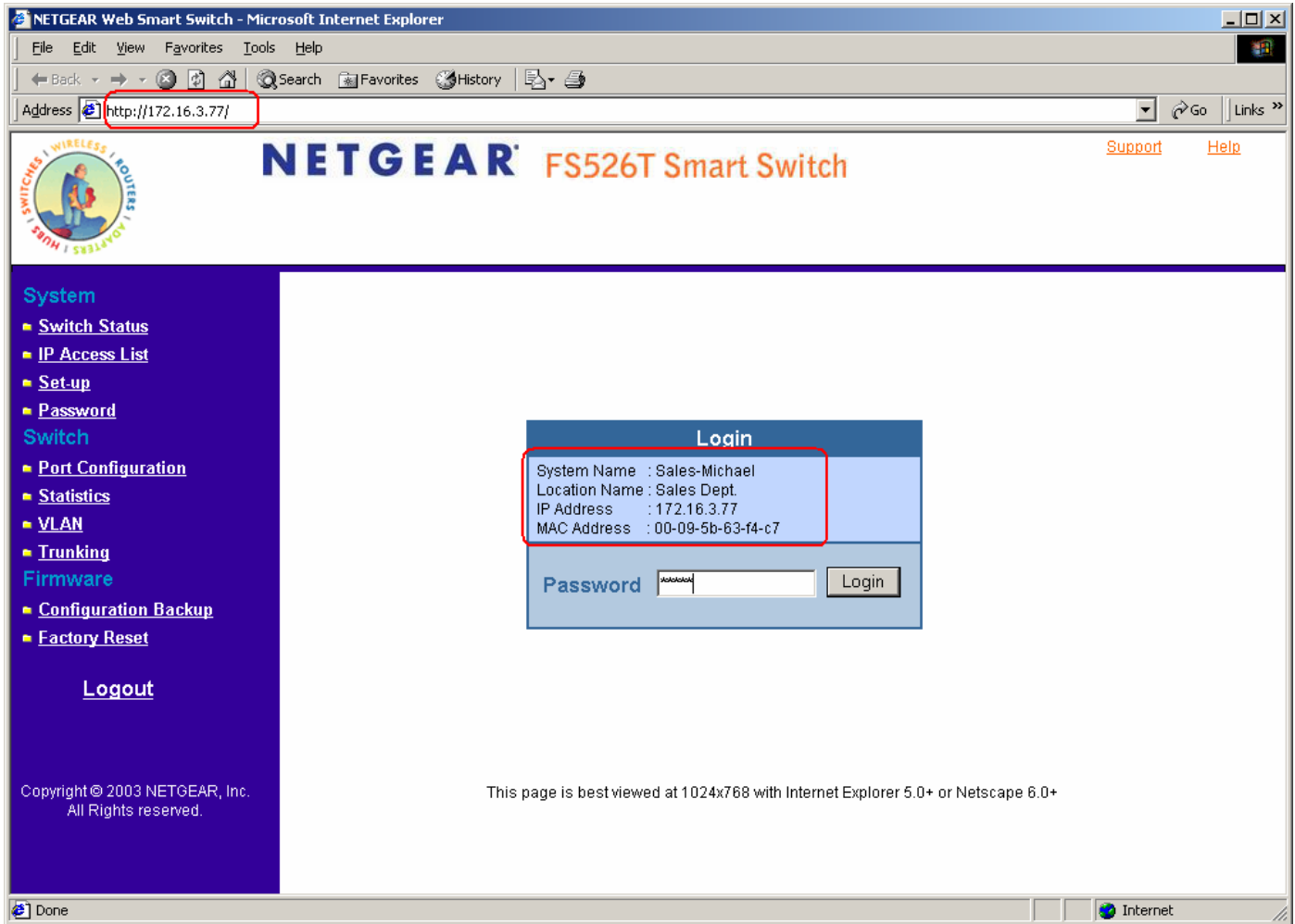


Figure 2-3. Web Management Front page after click “web access” on GearDiscovery utility

Network without DHCP server

1. Connect FS526T to your existing network.
2. Power on FS526T by plugging in power cord.
3. Install GearDiscovery Utility program on your computer.
4. Start GearDiscovery Utility. (Default IP is 192.168.0.239. Chapter 4 has detailed instructions on the GearDiscovery Utility)
5. Click Discover for the GearDiscovery program to find your FS526T switch. You should see a something similar to Figure 2-1.
6. Click on Configuration Setting (See figure 2-4).

Note: You can always assign a Static IP address to your FS526T whether or not your network has a DHCP server.

GearDiscovery > Configuration Setting > Default

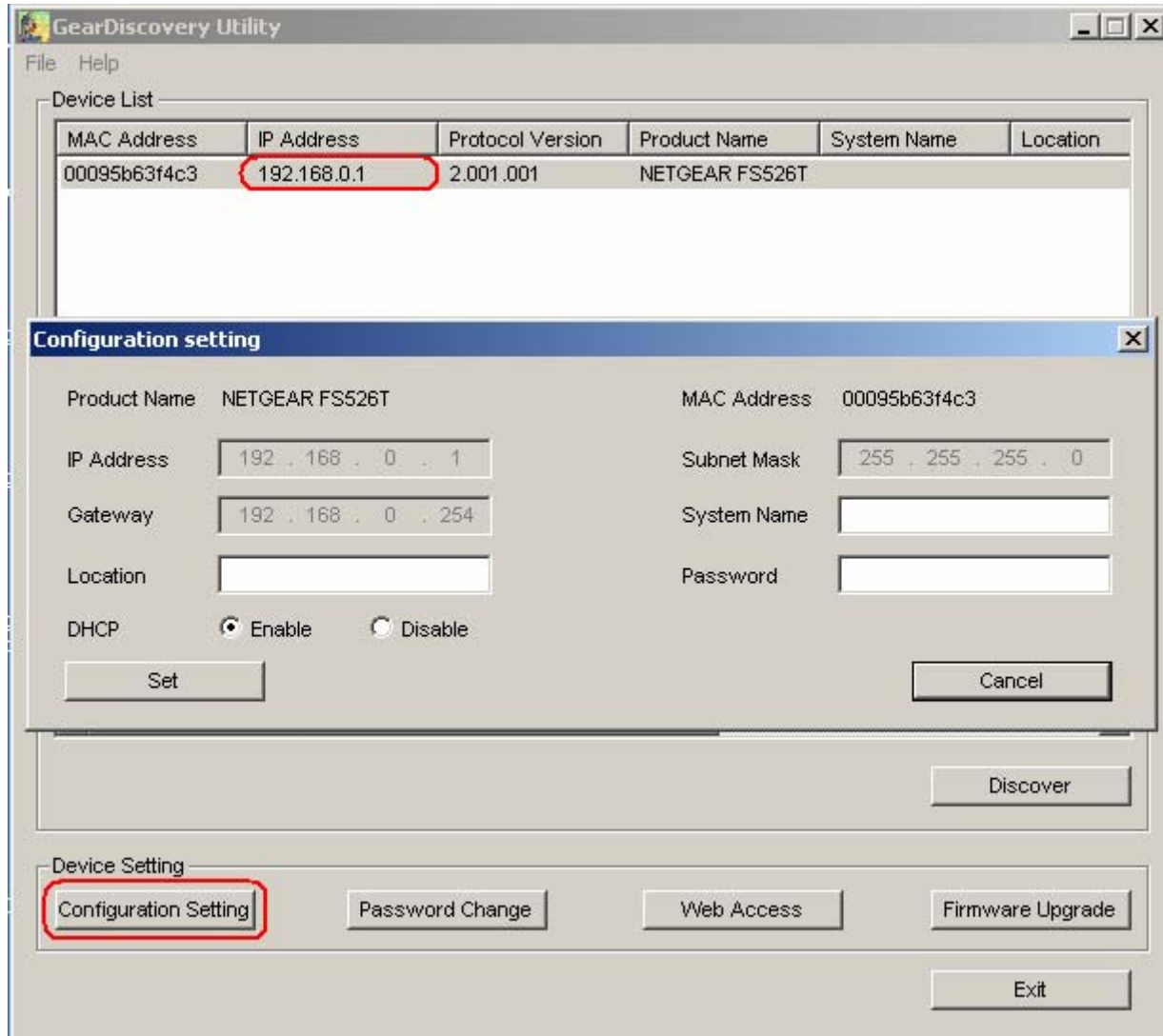


Figure 2-4. Configuration Setting

7. Choose Disable on DHCP. See Figure 2-5.
8. Enter your IP address, Gateway and Subnet, and then type your password and click "Set". Please make sure your PC and FS526T are in the same subnet. (See Figure 2-6.)

GearDiscovery > Configuration Setting > Assign Static IP

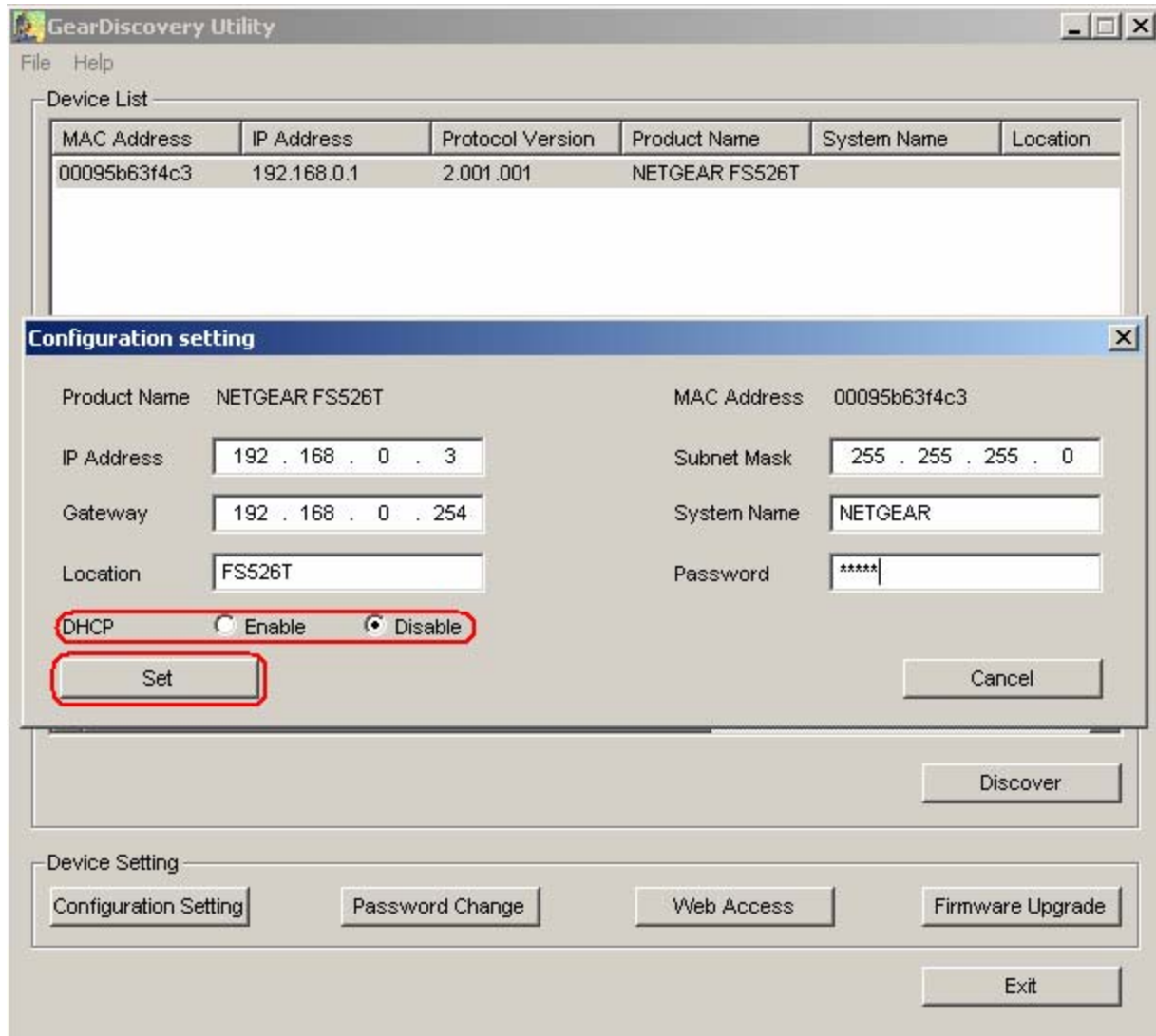


Figure 2-5. Manually setting IP address

NIC setting on the PC that accesses FS526T

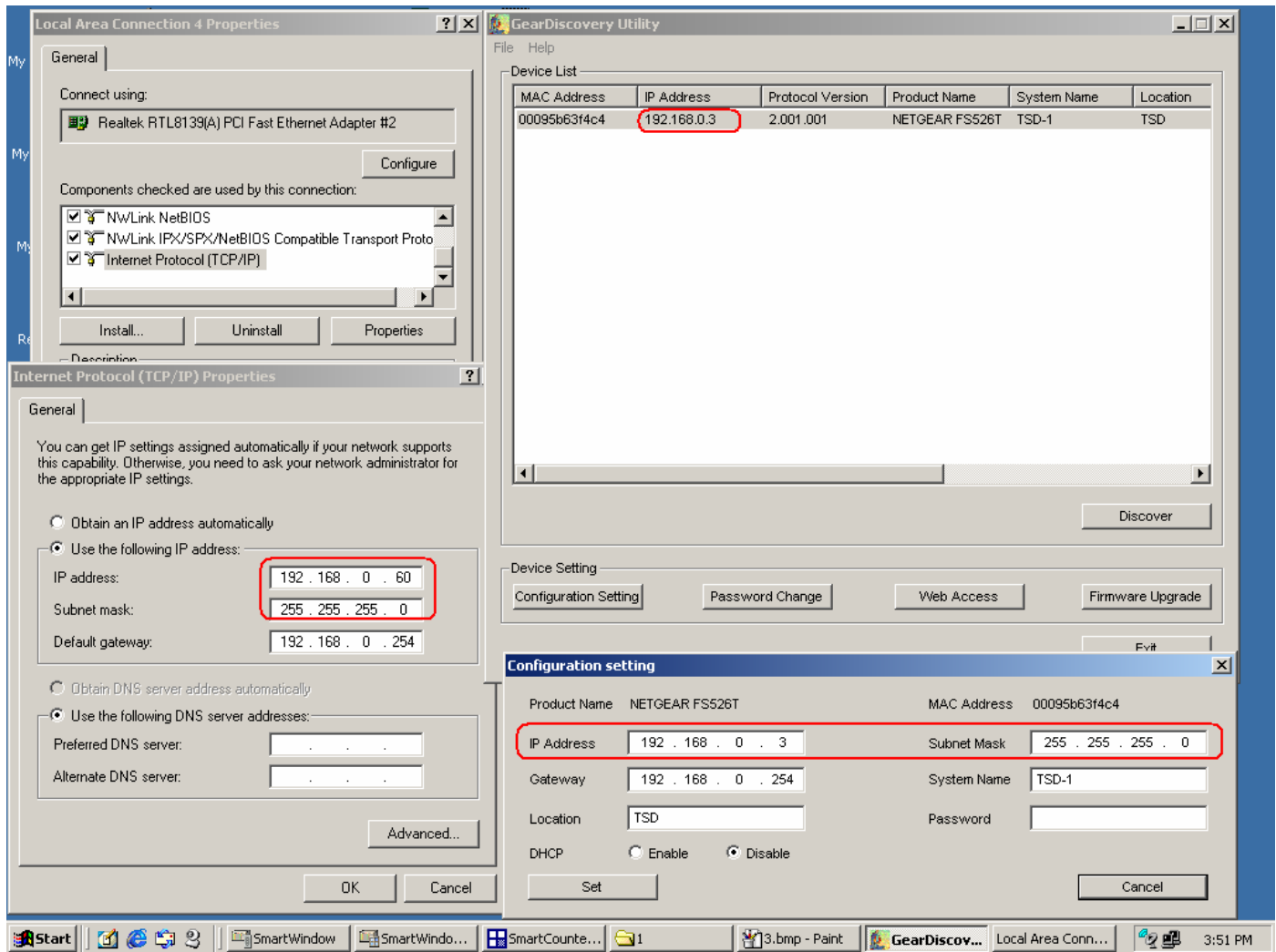


Figure 2-6. Setting IP address and Subnet Mask

9. Select your switch by clicking on it. Then click on Web Access, as highlighted in Figure 2-2.
10. Start managing your switch via your web browser. The default password is 'password'. For a detailed description on web management access, please refer to Chapter 5.

Web Management

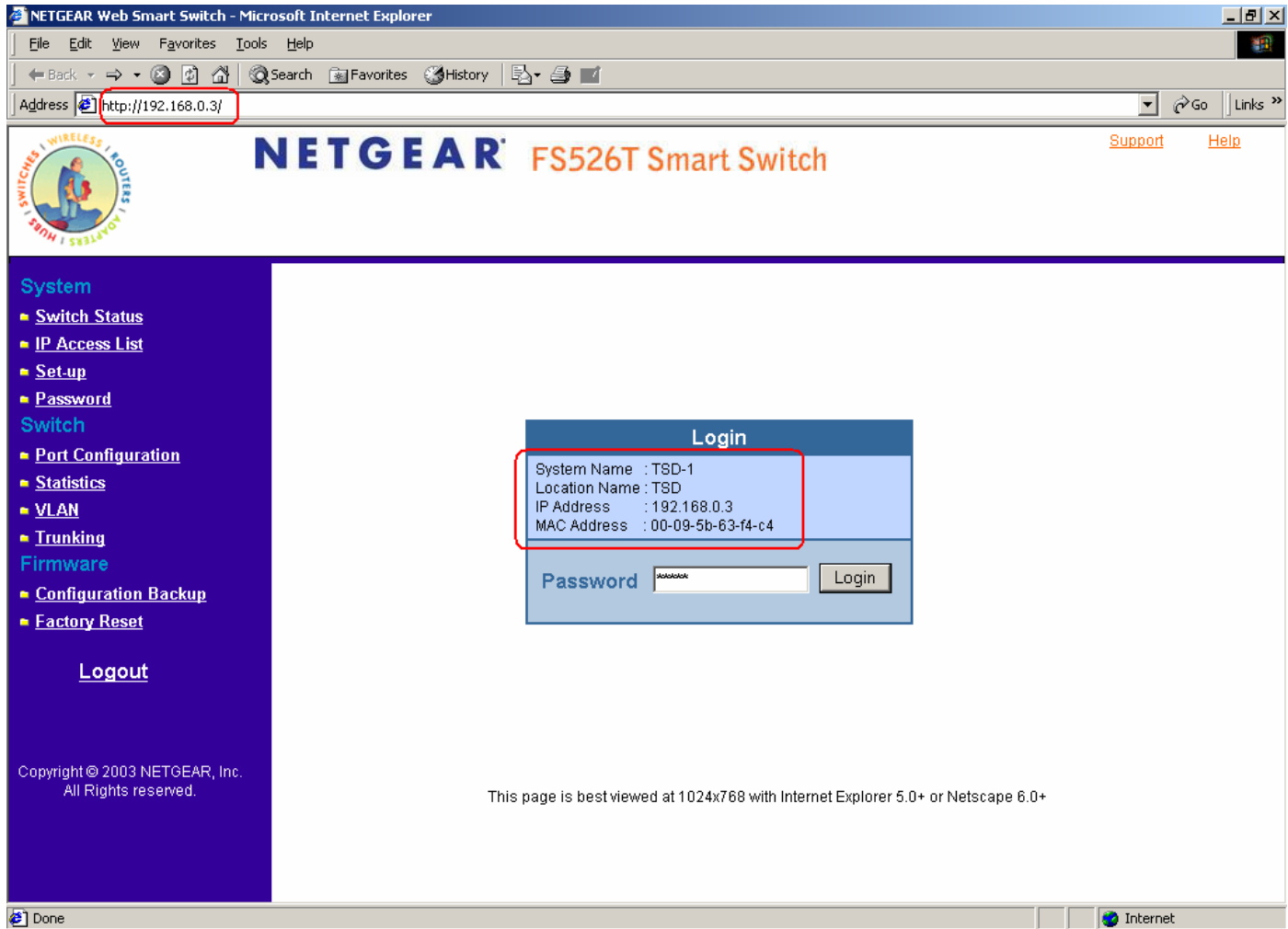


Figure 2-7. Web Management Front page after click "web access" on GearDiscovery utility

CHAPTER 3: Software Upgrade Procedure

The application software for the FS526T 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 follow:

1. Save the new firmware to your computer.
2. Start the GearDiscovery utility program.
3. Select your switch by clicking on it. Then click on Firmware Upgrade, as highlighted in Figure 3-1.

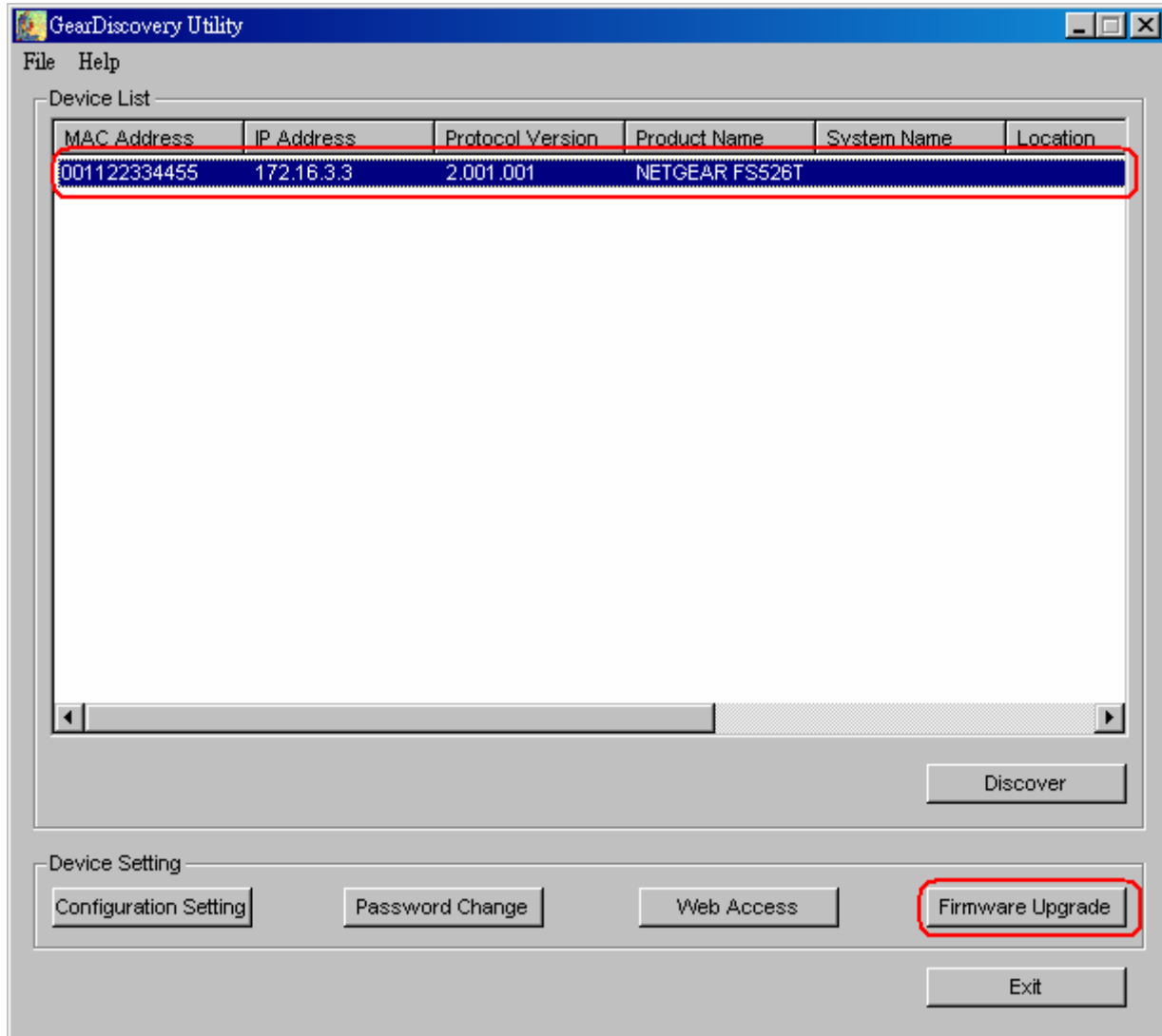


Figure 3-1. Select the switch you want to upgrade and click Firmware Upgrade.

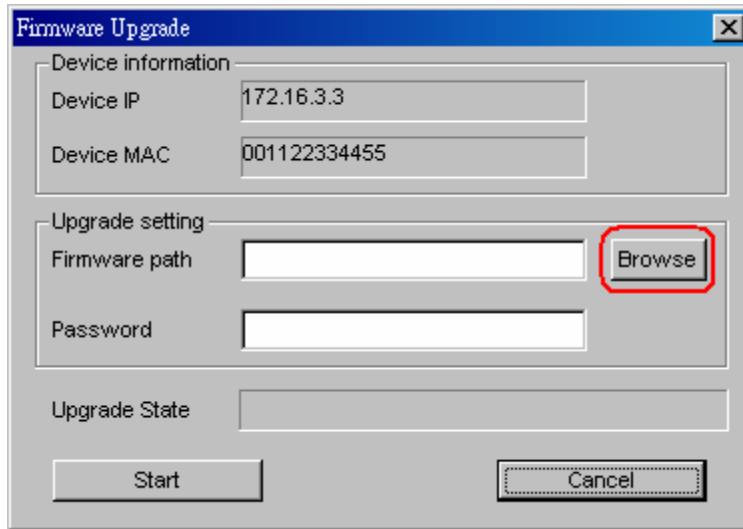


Figure 3-2. Locate New Firmware.

4. Enter the location of the new firmware in the Firmware path below Firmware setting. Alternatively, you can click Browse to locate the file. See Figure 3-2.
5. Click Start to download the new firmware file in non-volatile memory.

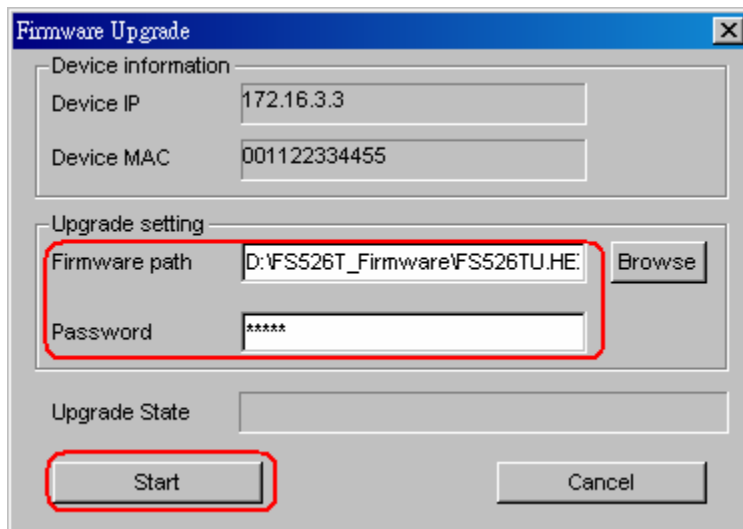


Figure 3-3. Enter Password and click Start.

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

CHAPTER 4: GearDiscovery Utility Program

The GearDiscovery utility program is a user-friendly, easy to install tool. Using this program, you can view and configure all the FS526T Smart Switches in your network.

The installation of the GearDiscovery utility is as follows:

1. Insert the disc into your CD-ROM drive.
2. Select the GearDiscovery\Output folder.
3. Run the Setup program to install the GearDiscovery Utility.
4. The Installation Wizard will guide you through.
5. Run 'GearDiscovery' from the window start bar.

Main Screen

The main screen displays the available functions. As shown in Figure 4-1, there are six function items to choose from:

- Discover
- Configuration Setting
- Password Change
- Web Access
- Firmware Upgrade
- Exit

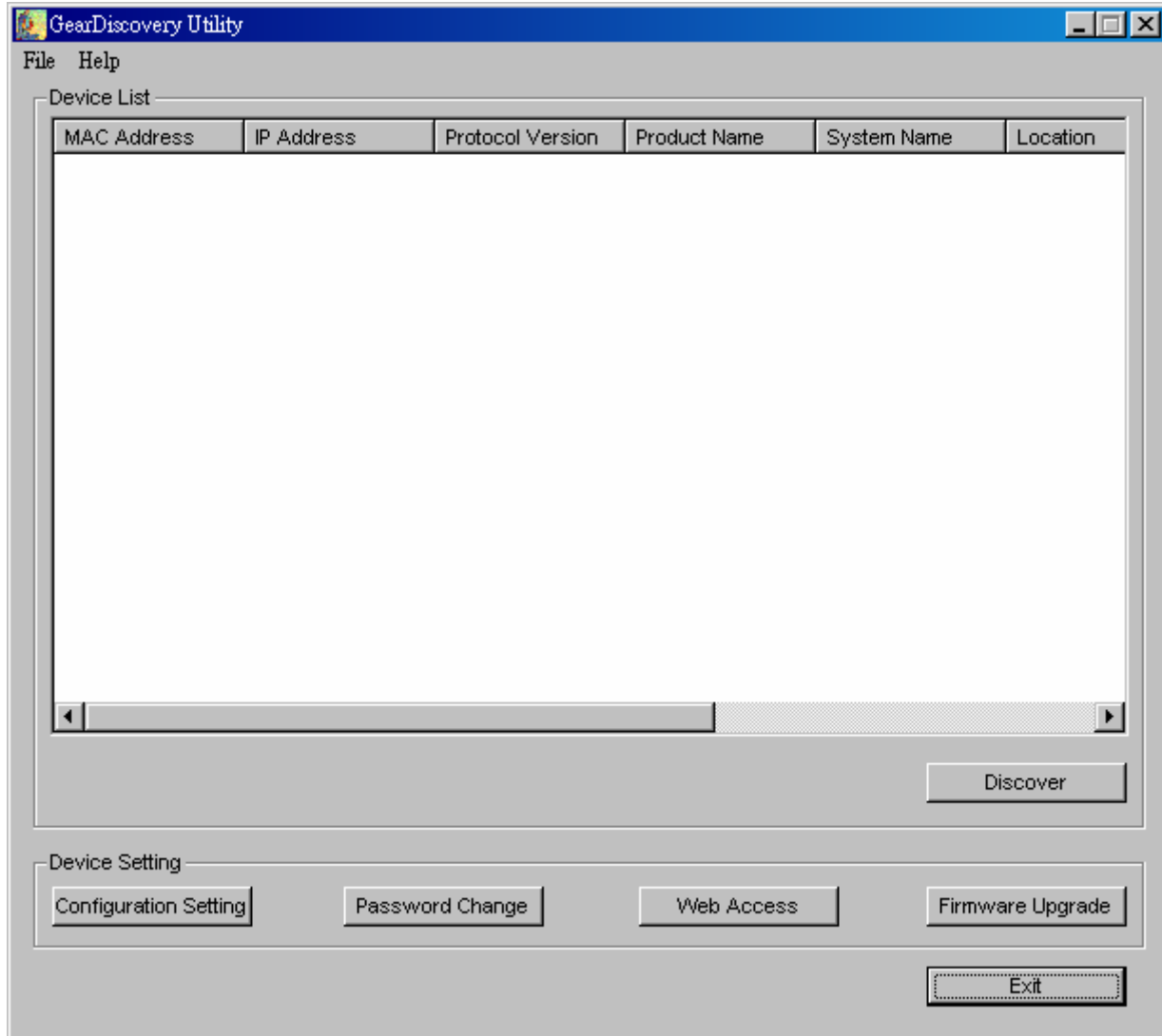


Figure 4-1. GearDiscovery Utility Main Screen

Main Screen> Device List> Discover

The GearDiscovery can discover all switches currently connected on the network. Click 'Discover' to view the following switch information of any listed switch:

- MAC Address
- IP Address
- Protocol Version
- Product Name
- System Name
- Location
- DHCP
- Subnet Mask
- Gateway

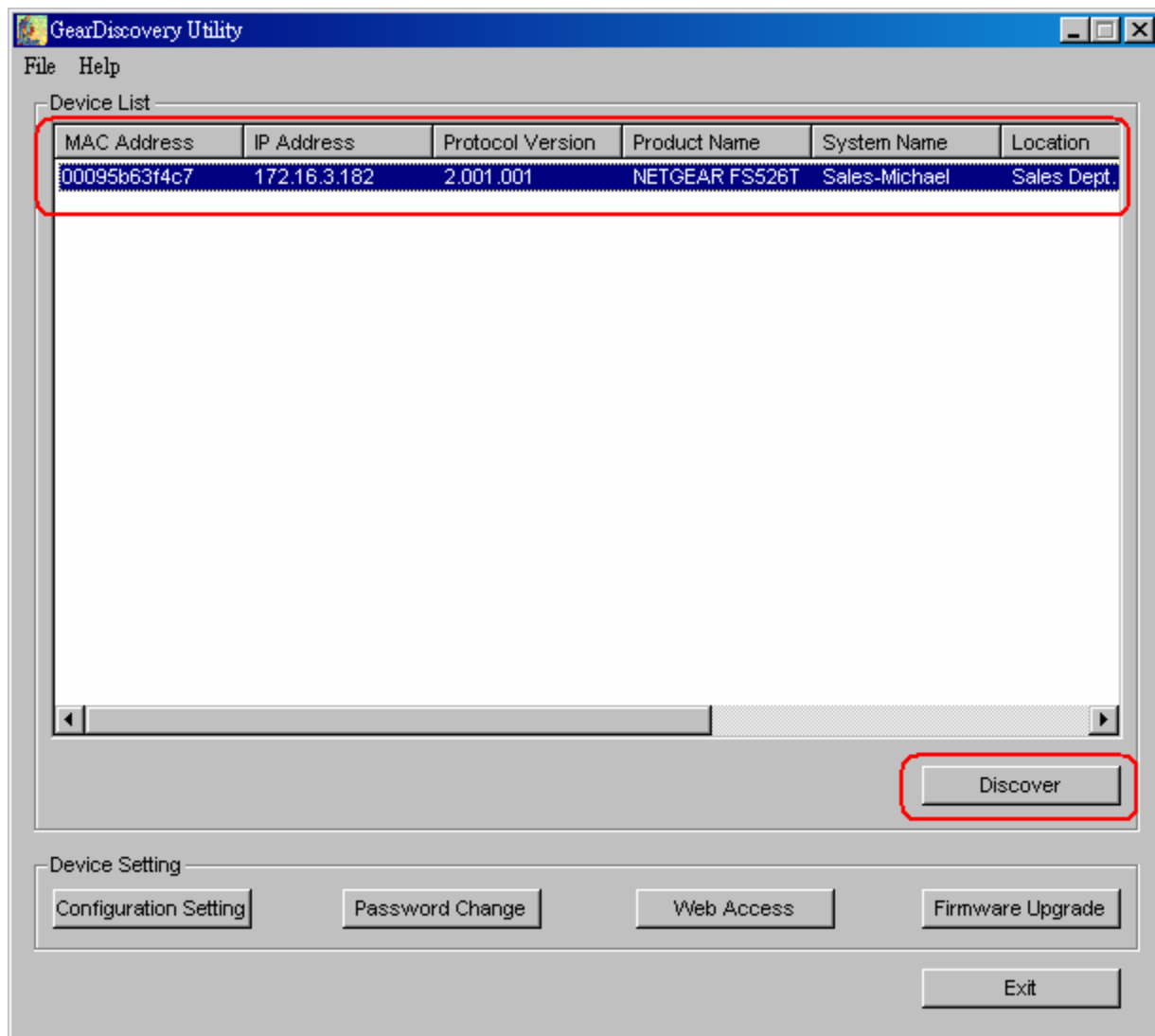


Figure 4-2. Main Screen: Device List> Discover

By double-clicking a listed switch, you can open the Web management for that switch. Alternatively, you can select a switch by clicking on it once, and then clicking Web Access. For more information on Web management, see Chapter 5.

Main Screen> Switch Setting> Configuration Setting

Select a switch by clicking on it. Then click Configuration Setting. The following screen pops up, enabling you modify:

- o System Name This field is to help you keep track of your switches. It can be any combination of letters and/or numbers.
- o Location This field is to help you keep track of where this switch is. It can be any combination of letters and/or numbers.
- o Password The default password is 'password'. You must enter your password for and modifications to take affect.
- o DHCP DHCP automatically obtains the IP information for the switch.

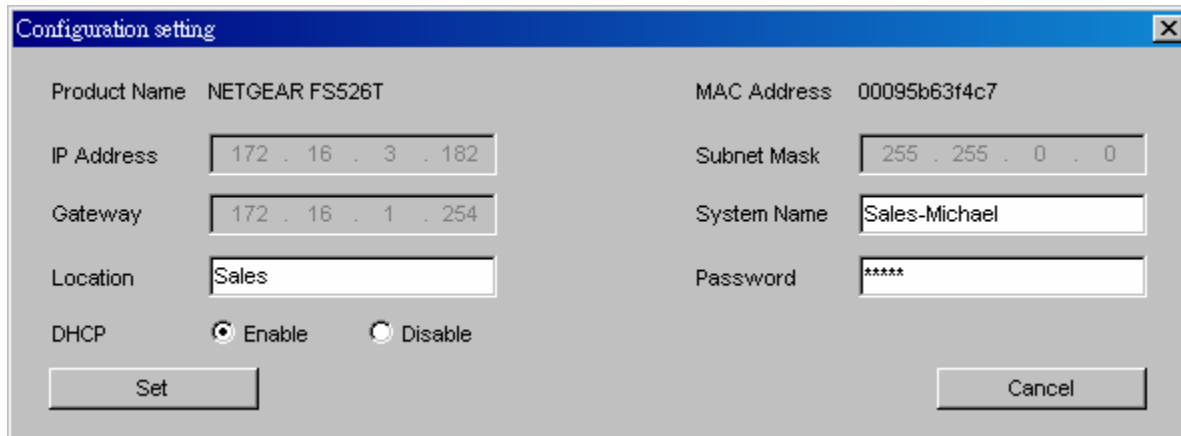


Figure 4-3. Main Screen: Switch Setting> Configuration Setting

- o System Name Any desired description for System Name.
- o Location Any desired description for Location.
- o Password The default password is 'password'.
- o DHCP This function is enabled by default. Click 'Disable' to abort the function.

Main Screen> Device Setting> Configuration Setting> Set

Click 'Set' to enable new settings. You must enter your password for these settings to be accepted.

Main Screen> Device Setting> Configuration Setting> Cancel

Click 'Cancel' to abort the above settings.

Main Screen> Switch Setting> Password Change

Click 'Password Change' from the Switch Setting section. The following screen pops up as shown in Figure 4-4.

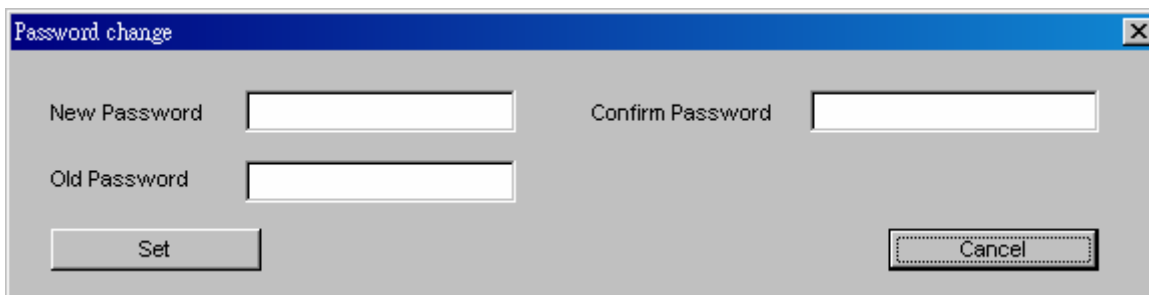


Figure 4-4. Main Screen: Switch Setting> Password Change

- o New Password Type any desired password. Passwords are case-sensitive and can have a maximum of 20 characters.
- o Confirm Password Re-type the new password to confirm it.
- o Old Password The default password is 'password'.

Click 'Set' to enable new password.

Main Screen> Switch Setting> Web Access

Select a listed switch from the Device List section. Then click Web Access from the Switch Setting (see Figure 4-5).

Enter the default password 'password', and click Login.

For more on Web management, see Chapter 5.

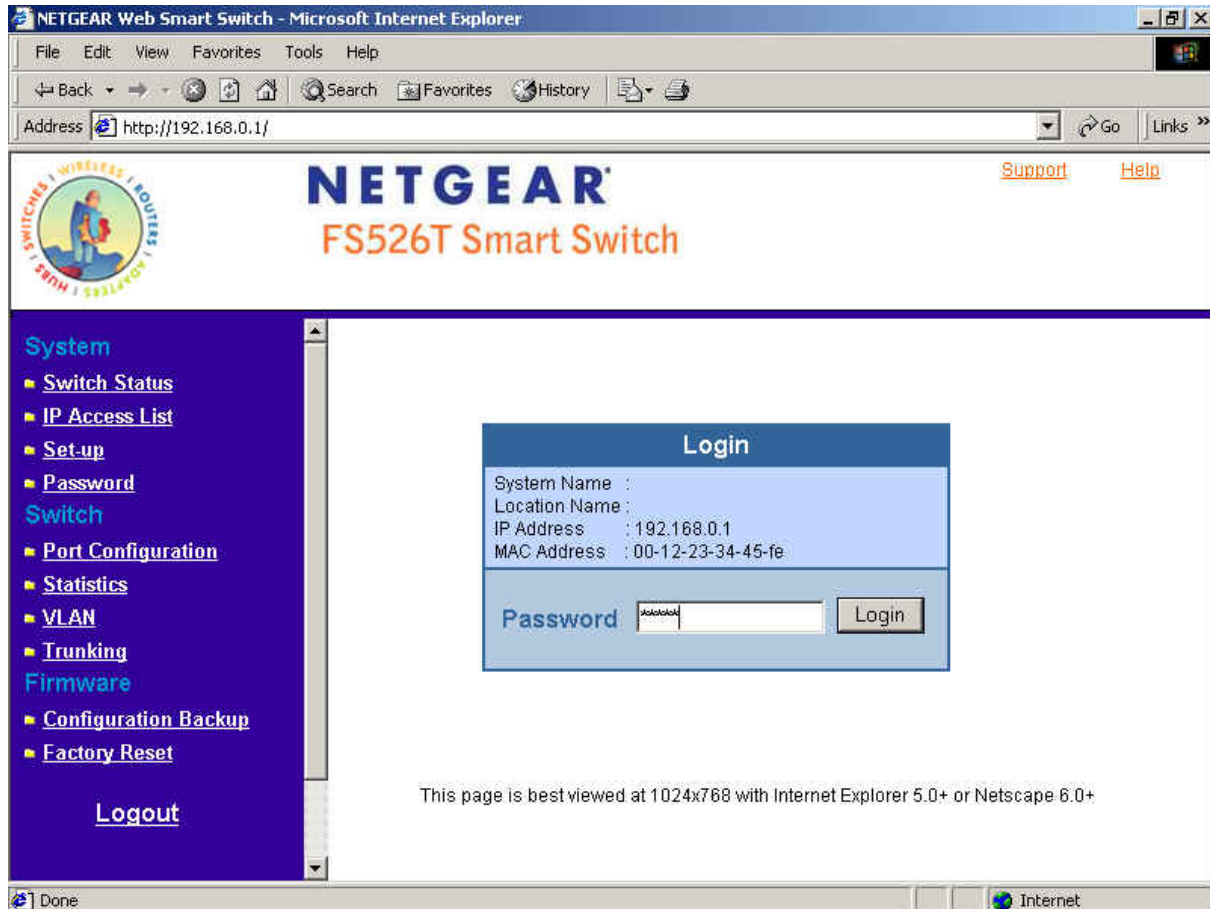


Figure 4-5. Web Management Login Page

Main Screen> Switch Setting> Firmware Upgrade

Click Firmware Upgrade from the Switch Setting section. The following screen will pop up.

The screenshot shows a 'Firmware Upgrade' dialog box. It contains the following fields and controls:

- Device information:**
 - Device IP: 192.168.0.1
 - Device MAC: 00095b63f4c7
- Upgrade setting:**
 - Firmware path: [Empty text box] [Browse button]
 - Password: [Empty text box]
- Upgrade State:** [Empty text box]
- Buttons:** [Start button] [Cancel button]

Figure 4-6. Main Screen: Switch Setting> Firmware Upgrade

- o Firmware Path The location of the new firmware. If you don't know, you can click Browse to locate file.
- o Password The default password is 'password'.
- o Upgrade State Show upgrading in progress.

Click Start to start upgrading.

Main Screen> Switch Setting> Exit

Click Exit from the Switch Setting section to close the GearDiscovery Utility program.

CHAPTER 5: WEB MANAGEMENT ACCESS

Your NETGEAR Model FS526T 26-Port 10/100 Mbps Smart Fast Ethernet Switch with Gigabit Ports 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.

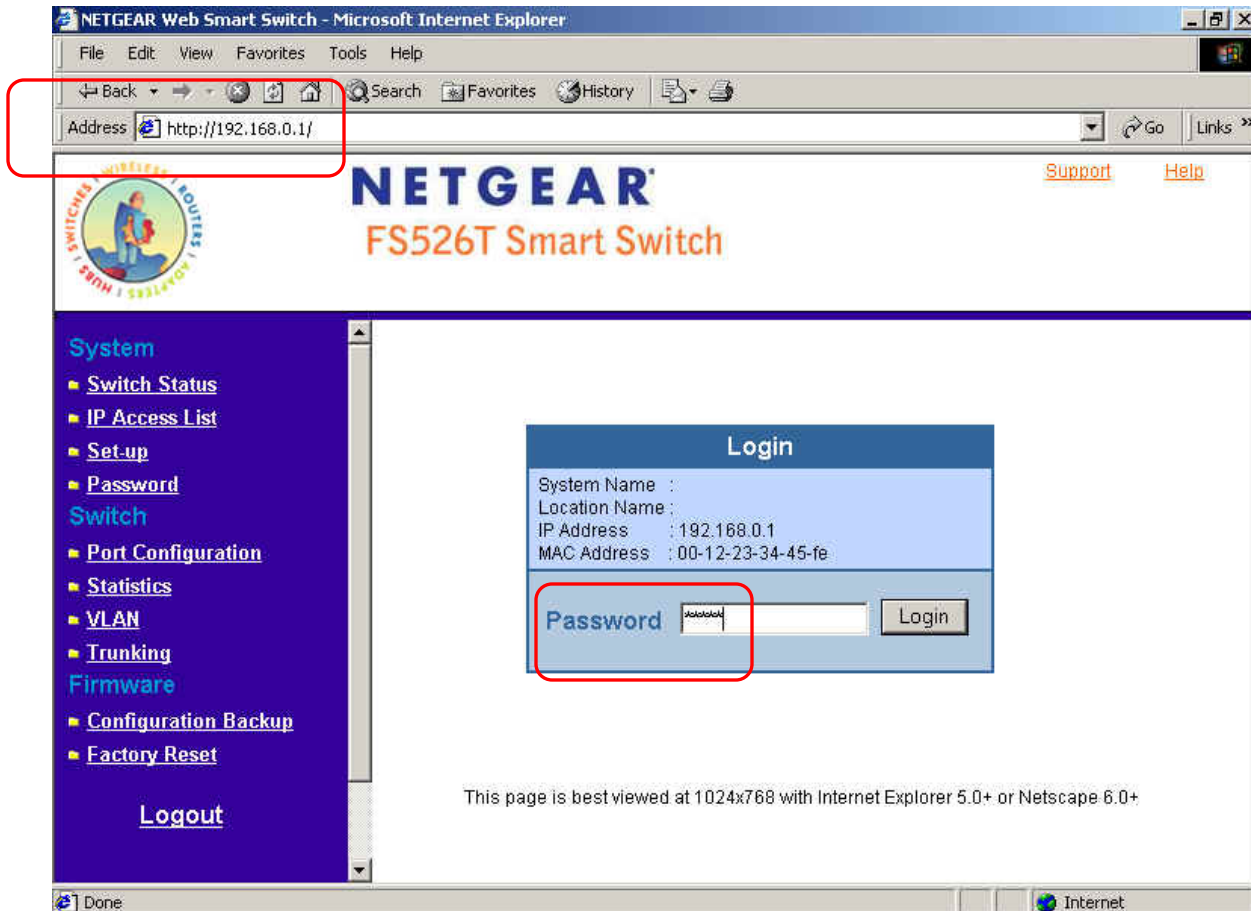


Figure 5-1. Web Management Login page

There are 3 menu options available:

- o System
- o Switch
- o 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:

Refresh:	Pulls that screen's data from 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
Browse:	Locates a certain path for a desired file.
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

There are 4 options available:

- Switch Status
- IP Access List
- Set-up
- Password

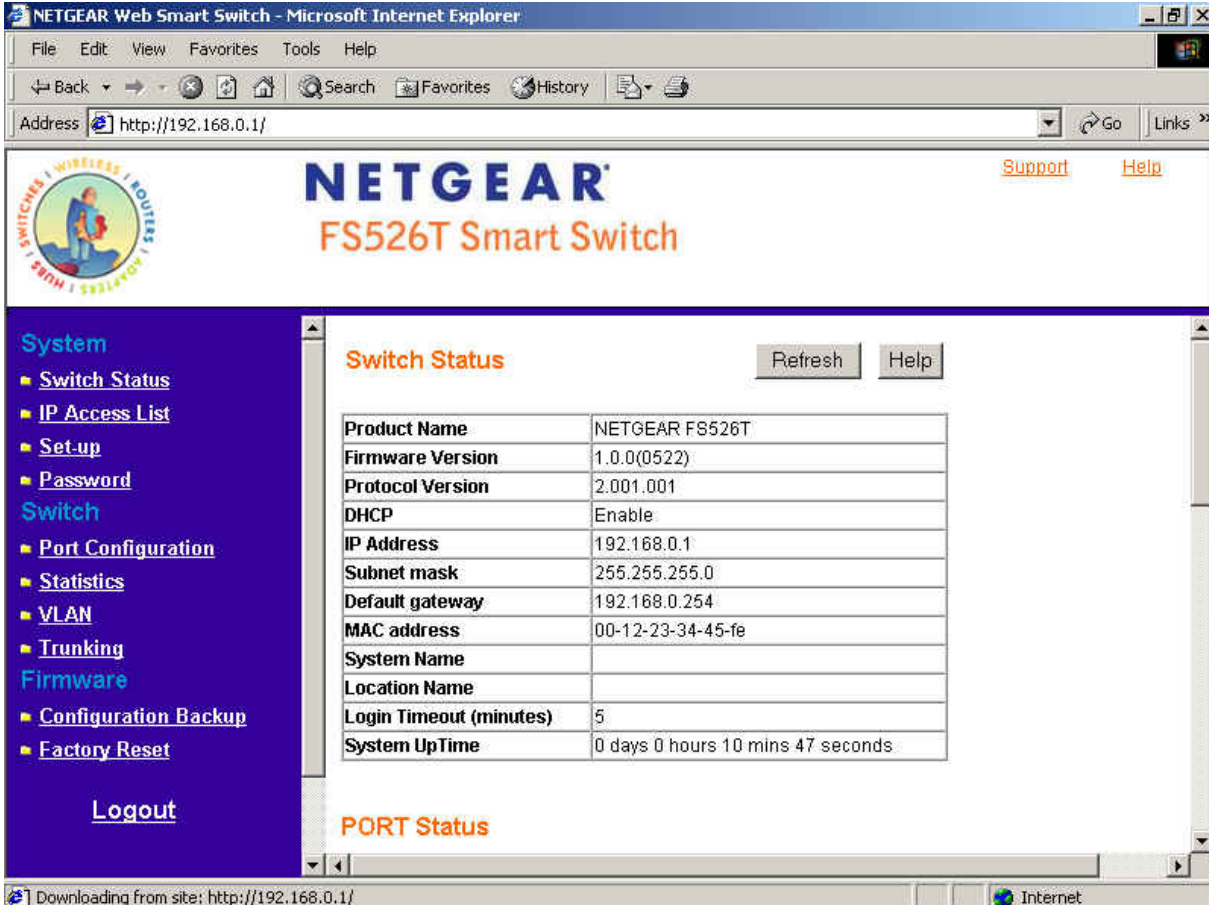
System> Switch Status

System> Switch Status

The top part of this page displays switch information, such as:

- Product Name: (NETGEAR FS526T)
- Firmware Version
- Protocol Version
- DHCP: (shows if enabled or disabled)
- IP Address
- Subnet Mask
- Default Gateway
- MAC Address
- System Name
- Location Name
- Login Timeout:
- System Up Time

These parameters are not editable from this screen. Only System Name and Location Name can be modified in the Set-up> System Setting page.



The screenshot shows the NETGEAR Web Smart Switch interface in Microsoft Internet Explorer. The browser address bar shows the URL <http://192.168.0.1/>. The page title is "NETGEAR FS526T Smart Switch". The main content area is titled "Switch Status" and contains a table of switch information. The table has two columns: the parameter name and its value. The parameters and their values are: Product Name (NETGEAR FS526T), Firmware Version (1.0.0(0522)), Protocol Version (2.001.001), DHCP (Enable), IP Address (192.168.0.1), Subnet mask (255.255.255.0), Default gateway (192.168.0.254), MAC address (00-12-23-34-45-fe), System Name (empty), Location Name (empty), Login Timeout (minutes) (5), and System Up Time (0 days 0 hours 10 mins 47 seconds). There are "Refresh" and "Help" buttons above the table. A "PORT Status" section is visible at the bottom of the page. The left sidebar contains a navigation menu with options like "System", "Switch Status", "IP Access List", "Set-up", "Password", "Switch", "Port Configuration", "Statistics", "VLAN", "Trunking", "Firmware", "Configuration Backup", "Factory Reset", and "Logout".

Product Name	NETGEAR FS526T
Firmware Version	1.0.0(0522)
Protocol Version	2.001.001
DHCP	Enable
IP Address	192.168.0.1
Subnet mask	255.255.255.0
Default gateway	192.168.0.254
MAC address	00-12-23-34-45-fe
System Name	
Location Name	
Login Timeout (minutes)	5
System Up Time	0 days 0 hours 10 mins 47 seconds

Figure 5-2. System> Switch Status: Switch Status

The next part of 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.

- o ID: The port number on the switch
- o 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.
- o Flow Control: Indicates whether Flow Control support is set for on (Enabled) or off (Disabled). The default setting for all ports is enabled.
- o QOS: Indicate the priority for the port. The default setting for all ports is Normal. Quality of Service (QoS) is a way of managing traffic in a network, by treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion.
- o Link Status: Indicates the current speed and duplex for the port. DOWN means no link.

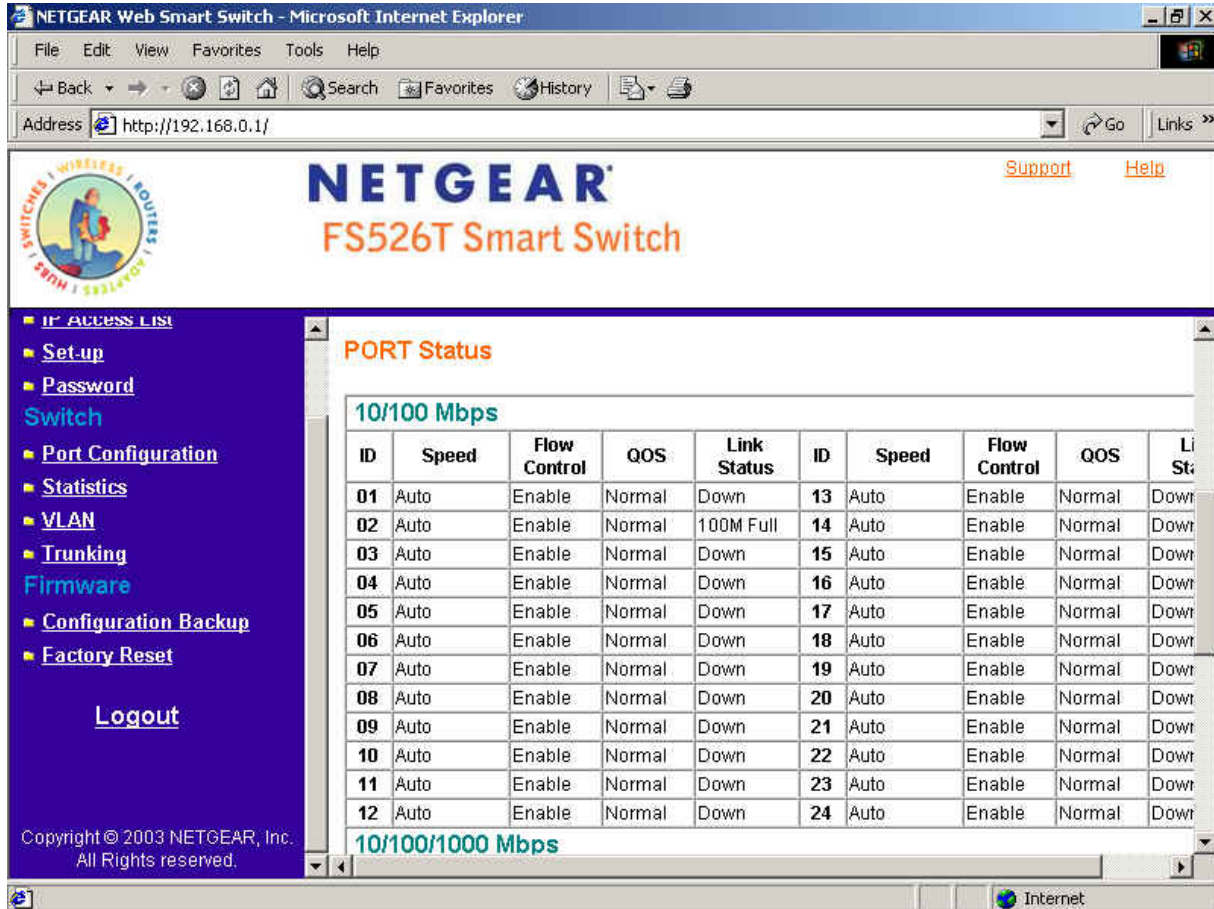


Figure 5-3. System> Switch Status: Port Status

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 switch supports 26 VLANs.

This page displays the port-based VLAN settings. The default VLAN setting is all ports belong to VLAN 1 as shown in Figure 2-4. To configure user-defined VLAN groups, go to the Switch> VLAN page.

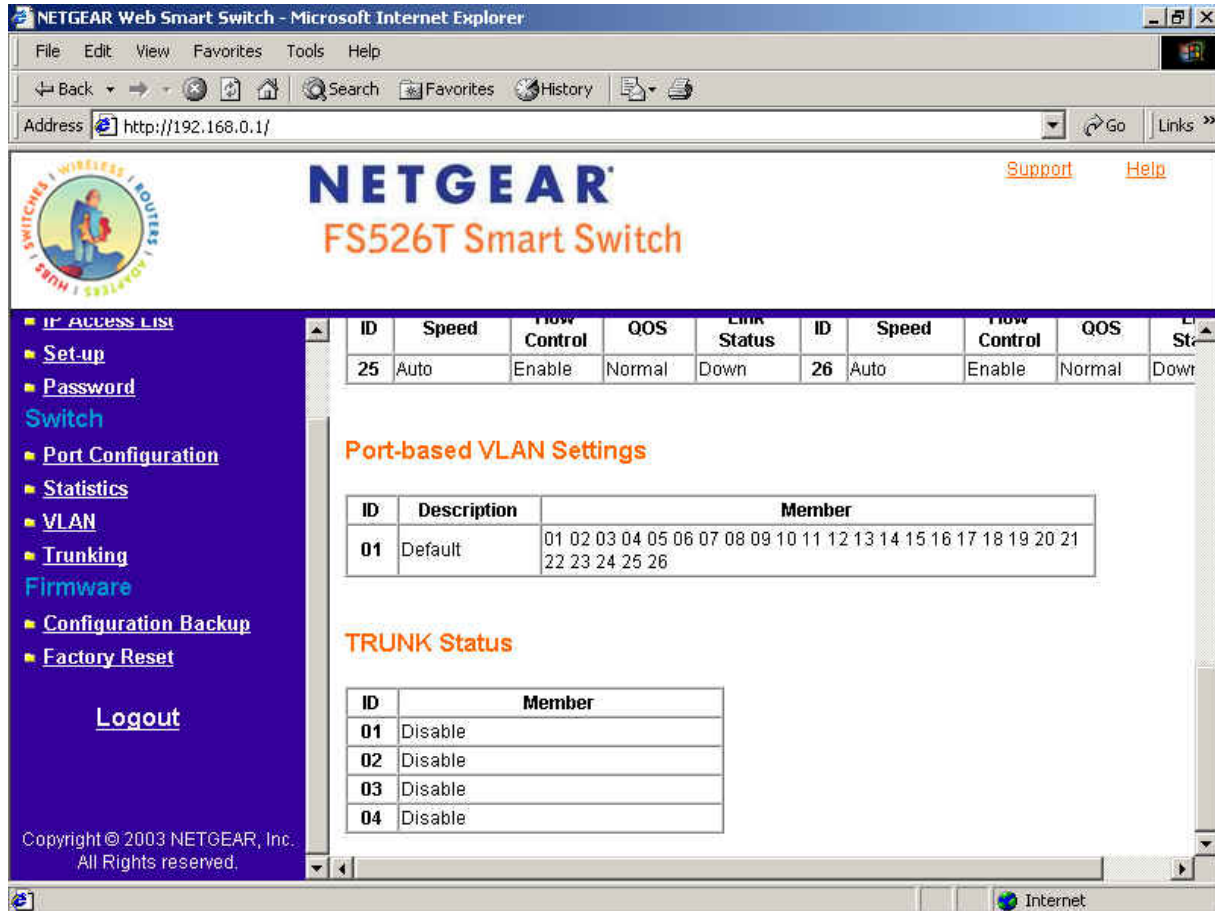


Figure 5-4. System> Switch Status: Port-based VLAN & TRUNK

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. Up to four trunks can be operating at the same time.

This page displays the Trunk status as shown in Figure 2-4. The default Trunk setting is all four groups disabled. To configure user-defined trunk groups, go to the Switch> Trunking page.

If the IEEE802.1Q VLAN is enabled, this page will display the Tagged VLAN status as shown in Figures 2-5 and 2-6. To know more about Tag VLAN, see Switch> VLAN for details.

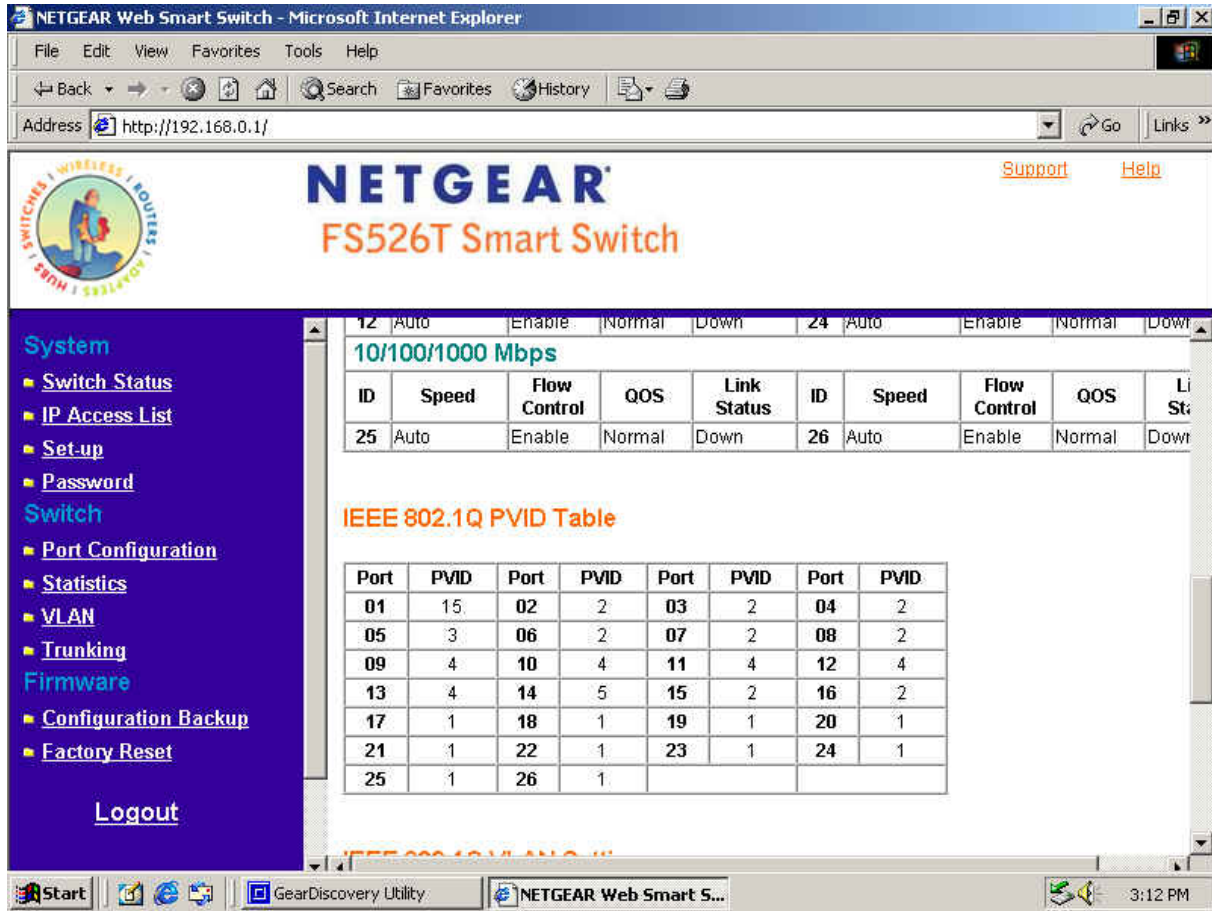


Figure 5-5. System> Switch Status: Tag VLAN PVID Table

NETGEAR Web Smart Switch - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address http://192.168.0.1/ Go Links >>

NETGEAR
FS526T Smart Switch

[Support](#) [Help](#)

System

- Switch Status
- IP Access List
- Set-up
- Password

Switch

- Port Configuration
- Statistics
- VLAN
- Trunking

Firmware

- Configuration Backup
- Factory Reset

[Logout](#)

Port	PVID	Port	PVID	Port	PVID	Port	PVID
01	15	02	2	03	2	04	2
05	3	06	2	07	2	08	2
09	4	10	4	11	4	12	4
13	4	14	5	15	2	16	2
17	1	18	1	19	1	20	1
21	1	22	1	23	1	24	1
25	1	26	1				

IEEE 802.1Q VLAN Settings

VLAN ID	Member Port																									
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	U	U																								
3	U			U	U																					
4	T							T	T	U	U															
5	U	U												U												

Internet

Figure 5-6. System> Switch Status: Tag VLAN Settings

System> IP Access List

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 to 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 as shown in Figure 5-7.

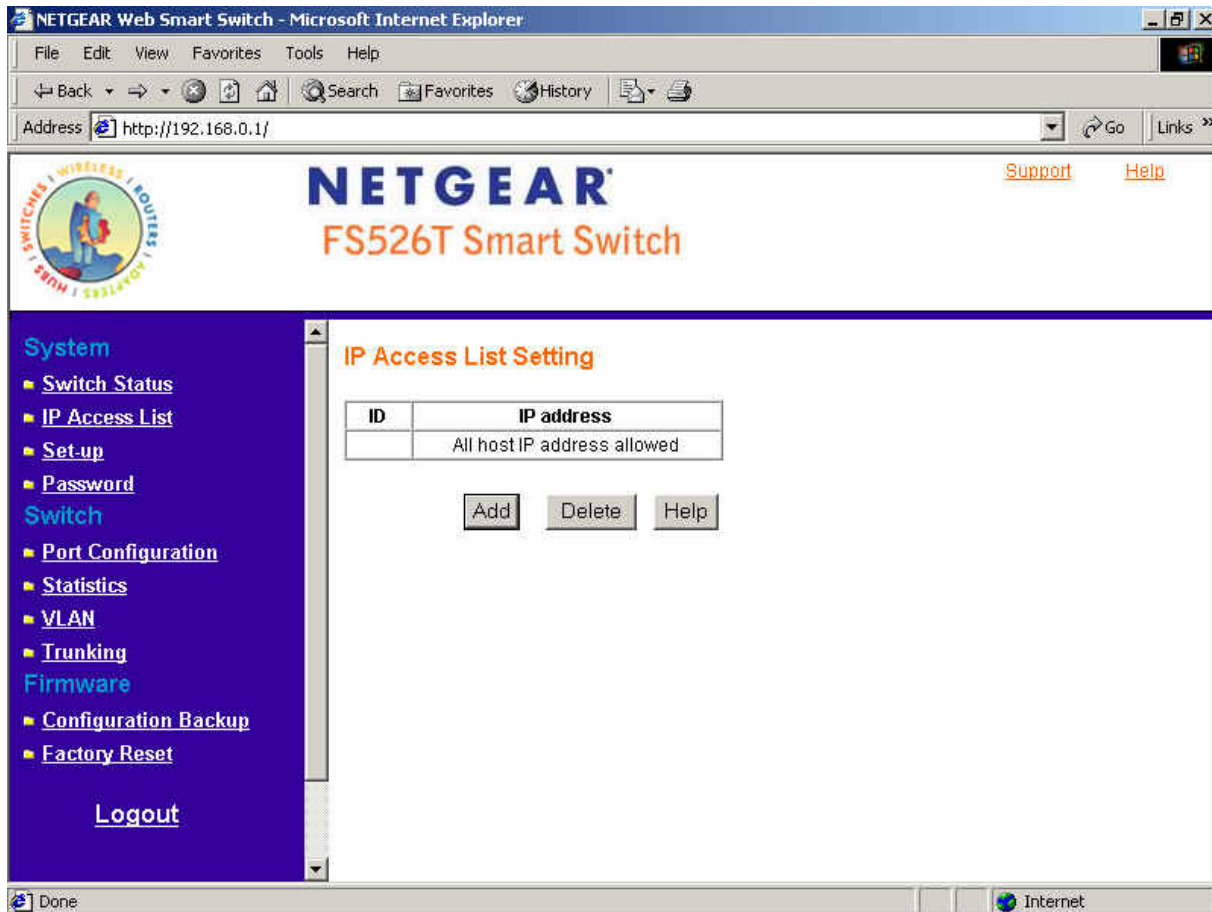


Figure 5-7. System> IP Access List

Add a new entry

- Click Add to bring up the page as shown in Figure 5-8
- Enter site-specific IP address in the appropriate boxes
- Click Apply to activate the setting

Note: Once this new IP access is enabled, you can only access the switch via devices with approved IP addresses. Make sure that your current PC has one of the addresses in the list.

Delete an existing entry

- Click Delete to bring up the IP Access List Delete screen
- Click to select the entry in the list
- Click Apply to delete this IP Access

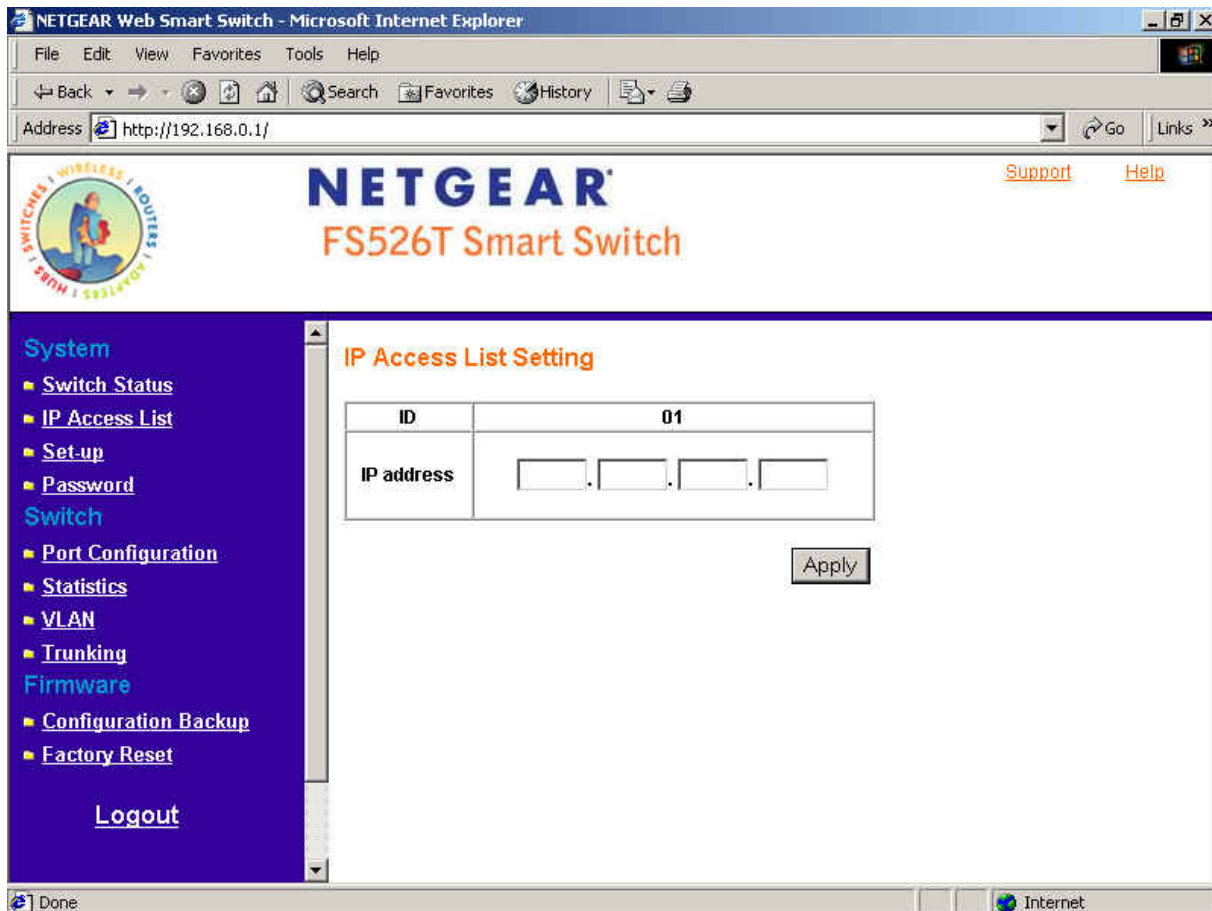


Figure 5-8. System> IP Access List> Add new IP

System> Set-up

This page will allow access to the system information parameters.

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

NETGEAR Web Smart Switch - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print

Address http://192.168.0.1/ Go Links >>

NETGEAR FS526T Smart Switch [Support](#) [Help](#)

System

- Switch Status
- IP Access List
- Set-up**
- Password

Switch

- Port Configuration
- Statistics
- VLAN
- Trunking

Firmware

- Configuration Backup
- Factory Reset

[Logout](#)

System Setting

System Name

Location Name

Login Timeout (3 - 30 minutes)

IP Address

Get Dynamic IP from DHCP Server

DHCP server VID

Static IP Address

IP address . . .

Subnet mask . . .

Gateway . . .

Done Internet

Figure 5-9. System> Set-up> System Setting

System> Password

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.

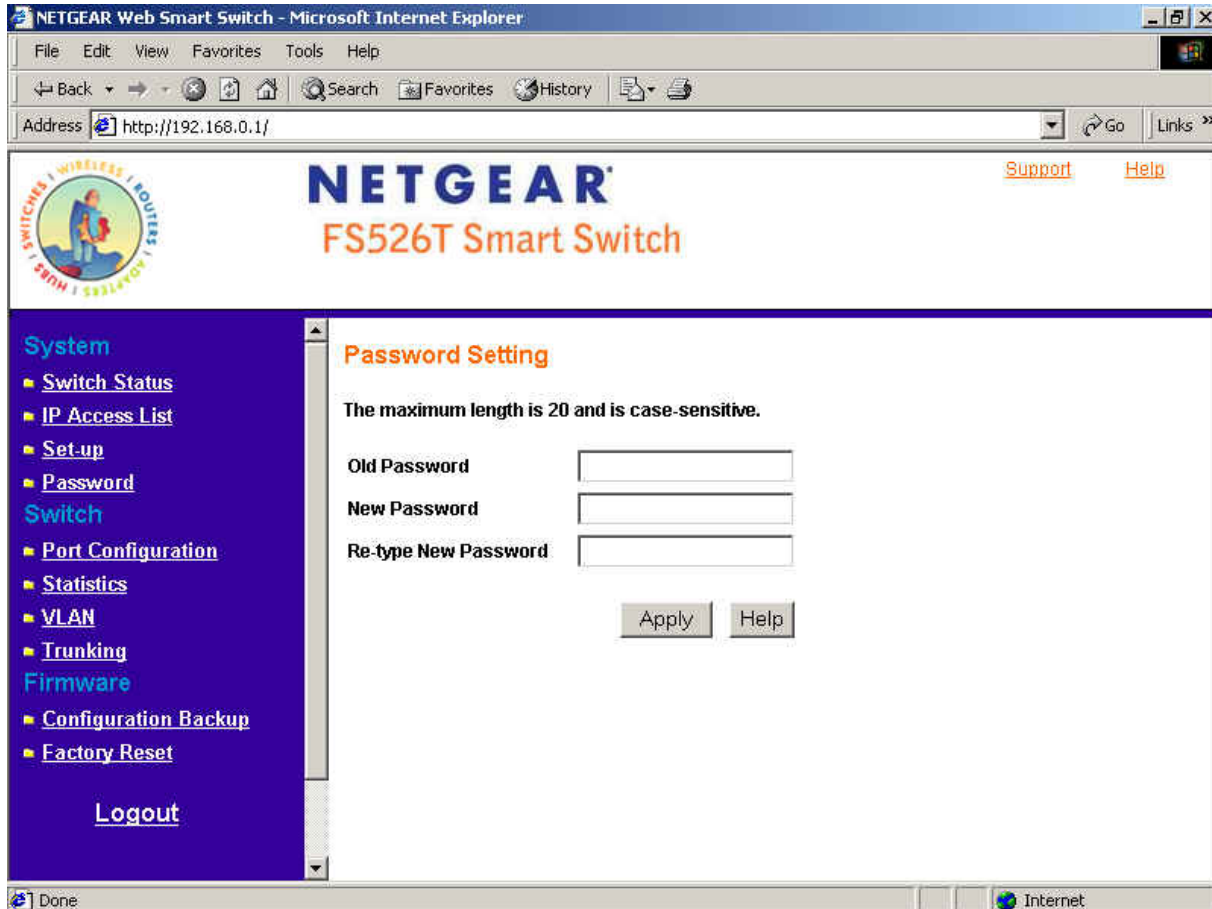


Figure 5-10. System> Password> Password Setting

Switch

There are 4 options available:

- o Port Configuration
- o Statistics
- o VLAN
- o Trunking

Switch> Port Configuration

Switch> Port Configuration: Port Setting menu

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

- o ID: The port number on the switch. Click this number to configure the port.
- o 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.
- o Flow Control: Indicates whether Flow Control support is set for on (Enabled) or off (Disabled). The default setting for all ports is enabled.
- o QoS: Indicate the priority for the port. The default setting for all ports is Normal. Quality of Service (QoS) is a way of managing traffic in a network, by treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion.
- o Link Status: Indicates the current speed and duplex for the port. DOWN means no link.

The screenshot shows the NETGEAR Web Smart Switch interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.0.1/>. The page title is "NETGEAR Web Smart Switch - Microsoft Internet Explorer". The main content area is titled "PORT Setting" and displays a table of port configurations. The table is divided into two sections: "10/100 Mbps" and "10/100/1000 Mbps". Each section contains a table with columns for ID, Speed, Flow Control, QoS, and Link Status. The "10/100 Mbps" section shows ports 01 through 12, and the "10/100/1000 Mbps" section shows ports 13 through 24. The "Link Status" column for all ports is "Down".

ID	Speed	Flow Control	QoS	Link Status
01	Auto	Enable	Normal	Down
02	Auto	Enable	Normal	100M Full
03	Auto	Enable	Normal	Down
04	Auto	Enable	Normal	Down
05	Auto	Enable	Normal	Down
06	Auto	Enable	Normal	Down
07	Auto	Enable	Normal	Down
08	Auto	Enable	Normal	Down
09	Auto	Enable	Normal	Down
10	Auto	Enable	Normal	Down
11	Auto	Enable	Normal	Down
12	Auto	Enable	Normal	Down
13	Auto	Enable	Normal	Down
14	Auto	Enable	Normal	Down
15	Auto	Enable	Normal	Down
16	Auto	Enable	Normal	Down
17	Auto	Enable	Normal	Down
18	Auto	Enable	Normal	Down
19	Auto	Enable	Normal	Down
20	Auto	Enable	Normal	Down
21	Auto	Enable	Normal	Down
22	Auto	Enable	Normal	Down
23	Auto	Enable	Normal	Down
24	Auto	Enable	Normal	Down

Figure 5-11. Switch> Port Configuration> Port Setting menu

Switch> Port Configuration: Set speed

- Click a port ID as shown in Figure 5-11
- 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.

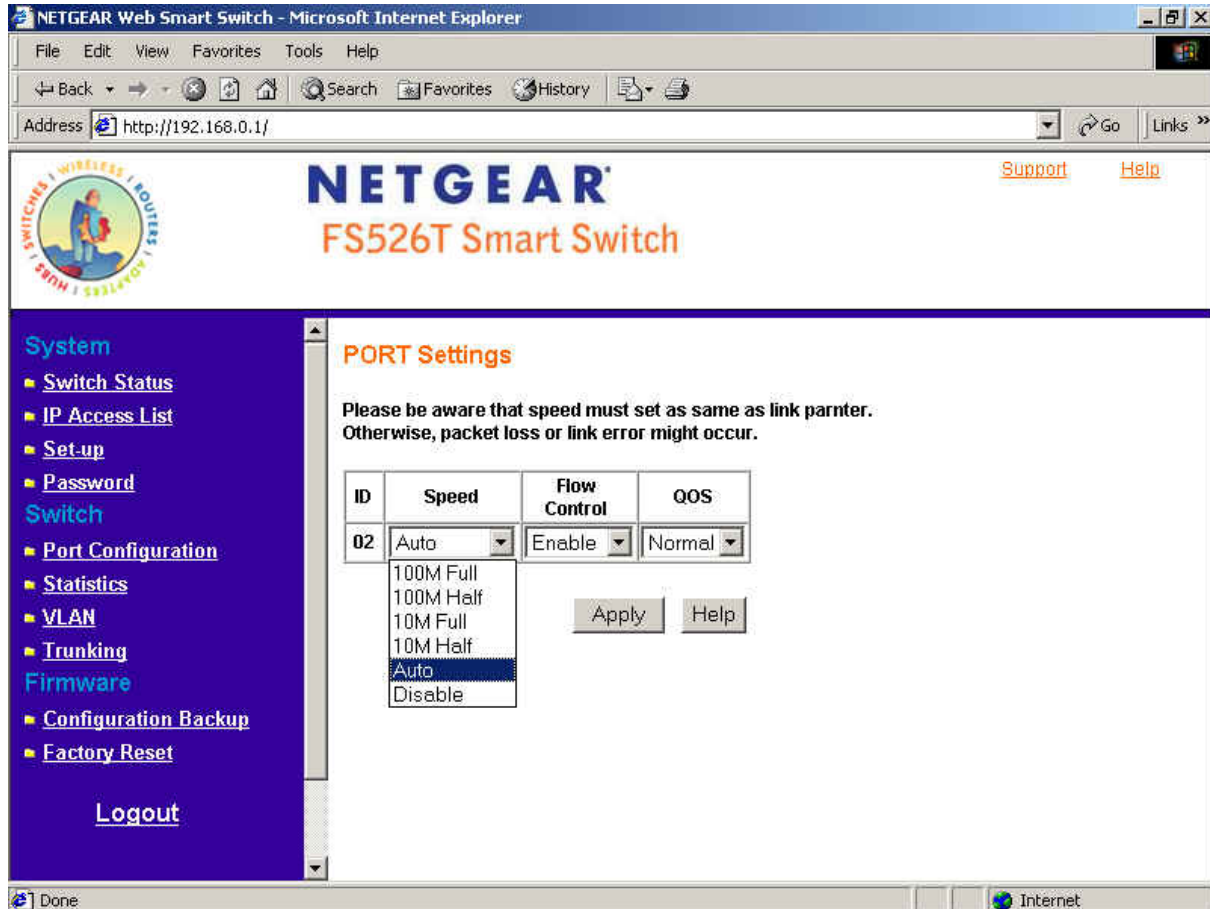


Figure 5-12. Switch> Port Configuration> Port Settings: Speed

Switch> Port Configuration: Set flow control

- Click a port ID as shown in Figure 5-11
- Click to select Enable or Disable from the pull-down menu under Flow Control
- Click Apply to activate the new setting

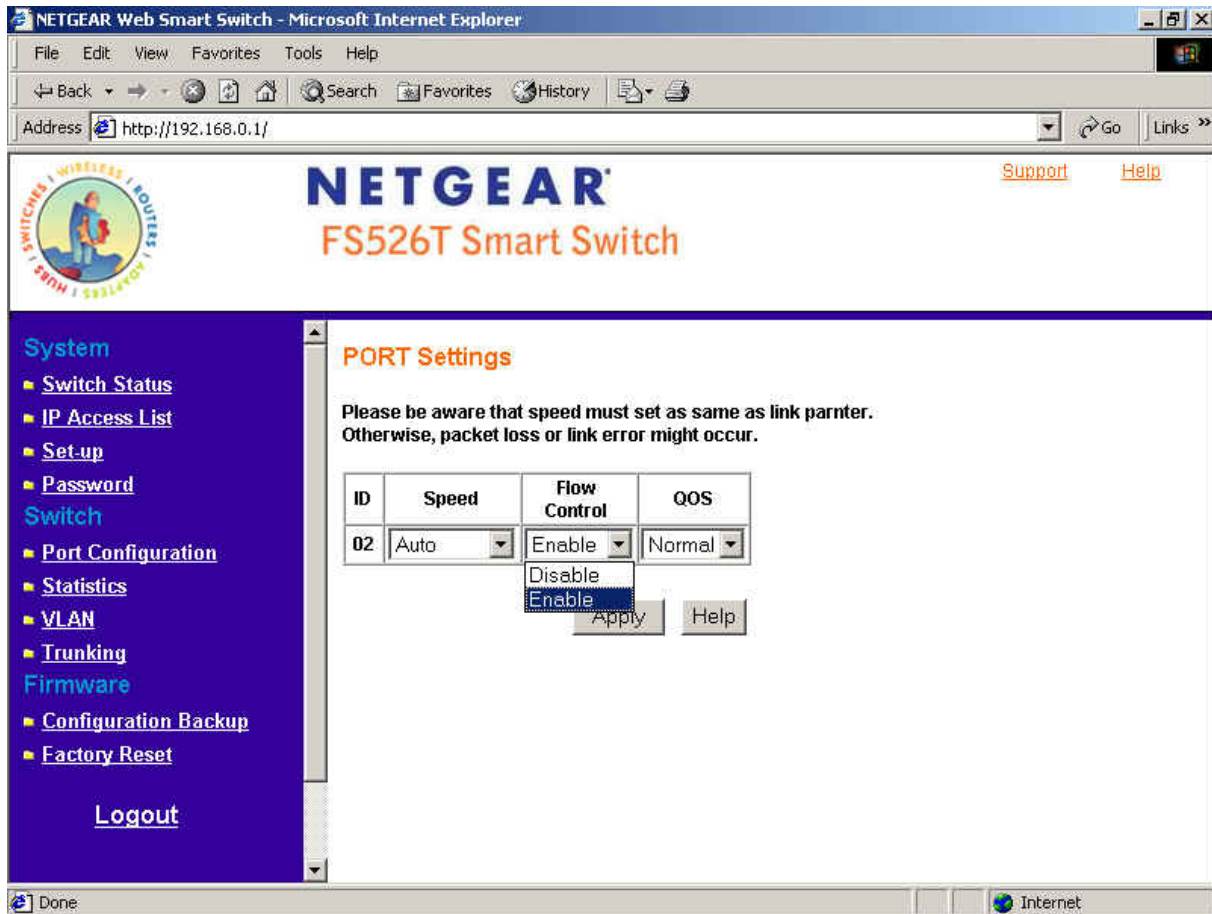


Figure 5-13. Switch> Port Configuration> Port Settings: Flow Control

Switch> Port Configuration: Set QOS

- Click a port ID as shown in Figure 5-11
- Click to select Normal or High from the pull-down menu under QOS
- Click Apply to activate the new setting

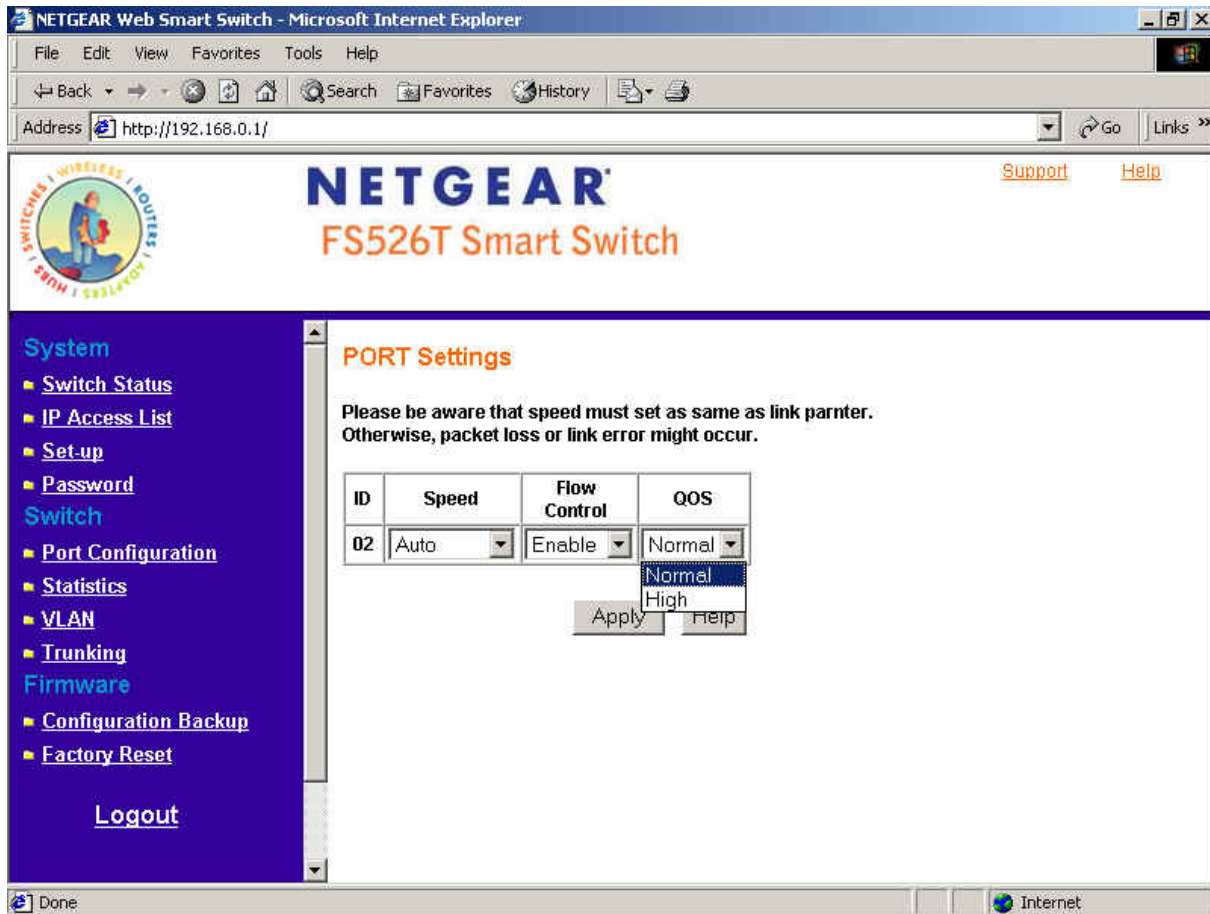


Figure 5-14. Switch> Port Configuration> Port Settings: QOS

Switch> Statistics

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

- o ID: The port number on the switch
- o Tx: Transmitted packet/s.
- o Rx: Received packet/s.
- o Tx Error: Transmitted packet/s with an error.
- o Rx Error: Received packet/s with an 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.

The screenshot shows the NETGEAR Web Smart Switch interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.0.1/>. The page title is "NETGEAR FS526T Smart Switch". The main content area is titled "Statistics" and features a table with columns for ID, Tx, Rx, Tx Error, and Rx Error. The table is divided into sections for "10/100 Mbps" and "10/100/1000 Mbps". The "10/100 Mbps" section shows data for ports 01 through 12, with port 02 having 222 Tx and 466 Rx packets. The "10/100/1000 Mbps" section shows data for ports 13 through 24, all with 0 Tx and Rx packets. The interface also includes a "Refresh" button and a "Clear Counter" button. A navigation menu on the left lists various system and switch configuration options.

ID	Tx	Rx	Tx Error	Rx Error	ID	Tx	Rx	Tx Error	Rx Error
10/100 Mbps									
01	0	0	0	0	13	0	0	0	0
02	222	466	0	0	14	0	0	0	0
03	0	0	0	0	15	0	0	0	0
04	0	0	0	0	16	0	0	0	0
05	0	0	0	0	17	0	0	0	0
06	0	0	0	0	18	0	0	0	0
07	0	0	0	0	19	0	0	0	0
08	0	0	0	0	20	0	0	0	0
09	0	0	0	0	21	0	0	0	0
10	0	0	0	0	22	0	0	0	0
11	0	0	0	0	23	0	0	0	0
12	0	0	0	0	24	0	0	0	0
10/100/1000 Mbps									

Figure 5-15. Switch> Statistics

Switch> VLAN

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:

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

Switch> VLAN> Port-based VLAN

There are up to 26 port-based VLAN groups supported on this switch. A port can participate in more than one VLAN group.

For port-based VLANs, the default VLAN group is VLAN 01.

NETGEAR Web Smart Switch - Microsoft Internet Explorer

Address: http://192.168.0.1/

NETGEAR FS526T Smart Switch

Support Help

System

- Switch Status
- IP Access List
- Set-up
- Password

Switch

- Port Configuration
- Statistics
- VLAN
- Trunking

Firmware

- Configuration Backup
- Factory Reset

Logout

IEEE 802.1Q VLAN Port-based VLAN

ID	Description	Member
01	Default	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Add Group Delete Group Help

Figure 5-16. Switch> VLAN

Change members

- Click a VLAN ID as shown in Figure 5-16
- Click to select port/s for VLAN members
- Click Apply to activate the new setting

Add Group

- Click Add Group as shown in Figure 5-16
- Enter a description for this VLAN group
- Click to select port/s for VLAN members
- Click Set all to select all ports
- Click Clear all to unselect all ports
- Click Apply to activate the new setting

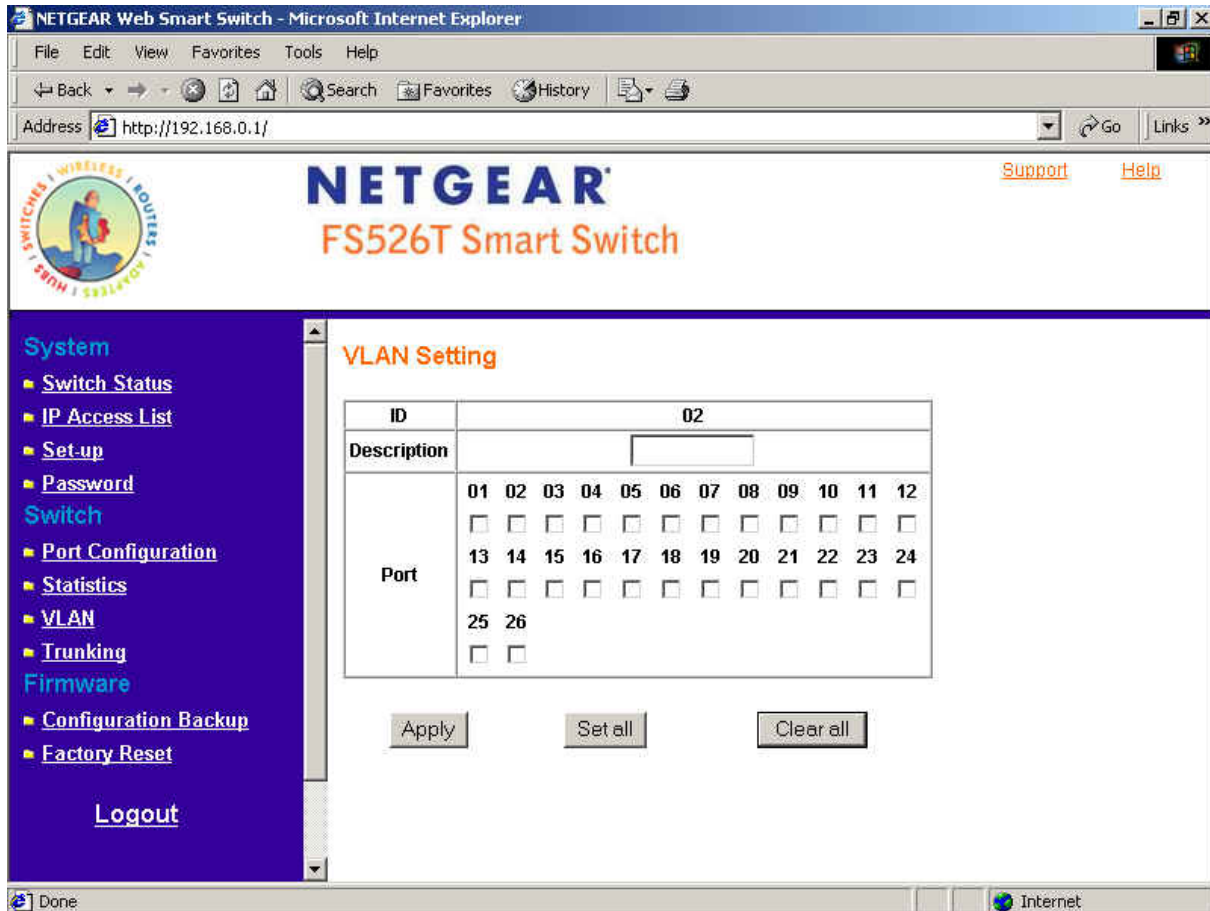


Figure 5-17. Switch> VLAN Setting> Port-based VLAN: Add Group

Delete Group

- Click Delete Group as shown in Figure 5-16
- Click to select a VLAN ID as shown in Figure 5-18
- Click Apply to confirm delete this VLAN

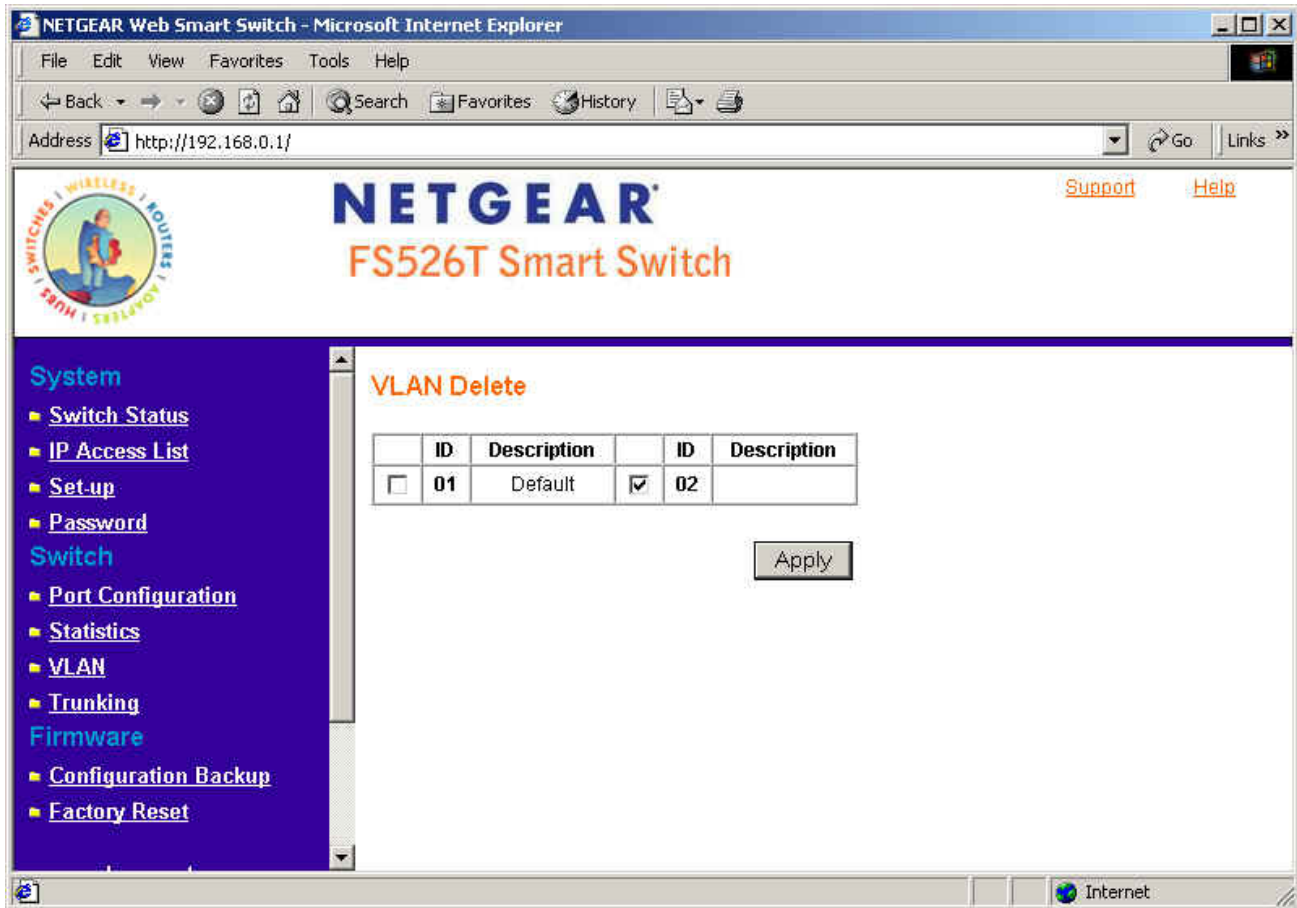


Figure 5-18. Switch> VLAN Setting> Port-based VLAN: Delete Group

Switch> VLAN> IEEE802.1Q Tag VLAN

There are up to 64 static Tag VLAN groups supported on this switch. The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches (Reference: Appendix B and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks).

Click to select IEEE802.1Q VLAN as shown in Figure 2-16. The following screen pops up to confirm this change.

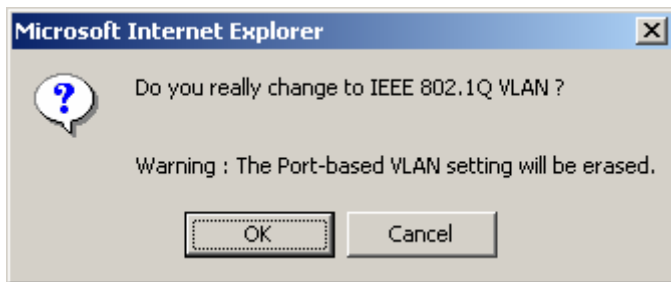


Figure 5-19. Switch> VLAN Setting> Tag VLAN

All ports are set belonging to VLAN 1 by default, all untagged, as shown in Figure 2-20.

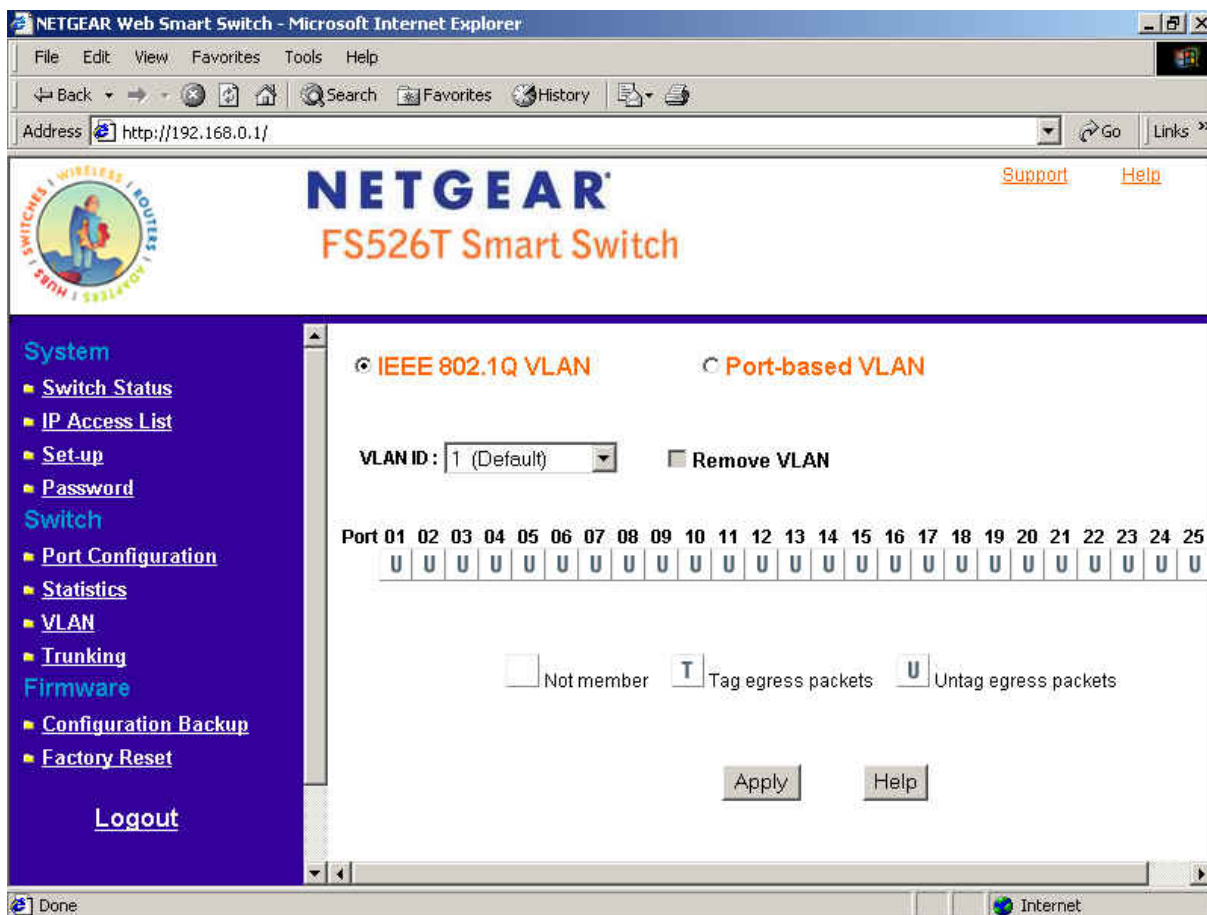


Figure 5-20. Switch> VLAN Setting> Tag VLAN: default

From the page as shown in Figure 5-21, you can create a new VLAN, add new ports to an existing VLAN, remove ports from an existing VLAN or, delete a VLAN.

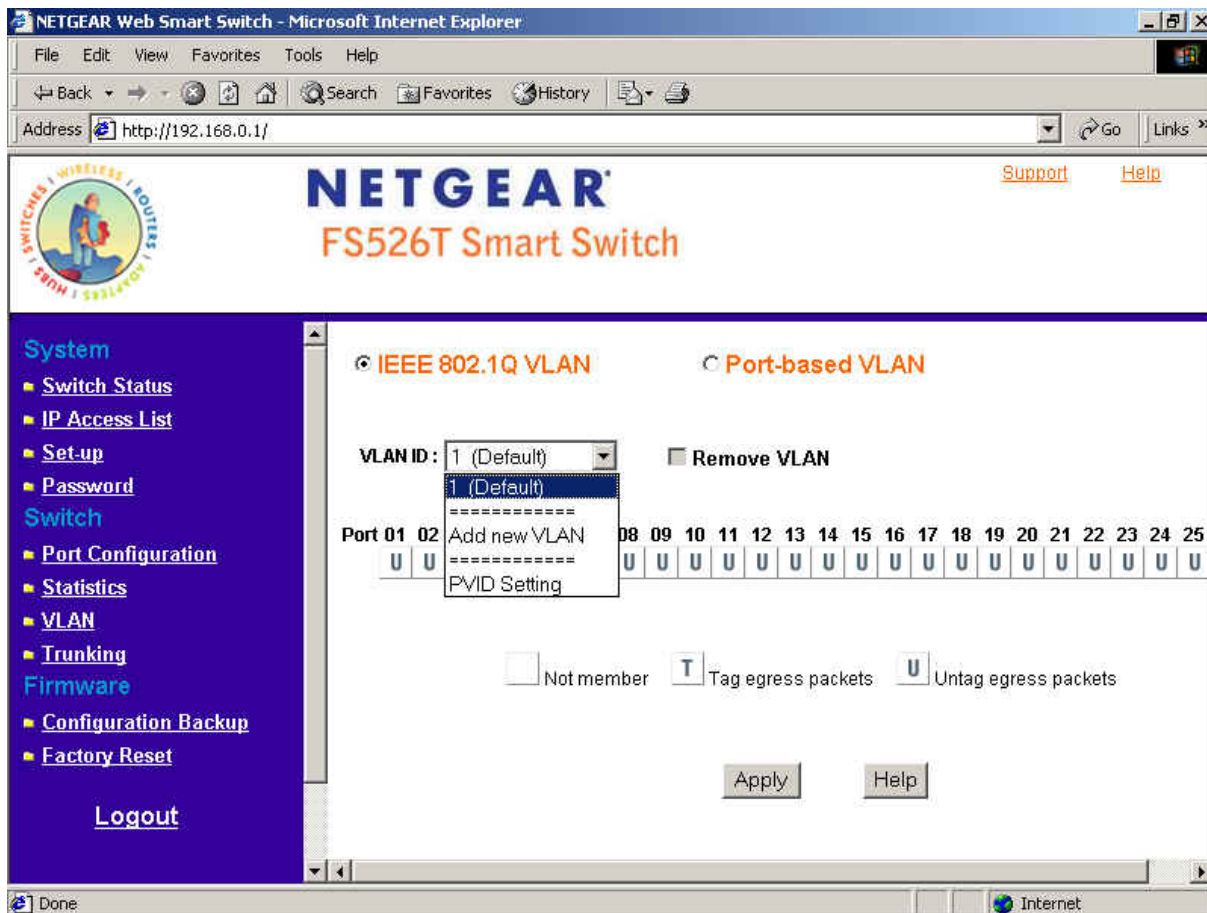


Figure 5-21. Switch> VLAN Setting> Tag VLAN menu

Add a port to a VLAN Group

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

Remove a port from a VLAN Group

- o Click the box again until a blank box appears. This will remove VLAN membership from the port.
- o 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. See Figures 2-22 and 2-23 for an example of creating VLAN 2.
- 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.

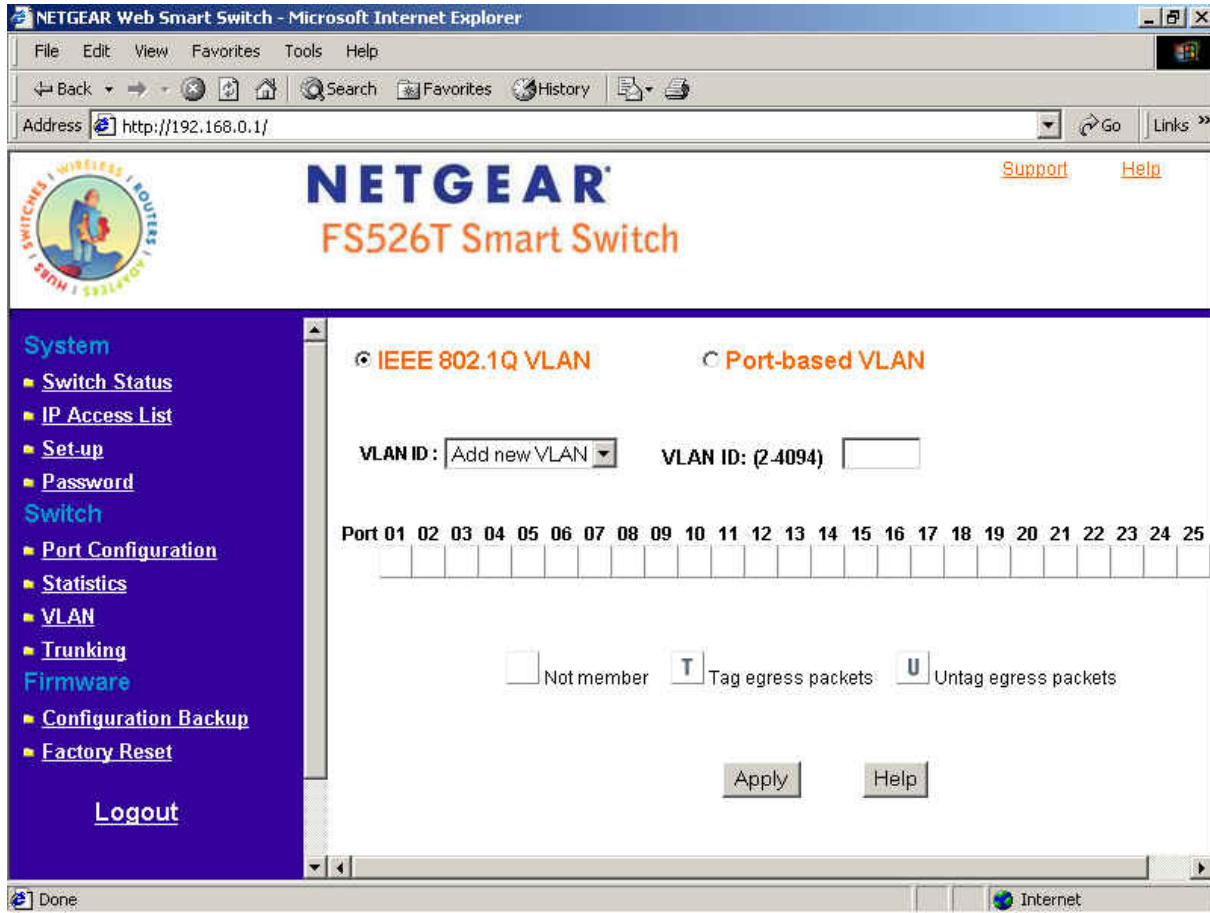


Figure 5-22. Switch> VLAN Setting> Tag VLAN: Add new VLAN

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.

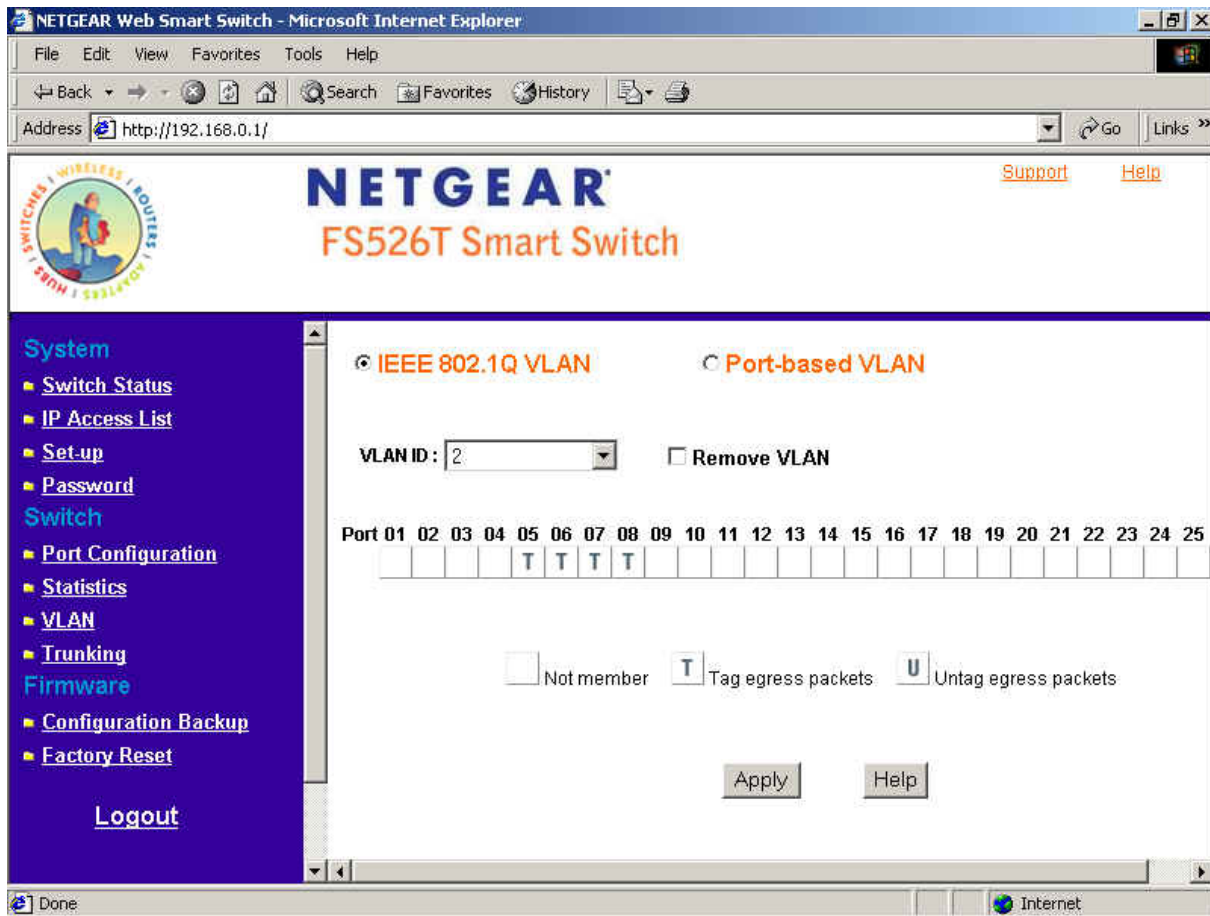


Figure 5-23. Switch> VLAN Setting> Tag VLAN: Delete a VLAN

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.

The screenshot shows the NETGEAR Web Smart Switch configuration interface in Microsoft Internet Explorer. The browser address bar shows <http://192.168.0.1/>. The page title is "NETGEAR FS526T Smart Switch". The navigation menu on the left includes System (Switch Status, IP Access List, Set-up, Password), Switch (Port Configuration, Statistics, VLAN, Trunking), and Firmware (Configuration Backup, Factory Reset). The main content area is titled "IEEE 802.1Q VLAN" and "Port-based VLAN". The "VLAN ID" dropdown menu is set to "PVID Setting". Below this is a table of 26 ports with their corresponding PVID values.

Port	PVID	Port	PVID	Port	PVID	Port	PVID
01	1	02	1	03	1	04	1
05	2	06	2	07	2	08	2
09	1	10	1	11	1	12	1
13	1	14	1	15	1	16	1
17	1	18	1	19	1	20	1
21	1	22	1	23	1	24	1
25	1	26	1				

Figure 5-24. Switch> VLAN Setting> Tag VLAN: PVID Setting

Switch> Trunking

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.

- Click to select Trunk members from a pull-down menu for a Trunk group
- Click Apply to activate the new setting

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

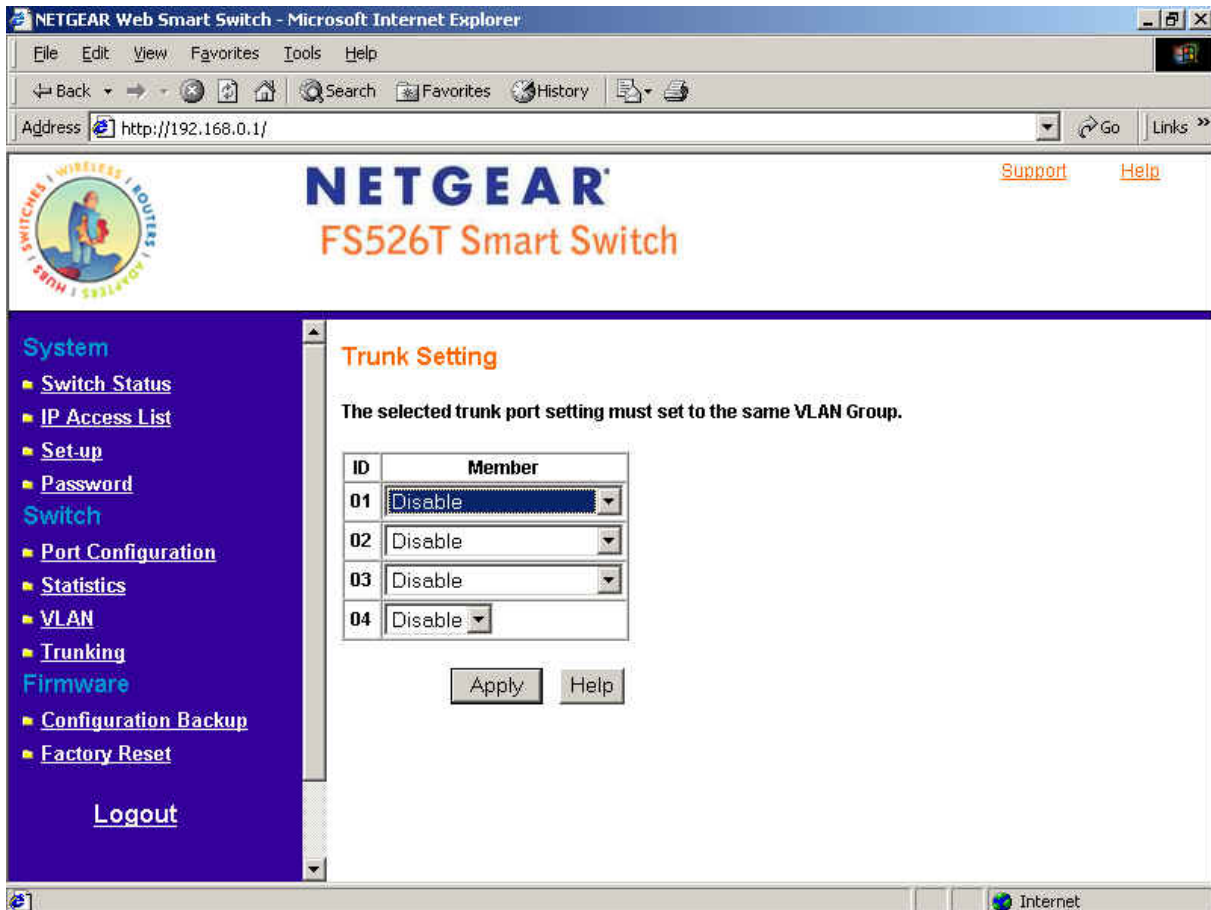


Figure 5-25. Switch> Trunk Setting

For Trunk Group 01, there are four types of member selection:

- o Disable: Trunk Group 01 is disabled.
- o 01, 02: These two ports are trunked as Trunk Group 01.
- o 01, 02, 03, and 04: These four ports are trunked as Trunk Group 01.
- o 01 ~ 08: These eight ports are trunked as Trunk Group 01.

The other Trunk Groups behave in a similar manner.

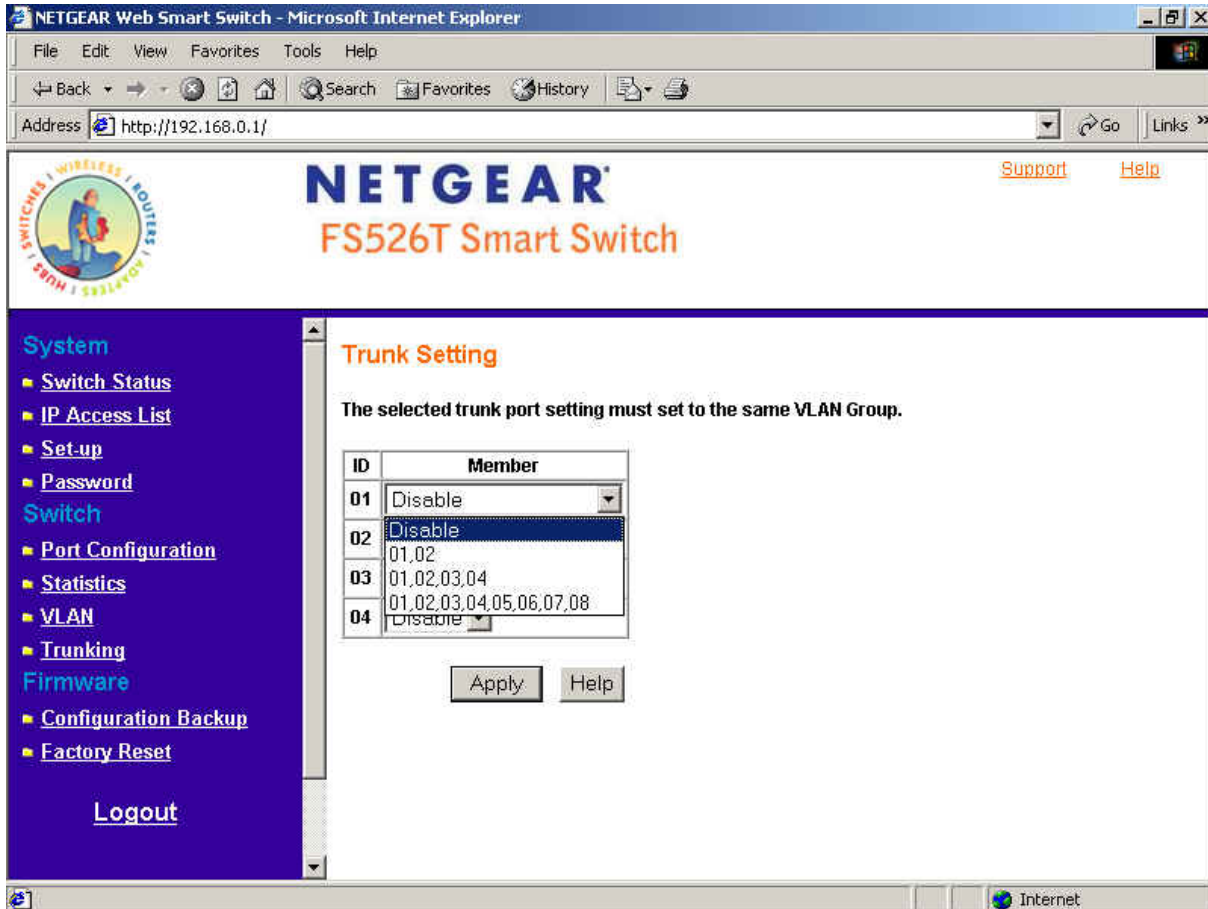


Figure 5-26. Switch> Trunk Setting: Trunk Group 01

Firmware

There are 2 options available:

- Configuration Backup
- Factory Reset

Firmware> Configuration Backup

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 as shown in Figure 5-31.
- When download process is finished, click OK to confirm disconnection of current browser connection as shown in Figure 5-32.

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

Note: The Backup file does not affect the password or MAC address of the switch

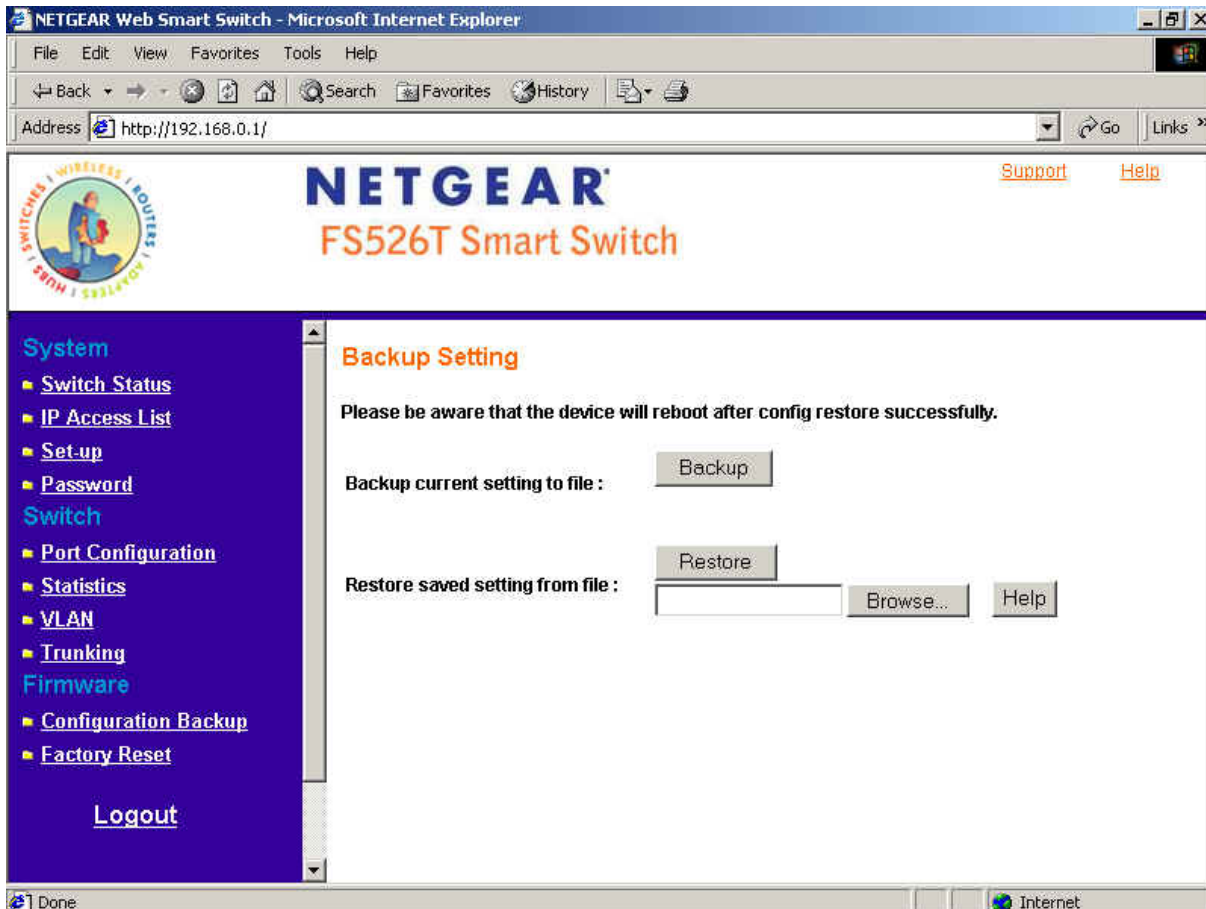


Figure 5-30. Firmware> Configuration Backup> Backup Setting: Backup

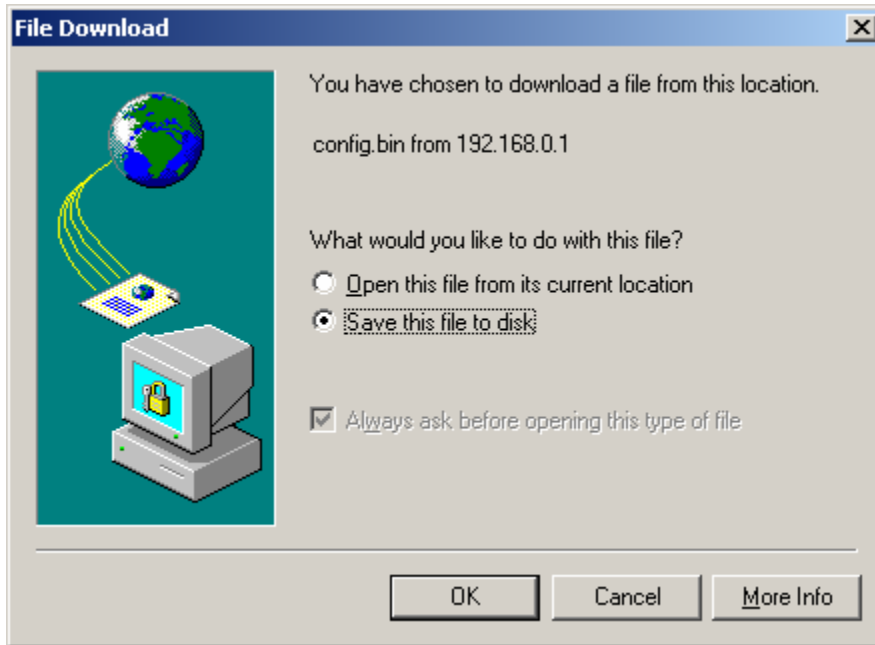


Figure 5-31. Firmware> Configuration Backup> Backup Setting: Restore

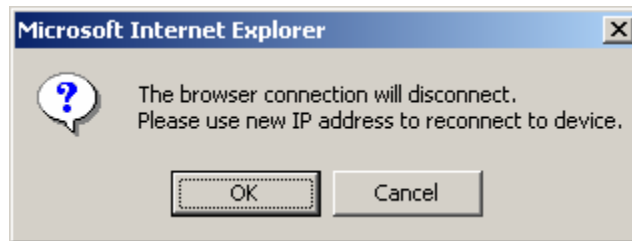


Figure 5-32. Firmware> Configuration Backup> Backup Setting: Reboot

Firmware> Factory Reset

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.

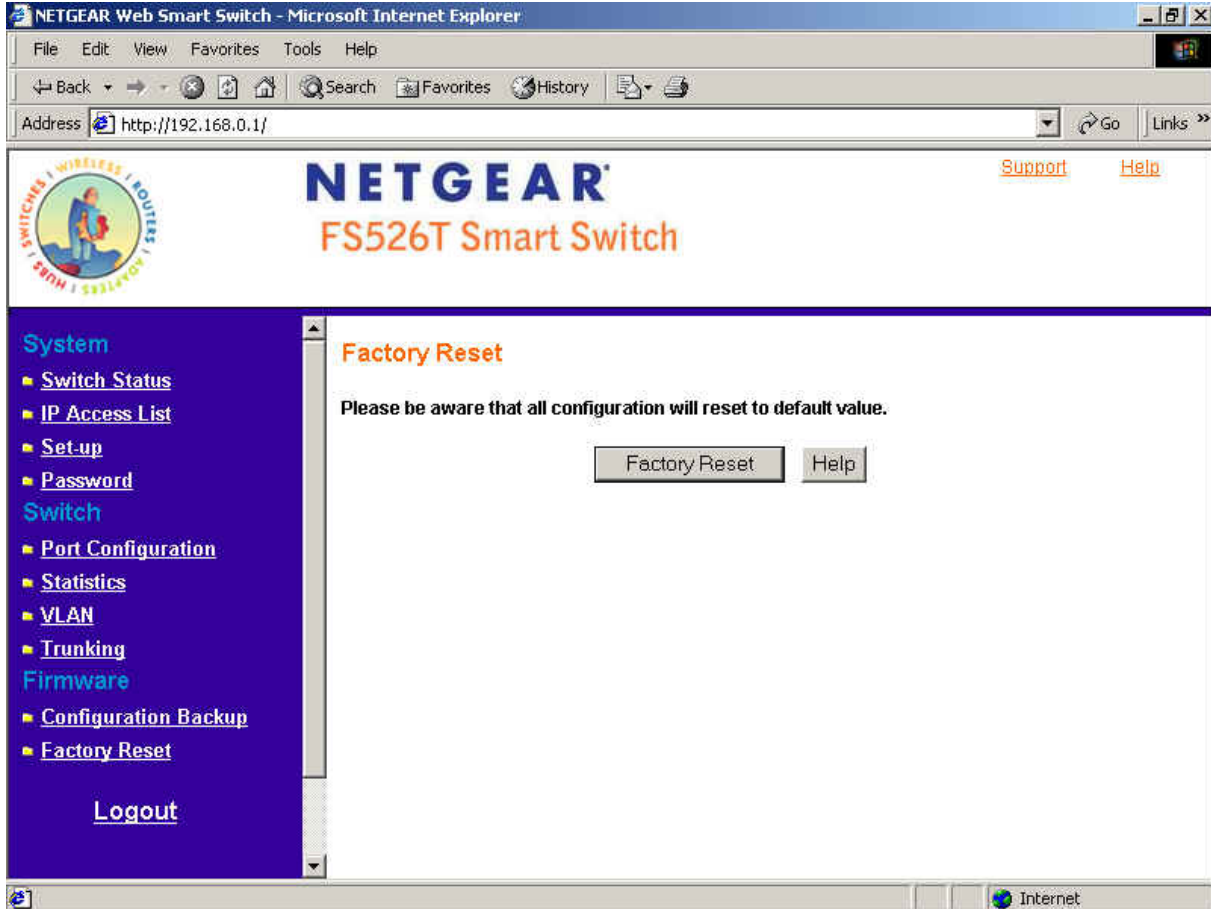


Figure 5-33. Firmware> Factory Reset

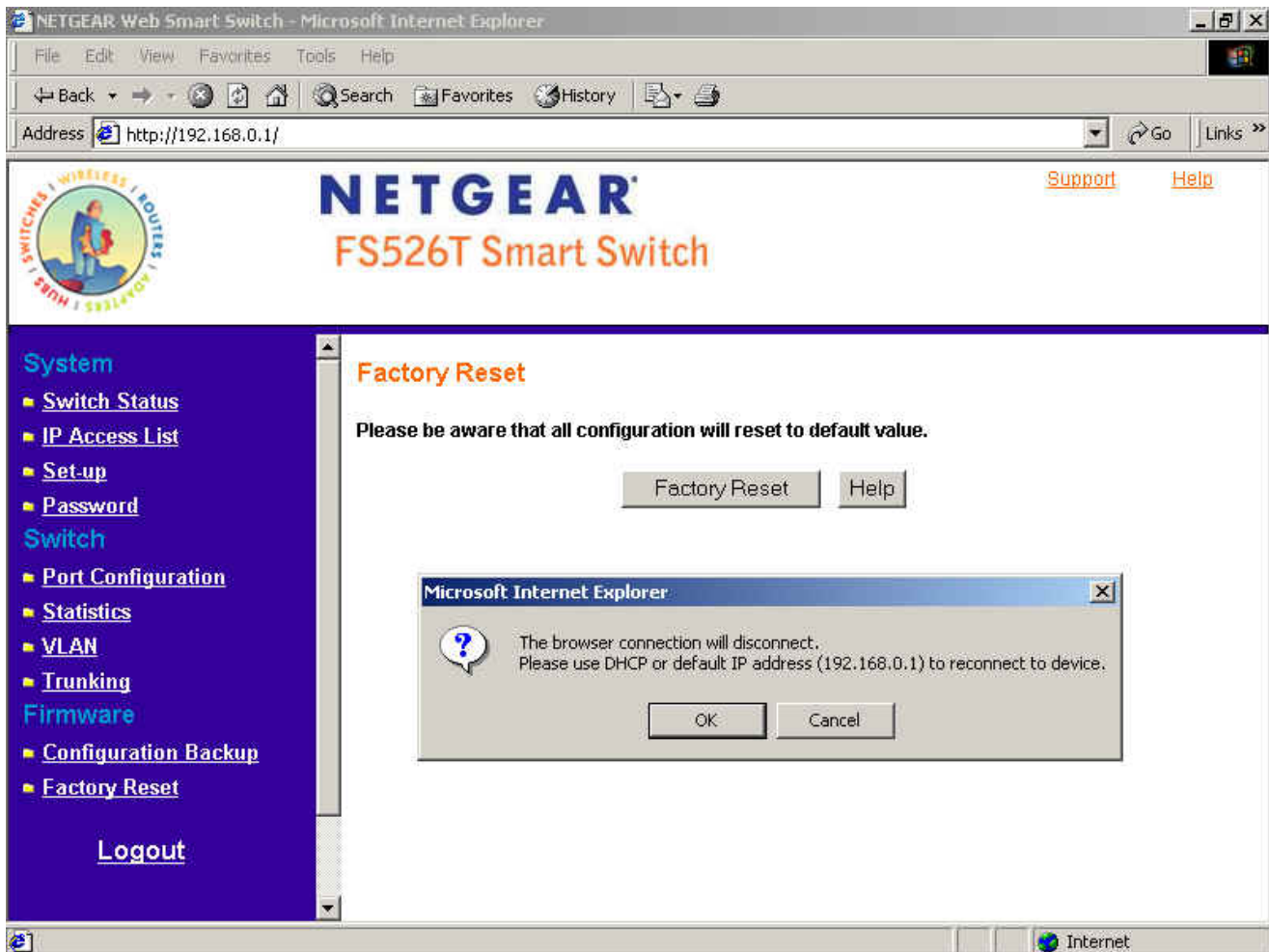


Figure 5-34. Firmware> Factory Reset: reboot

Logout

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

APPENDIX A: DEFAULT SETTINGS

This appendix provides default settings for the NETGEAR Model FS526T Smart Fast Ethernet Switch. 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	FS526T DEFAULT SETTING
Port Speed	Auto-negotiation
Port Duplex	Auto-negotiation
Flow Control (half duplex)	Enabled
Flow Control (full duplex)	Enabled
IP Configuration	DHCP enabled
Default IP address (if no DHCP server)	192.168.0.239
Password	password
VLAN	Port-Based VLAN
Link Aggregation (Trunk)	Disabled
Traffic Prioritization (QoS)	All ports set normal priority

APPENDIX B: Virtual Local Area Network (VLAN) IEEE 802.1Q

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 switches. 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 VLAN Behavior in the FS526T

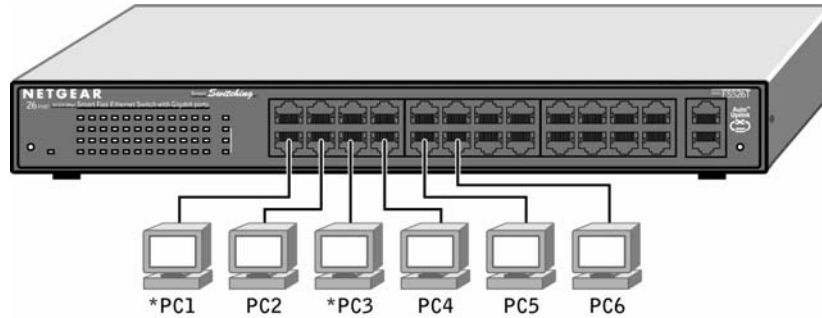
Packets received by the switch will be treated in the following way:

- 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. Please see the following figure for detail setting.



- 1) Setup the following VLANs: VLAN 10, 20.
 - 2) Configure the VLAN membership. Each figure below shows a different VLAN to be setup. Be sure to set all of them as follows.
1. Setting up first VLAN group, VLAN ID = 10:

NETGEAR Web Smart Switch - Microsoft Internet Explorer

Address: http://172.16.3.122/

NETGEAR FS526T Smart Switch

System

- Switch Status
- IP Access List
- Set-up
- Password

Switch

- Port Configuration
- Statistics
- VLAN
- Trunking

Firmware

- Configuration Backup
- Factory Reset

Logout

Copyright © 2003 NETGEAR, Inc. All Rights reserved.

Done Internet

IEEE 802.1Q VLAN (selected) Port-Based VLAN

VLAN ID: 10 (selected) Remove VLAN

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	U	U	T																							

Not member Tag egress packets (selected) Untag egress packets (selected)

Apply Help

2. Setting up second VLAN group, VLAN ID = 20:

NETGEAR Web Smart Switch - Microsoft Internet Explorer

Address: http://172.16.3.122/

NETGEAR FS526T Smart Switch

Support Help

- System
 - Switch Status
 - IP Access List
 - Set-up
 - Password
- Switch
 - Port Configuration
 - Statistics
 - VLAN
 - Trunking
- Firmware
 - Configuration Backup
 - Factory Reset

Logout

Copyright © 2003 NETGEAR, Inc. All Rights reserved.

IEEE 802.1Q VLAN Port-Based VLAN

VLAN ID: 20 Remove VLAN

Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
				U	T	U																				

Not member Tag egress packets Untag egress packets

Apply Help

Done Internet

3. Modify PVID Setting to apply previous two VLAN groups:

NETGEAR Web Smart Switch - Microsoft Internet Explorer

Address: http://172.16.3.122/

NETGEAR FS526T Smart Switch

Support Help

System

- Switch Status
- IP Access List
- Set-up
- Password

Switch

- Port Configuration
- Statistics
- VLAN
- Trunking

Firmware

- Configuration Backup
- Factory Reset

[Logout](#)

Copyright © 2003 NETGEAR, Inc. All Rights reserved.

IEEE 802.1Q VLAN Port-Based VLAN

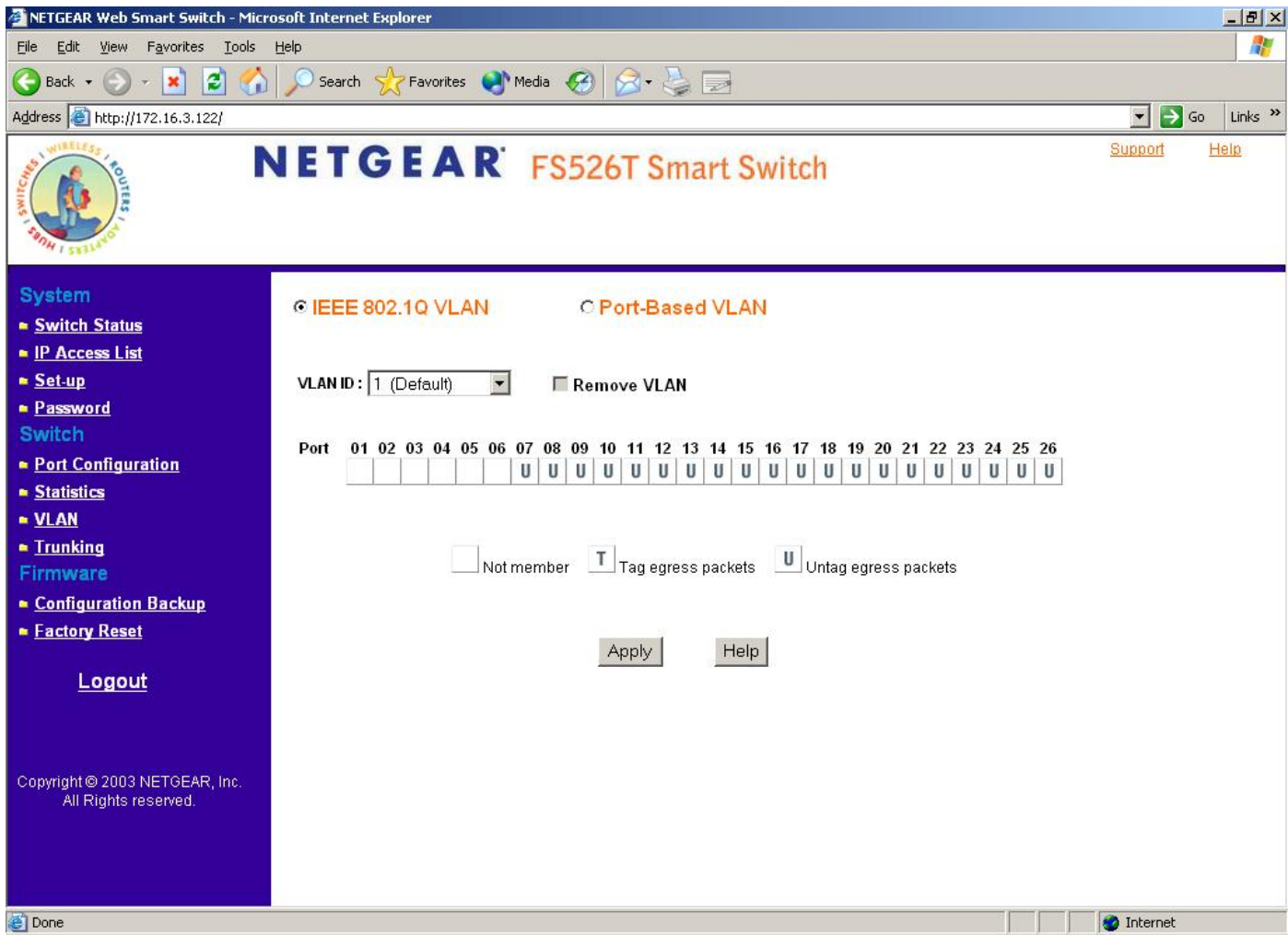
VLAN ID: PVID Setting

Port	PVID	Port	PVID	Port	PVID	Port	PVID
01	10	02	10	03	10	04	20
05	20	06	20	07	1	08	1
09	1	10	1	11	1	12	1
13	1	14	1	15	1	16	1
17	1	18	1	19	1	20	1
21	1	22	1	23	1	24	1
25	1	26	1				

Apply Help

Done Internet

4. 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.

5. 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: Virtual Local Area Network (VLAN): Port-based VLAN

Port-based VLANs will help efficiently confine the broadcast traffic to the switch ports with the specific VLAN. This switch allows up to 26 port-based VLAN groups, so each port can be in its own VLAN. A port may be a member of more than one VLAN. The default VLAN group port-based VLAN that have all ports belonging to VLAN 1.

Port-based VLAN Behavior in the FS526T

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

- When a packet enters a port, it only can proceed to other ports on that same VLAN. The packet will only 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.

- 1) Setup the following VLANs, each with defined descriptions:
VLAN 1 (IT department)
VLAN 2 (Sales department)
VLAN 3 (Marketing department)
VLAN 4 (Accounting department).
- 2) Configure the VLAN membership. The figure below shows all different VLANs to be setup. Be sure to set all of them as shown below.

NETGEAR Web Smart Switch - Microsoft Internet Explorer

Address: http://192.168.0.2/

NETGEAR FS526T Smart Switch

Support Help

IEEE 802.1Q VLAN Port-Based VLAN

ID	Description	Member
01	IT Dept.	15 16 17 18 21 22 23 24 25 26
02	Sales	01 02 03 04 05 06 07 08 25
03	Marketin	07 08 09 10 11 12 13 14 25
04	Account	19 20 25

Add Group Delete Group Help

System

- Switch Status
- IP Access List
- Set-up
- Password

Switch

- Port Configuration
- Statistics
- VLAN
- Trunking

Firmware

- Configuration Backup
- Factory Reset

Logout

Copyright © 2003 NETGEAR, Inc. All Rights reserved.

- 3) Setting up second VLAN group (Sales), VLAN ID = 02, with membership of ports 1–8, 25.
- 4) Setting up third VLAN group (Marketing), VLAN ID = 03, with membership of ports 7–14, 25.
- 5) Setting up fourth VLAN group (Accounting), VLAN ID = 04, with membership of ports 19–20, 25.
- 6) 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.
- 7) Ports 7 and 8 are on both VLAN 02 and 03 because they connect to a file server and print server. Sales and Marketing departments can both use these servers.
- 8) Port 25 provides Gigabit speed for email server and Internet connection so each VLAN included port 25. It is the uplink port, so each VLAN must have it to communicate to the rest of the network.

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 accounting 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.