700 Series Software Manual v2.1

NETGEAR

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

202-10132-01
September 2005

© 2005 by NETGEAR, Inc. All rights reserved.

Trademarks

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.

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

Audience 1-1
Why the Document was Created 1-1
How to Use This Document 1-1
Typographical Conventions 1-2
Special Message Formats 1-2
Features of the HTML Version of this Manual 1-3
How to Print this Manual 1-4

Chapter 2
Switch Management Overview

Management Access Overview 1-1
Protocols 1-2
Virtual Terminal Protocols 1-3
SNMP Protocol 1-3
SNMP Access 1-3

Chapter 3
Software Upgrade Procedure

Chapter 4
Administration Console Telnet Interface

Set Up Your Switch Using Direct Console Access 3-1
Introduction to the Command Menu Interface 3-3
Main Menu> System 3-5
Main Menu> Status 3-5
Main Menu> Status >Switch Statistics 3-5
Main Menu> Status >Reset Statistics 3-6
Main Menu> Status > MAC Address Table 3-6
Main Menu> Set-Up 3-7
Main Menu> Set-Up> System Configuration 3-7
Main Menu> Set-Up> IP Configuration 3-8
Main Menu> Set-Up> Port Configuration 3-9

Main Menu> Set-Up> GBIC 3-10
Main Menu> Tools 3-11
Main Menu> Security 3-12
Main Menu> Advanced 3-12
Main Menu> Advanced> Port Mirroring 3-14
Main Menu> Advanced> Port Trunking 3-15
Main Menu> Advanced> Virtual Cable Tester 3-15
Main Menu> Advanced> Advanced Security 3-16
Main Menu> Advanced> Advanced Security> System Authentication 3-16
Main Menu> Advanced> Advanced Security > Port-Based Authentication 3-16
Main Menu> Advanced > Trusted MAC Address Table 3-17
Main Menu > Advanced > MAC Address Lockdown Table 3-17
Main Menu> Advanced> Advanced Tools 3-18
Main Menu> Advanced> Advanced Tools> Software Upgrade 3-18
Main Menu> Advanced> Advanced Tools> Configuration Management 3-19
Main Menu> Advanced> Traffic Management 3-19
Main Menu> Advanced> Traffic Management> Port Priority 3-20
Main Menu> Advanced> Traffic Management> DiffServ 3-20
Main Menu> Advanced> Traffic Management> Broadcast Control 3-21
Main Menu> Advanced> VLANS 3-21
Main Menu> Advanced> VLANS> VLAN Admin 3-21
Main Menu> Advanced> VLANS> VLAN Membership 3-22
Main Menu> Advanced> VLANS> VLAN Ports 3-22
Main Menu> Advanced> Spanning Tree 3-23
Main Menu> Advanced> Spanning Tree> Bridge Settings 3-23
Main Menu> Advanced> Spanning Tree> Port Settings 3-24
Main Menu> Advanced> MAC Address Manager 3-25
Main Menu> Advanced> MAC Address Manager> Aging Time 3-26
Main Menu> Advanced> MAC Address Manager> Static Addresses 3-26
Main Menu> Advanced> Multimedia Support 3-27
Main Menu> Advanced> Multimedia Support> Enable/Disable IGMP 3-27
Main Menu> Advanced> Multimedia Support> Static Multicast Administration 3-27
Main Menu> Advanced> Multimedia Support> Static Multicast Membership ..3-28
Main Menu> Advanced> SNMP 3-29
Main Menu> Advanced> SNMP> Community Table 3-29

Main Menu> Advanced> SNMP> Host Table 3-30
Main Menu> Advanced> SNMP> Trap Settings 3-30

Chapter 5
Web-Based Management Interface

Web Based Management Overview 4-2
System Information 4-3
Status Menus 4-4
Status > Switch Statistics 4-5
Status > Port Statistics 4-7
Status > Error Statistics 4-8
Status > Most Active Ports 4-9
Status > Reset Statistics 4-10
Status > Port Settings 4-10
Status > MAC Address Table 4-11
Set-up Menu 4-12
Set-up> System Configuration 4-12
Set-up> IP Configuration 4-13
Set-up> Port Configuration 4-14
Set-up> GBIC 4-15
Tools Menu 4-16
Tools> Save Configuration 4-16
Tools> Restore Factory Defaults 4-17
Tools> Device Reset 4-18
Security> Passwords 4-18
Advanced Options 4-19
Advanced > Disable Advanced Alerting 4-22
Advanced > Port Mirroring 4-22
Advanced > Port Trunking 4-23
Advanced > Virtual Cable Tester 4-23
Advanced> Advanced Security 4-24
Advanced > Advanced Security > System Authentication 4-25
Advanced > Advanced Security > Port-Based Authentication 4-25
Advanced > Advanced Security > Trusted MAC Address Table 4-26
Advanced > Advanced Security > MAC Address Lockdown Table 4-27
Advanced > Advanced Tools 4-28

Advanced > Advanced Tools > Software Upgrade 4-29
Advanced > Advanced Tools > Configuration Management 4-30
Advanced > Traffic Management 4-31
Advanced > Traffic Management > Traffic Priority 4-31
Advanced > Traffic Management > Broadcast Control 4-32
Advanced> VLANS 4-32
Advanced> VLAN> Primary VLAN 4-33
Advanced> VLAN> VLAN Ports 4-34
Advanced> Spanning Tree 4-35
Advanced> Spanning Tree >Bridge Settings 4-35
Advanced> Spanning Tree > Port Settings 4-36
Advanced> MAC 4-37
Advanced> MAC> Address Aging 4-38
Advanced> MAC> Static Addresses 4-38
Advanced> Multimedia Support 4-39
Advanced> Multimedia Support>Enable/Disable IGMP 4-39
Advanced>Multimedia Support> Static Multicast Groups 4-40
Advanced> SNMP 4-40
Advanced> SNMP> Community Table 4-41
Advanced> SNMP> Host Table 4-41
Advanced> SNMP> Trap Setting 4-42

Chapter 6
Command Line Interface

Manual Syntax 5-1
Entering the CLI 5-1
Help 5-2
Ping 5-2
Exit 5-3
Show 5-3
Show DiffServ 5-4
Show Dot1x 5-4
Show Interfaces 5-4
Show IP 5-5
Show Mac-Address-Table 5-5
Show Mirror 5-7

Show Multimedia 5-7
Show Running-Config 5-7
Show SNMP 5-8
Show Spanning Tree 5-9
Show System 5-10
Show Trunking 5-11
Show VLAN 5-11
Configure 5-13
DiffServ 5-13
Dot1x 5-14
Exit 5-15
Interface 5-15
CoS (Class or Service) 5-16
Exit 5-16
Flow Control 5-17
Mirror 5-17
No 5-18
Type 5-18
Shutdown 5-18
Spanning Tree 5-19
Speed 5-19
Switchport 5-19
Trunking 5-20
Mac-address-table 5-21
Multimedia 5-22
No 5-23
SNMP Server 5-23
Spanning Tree 5-26
System 5-27
IP 5-28
IP-Filter 5-28
IP-filter address 5-29
IP-Mode 5-29
Mask 5-29
Gateway 5-29

Save 5-30
Restore 5-30
Web 5-30
Telnet 5-30
Username 5-31
Password 5-31
Firmware boot 5-31
Firmware TFTP-IP 5-32
Firmware TFTP-File 5-32
RADIUS 5-32
Reset 5-33
Stat-Reset 5-34
VLAN 5-34

Appendix A
Virtual Local Area Network

VLAN Behavior in a 700 Series Managed Switch A-2

Appendix B
Cabling Guidelines

Fast Ethernet Cable Guidelines B-1
Category 5 Cable B-2
Category 5 Cable Specifications B-2
Twisted Pair Cables B-3
Patch Panels and Cables B-4
Using 1000BASE-T Gigabit Ethernet over Category 5 Cable B-5
Cabling B-5
Near End Cross Talk (NEXT) B-6
Patch Cables B-6
RJ-45 Plug and RJ-45 Connectors B-6
Conclusion B-8

Appendix C
802.1x Port-Based Authentication Overview

Understanding 802.1x Port Based Network Access Control C-1

Glossary

Index

Chapter 1
About This Guide

Thank you for purchasing the NETGEAR™ 700 Series Switches.

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 700 Series Switches 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 700 Series Switches software. It is intended to provide an understanding of the configuration options of 700 Series Switches 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 700 Series Switches software. The commands can be accessed from the CLI, telnet (CMI), and Web interfaces.

- Chapter 4, “Administration Console Telnet Interface” describes the CMI.
- Chapter 5, “Web-Based Management Interface” describes the Web interface.
- Chapter 6, “Command Line Interface” describes the CLI, which can be reached through the telnet (CMI) interface.

Note: Refer to the release notes for the 700 Series Switches 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 700 Series Switches according to these specifications:

Table 1-1. Manual Specifications

Product Version	700 Series Switches
Manual Publication Date	September 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 700 Series Switches. Topics include:

- Management Access Overview
- SNMP Access
- Protocols

Management Access Overview

Your NETGEAR 700 Series Switches gives you the flexibility to access and manage the switch using any or all of the following methods:

- An administration console
- Web browser interface
- External Simple Network Management Protocol (SNMP)-based network-management application

The administration console and Web browser interface support are embedded in the switch's firmware and available for immediate use. Each of these management methods has advantages. Table 1-1 compares the three management methods.

Table 2-1. Comparing Switch Management Methods

Management Method	Advantages	Disadvantages
Administration console	• Out-of-band access via direct cable connection means network bottlenecks, crashes, and downtime do not slow or prevent access • No IP address or subnet needed • Menu or CLI based • HyperTerminal access to full functionality (HyperTerminal are built into Microsoft Windows 95/98/NT/2000 operating systems) • Secure – make sure the switch is installed in a secure area.	• Must be near switch or use dial-up connection • Not convenient for remote users • Not graphical
Web browser or Telnet	• Can be accessed from any location via the switch's IP address • Ideal for configuring the switch remotely • Compatible with Internet Explorer and Netscape Navigator Web browsers • Familiar browser interface • Graphical data available • Most visually appealing • Menu or CLI interfaces available	• 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)

For a more detailed discussion of the Administration Console, see Chapter 4. For a more detailed discussion of the Web Browser Interface, see Chapter 5.

Protocols

Your NETGEAR 700 Series Switches supports the following protocols:

- Virtual terminal protocols, such as Telnet
- SNMP

Virtual Terminal Protocols

A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on a NETGEAR 700 Series Switches before you can establish access to it with a virtual terminal protocol.

Terminal emulation differs from a virtual terminal protocol in that you must connect a terminal or PC directly to the console port. Figure 2-1 shows a UNIX workstation connected to the system through a virtual terminal protocol (Telnet), and a terminal connecting directly to the console port through a null-modem cable.

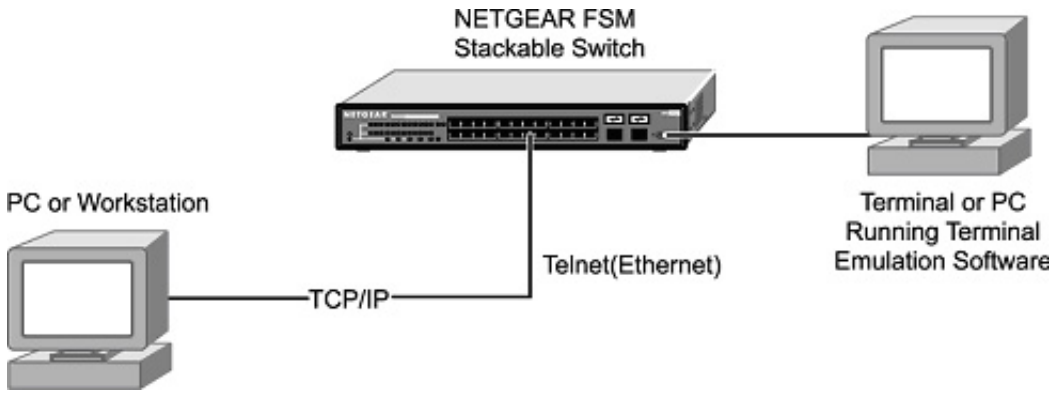


Figure 2-1: Administration Console Access

SNMP Protocol

SNMP is the standard management protocol for multi-vendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

SNMP Access

With this access method, you can use an external SNMP-based application to manage your NETGEAR 700 Series Switches. Figure 2-2 shows an example of this management method.

This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string and that the SNMP Network Management Station is entered in the SNMP Host table on the switch. This management method, in fact, uses two community strings: the GET community string and the SET community string. If the SNMP Network management Station only knows the SET community string, it can read from and write to the MIBs. However, if it only knows the GET community string, it can only read MIBs. The default GET community string for the switch is ‘public’, and the host table is empty.

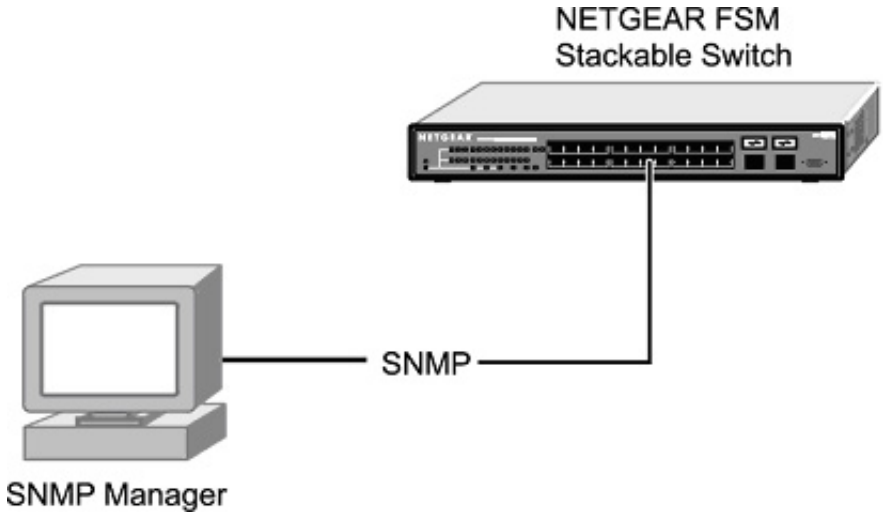


Figure 2-2: SNMP-Based Management Method

Chapter 3
Software Upgrade Procedure

As networking technology advances, NETGEAR will release new versions of the software that runs the switch. These software releases will provide new capabilities that can extend the useful life of your switch. This manual is updated whenever there is a change in either the first or second positions of the software version number. The third position in the software version number identifies bug fix and patch versions for which this manual is not updated. The upgrade procedure and the required equipment are described in this chapter.

IP address, Network Mask, and Default Gateway are not affected by upgrading the software. These settings will be preserved in non-volatile memory (NVRAM).

The upgrade process is accomplished by having the switch boot from a TFTP server instead of its own NVRAM. To initiate this sequence, the user must set the ‘Next Boot From’ configuration parameter to ‘Boot from Net’, and then perform a ‘reset’. When the ‘Boot from Net’ option is set, the switch will start using an image residing on a TFTP server on the network. Be sure that the TFTP server residing on the network is accessible by the switch. Once completed, the software version should be verified in the System page.

	Note: It is highly recommended, though not necessary, to use a RS-232 serial port connection to the switch during the software upgrade procedure. When using a Telnet Session or Web interface alone, your connection to the switch will not be available until the switch has completed its boot up and entered the Spanning Tree forwarding mode. This can take up to three minutes.

The upgrade procedure below gives the exact steps to follow when using the Web interface. The process is similar with either the CMI or CLI interfaces.

1. Select Advanced > Advanced Tools > Software Upgrade.
2. Select Next boot from: Net.
3. Verify information such as the IP address for the TFTP Server and the file name of the new software image.
4. Save the setting in non-volatile memory. Press the Apply button and then go to the Tools > Save Configuration to NVRAM option.

5. Restart the system via the Tools > Reset command. Bootstrap will retrieve the new software image then pass control to it. The system executes the new software image.

   The previous software image in non-volatile memory will not be replaced by the new software image. This enables you to return to the previous image if you do not like the new image.

6. Verify that the new software is loaded by going to the Advanced > Advanced Tools > Software Upgrade screen and checking the Software Version.

   Test your switch to make sure the new image is working correctly. If you decide to keep the new image, go to Software Upgrade again. Select the Next boot from: Net & Save option.

7. Save the setting in non-volatile memory. Press the Apply button, and then go to the Tools > Save Configuration to NVRAM option.

8. Restart the system via the Tools > Reset command

   The new image should overwrite the old image in NVRAM. Verify it by going to the Advanced > Advanced Tools > Software Upgrade screen and checking the Software Version.

Chapter 4
Administration Console Telnet Interface

The administration console is an internal, character-oriented, VT-100/ANSI menu-driven user interface for performing management activities. Using this method, you can view the administration console from a terminal, PC, Apple Macintosh, or UNIX workstation connected to the switch's console port. Figure 4-1 shows an example of this management method.

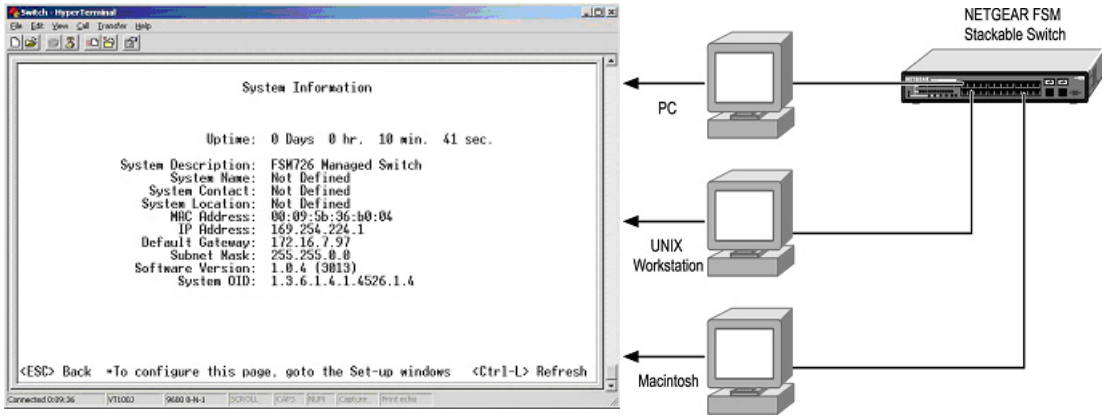


Figure 4-1: Administration Console Management Method

Set Up Your Switch Using Direct Console Access

The direct access management method is required when you initially set up your switch. Thereafter, the convenience and additional features of the Web management access method (described in Chapter 5) make it the best method to manage the switch.

Direct access to the switch console is achieved by connecting the switch's console port to a VT-100 or compatible terminal or to a PC, Apple Macintosh, or UNIX workstation equipped with a terminal-emulation program. This connection is made using the null-modem cable supplied with the switch.

Examples of terminal-emulation programs include:

- HyperTerminal, which is included with Microsoft Windows operating systems
- ZTerm for the Apple Macintosh
- TIP for UNIX workstations

This example describes how to set up the connection using a HyperTerminal on a PC, but other systems follow similar steps.

1. Click the Windows Start button. Select Accessories and then Communications. HyperTerminal should be one of the options listed in this menu. Select HyperTerminal
2. The following screen will appear. Enter a name for this connection. In the example below, the name of the connection is FSM726. Click OK.

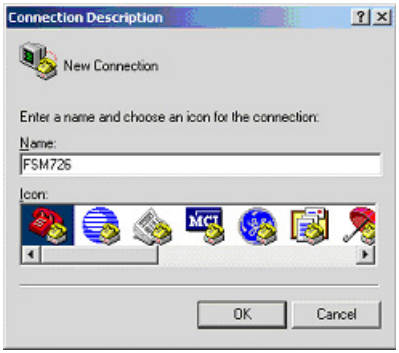


Figure 4-2: Connection Description

3. The following screen will appear. In the bottom, drop down box labeled **Connect Using**, click the arrow and choose the COM port to which the switch will connect. In the example below, COM1 is the port selected. Click **OK**.

Figure 4-3: COM Port Selection

4. When the following screen appears, make sure that the port setting are as follows:

Baud Rate:	9600
Data Bits:	8
Parity:	None
Stop Bits:	1
Flow Control:	None

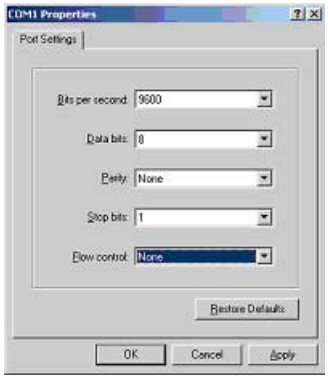


Figure 4-4: Connection Settings

5. Click OK.

The HyperTerminal window will open and you should be connected to the switch. If you do not see the welcome screen or a system menu, press the return key.

In order to use the arrow keys when attached to the User Interface via a Telnet Session, make sure the VT100 Arrows option is turned on. Under the terminal pull-down menu, choose Properties to set this option.

Introduction to the Command Menu Interface

The switch offers a Command Menu Interface (CMI), which is a menu-driven method for managing the switch, as well as a Command Line Interface (CLI), which uses text inputs to manage the switch. The CLI is accessed through the CMI, but is not addressed in this chapter. Chapter 6 discusses the CLI in detail.

There are several characteristics to the CMI pages that are necessary to know before proceeding to use it. The TAB key or the arrow keys may be used to move within menus and sub-screens. At the bottom of every screen are some key commands available for that particular screen, as well as some helpful information.

The common keystrokes and their definitions and intricacies are listed below:

ESC	Return to the previous menu or screen, or abort editing
Tab	Select field
Ctrl-L	Refresh the screen
Ctrl-D	Log off (password enabled)
Ctrl-M	Move to field (Switch Statistics and Port Configuration menus only)
Ctrl-W	Saves current configuration to Non-Volatile RAM (NVRAM)
Spacebar	Toggles between possible settings for a field
Enter	Select a menu item, edit a field, or accept a value after editing a field
Ctrl-X	Delete a table entry

The main menu displays all the sub-menus that are available. Pressing ‘Enter’ when an option is highlighted will confirm the choice of the specified sub-menu. The ‘hotkey’ or letter in front of each menu option can also be typed to directly choose that option. As shown below, there are six menu items to choose from:

Figure 4-5: Main Menu

To log out of the user interface, press Ctrl-D at any time during your telnet session. You will be brought back to the login screen (password enabled) or Main Menu (password disabled).

Main Menu> System

This screen displays the main menu System Information options. The user-definable options are: System Name, System Contact, System Location, IP Address, Default Gateway, and Subnet Mask. The System OID option is used for production testing.

```
                    System Information


              Uptime:  0 Days  0 hr.  10 min.  41 sec.

System Description:  FSM726 Managed Switch
       System Name:  Not Defined
     System Contact:  Not Defined
    System Location:  Not Defined
        MAC Address:  00:09:5b:36:b0:04
         IP Address:  169.254.224.1
    Default Gateway:  172.16.7.97
        Subnet Mask:  255.255.0.0
   Software Version:  1.0.4 (3013)
         System OID:  1.3.6.1.4.1.4526.1.4
```

Figure 4-6: System Information

Main Menu> Status

There are three Status sub-menus: Switch Statistics, Reset Statistics, and MAC Address Table.

Main Menu> Status >Switch Statistics

The Port-ID field allows you to choose a port to be observed. To get to the left side, use Ctrl-M to move to that field. The screen displays basic statistics associated with the highlighted port.

```
Unit   1                Status > Switch Statistics

 Port                Uptime:   0 Days  1 hr.  16 min.  48 sec.
  1
  2
  3                  Inbound                              Outbound
  4
  5
  6                  Octets:  34742999                  Octets:  4578300
  7          Unicast Packets:  34171            Unicast Packets:  29033
  8      Non-unicast Packets:  27391        Non-unicast Packets:  149
  9          Packet Discards:  0                Packet Discards:  0
 10            Packet Errors:  0                  Packet Errors:  0
 11       Undersized Packets:  0
 12        Oversized Packets:  0
 13
 14
 15
 16
```

Figure 4-7: Switch Statistics

Main Menu> Status >Reset Statistics

The Reset Statistics menu allows you to reset the statistics counter to zero. When you choose this option, a prompt will appear asking you for a confirmation. Once the confirmation is made, the statistics counters will be reset to zero.

```
a. Switch Statistics
b. Reset Statistics
c. MAC Address Table


++++++++++++++++++++++++++++++++++++++++++++++++
+                                              +
+  Do you want to reset the counters? Yes/No   +
+                                              +
++++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 4-8: Reset Switch Statistics

Main Menu> Status > MAC Address Table

The MAC Address lookup table displays the MAC addresses that are currently in the address database. When addresses are in the database, the packets intended for those addresses are forwarded directly to those ports. You can filter out addresses in the table by port, VLAN, or MAC address by entering a value in those fields, and selecting Query.

```
                    Status > MAC Address Table

  Port: [   ] VLAN ID:      MAC Address:                    Query  Next  Prev

  Port    VLAN     MAC Address            Port    VLAN     MAC Address
-------------------------------------------------------------------------------
  1:1     1     00:00:39:da:5a:1e         1:1     1     00:06:5b:7c:22:06
  1:1     1     00:00:86:45:b8:87         1:1     1     00:06:5b:7e:21:1b
  1:1     1     00:00:e2:82:94:40         1:1     1     00:06:5b:7e:48:59
  1:1     1     00:00:e2:82:c6:80         1:1     1     00:06:5b:7e:48:69
  1:1     1     00:02:a5:9a:fa:f0         1:1     1     00:06:5b:a8:9a:7c
  1:1     1     00:06:5b:21:0e:0e         1:1     1     00:06:5b:a8:9a:f4
  1:1     1     00:06:5b:6d:a6:4a         1:1     1     00:06:5b:cd:54:f1
  1:1     1     00:06:5b:6d:a6:4b         1:1     1     00:08:02:63:bd:73
  1:1     1     00:06:5b:6e:32:c6         1:1     1     00:08:02:64:ed:13
  1:1     1     00:06:5b:72:5c:8d         1:1     1     00:08:02:65:11:a6
  1:1     1     00:06:5b:72:5c:94         1:1     1     00:08:02:66:14:d7
  1:1     1     00:06:5b:7b:7e:b2         1:1     1     00:08:02:9d:a0:6e
  1:1     1     00:06:5b:7b:bc:80         1:1     1     00:08:74:36:df:38
  1:1     1     00:06:5b:7c:22:03         1:1     1     00:08:74:38:91:3b

Enter a Unit:Port Number
<ESC> Back  <Tab> Move the Cursor              <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-9: Address Manager: MAC Address Table

Main Menu> Set-Up

There are four sub-menus under the Set-Up menu:

- System Configuration
- IP Configuration
- Port Configuration
- GBIC

Main Menu> Set-Up> System Configuration

The System Configuration allows you to enter a number of system-related information for easy reference in the future. Such items include System Name, Contact Person, and System Location. The MAC address is also shown, but it is not user configurable.

```
System Description:  FSM726 Managed Switch
       System Name:  Not Defined
    System Contact:  Not Defined
   System Location:  Not Defined
       MAC Address:  00:09:5b:36:b0:04
```

Figure 4-10: System Configuration

Main Menu> Set-Up> IP Configuration

This menu manages the IP related information of the system.

IP Assignment Mode. You can manually enter IP-related information:

- Bootstrap Protocol, which allows the switch to discover its own IP address from a BootP server on the network
- DHCP, which allows the switch to accept DHCP broadcasts from a DHCP server and automatically configures IP related information

The default setting is DHCP, to enable quick and easy set-up. However, since you need to know the IP address of your switch to remotely manage it and DHCP assignments can change, change the IP assignment mode from DHCP to manual after the switch has obtained its IP address.

```
IP Assignment Mode:  Manual

        IP Address:  169.254.224.1
       Subnet Mask:  255.255.0.0
   Default Gateway:  172.16.7.97
```

Figure 4-11: Set-up Manager: IP Configuration

Note: In DHCP mode, if the switch fails to get a DHCP assignment, the switch defaults to 192.168.0.1 as its IP address.

If you are in the manual mode and need to configure the IP information, enter a site-specific IP address, Gateway Address, and Network Mask (or subnet mask). Consult your network administrator for the information.

Press Ctrl-W to save any changes to NVRAM.

Main Menu> Set-Up> Port Configuration

On this page, you can set up the port characteristics related to link operations. All of the parameters on this page are toggle settings. To change, or toggle, between options, press Ctrl-M to move the curser to the ports field and simply press the space bar when the appropriate option is highlighted. To modify ports 17 to 26, you must tab through ports 1 to 16. The comments field is available for you to enter a description of the port.

Unit 1 Set-up > Port Configuration

Port	Name	Link	On/Off	State	Rate/Duplex	Flow Ctrl
1	Not Defined	Down	On	Blocking	(Auto)	(Auto)
2	Not Defined	Down	On	Blocking	(Auto)	(Auto)
3	Not Defined	Down	On	Blocking	(Auto)	(Auto)
4	Not Defined	Down	On	Blocking	(Auto)	(Auto)
5	Not Defined	Down	On	Blocking	(Auto)	(Auto)
6	Not Defined	Down	On	Blocking	(Auto)	(Auto)
7	Not Defined	Down	On	Blocking	(Auto)	(Auto)
8	Not Defined	Down	On	Blocking	(Auto)	(Auto)
9	Not Defined	Down	On	Blocking	(Auto)	(Auto)
10	Not Defined	Down	On	Blocking	(Auto)	(Auto)
11	Not Defined	Down	On	Blocking	(Auto)	(Auto)
12	Not Defined	Down	On	Blocking	(Auto)	(Auto)
13	Not Defined	Down	On	Blocking	(Auto)	(Auto)
14	Not Defined	Down	On	Blocking	(Auto)	(Auto)
15	Not Defined	Down	On	Blocking	(Auto)	(Auto)
16	Not Defined	Down	On	Blocking	(Auto)	(Auto)

Figure 4-12: Port Configuration

Port. The port number on the switch.

Name. The name of the port. This is a user-defined label.

Link. Indicates if the port is Up or Down.

On/Off. Indicates if the port is enabled or disabled by the Administrator.

Admin field. Allows you to Enable or Disable the port.

State field. The State field displays the Spanning Tree State of the port (Blocking, Listening, Learning, Forwarding, or Disabled). You can only observe the status of the ports; you cannot modify this field. The Spanning Tree Protocol controls this field.

Rate/Duplex field. Indicates the speed and duplex for the port. 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); or 100 Mbps full duplex (100M Full).

Enabling auto-negotiation on a port allows a port to sense the communication speed and negotiate the duplex mode (full duplex or half duplex) automatically. The ports will select the highest possible throughput. The port can auto-negotiate with any port that is compliant with IEEE 802.3u. If the other port is not IEEE802.3u compliant, the port will default to half-duplex, 10 Mbps mode. You can operate the communication speed and duplex mode manually.

Flow Control. Allows you to enable or disable Flow Control.

Flow control is a protocol that prevents packets from being dropped by reducing the amount of traffic to a level that can be accommodated. If enabled on both ends of a connection, it will prevent the sender from sending data until the receiver can accept it. This switch complies with the IEEE802.3x flow control standard.

Main Menu> Set-Up> GBIC

This page allows you to choose the port type for the gigabit ports. The default is 1000BASE-T (RJ-45).

```
Set-up > GBIC

Port 9   (Built-In TP   )
Port 10  (Auto Detection)
Port 11  (Auto Detection)
Port 12  (Auto Detection)
```

Figure 4-13: GBIC Port Configuration

All of the parameters on this page are toggle settings. To change, or toggle, between options, press Ctrl-M to move the curser to the ports field and simply press the space bar when the appropriate option is highlighted.

If you want to use a GBIC, the settings on this page must be set accordingly. The switch auto-detects if the media is copper or GBIC. This Auto-detect feature is enabled by default.

Note: Enabling the GBIC connector for a Gigabit Ethernet port disables the built-in 1000BASE-T port.

Main Menu> Tools

These system tools are provided:

- Save Configuration to NVRAM
- Restore Factory Values
- Reset Switch

After making changes to any of the information on the screens in the console interface, you must save the changed settings to NVRAM. Save Configuration to NVRAM.

```
a. Save Configuration to NVRAM
b. Restore Factory Values
c. Reset Switch


+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+                                                           +
+  Do you want to save configuration to NVRAM? Yes/No       +
+                                                           +
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Figure 4-14: Save Settings to NVRAM & Restore Factory Values

- To Save Configuration to NVRAM, select the Save option, and press either ‘Enter’ or ‘Y’ to save the configuration to NVRAM.
- To Restore Factory Values, select the Restore Factory Values to reset the switch parameters to their original default settings. In order for changes to take effect, you must Reset the switch.

  Note: Network IP settings (i.e. IP address, Gateway Address, Network Mask) will not be affected by this command.
- To use the Reset Switch option, select it from the menu, which will restart the switch. Resetting the switch is the equivalent of turning the power off and on. Resetting the switch will clear the statistical counters to zero.

Main Menu> Security

This screen allows you to enable or disable the web and/or telnet interfaces, as well as change the user name and password. To use password protection, you must enable it. User names and passwords are case sensitive and can be up to 20 characters long. The factory default password is **password** in lower case letters.

```
                    Security


        Telnet Access is:  Enabled
           Web Access is:  Enabled

Password Protection is:  Disabled
             User Name:  admin
          New Password:
        Verify Password:
```

Figure 4-15: Security

Note: Using telnet, you can only enable/disable the web interface. You cannot enable/disable the telnet interface.

If you forget your password, contact NETGEAR technical support at 1-888-NETGEAR (in North America).

Main Menu> Advanced

The Advanced page allows professional users to operate more complicated features of the device, which include VLAN, Spanning Tree, Port Trunking, Multimedia support (IGMP), traffic prioritization, SNMP, and port mirroring. These features are powerful and can degrade or disable a network if improperly used. The submenus are introduced below.

- Port Mirroring: You can designate a port for monitoring traffic from one or more other ports or of a single VLAN configured on the switch. The switch monitors the network activity by copying all traffic from the specified monitoring sources to the designated monitoring port, to which a network analyzer can be attached.

- Port Trunking: 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. Toggle the ports to the correct trunk number to set up a trunk. After clicking Apply, the trunk will be enabled. Spanning Tree will treat trunked ports as a single virtual port.
- Virtual Cable Tester (available on some models): You can use this feature to test the continuity of the cable circuit.
- Advanced Security: This menu option allows you to configure the advanced security settings of the switch to limit the access to the management interfaces with the following submenus:
    - System Authentication: You can configure the security settings of the switch by choosing either to use basic password or RADIUS server to authenticate the user attempting to configure the switch. In addition, you can also set up IP filtering to allow only approved users on the network to configure the switch.
    - Port-Based Authentication: You can configure the ports of the switch for authentication through a RADIUS server to authenticate a user attempting to connect to the network through a port on the switch.
    - Trusted MAC Address Table: You can set trusted MAC addresses to allow the switch to forward traffic from.
    - MAC Address Lockdown Table: Shows all of the locked down MAC addresses that the switch has learned. As it reaches the maximum number of MAC addresses (either per port or per system), the switch will lock down address learning for that saturated port or the whole system.
- Advanced Tools: You can upgrade the software of the switch or save/load the switch configuration file to a TFTP server.
- Traffic Management: Class of Service (CoS), also referred to as 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. Priority can be based on VLAN tags, ports, or Differentiated Service Code Points (DSCP). You can configure the threshold for the maximum broadcast packets per port.
- VLANs: 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, you can group by logical function instead of physical location. There are 64 VLAN supported on this switch.

- Spanning Tree: Spanning Tree Protocol (STP) ensures that only one path at a time is active between any two network nodes. There are maybe more than two physical path between any two nodes for redundant paths; STP ensures only one physical path is active and the others are blocked. STP will prevent an inadvertent loop in a network, which can disable your network due to a “Broadcast storm”, the result of a broadcast message traveling through the loop again and again.
- MAC: MAC address table. This menu allows you to set the aging time, as well as entering static MAC addresses to the switch.
- Multimedia Support (IGMP): The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for network devices to report multicast group membership to adjacent routers.
- SNMP: You can use an SNMP-based Network Management Software program to manage your switch. This menu allows you to set up the appropriate tables to enable the switch to respond to SNMP queries.
- Command Line: A user interface that allows you to configure the switch via a command line interface. See Chapter 6 for information about the Command Line Interface (CLI)

Main Menu> Advanced> Port Mirroring

This menu option allows you to enable the Port Mirroring capability. You need to specify both the Source and Monitor port.

```
Advanced > Port Mirroring

Port Mirroring is:        Disabled

   Mirrored Port:  Unit 1  Port  1
  Mirroring Port:  Unit 1  Port  2
```

Figure 4-16: Port Mirroring

The Monitor port will show a copy of every packet that arrives and departs at the Source port.

Main Menu> Advanced> Port Trunking

Port Trunking is a feature that allows multiple links between switches to work as one virtual link or aggregate link.

```
                    Advanced > Port Trunking


            00000000 01111111 11122222 22222333 33333334 44444444 45
Port        12345678 90123456 78901234 56789012 34567890 12345678 90

unit 1      -11----- 22222--- 33------ --
```

Figure 4-17: Port Trunking

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 ports 1 to 8, ports 9 to 16, ports 17 to 24, or port 25 and port 26 (using an FSM726 as an example), on the same switch unit. Up to four trunks can be enabled at the same time. To set up a trunk, use the space bar to select the ports that will participate in the trunk. Spanning Tree will treat trunked ports as a single virtual port.

Note: You must use straight-though cables for all links in the trunk. Do not use crossover cables. And, you must disable auto-negotiation on the ports in a trunk prior to setting up the trunk.

Main Menu> Advanced> Virtual Cable Tester

The virtual cable tester feature lets you test the continuity of the GBIOC cable circuit.

```
                    Advanced > Virtual Cable Tester



                    Port 9              Test
Pair 1,2: Test result is good.
Pair 3,6: Test result is good.
Pair 4,5: Test result is good.
Pair 7,8: Test result is good.
```

Figure 4-18: Virtual Cable Tester

The results are reported for the selected port. The test can take up to one minute.

Note: Only the console menu will let you run the virtual cable tester on any port. Other management interfaces require port access and therefore cannot reliably test the cable continuity of the port they are using to access the switch.

Main Menu> Advanced> Advanced Security

This menu option allows you to configure the advanced security settings of the switch to limit the access to the management interfaces.

Main Menu> Advanced> Advanced Security> System Authentication

```
                    Advanved > Advanced Security

          User Authentication Mode:  Basic Password only
          RADIUS Server IP Address:  0.0.0.0
              RADIUS Shared Secret:

                   IP Filtering is:  Disabled

IP Addresses      IP Addresses      IP Addresses      IP Addresses
```

Figure 4-19: Advanced Security

There are two advanced security options beyond the basic password protection: RADIUS client authentication and IP Filtering. If you have a RADIUS server on your network, you can have authentication of management access done through the RADIUS server. This does not affect traffic passing through the switch, but only authenticates access to the switch management. The same is true for IP Filtering. Here, you can allow only users with specific IP addresses to access the management features, thus preventing unauthorized personnel from configuring to the switch.

Main Menu> Advanced> Advanced Security > Port-Based Authentication

This menu option allows you to configure the 802.1x security settings of the switch to require RADIUS authentication to access ports on the switch.

```
Advanced > Advanced Security > Port-Based Authentication

 RADIUS Server IP Address:  192.168.0.1
     RADIUS Shared Secret:
  Re-Authentication Timer:  3600       (1 - 65535 seconds)
                     Port   Auth_Status
                   ------   ------------
                     1G     Authorized
                     2G     Authorized
                     3G     Authorized
                     4G     Authorized
                     5G     Authorized
                     6G     Authorized
                     7G     Authorized
                     8G     Authorized
                     9G     Authorized
                    10G     Authorized
                    11G     Authorized
```

Figure 4-20: Port-Based Authentication

802.1x port-based authentication provides RADIUS client authentication and data encryption features (see Appendix C, “802.1x Port-Based Authentication Overview”). If you have a RADIUS server on your network, you can have authentication of port access done through the RADIUS server. This does affect traffic passing through the switch, which can be helpful is securing your network from wireless eavesdropping when a wireless access point is connected to the switch. To enable 802.1x, provide the IP address of the RADIUS server, and the shared secret authentication key. The re-authentication timer determines how frequently the session will refresh the data encryption with a new key.

Main Menu> Advanced > Trusted MAC Address Table

This page shows all of the trusted MAC addresses you can set to allow the switch to forward traffic from. The maximum number of trusted MAC addresses is 128 per port and 1024 per system. Any traffic from MAC addresses that are not included in the trusted MAC address table will be dropped. There are three functions, which allow you to Add, Delete, or Query entries from the Trusted MAC Address Table.

Main Menu > Advanced > MAC Address Lockdown Table

This page shows all of the locked down MAC addresses that the switch has learned. To use the lockdown feature, you have to enable it first. After triggering the lockdown function, the maximum number of MAC addresses that a system can learn is 1024. As it reaches the maximun number of MAC addresses (either per port or per system), the switch will lock down address learning for that saturated port or the whole system. If an individual port has locked down, it will not accept any new MAC addresses until you remove some MAC addresses from the table.

Menu choices are Per Port Lockdown or Table. You can enable lockdown of a specific port in the Per Port Lockdown page. The Table page has two functions, which allow you to Remove or Query entries from the MAC Address Lockdown Table.

Main Menu> Advanced> Advanced Tools

This menu provides you with the ability to upgrade the software for the switch as well as saving or loading the switch configuration file to a TFTP server.

Main Menu> Advanced> Advanced Tools> Software Upgrade

If new improvements to the software that runs the switch become available, this menu enables you to upgrade your switch to the new software release.

```
Advanced > Advanced Tools > Software Upgrade

        Hardware Version:  RA
        Firmware Version:  1.2 (2495)
        Software Version:  1.0.4 (3013)

          Next boot from:  Last Saved
TFTP Server IP Address:  172.16.7.146
    TFTP Path/Filename:  /fsm750s/app/RDUx_ng.3013
```

Figure 4-21: Software Upgrade

Once the IP address of the TFTP and the path location of the new software image file is properly configured, you can choose to boot the switch using one of three options. *Please refer to Chapter 3, "Software Upgrade Procedure" when updating software.*

- **Net option**:. This option allows you to try out a new image before upgrading. It requires a TFTP filename and a server IP address to retrieve the specified image from the given IP address. The new image will not overwrite the one in non-volatile memory.
- **Net & save option**.This option requires the same setup as the Net option, i.e. TFTP server and a new image. However, it copies the image to non-volatile memory directly and then the system boots from non-volatile memory.
- **Warning**: The previous image in non-volatile memory will be lost when the procedure completes.

- **Last Saved option**. The system will boot from non-volatile memory. This option will automatically show up after the 'Net & save' option is selected and the unit is reset.

Main Menu> Advanced> Advanced Tools> Configuration Management

This menu allows you to save your configuration, in case you want to keep a copy for back-up purposes.

Warning: Do not edit your configuration file. Editing your file can cause your switch to lose its management capabilities, and possibly degrade its performance. Editing the configuration file will void your warranty.

```
Advanced > Advanced Tools > Configuration Management

          TFTP Server IP Address:  0.0.0.0
TFTP Path/Configuration Filename:

                                   Download from server
                                   Upload to server
```

Figure 4-22: Configuration Management

This menu also allows you to download your configuration file back to the switch to restore your settings.

Main Menu> Advanced> Traffic Management

Traffic management covers the methods to improve the performance of your network by differentiating traffic and limiting excess broadcast traffic.

```
Advanced > Traffic Management

a. Port Priority
b. DiffServ
c. Broadcast Control
```

Figure 4-23: Traffic Management

There are two means to differentiate traffic with this switch- VLAN tags or Differentiated Service Code Points (DSCP) in the header of data packets. By using either the VLAN tags (port-based) or DSCP (DiffServ), you can configure the switch so that certain traffic will take priority over less critical traffic.

Main Menu> Advanced> Traffic Management> Port Priority

```
Unit   1          Advanced > Traffic Management > Port Priority

                    Traffic Optimization is:  Flow Control Optimized

   Port  Priority     Port  Priority     Port  Priority     Port  Priority
   ----  --------     ----  --------     ----  --------     ----  --------
    1    Normal        2    Normal        3    Normal        4    Normal
    5    Normal        6    Normal        7    Normal        8    Normal
    9    Normal       10    Normal       11    Normal       12    Normal
   13    Normal       14    Normal       15    Normal       16    Normal
   17    Normal       18    Normal       19    Normal       20    Normal
   21    Normal       22    Normal       23    Normal       24    Normal
   25GT  Normal       26GT  Normal
```

Figure 4-24: Traffic Prioritization

Main Menu> Advanced> Traffic Management> DiffServ

Differentiated Service (DiffServ) uses a priority tag in the packet, the Differentiated Service Code Point (DSCP), to determine the priority of the packet.

```
                    Advanced > Traffic Management > DiffServ

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

Figure 4-25: DiffServ

There are 64 different tags available. This menu maps the various DSCP tags to the two output queues on each port.

Main Menu> Advanced> Traffic Management> Broadcast Control

Broadcast control lets you set a threshold for the number of broadcast packets sent over a port.

```
Unit   1          Advanced > Traffic Management > Broadcast Control

                    Broadcast Control Rate:  _       Packets/s

      Port  Packets/s  Port  Packets/s  Port  Packets/s  Port  Packets/s
      ----  ---------  ----  ---------  ----  ---------  ----  ---------
       1    1488100     2    1488100     3    1488100     4    1488100
       5    1488100     6    1488100     7    1488100     8    1488100
       9    1488100    10    1488100    11    1488100    12    1488100
      13    1488100    14    1488100    15    1488100    16    1488100
      17    1488100    18    1488100    19    1488100    20    1488100
      21    1488100    22    1488100    23    1488100    24    1488100
      25GT  1488100    26GT  1488100
```

Figure 4-26: Broadcast Control

Main Menu> Advanced> VLANS

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.

```
Advanced > VLANS

a. VLAN Admin.
b. VLAN Membership
c. VLAN Ports
```

Figure 4-27: VLANS

By using VLAN, you can group by logical function instead of physical location. This switch supports up to 64 VLANs. This switch supports static, port-based VLANs. The VLAN Setup options are as follows:

Main Menu> Advanced> VLANS> VLAN Admin

Up to 64 VLANs with unique ID numbers and names can be added. VLAN ID numbers must be in the range of 1-4094. Per industry standard, the default VLAN has an ID of 1.

```
                    Advanced > VLANS > VLAN Administration

ID   Name         ID   Name         ID   Name         ID   Name
---- ------------ ---- ------------ ---- ------------ ---- ------------
1    Default      434  XYZ Inc.     1123 ABC Corporat 2034 Netgear
```

Figure 4-28: VLAN Administration

To add a VLAN, enter a unique numeric VLAN ID and then enter a unique VLAN name.

To remove a port or an entire VLAN, just press Ctrl-X anywhere on the line of the VLAN.

Main Menu> Advanced> VLANS> VLAN Membership

This matrix allows for real time management of up to 64 VLANs.

```
                    Advanced > VLANS > VLAN Membership

  VLAN ID:  1     Next VLAN
VLAN Name:  Default
            00000000 01111111 11122222 22222333 33333334 44444444 45
Port        12345678 90123456 78901234 56789012 34567890 12345678 90


unit 1      UUUUUUUU UUUUUUUU UUUUUUUU UU
```

Figure 4-29: VLAN Membership

To add a port to a VLAN, position the cursor in the desired matrix location and toggle the options with the SPACE bar.

A ‘U’ or ‘T’ will be displayed for each port assigned to the VLAN, where ‘U’ stands for untagged and ‘T’ for tagged. If a port is an untagged member of a VLAN, the VLAN tag will be striped from the frame before it is sent out that port. If the port is a tagged member of a VLAN, the VLAN tag will stay in the frame when it is sent. A ‘_’ space indicates that the port is not a member of the particular VLAN, and will not receive or forward any traffic for that VLAN. VLAN tagging 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).

Main Menu> Advanced> VLANS> VLAN Ports

All untagged packets entering the switch will by default be tagged with the ID specified by the port’s PVID.

```
Unit   1                Advanced > VLANS > VLAN Ports

          Port  PVID      Port  PVID      Port  PVID      Port  PVID
          ----  ----      ----  ----      ----  ----      ----  ----
           1    1          2    1          3    1          4    1
           5    1          6    1          7    1          8    1
           9    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
          25GT  1         26GT  1
```

Figure 4-30: PVID Settings

This screen allows you to specify the PVID for each port. The number next to each port indicates which PVID is set for each port. Following industry standards, PVID 1 is the default PVID.

Main Menu> Advanced> Spanning Tree

This switch is compliant with IEEE802.1D Spanning Tree Protocol (STP).

```
Advanced > Spanning Tree


a. Bridge Settings
b. Port Settings
```

Figure 4-31: Spanning Tree

STP ensures that only one path at a time is active between any two network nodes. There may be more than one physical path between any two nodes, forming a loop, either created for redundancy or by accident. STP ensures only one physical path is active and the others are blocked. If a loop is created for redundancy, STP will monitor the two paths and activate the stand-by path if the primary path fails. If a loop was created inadvertently, STP will disable one of the two paths. A loop in a network can disable your network by causing a “Broadcast storm”, the result of a broadcast message traveling through the loop again and again.

Main Menu> Advanced> Spanning Tree> Bridge Settings

Spanning Tree can be enabled or disabled in this screen.

```
Advanced > Spanning Tree > Bridge Settings

            Root Port:  Itself
   Root Port Path Cost:  0
     Bridge Hello Time:  2
        Bridge Max Age:  20
  Bridge Forward Delay:  15
  Root Bridge Priority:  32768
      Root MAC Address:  00:09:5b:36:b0:04
    Switch MAC Address:  00:09:5b:36:b0:04

      Spanning Tree is:  Disabled

            Hello Time:  2       (1 - 10 seconds)
               Max Age:  20      (6 - 40 seconds)
         Forward Delay:  15      (4 - 30 seconds)
        Bridge Priority:  32768   (0 - 65535)
```

Figure 4-32: Spanning Tree: Bridge Settings

When Spanning tree is used in conjunction with a set of aggregated ports, otherwise known as a port trunking, Spanning Tree will treat the trunk as a single virtual port.

- **Enable**: There are four other tunable parameters to be addressed when enabled.

Hello Time	Time between configuration messages sent by the Spanning Tree algorithm
Max Age	Amount of time before a configuration message is discarded by the system
Forward Delay	Amount of time system spent transitioning from the ‘learning’ to the ‘listening’ to the ‘forwarding’ states
Bridge Priority	Priority setting among other switches in the Spanning Tree

- **Disable**: Disable Spanning Tree algorithm on the system.

Main Menu> Advanced> Spanning Tree> Port Settings

For the Port Settings options, you can specify Spanning Tree port priority, cost, and Fastlink parameters for each port.

Table 4-1. STP Port Setting Parameters

PARAMETERS	RANGE	DESCRIPTION
Prty (Priority)	0-255	STP uses this to determine which path (which port) to use for forwarding. The port with the lowest number has the highest priority.
Cost	1-65535	The switch uses this to determine which port is the forwarding port when the priority is equal. All other factors equal, the path with the lowest cost to the root bridge will be the active path. The estimated path cost is the industry standard for the port speed. The default path cost is the maximum speed for the port.
Fastlink	Enabled or Disabled	When a Fastlink enabled port running standard STP is connected, it will go through the STP negotiation (listening -> learning -> forwarding or blocking) before it will be fully available.

Unit 1 Advanced > Spanning Tree > Port Settings

Port	Priority	Esti. Cost	Path Cost	FastLink	Port	Priority	Esti. Cost	Path Cost	FastLink
1	128	19	19	Disabled	16	128	19	19	Disabled
2	128	19	19	Disabled	17	128	19	19	Disabled
3	128	19	19	Disabled	18	128	19	19	Disabled
4	128	19	19	Disabled	19	128	19	19	Disabled
5	128	19	19	Disabled	20	128	19	19	Disabled
6	128	19	19	Disabled	21	128	19	19	Disabled
7	128	19	19	Disabled	22	128	19	19	Disabled
8	128	19	19	Disabled	23	128	19	19	Disabled
9	128	19	19	Disabled	24	128	19	19	Disabled
10	128	19	19	Disabled	25GT	128	4	4	Disabled
11	128	19	19	Disabled	26GT	128	4	4	Disabled
12	128	19	19	Disabled					
13	128	19	19	Disabled					
14	128	19	19	Disabled					
15	128	19	19	Disabled					

Figure 4-33: Spanning Tree: Port Settings

Fastlink in STP mode. If a client is trying to access a server 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 to direct forwarding mode, thus allowing any server access request to be forwarded. Fastlink mode can cause temporary loops in your network, but STP will find and eliminate them. Fastlink is best used on end node ports, i.e. ports connected to PCs or servers, and not on uplink ports to other switches.

Main Menu> Advanced> MAC Address Manager

Static Address and Address Aging can be configured here.

```
Advanced > MAC

a. Aging Time
b. Static Address
```

Figure 4-34: MAC

Main Menu> Advanced> MAC Address Manager> Aging Time

The aging time is the amount of time that an entry is kept in the bridge tables prior to being purged (or aged). The range (in parentheses) represents the minimum and the maximum values that the timer can be set. The industry standard default is 300 seconds.

Main Menu> Advanced> MAC Address Manager> Static Addresses

The Static Address Table allows you to specify Media Access Control (MAC) addresses for specific ports that will not be purged from the bridge table by the aging function.

```
                    Advanced > MAC > Static Address

    MAC Address        Unit   Port         MAC Address        Unit   Port
-------------------------------------------------------------------------------
    00:11:22:31:53:12  1        19
    00:11:22:33:43:12  1        17
    00:19:22:21:51:11  1        17
    00:31:92:33:44:12  1         6
```

Figure 4-35: MAC: Static Address

- **Adding an entry**. Type the MAC address under the first column, and press Enter. Then, enter the port number associated with that MAC address.If all the information is correct, the new entry will appear in the list, which is listed by port ID. Otherwise, an error message will be displayed and the cursor will return to the MAC Address field.
- **Removing an entry.** Tab to the entry and press Ctrl-X. This will erase the MAC address from NVRAM. This action takes effect immediately; you do not need to use Ctrl-W to save the update.

Main Menu> Advanced> Multimedia Support

In networks where multimedia applications generate multicast traffic, Internet Group Multicast Protocol (IGMP) can greatly reduce unnecessary bandwidth usage by limiting traffic forwarding that is otherwise broadcast to the whole network. Enabling IGMP will allow individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.

Main Menu> Advanced> Multimedia Support> Enable/Disable IGMP

```
Advanced > Multimedia Support > Enable/Disable IGMP

IGMP is:  Disabled
```

Figure 4-36: Multimedia Support

- **Enable**. The system will detect IGMP queries, report packets, and manage IP multicast traffic through the switch
- **Disable**. The switch will forward traffic and disregard any IGMP requests.

Main Menu> Advanced> Multimedia Support> Static Multicast Administration

Use this menu to configure permanently reachable multicast groups.

```
Advanced > Multimedia Support > Static Multicast Admin.

MAC Address              MAC Address              MAC Address
[redacted]

Enter a MAC Address (01:00:5e:xx:xx:xx)
<ESC> Back  <Tab> Move Cursor  <Ctrl-X> Delete  <Ctrl-L> Refresh  <Ctrl-W> Save
```

Figure 4-37: Static Multicast Administration

The Static Multicast Administration menu lets you create individual groups by entering MAC addresses for your static multicast group. The membership of each group is configured in the Static Multicast Membership menu.

Main Menu> Advanced> Multimedia Support> Static Multicast Membership

Once the static multicast groups are defined in the Static Multicast Administration menu, you can use this menu to specify the membership of each group by specifying the ports that belong to each group.

```
            Advanced > Multimedia Support > Multicast Membership

MAC Address:  none                Next MAC

              00000000 01111111 11122222 22222333 33333334 44444444 45
  Port        12345678 90123456 78901234 56789012 34567890 12345678 90

  unit 1      -------- -------- -------- --
```

Figure 4-38: Static Multicast Membership

Main Menu> Advanced> SNMP

```
Advanced > SNMP

a. Community Table
b. Host Table
c. Trap Settings
```

Figure 4-39: SNMP Management

You can manage this switch using the Simple Network Management Protocol (SNMP) from a network management station. To do so, you must configure your switch to participate in the SNMP community and you must add the SNMP host agent to the host table. This prevents unauthorized SNMP access to your switch from non-approved SNMP hosts.

Support for these Standard MIBs is included:

- MIB II (RFC1213)
- Ethernet Interface MIB (RFC1643)
- Bridge MIB (RFC1493)
- Private Enterprise MIB (see the Resource CD for Managed Switches)
- 4-Group RMON (RFC1757)

Main Menu> Advanced> SNMP> Community Table

You can create up to eight community strings which combine GET, SET, and TRAP privileges.

```
Advanced > SNMP > Community Table

Community String   Get   Set   Trap   Status
 public            On    Off   Off    Active
                   Off   Off   Off    N/A
                   Off   Off   Off    N/A
                   Off   Off   Off    N/A
                   Off   Off   Off    N/A
                   Off   Off   Off    N/A
                   Off   Off   Off    N/A
                   Off   Off   Off    N/A
```

Figure 4-40: SNMP Management: Community Table

These community strings need to be set prior to setting host access, as the host table depends on the existence of community strings. The public string has GET privileges by default.

Main Menu> Advanced> SNMP> Host Table

The screen, shown in Figure 6-29, grants a host the access rights to the switch. Host Authorization is a security feature to limit people who are not listed in the host table from accessing the switch using SNMP.

```
                    Advanced > SNMP > Host Table

    Host Name        IP Address      Community String     Host Status

1   166              172.16.50.166   public               Active
2
3
4
5
```

Figure 4-41: SNMP Management: Host Table

To add a host, enter the host name, IP address, and the community string. Press Enter after each entry to move to the next field. In the Status field, press the Spacebar until the desired Status is displayed. Press Ctrl-W to save all changes.

Main Menu> Advanced> SNMP> Trap Settings

When on, the system will generate an SNMP trap upon a host authorization failure. This failure occurs when a host tries to gain access to the system but the host's IP is not in the SNMP host table.

```
Advanced > SNMP > Trap Settings



Authentication Trap is:  Enabled
```

Figure 4-42: SNMP Management: Trap Settings

With authentication traps enabled, the system generates a SNMP trap when a host authorization fails. Hosts in community strings with TRAP privileges are notified when a trap occurs.

Main Menu> Advanced> Command Line

A user interface that allows you to configure the switch via a command line interface. See Chapter 6 for information about the Command Line Interface (CLI)

Chapter 5
Web-Based Management Interface

Your NETGEAR 700 Series Switches provides a built-in browser interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer 5.0 or later or Netscape Navigator 6.0 or later.

This interface also allows for system monitoring and management of the switch. The ‘help’ page will cover many of the basic functions and features of the switch and it’s web interface.

When you configure the switch for the first time from the console, you can assign an IP address and subnet mask to the switch. Thereafter, you can access the switch’s Web interface directly using your Web browser by entering the switch’s IP address into the address bar. In this way, you can use your Web browser to manage the switch from a central location, just as if you were directly connected to the switch’s console port. Figure 4-1 shows this management method.

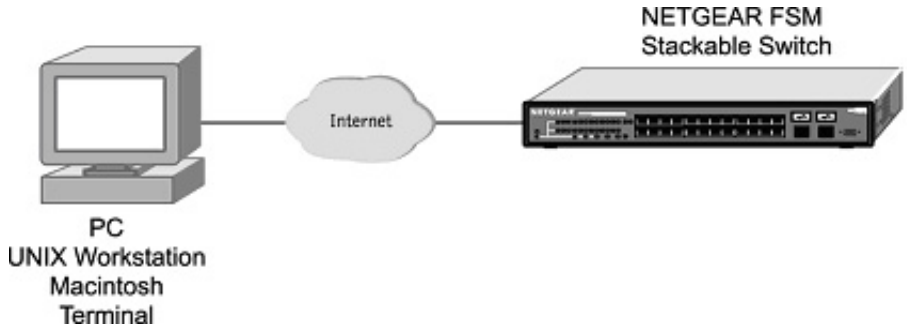


Figure 5-1: Web Management Method

Web Based Management Overview

The 6 menu options available are: System, Status, Set-up, Tools, Security, and Advanced. There is a help menu in the top of right side of screen; you can click the ‘help’ or the question mark to read the help menu.

The help menu contains:

- Web-Based Management — Introduction to the Web management features.
- Device Management — Introduction of the basic icons and management of the device
- Interface Operations — Describes Web browser requirements, and common commands
- Product Overview — Describes supported SNMP and Web management features
- Summary of Features — Feature List

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

- Reload: — 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
- Remove: — Removes selected entries from table and refreshes screen data
- Reset: — Resets the system, which is equivalent to power off /on.
- Restore: — Restores system factory default values, except password and IP.
- Query: — System will retrieve the useful information in database.

System Information

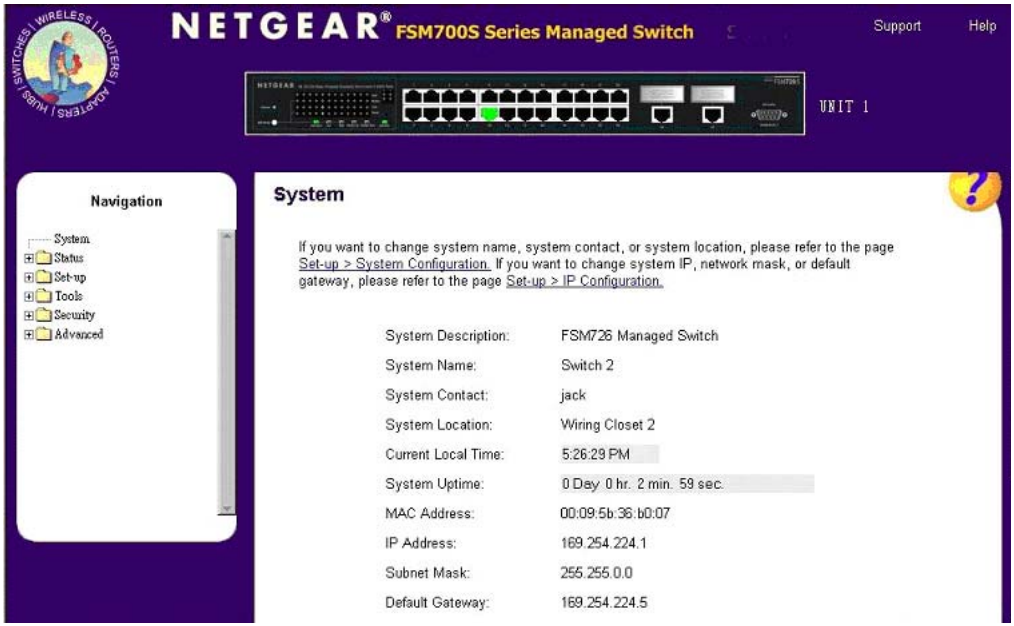


Figure 5-2: System information page

This welcome page displays system information, such as:

- System Description
- System Name
- System Contact
- System Location
- Current Local Time (according to your computer)
- System Uptime
- MAC Address
- IP Address
- Subnet Mask
- Default Gateway
- Software Version
- System OID (used for production testing)

These parameters are not editable from this screen. Some of these can be modified in the Set Up> System Configuration page or the Set Up> IP Configuration page.

Status Menus

The Status page contains the following menu choices:

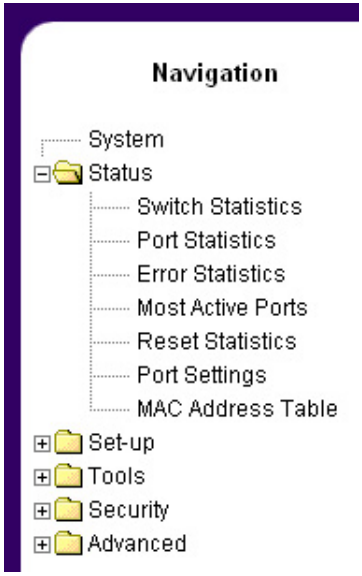


Figure 5-3: Status Menu navigation

- “Status > Switch Statistics” on page 4-5
- “Status > Port Statistics” on page 4-7
- “Status > Error Statistics” on page 4-8
- “Status > Most Active Ports” on page 4-9
- “Status > Reset Statistics” on page 4-10
- “Status > Port Settings” on page 4-10
- “Status > MAC Address Table” on page 4-11

Each of these menus is covered in the following sections.

Status > Switch Statistics

The Switch Statistics Chart allows you to compare one type of statistic across all the ports. You can reset the counters in the Reset Statistics page.

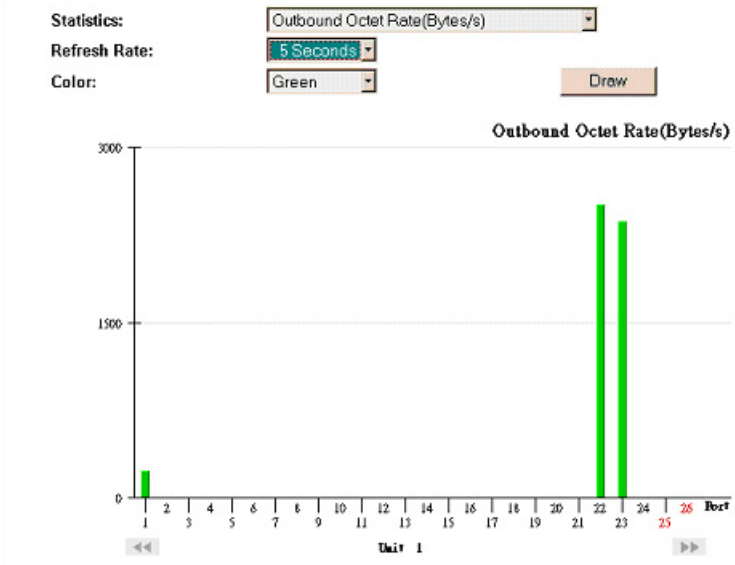


Figure 5-4: Switch Statistics

You can configure the following options on the Switch Statistics Chart:

- Statistics — The type of system data to be monitored
- Refresh Rate — The time interval between automatic refreshes (5, 10, 15, 30 seconds)
- Color — The color setting for the chart

There are 24 kinds of Statistics that you can review on this screen:

- Inbound Octet Rate: Received Byte per second.
- Inbound Unicast Packet Rate: Received Unicast packet per second.
- Inbound Non-unicast Packet rate: Received Non-unicast packet per second.
- Inbound Discard Rate: Received and is discarded packet per second.
- Inbound Error Rate: Received error packet per second.
- Outbound Octet Rate: Transmitted byte per second.
- Outbound Unicast Packet Rate: Transmitted unicast packet per second.

- Outbound Non-unicast Packet Rate: Transmitted non-unicast packet per second.
- Outbound Discard Rate: Transmitted and is discarded packet per second.
- Outbound Error Rate: Transmitted error packet per second.
- Ethernet Undersize Packet Rate: Less than 64byte length packet per second.
- Ethernet Oversize Packet Rate: More than 1518byte length packet per second
- Inbound Octets: Received bytes
- Inbound Unicast Packets: Received unicast packet
- Inbound Non-unicast Packets: Received non-unicast packet
- Inbound Discards: Received and is being discarded packet.
- Inbound Errors: Received and is a error packet
- Outbound Octets: Transmitted byte
- Outbound Unicast Packets: Transmitted unicast packet
- Outbound Non-unicast Packets: Transmitted non-unicast packet.
- Outbound Discards: Transmitted and is being discarded packet
- Outbound Errors: Transmitted and is an Error packet.
- Ethernet Undersize Packets: Less than 64byte length packet
- Ethernet Oversize Packets: more than 1518 byte length packet.

Status > Port Statistics

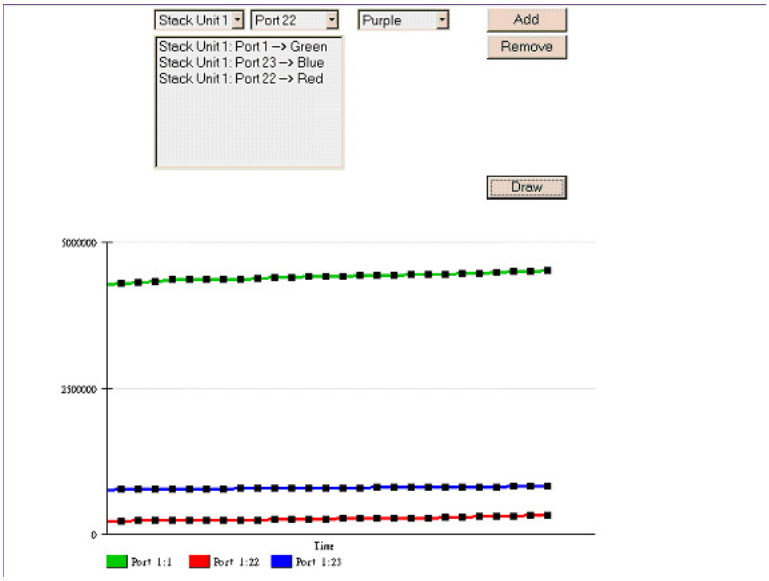


Figure 5-5: Port Statistics

The Port Statistics Chart shows all the statistic types for one port over time. You can reset the counters in the Reset Statistics page.

- Port — The port on which data will be monitored.
- Refresh Rate — The time interval between automatic refreshes
- Color — The color setting for the data

There are 12 kinds of Port Statistics

- Inbound Octets: Received bytes
- Inbound Unicast Packets: Received unicast packet
- Inbound Non-unicast Packets: Received non-unicast packet
- Inbound Discards: Received and is being discarded packet.
- Inbound Errors: Received and is a error packet
- Outbound Octets: Transmitted byte
- Outbound Unicast Packets: Transmitted unicast packet
- Outbound Non-unicast Packets: Transmitted non-unicast packet.

- Outbound Discards: Transmitted and is being discarded packet
- Outbound Errors: Transmitted and is an Error packet.
- Ethernet Undersize Packets: Less than 64byte length packet
- Ethernet Oversize Packets: more than 1518 byte length packet.

Status > Error Statistics

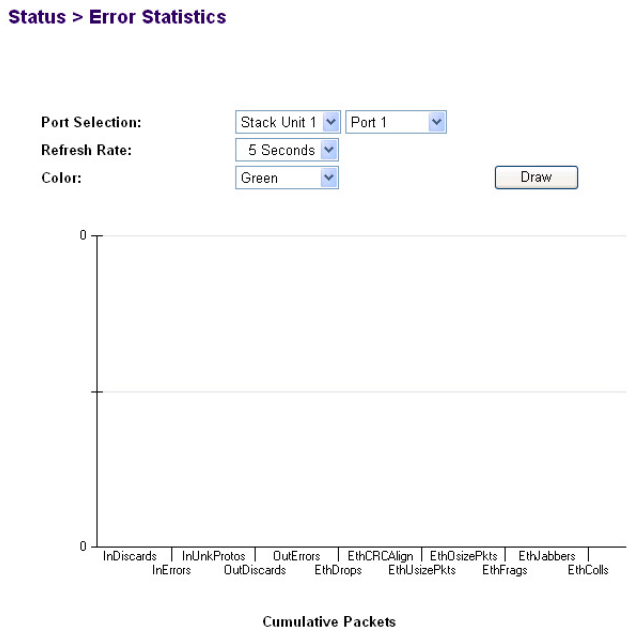


Figure 5-6: Error Statistics

The Error Statistics Graph allows you to chart one type of statistic for any combination of ports. In the case of the Error Statistics Graph, the chart will present data across time so that fluctuations in time can be easily seen.

All charts have a maximum ceiling of more than 2.1 billion (2,147,483,647). You can see the value of each bar or line in the chart by clicking on the bar. The following will outline the settings for each type of graph.

- Statistics The type of system errors to be monitored
- Refresh Rate The time interval between automatic refreshes (5,10,15, 30 seconds)
- Port Selection The port for data to be monitored

When all of the variables are set, click Draw.

Status > Most Active Ports

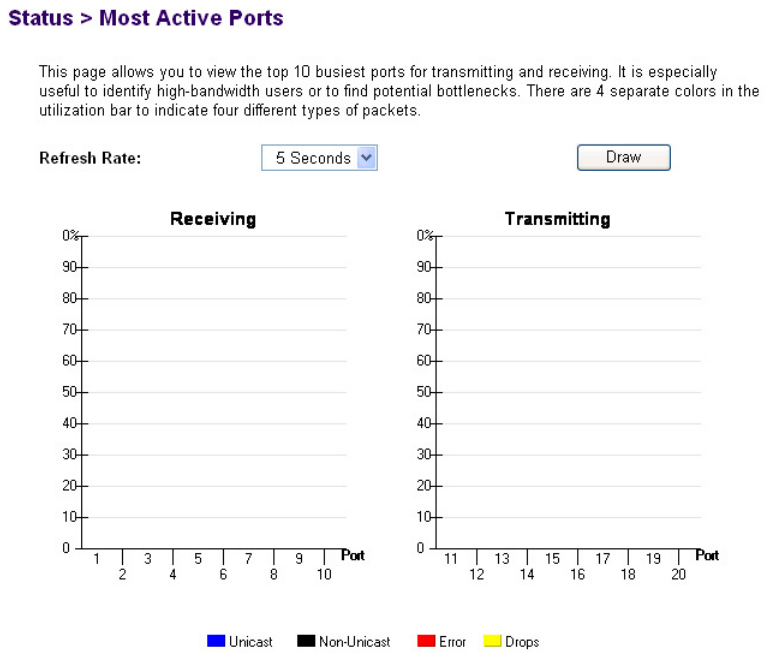


Figure 5-7: Error Statistics

This page allows you to view the transmission and reception utilization of top 10 ports. It is especially useful when you want to see the potential bottlenecks in the switch. A bottleneck is a port with egress traffic closing to line rate. The receive side picture indicates potential nodes causing the problem.

Refresh Rate**:** The time interval between automatic refreshes (5, 10, 15, 30 seconds).

There are four separate colors in the utilization bar to indicate four different types of packets:

- Unicast: blue
- Non-Unicast: black
- Error: red
- Drops: amber

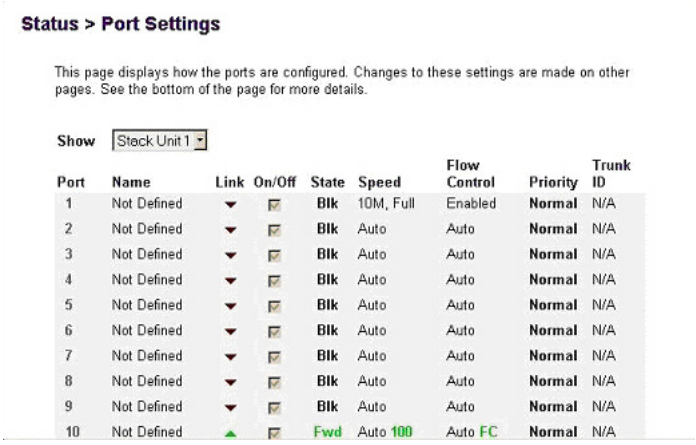
All colors stack together to form a single column (total is up to 100%). There is a scale on the side to indicate the packet/seconds grid with 10% per notch.

Status > Reset Statistics

Figure 5-8: Statistics Counter Reset

The Reset Statistics screen lets you reset all statistics counters of the switch. By pressing on the Reset button, all counters will be set to 0.

Status > Port Settings



Port	Name	Link	On/Off	State	Speed	Flow Control	Priority	Trunk ID
1	Not Defined			Blk	10M, Full	Enabled	Normal	N/A
2	Not Defined			Blk	Auto	Auto	Normal	N/A
3	Not Defined			Blk	Auto	Auto	Normal	N/A
4	Not Defined			Blk	Auto	Auto	Normal	N/A
5	Not Defined			Blk	Auto	Auto	Normal	N/A
6	Not Defined			Blk	Auto	Auto	Normal	N/A
7	Not Defined			Blk	Auto	Auto	Normal	N/A
8	Not Defined			Blk	Auto	Auto	Normal	N/A
9	Not Defined			Blk	Auto	Auto	Normal	N/A
10	Not Defined			Fwd	Auto 100	Auto FC	Normal	N/A

Figure 5-9: Port Settings

This page displays the port settings. To configure the ports, go to the ‘Port Configuration’ under the ‘Set-up’ sub menu.

- Port: The port number on the switch
- Name: The name of the port. This is a user-defined label.

- Link: A green triangle pointing up indicates a valid link, while a red triangle pointing down indicates no link.
- On/Off: Indicates if the port is enabled or disabled by the Administrator.
- State: This refers to the Spanning Tree state of the port. Ports will be Blocking (Blk), Listening (Lis), Learning (Lrn), Forwarding (Fwd) or Disabled (Dis).
- Speed: Indicates the speed and duplex for the port. 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); or 100 Mbps full duplex (100M Full).
- Flow Control: Indicates whether Flow Control support is set for automatic (Auto) or off (Disabled)
- Priority Indicates if the port is set to high priority or normalpriority. This is an advanced feature that is configured under Traffic Prioritization
- Trunk ID Indicates if the port is a member of a trunk by showing the ID number of the trunk. This is an advanced feature that is configured under Port Trunking

Status > MAC Address Table

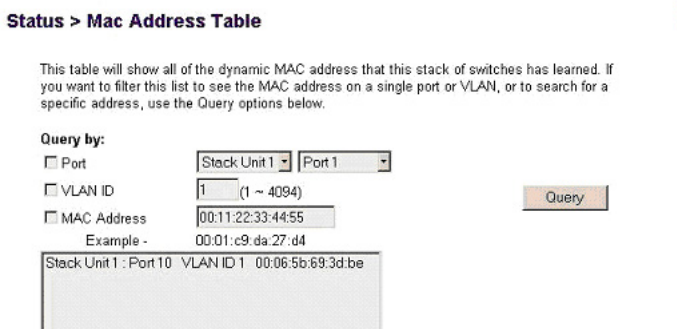


Figure 5-10: MAC Address Table

The MAC Address Table is a dynamic address lookup table that allows you to view the dynamic MAC addresses that are currently in the address database. When a MAC address is in the database, the packets intended for that address are forwarded directly to that port. You can filter the displayed addresses by port, VLAN, and/or MAC address by checking those fields.

Set-up Menu

There are four kinds of configuration in the Setup page:

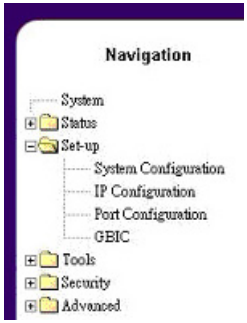


Figure 5-11: Setup menu

- "Set-up> System Configuration" on page 4-12
- "Set-up> IP Configuration" on page 4-13
- "Set-up> Port Configuration" on page 4-14
- "Set-up> GBIC" on page 4-15

Set-up> System Configuration

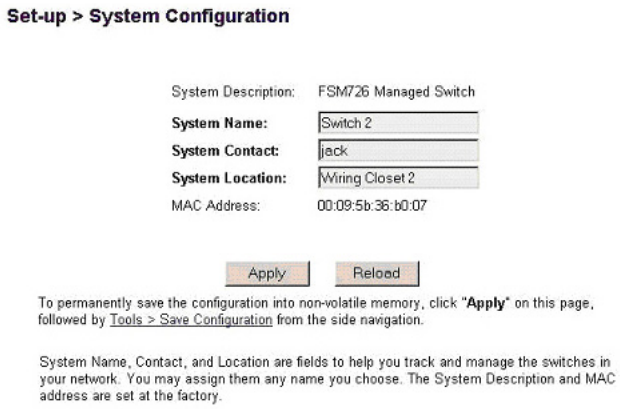


Figure 5-12: System Configuration

This page will allow access to the system information parameters. To do so:

1. Enter System Name, System Contact, or System Location.
2. Click Apply to change the System Configuration and save it in NVRAM.
3. Reset the system to implement the changes (> Save Configuration).

Set-up> IP Configuration

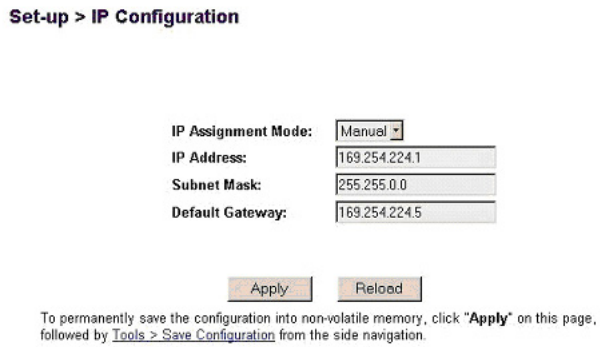


Figure 5-13: IP Configuration

This menu manages the IP related information of the system.

IP Assignment Mode

- Manual – You manually enter IP-related information
- BootP – Bootstrap Protocol, which allows the FSM726 switch to discover its own IP address from a BootP server on the network
- DHCP – The switch accepts DHCP broadcast from a DHCP server and automatically configures IP related information

Note: In DHCP mode, if the switch fails to get a DHCP assignment, the switch defaults to 192.168.0.1 as its IP address.

To enable quick and easy set-up, the default setting is DHCP. However, DHCP addresses change over time, and you need to know the IP address of your switch so that you can remotely manage it. After completing the initial setup, change the IP assignment mode from DHCP to manual.

If you choose Manual mode, enter site-specific IP address, Gateway address and Net mask.

Click Apply to change the IP settings

Save Configuration to NVRAM and reset the system to implement the changes (Tools > Save Configuration).

Set-up> Port Configuration

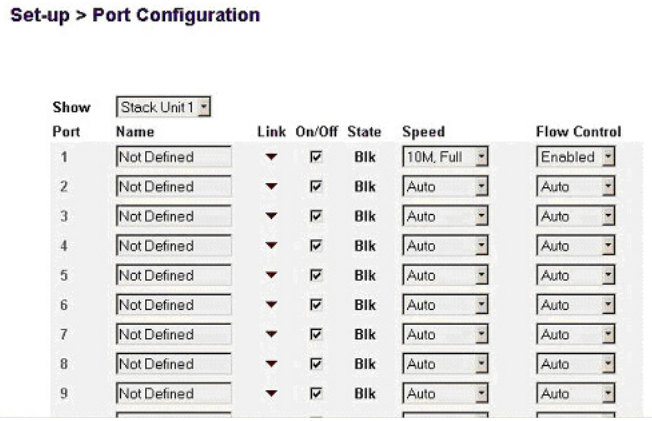


Figure 5-14: Port Configuration

This menu allows you can configure the status of each port.

- Port: The port number on the switch
- Name: The name of the port. This is a user-defined label.
- Link: A green triangle pointing up indicates a valid link, while a red triangle pointing down indicates no link.
- On/Off: Indicates if the port is enabled or disabled by the Administrator.
- State: This refers to the Spanning Tree state of the port. Ports will be Blocking (Blk), Listening (Lis), Learning (Lrn), Forwarding (Fwd) or Disabled (Dis).
- Speed: Indicates the speed and duplex for the port. 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); or 100 Mbps full duplex (100M Full).

- Flow Control: Indicates whether Flow Control support is set for automatic (Auto) or off (Disabled)

Set-up> GBIC

This page allows you to choose the port type for the gigabit ports. The default is 1000BASE-T (RJ-45).

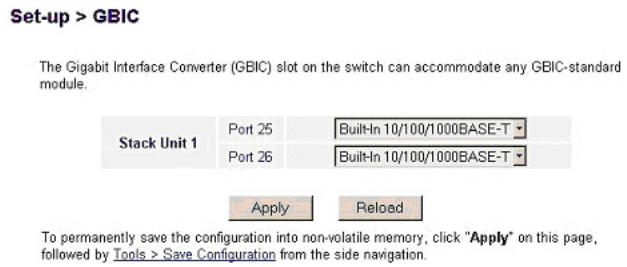


Figure 5-15: Setup: GBIC

If you want to use a GBIC, the setting on this page must be set accordingly. The switch auto-detects if the media is copper or GBIC. This Auto-detect feature is enabled by default.

Note: Enabling the GBIC connector for a Gigabit Ethernet port disables the built-in 1000BASE-T port.

Tools Menu

The Tools page contains functions to maintain your switch.

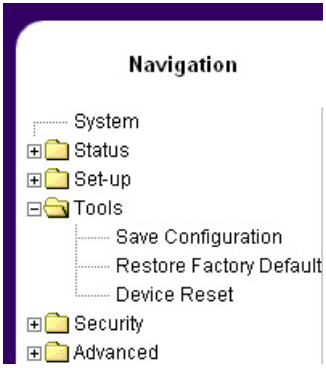


Figure 5-16: Tools Menu

There is a firmware upgrade; the means to save current settings to non-volatile memory (NVRAM); as well as software reset mechanism. The page has two sub-pages:

- “Tools> Save Configuration ” on page 4-16
- “Tools> Restore Factory Defaults” on page 4-17
- “Tools> Device Reset ” on page 4-18

Tools> Save Configuration

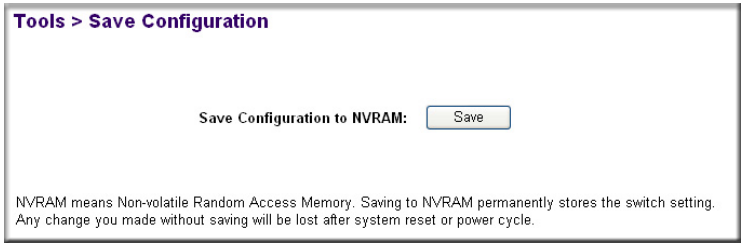


Figure 5-17: Save Configuration

After making any changes to the screens within the Web Interface, you can save the changed settings to NVRAM. If changes are not saved to NVRAM, then they will be lost during the next switch reset or reboot.

Tools> Restore Factory Defaults

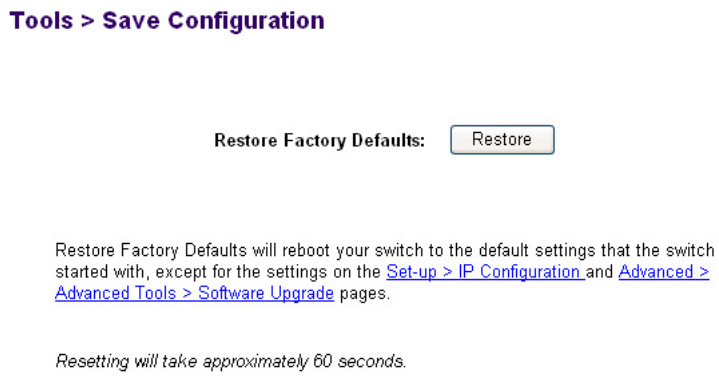


Figure 5-18: Save Configuration

This page allows you to restore the factory configuration by clicking "**Restore**", the system saves the default settings (including password) into the NVRAM and resets itself.

Note: Network IP settings (i.e. IP address, Gateway Address, Network Mask) will not be affected by the Restore command.

Tools> Device Reset

Figure 5-19: Device Reset

In this screen you can reset (power cycle) the switch. Reset the switch by selecting 'Reset'

Security> Passwords

Figure 5-20: Security Menu

The user name and password can be up to 20 characters and are case sensitive. The password entered is encrypted on the screen and will display as a sequence of asterisks (*). The factory default password is **password** in lower case letters.

On this page, you can:

- Enable or disable password protection
- Change the user name and password
- Click Apply to activate the new password

Note: If you have enabled password protection without setting your own password, the default password is **password** in all lower case letters.

Advanced Options

The following menu choices are available in the Advanced Section:

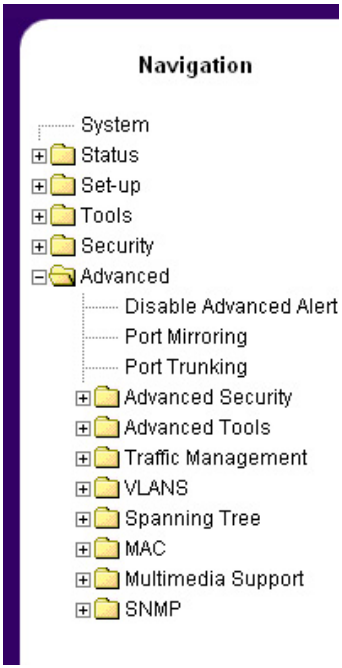


Figure 5-21: Advanced menu

- “Advanced > Disable Advanced Alerting” on page 4-22
- “Advanced > Port Mirroring” on page 4-22
- “Advanced > Port Trunking” on page 4-23
- “Advanced > Virtual Cable Tester” on page 4-23
- “Advanced> Advanced Security” on page 4-24
- “Advanced > Advanced Tools ” on page 4-28
- “Advanced > Traffic Management” on page 4-31
- “Advanced> VLANS” on page 4-32
- “Advanced> Spanning Tree” on page 4-35
- “Advanced> MAC” on page 4-37
- “Advanced> Multimedia Support” on page 4-39
- “Advanced> SNMP” on page 4-40

The Advanced page allows professional users to operate more complicated features of the device, which include VLAN, Spanning Tree, Port Trunking, Multimedia support (IGMP), traffic prioritization, SNMP, and port mirroring. These features are powerful and can degrade or disable a network if improperly used.

- Disable Advanced Alerting: When you select a feature in the Advanced menu, an alert will pop up to inform you that the changes you are about to make may have adverse effect on your network. Experienced users may use this option to disable these alerts.
- Port Mirroring: You can designate a port for monitoring traffic from one or more other ports or of a single VLAN configured on the switch. The switch monitors the network activity by copying all traffic from the specified monitoring sources to the designated monitoring port, to which a network analyzer can be attached.
- Port Trunking: 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. Toggle the ports to the correct trunk number to set up a trunk. After clicking Apply, the trunk will be enabled. Spanning Tree will treat trunked ports as a single virtual port.
- Virtual Cable Tester (available on some models): You can use this feature to test the continuity of the cable circuit.
- Advanced Security: You can configure the security settings of the switch by choosing either to use basic password or RADIUS server to authenticate the user attempting to configure the switch. In addition, you can also set up IP filtering to allow only approved users on the network to configure the switch.

- Advanced Tools: You can upgrade the software of the switch or save/load the switch configuration file to/from a TFTP server.
- Traffic Management (CoS): Class of Service (CoS), also referred to as 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. Priority can be based on VLAN tags, ports, or Differentiated Service Code Points (DSCP).

  Broadcast Control: You can configure the threshold for the maximum broadcast packets per port.
- VLANs: 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, you can group by logical function instead of physical location. There are 64 VLAN supported on this switch.
- Spanning Tree Protocol (STP) ensures that only one path at a time is active between any two network nodes. There are maybe more than two physical path between any two nodes for redundant paths; STP ensures only one physical path is active and the others are blocked. STP will prevent an inadvertent loop in a network, which can disable your network due to a “Broadcast storm”, the result of a broadcast message traveling through the loop again and again.
- MAC: MAC address table. This menu allows you to set the aging time, as well as entering static MAC addresses to the switch.
- Multimedia Support (IGMP): The Internet Group Management Protocol (IGMP) is an Internet protocol that provides a way for network devices to report multicast group membership to adjacent routers.
- SNMP: You can manage the switch SNMP from a SNMP network management station. You can define SNMP communities and assign access rights to each SNMP community. The SNMP Host Table page allows you to add and remove access rights that have been granted to community groups from specified hosts. While enabled, the system generates an SNMP trap upon a host authentication failure.

Advanced > Disable Advanced Alerting

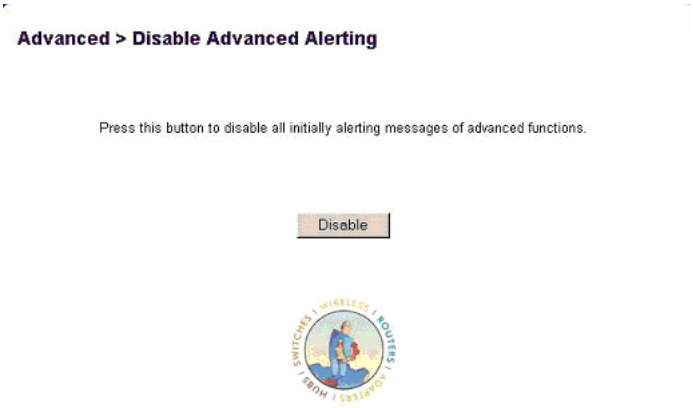


Figure 5-22: Advanced > Disable Advanced Alerting

To prevent accidental use, warnings appear when an advanced feature is selected. This screen allows experienced users to bypass these warnings during a browser session. The warnings will be re-activated at the next browser session in case another, less experienced user is accessing the switch.

Advanced > Port Mirroring

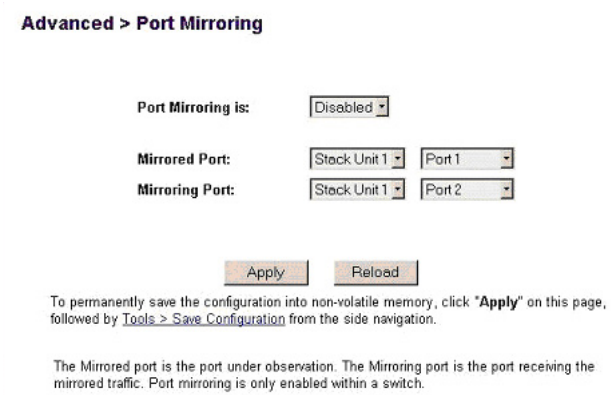


Figure 5-23: Figure 4-18. Port Mirroring

Port mirroring is a feature to help in the debugging of a network. This web interface page allows the enabling or disabling of port mirroring and the setting of source and monitor ports. The monitor port will show a copy of every packet that arrives or leaves the source port.

Advanced > Port Trunking

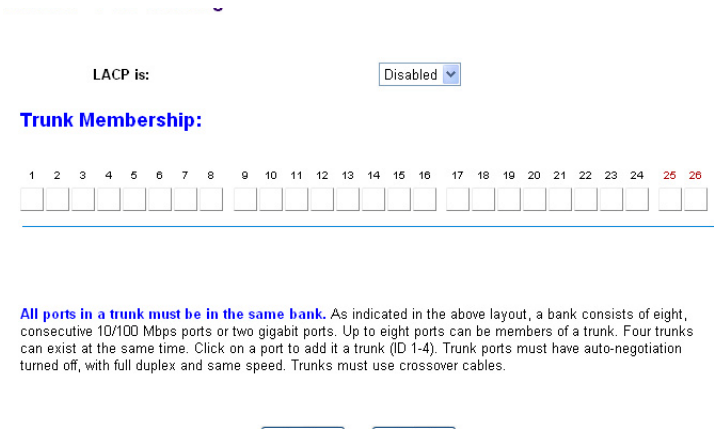


Figure 5-24: Port Trunking

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 group of 8 10/100 ports or 2 gigabit ports, for example, 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 enabled at the same time. To set up a trunk, click on the ports that will participate in the trunk. Spanning Tree will treat trunked ports as a single virtual port.

Note: You must use straight-though cables for all links in the trunk. Do not use crossover cables. Also, you must disable auto-negotiation on the ports in a trunk prior to setting up the trunk.

Advanced > Virtual Cable Tester

The virtual cable tester feature lets you test the continuity of the GBIOC cable circuit.

Note: This feature is available on some models of the 700 Series. It is not available on the FSM726.

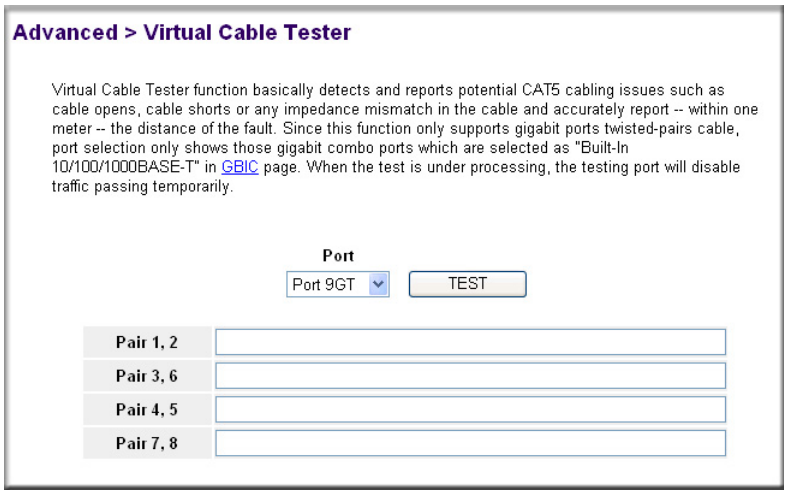


Figure 5-25: Virtual Cable Tester

The results are reported for the selected port. The test can take up to one minute.

Note: Only the console menu will let you run the virtual cable tester on any port. Other management interfaces require port access and therefore cannot reliably test the cable continuity of the port they are using to access the switch.

Advanced> Advanced Security

Advanced Security includes four subpages:

- System Authentication
- Port-Based Authentication
- Trusted MAC Address Table
- MAC Address Lockdown Table

Advanced > Advanced Security > System Authentication

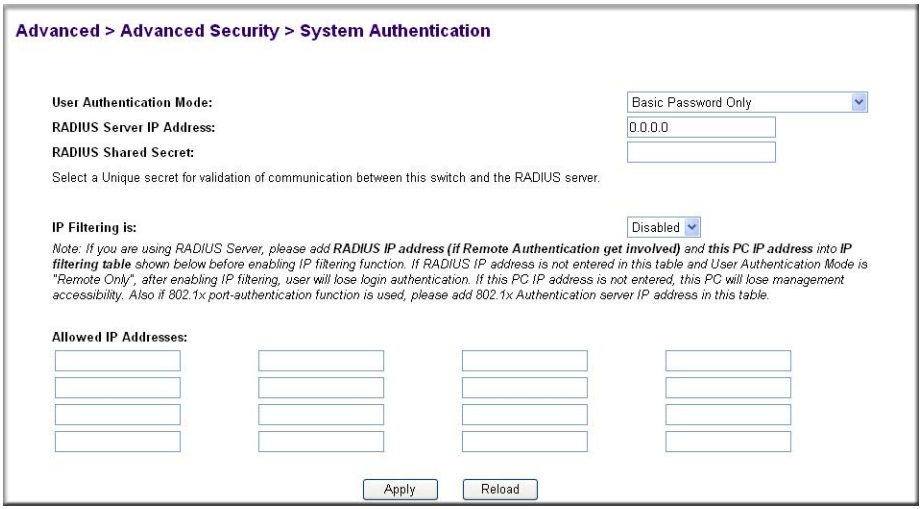


Figure 5-26: System Authentication

This menu option allows you to configure the advanced security settings of the switch to limit the access to the management interface. There are two advanced security options beyond the basic password protection: RADIUS client authentication and IP Filtering. If you have a RADIUS server on your network, you can have authentication of management access done through the RADIUS server. This does not affect traffic passing through the switch, but only authenticates access to the switch management. The same is true for IP Filtering. Here, you can allow only users with specific IP addresses to access the management features, thus preventing unauthorized personnel from configuring the switch.

Advanced > Advanced Security > Port-Based Authentication

This menu option allows you to configure the 802.1x security settings of the switch to require RADIUS authentication to access ports on the switch.

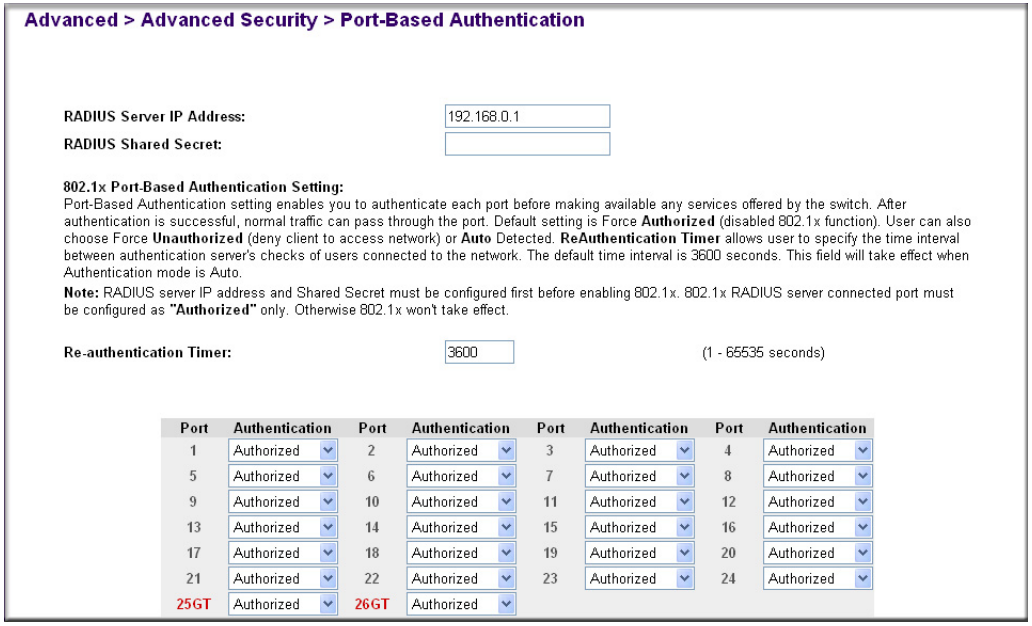


Figure 5-27: Port-Based Authentication

802.1x port-based authentication provides RADIUS client authentication and data encryption features (see Appendix C, “802.1x Port-Based Authentication Overview”). If you have a RADIUS server on your network, you can have authentication of port access done through the RADIUS server. This does affect traffic passing through the switch, which can be helpful in securing your network from wireless eavesdropping when a wireless access point is connected to the switch. To enable 802.1x, provide the IP address of the RADIUS server, and the shared secret authentication key. The re-authentication timer determines how frequently the session will refresh the data encryption with a new key.

Advanced > Advanced Security > Trusted MAC Address Table

This page shows all of the trusted MAC addresses you can set to allow the switch to forward traffic from. The maximum number of trusted MAC addresses is 128 per port and 1024 per system. Any traffic from MAC addresses that are not included in the trusted MAC address table will be dropped. There are three functions, which allow you to Add, Remove, or Query entries from the Trusted MAC Address Table.

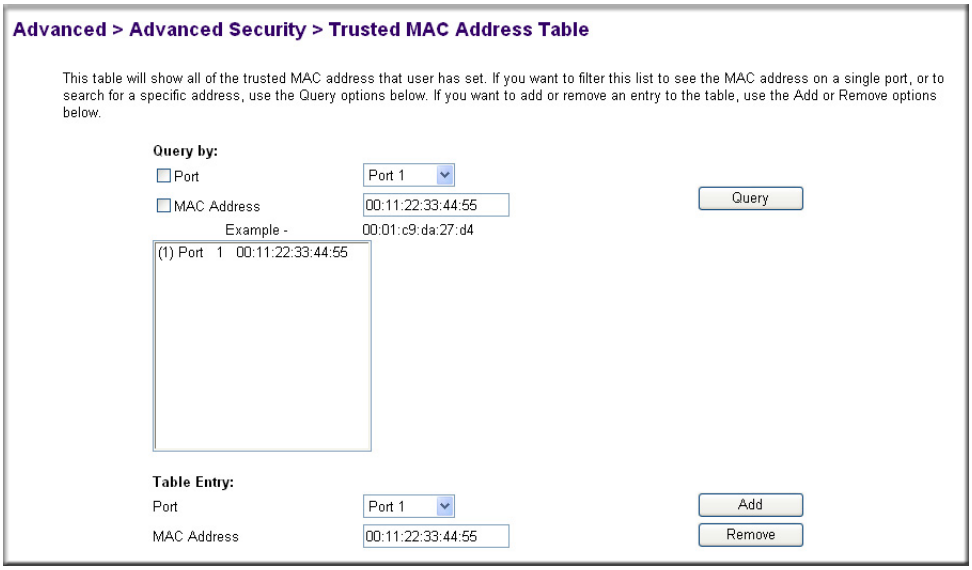


Figure 5-28: Trusted MAC Address Table

Advanced > Advanced Security > MAC Address Lockdown Table

This page shows all of the locked down MAC addresses that the switch has learned. To use the lockdown feature, you have to enable it first. After triggering the lockdown function, the maximum number of MAC addresses that a system can learn is 1024. As it reaches the maximun number of MAC addresses (either per port or per system), the switch will lock down address learning for that saturated port or the whole system. If an individual port has locked down, it will not accept any new MAC addresses until you remove some MAC addresses from the table. There are two functions, which allow you to Remove or Query entries from the MAC Address Lockdown Table.

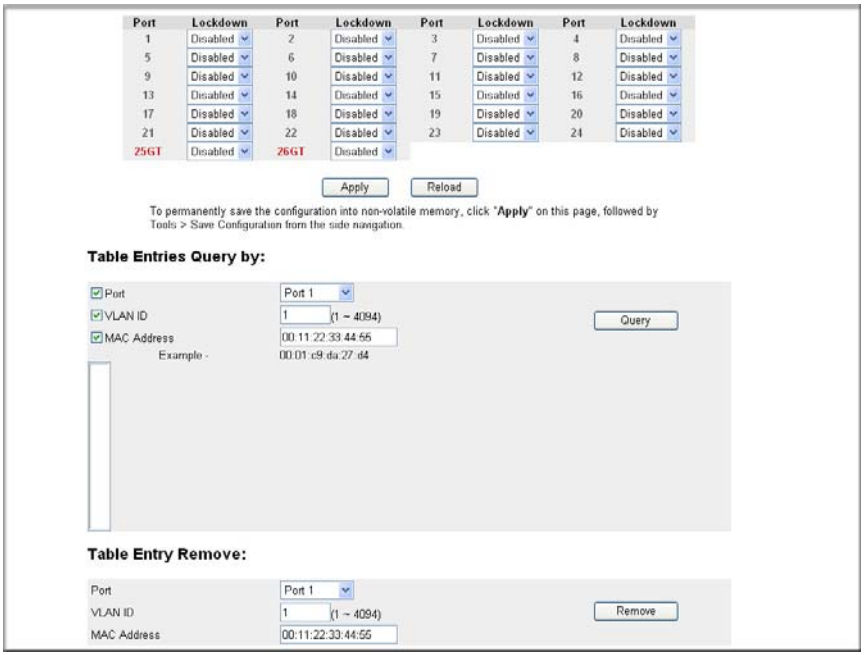


Figure 5-29: MAC Address Lockdown Table

Advanced > Advanced Tools

Use the advanced tools menu to upgrade the software for the switch through a variety of options using the TFTP protocol and to customize the configuration file of the switch. These are tasks that require advanced expertise.

Advanced > Advanced Tools > Software Upgrade

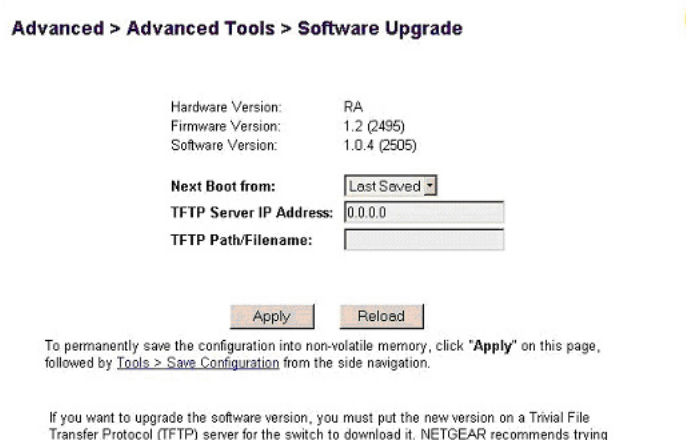


Figure 5-30: Advanced Tools, Software Upgrade menu

This menu provides you with the ability to upgrade the software for the switch through a variety of options using TFTP protocol.

If new improvements to the switch software become available, this menu enables you to upgrade to the new software. Once the IP address of the TFTP and the path location of the new software image file is properly configured, you can choose to boot the switch using one of three options. Please refer to Chapter 3, “Software Upgrade Procedure” when updating software.

Net option

This option allows the user to try out a new image before upgrading. It requires a TFTP filename and a server IP address to retrieve the specified image from the given IP address. The new image will not overwrite the one in non-volatile memory. This is the recommended first step.

Net & save option

This option requires the same setup as the Net option, i.e. TFTP server and a new image. However, it copies the image to non-volatile memory and then the system boots from non-volatile memory.

Warning: The previous image in non-volatile memory will be lost when this procedure completes.

Last Saved option

The system will boot from non-volatile memory. This option will automatically show up after the 'Net & save' option is selected and the unit is reset.

Advanced > Advanced Tools > Configuration Management

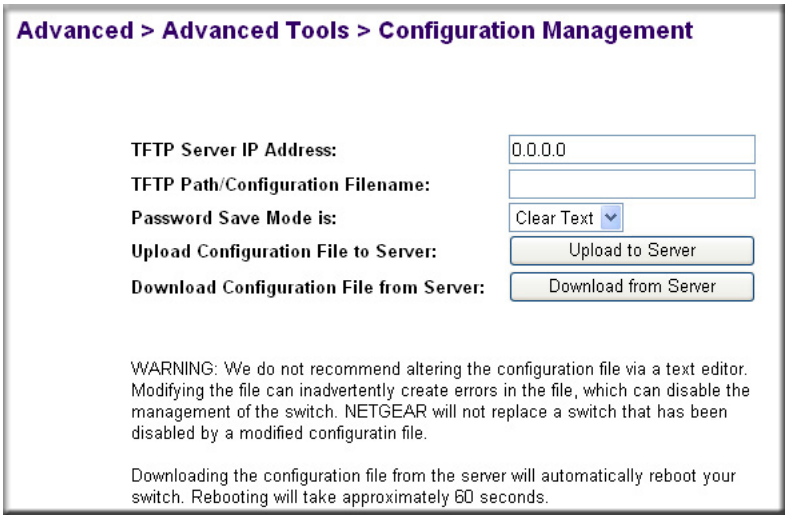


Figure 5-31: Configuration Management

Warning: Do not edit your configuration file. Editing your file can cause your switch to lose its management capabilities, and possibly degrade its performance. Editing the configuration file will void your warranty.

This menu allows you to save your configuration, in case you want to keep a copy for back-up purposes. We do not recommend editing your configuration file as many editors introduce unwanted characters that change the way the switch behaves.

You also can choose the switch password saving mode, either Clear Text or Encrypted for security reasons. If you select "Clear Text", your password will be readable in the configuration file.

This menu also allows you to download your configuration file back to the switch to restore your settings. After entering your settings, click "Upload to Server" if you want to upload the configuration file to a TFTP server or click "Download from Server" if you want to download configuration file from a TFTP server.

Advanced > Traffic Management

Traffic management covers the methods to improve the performance of your network by differentiating traffic and limiting excess broadcast traffic. There are two means to differentiate traffic with this switch- VLAN tags or using Differentiated Service Code Points (DSCP) in the header of data packets. By using either the VLAN tags (port-based) or DSCP (DiffServ), you can configure the switch so that certain traffic will take priority over less critical traffic.

Advanced > Traffic Management > Traffic Priority

Port Priority allows the user to specify which ports have greater precedence in situations where traffic may be buffered in the switch due to congestion.

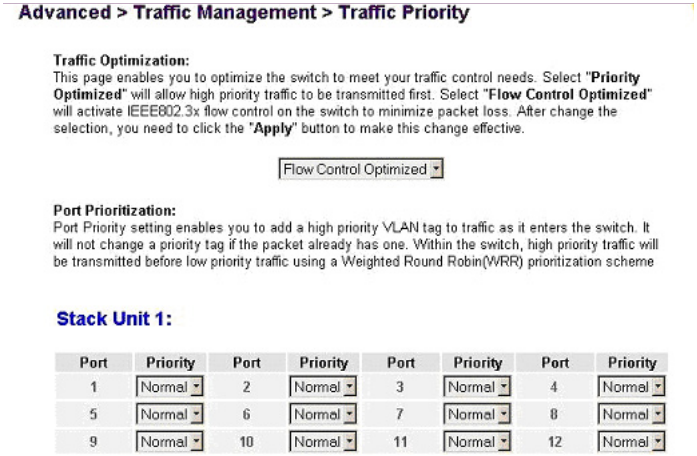


Figure 5-32: Traffic Prioritization Settings

Traffic that comes in on ports with a setting of ‘high’ will be transmitted before those that come in on a port with a ‘normal’ setting. The settings on this page only affect packets that do not already have VLAN priority tags. To raise the priority of a given port, toggle the port’s setting from ‘normal’ to ‘high’. The default setting for a port is ‘normal’.

You may choose to further differentiate packet priority by using the Differentiated Service (DiffServ) feature. DiffServ uses a priority tag in the packet, the Differentiated Service Code Point (DSCP), to determine the priority of the packet. There are 64 different tags available. This menu maps the various DSCP tags to the two queues in the switch.

Advanced > Traffic Management > Broadcast Control

Broadcast control lets you set a threshold for the number of broadcast packets sent over a port.

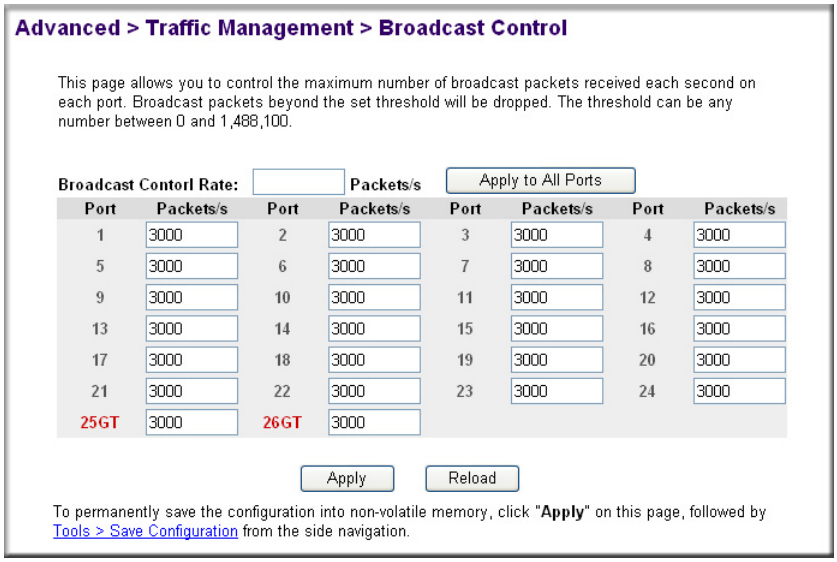


Figure 5-33: Broadcast Control menu

You can specify each port's threshold or apply the same threshold to all ports simply by entering the number in the Broadcast Control Rate field and clicking Apply to All Ports.

Advanced> VLANS

VLANs: 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. There are 64VLAN supported on this switch. This switch supports static, port-based VLANs.

Advanced> VLAN> Primary VLAN

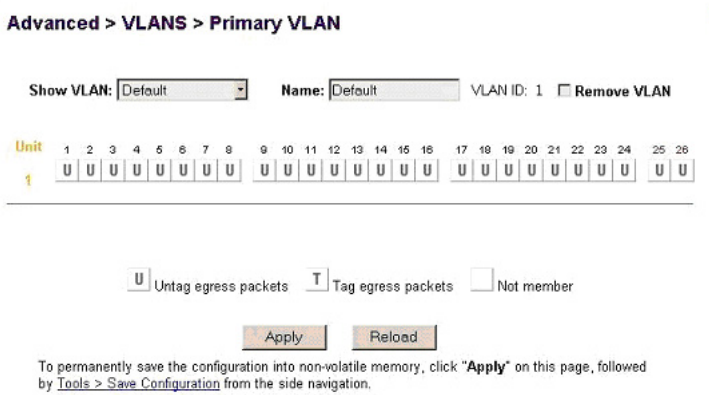


Figure 5-34: Primary VLAN

A ‘U’ or ‘T’ will be displayed for each port assigned to the VLAN, where ‘U’ stands for untagged and ‘T’ for tagged. If a port is an untagged member of a VLAN, the VLAN tag will be striped from the frame before it is sent out that port. If the port is a tagged member of a VLAN, the VLAN tag will stay in the frame when it is sent. A blank indicates that the port is not a member of the particular VLAN, and will not get any traffic for that VLAN. The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches (Reference: Appendix A, “Virtual Local Area Network” and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks).

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

Create a new VLAN Group:

1. Under the Show VLAN drop-down menu, select Add a new VLAN.
2. Enter the VLAN Id and name in the provided fields.
3. Add VLAN members if so desired. (See below).
4. Click Apply.

Delete a VLAN Group:

1. Check the Remove VLAN box for the VLAN you want to remove.
2. Click Apply.

Add a port to a VLAN Group:

1. Under the ‘Show VLAN’ drop down menu, select the VLAN you want to edit.
2. Click the box below the port number on the line of the VLAN so that a ‘T’ (tagged) or ‘U’ (untagged) appears.
3. Click Apply.

Remove a port from a VLAN Group:

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

Advanced> VLAN> VLAN Ports

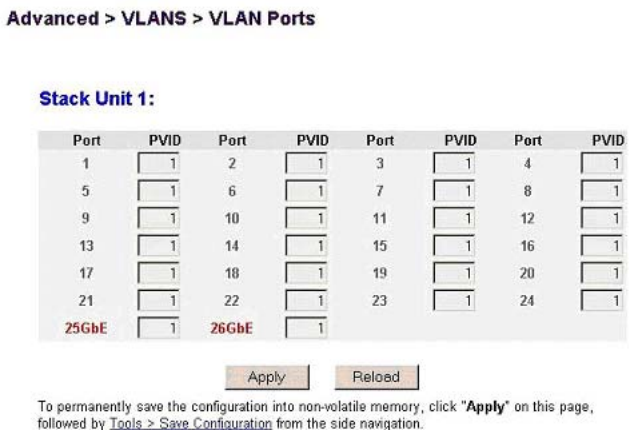


Figure 5-35: VLAN Port Settings

All untagged packets entering the switch will by default be tagged with the ID specified by the port’s PVID. This screen allows you to specify the PVID for each port. The number next to each port indicates which PVID is set for each port. Following industry standards, PVID 1 is the default PVID.

Advanced> Spanning Tree

This switch is compliant with IEEE802.1D Spanning Tree Protocol (STP). STP ensures that only one path at a time is active between any two network nodes. There maybe more than one physical path between any two nodes, forming a loop, either created for redundancy or by accident. STP ensures only one physical path is active and the others are blocked. If a loop is created for redundancy, STP will monitor the two paths and activate the stand-by path if the primary path fails. If a loop was created inadvertently, STP will disable one of the two paths. A loop in a network can disable your network by causing a “Broadcast storm”, the result of a broadcast message traveling through the loop again and again.

There are two sub-page of Spanning Tree configuration:

- Bridge Settings
- Port Settings

Advanced> Spanning Tree >Bridge Settings

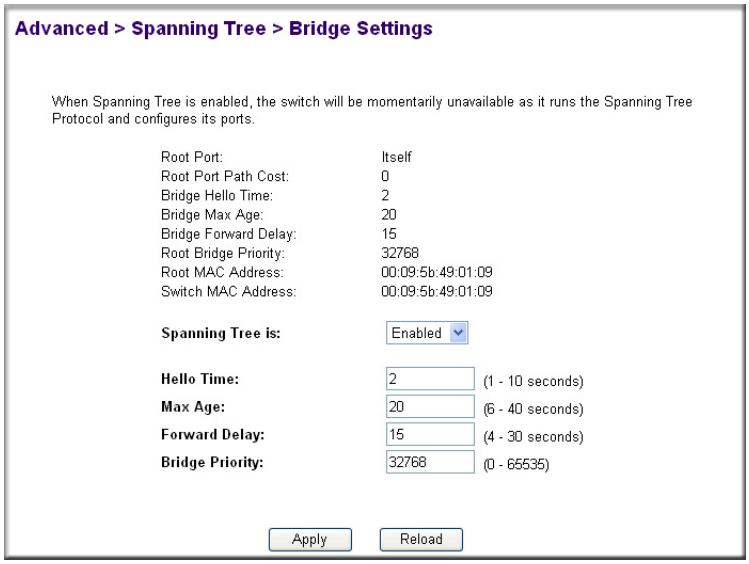


Figure 5-36: Spanning Tree: Bridge Settings

When Spanning tree is used in conjunction with a set of aggregated ports, also known as a port trunking, Spanning Tree will treat the trunk as a single virtual port.

Spanning Tree can be enabled or disabled in this screen.

Enable: There are four other tunable parameters to be addressed when enabled.

Hello Time	Time between configuration messages sent by the Spanning Tree algorithm
Max Age	Amount of time before a configuration message is discarded by the system
Forward Delay	Amount of time system spent transitioning from the ‘learning’ to the ‘listening’ to the ‘forwarding’ states
Bridge Priority	Priority setting among other switches in the Spanning Tree

Disable: Disable Spanning Tree algorithm on the system.

Advanced> Spanning Tree > Port Settings

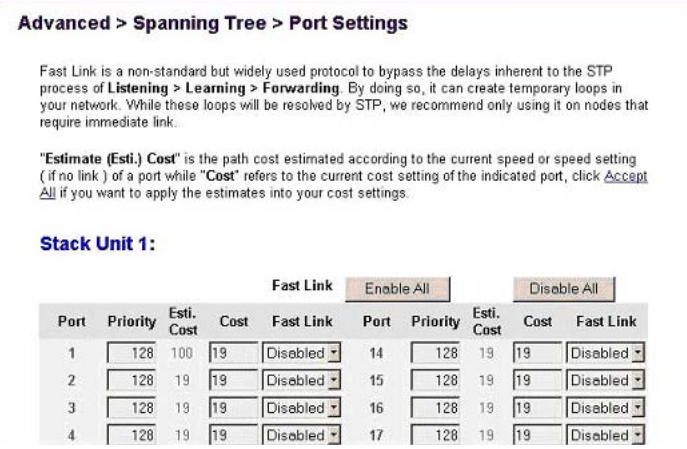


Figure 5-37: Figure 4-26. Spanning Tree: Port Settings

For the Port Settings options, you can specify Spanning Tree port priority, cost, and Fastlink parameters for each port.

Table 5-1. STP Port Setting Parameters

PARAMETERS	RANGE	DESCRIPTION
Prty (Priority)	0-255	STP uses this to determine which path (which port) to use for forwarding. The port with the lowest number has the highest priority.
Cost	1-65535	The switch uses this to determine which port is the forwarding port when the priority is equal. All other factors equal, the path with the lowest cost to the root bridge will be the active path. The estimated path cost is the industry standard for the port speed. The default path cost is the maximum speed for the port.
Fastlink	Enabled or Disabled	When a Fastlink enabled port running standard STP is connected, it will go through the STP negotiation (listening -> learning -> forwarding or blocking) before it will be fully available.

Fastlink in STP mode. If a client is trying to access a server 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 to direct forwarding mode, thus allowing any server access request to be forwarded. Fastlink mode can cause temporary loops in your network, but STP will find and eliminate them. Fastlink is best used on end node ports, i.e. ports connected to PCs or servers, and not on uplink ports to other switches.

Advanced> MAC

There are two advanced MAC setup configurations options:

- Aging Time
- Static Address

Advanced> MAC> Address Aging

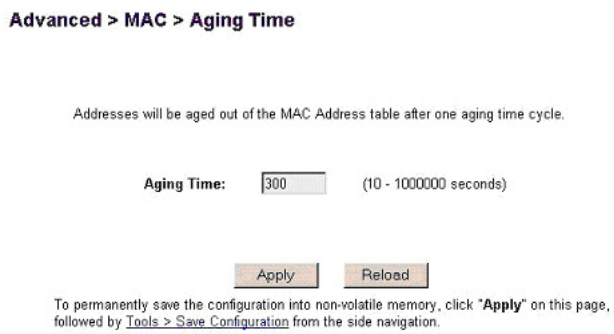


Figure 5-38: MAC > Address Aging

Aging Time is a variable that must be configured. Its purpose is to determine the amount of time an entry is held in the forwarding tables while no activity occurs from that address. Entries should be removed to update the table for MAC addresses that have moved or are turned off.

- The industry standard default value is 300 seconds (5 minutes).
- The administrator may change this value to any value between 10 and 1,000,000 seconds.
- After changing the value, click 'Apply'

Advanced> MAC> Static Addresses

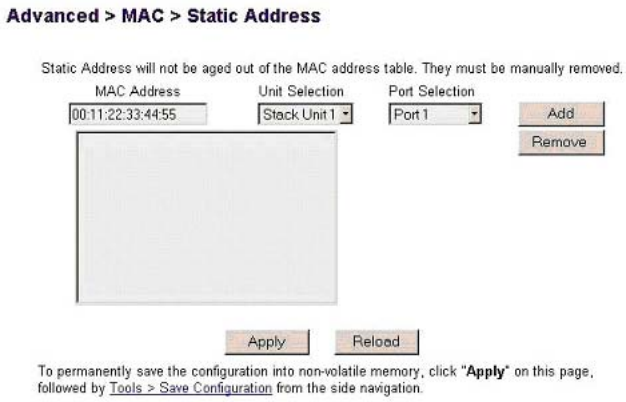


Figure 5-39: MAC > Static Addresses

Any system, whose MAC address and the port number are listed in this screen, will not be purged from the system's forwarding table by the aging process.

1. Add a new entry
2. Enter the MAC address and port in the appropriate boxes
3. Click Add
4. Remove an exist entry
5. Highlight that entry in the table, by clicking on the MAC address
6. Choose Remove

Advanced> Multimedia Support

Use the advanced multimedia support menu to manage high-bandwidth network traffic by enabling/disabling Internet Group Multicast Protocol (IGMP) traffic and configuring static multicast groups. These are tasks that require advanced expertise.

Advanced> Multimedia Support>Enable/Disable IGMP

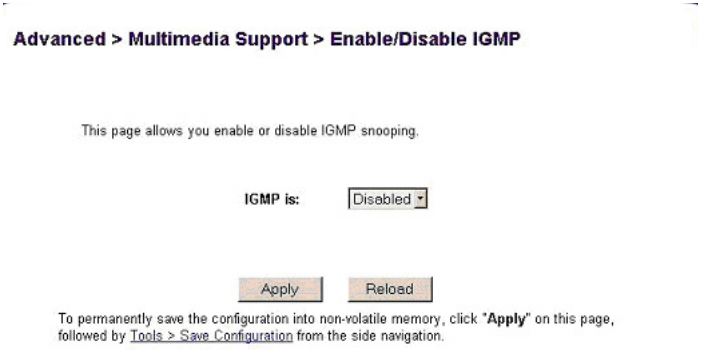


Figure 5-40: Multimedia Support > Enable/Disable IGMP

In networks where multimedia applications generate multicast traffic, IGMP can greatly reduce unnecessary bandwidth usage by limiting traffic forwarding that is otherwise broadcast to the whole network. Enabling IGMP will allow individual ports to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.

- **Enable**. The system will detect IGMP queries, report packets, and manage IP multicast traffic through the switch
- **Disable**. The switch will forward traffic and disregard any IGMP requests.

Advanced>Multimedia Support> Static Multicast Groups

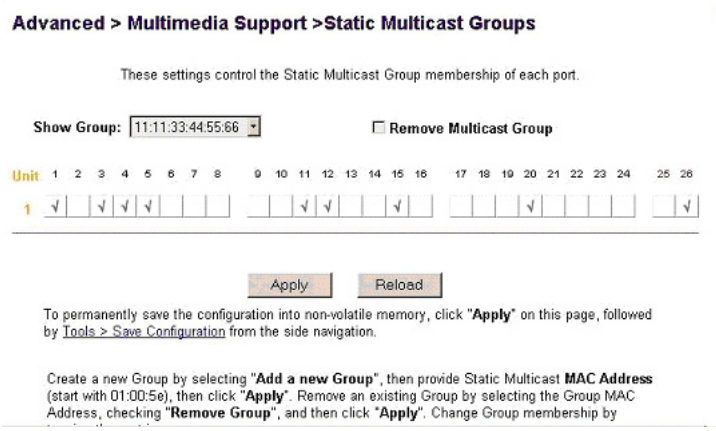


Figure 5-41: Multimedia Support > Static Multicast Groups

You can use this menu to configure permanently reachable multicast groups. The Static Multicast Administration menu lets you create individual groups by entering a MAC address of your static multicast group. Click on the ports to add them to the multicast group.

Advanced> SNMP

You can manage this switch using the Simple Network Management Protocol (SNMP) from a network management station. To do so, you must configure your switch to participate in the SNMP community and you must add the SNMP host agent to the host table. This prevents unauthorized SNMP access to your switch from non-approved SNMP hosts.

Support for these Standard MIBs is included:

- MIB II (RFC1213)
- Ethernet Interface MIB (RFC1643)
- Bridge MIB (RFC1493)
- Private Enterprise MIB (see the Resource CD for Managed Switches)

- 4-Group RMON (RFC1757)

Advanced> SNMP> Community Table

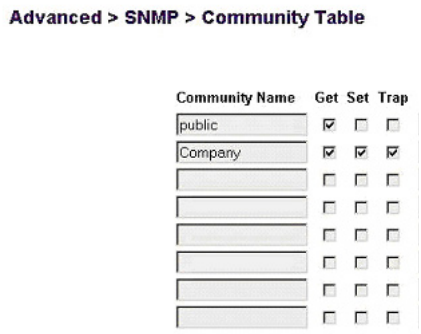


Figure 5-42: Figure 4-31. SNMP Management: Community Table

The administrator can create up to eight different community strings with combinations of GET, SET and TRAP privileges. These community strings need to be set prior to setting host access, as the host table depends on the existence of community strings. The public string has GET privileges by default.

Advanced> SNMP> Host Table

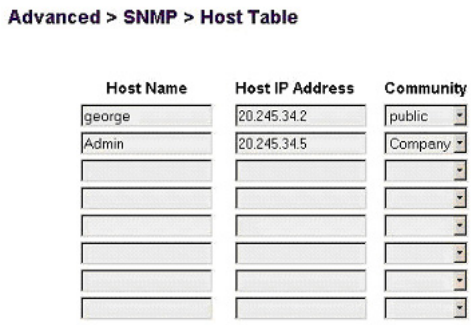


Figure 5-43: SNMP Management > Host Table

The SNMP Host Table screen allows you to add and remove hosts from access rights that have been granted to community groups. The permissions GET, SET and TRAP are assigned to a community name and then these permissions are assigned to individual machines by adding those machines and their IP address to the appropriate community string. Host Authorization can be Enabled or Disabled.

Host Authorization is a security feature to limit people who are not listed in the host table from accessing the switch using SNMP.

Advanced> SNMP> Trap Setting

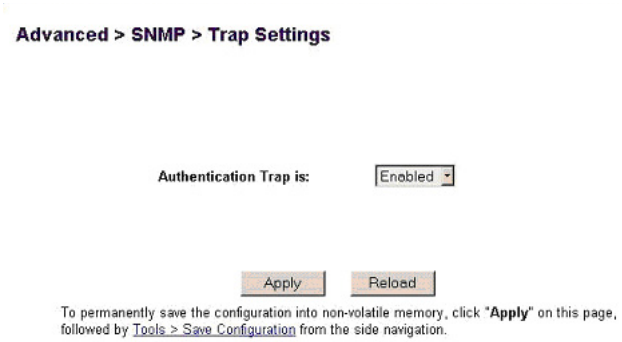


Figure 5-44: Figure 4-33. SNMP Management > Trap Settings

With authentication traps enabled, the system generates a SNMP trap when a host authorization fails. Hosts in community strings with TRAP privileges are notified when a trap occurs.

Chapter 6
Command Line Interface

The 700 Series Switches features a Command Line Interface (CLI) designed for expert users who are familiar with common CLIs in use in the market. The CLI follows a tiered structure, enabling different commands at different levels or sections of the CLI.

Manual Syntax

Before discussing the details of the CLI operation, the syntax of the CLI commands used in this manual are listed below:

- The CLI syntax is presented in bold ariel text with the 700 Series Managed switch model number followed by a “#”, such as in this example:

  FSM726# show spanning-tree interface ethernet <x/y>

- In a paragraph with other text, command keywords included are in regular courier font.
- The required fields in a command are enclosed in angle brackets (<>), for instance, system password <password>
- The optional field in a command are enclosed in square brackets ([]), for instance,

  ```
  system radius authen-mode [local | local-then-remote | remote]
  ```

- Command refers to a command used in the command line interface (CI Command)

Entering the CLI

The CLI is an option within the Command Menu Interface (CMI), so you must be using either the console port or a telnet session to use the CLI. See Chapter 4, “Administration Console Telnet Interface” for information on connecting to the CMI. Once in the CMI, select Advanced, then Command Line. You will see a prompt similar to this. This is known as the root prompt.

FSM726#

Note: Your prompt may look different if you gave your switch a different name.

Once you see the root prompt, you are in CLI mode.

If you have a question on what commands you can use, type a question mark '?' at the prompt. A list of available commands will be presented to you.

There are five items in the root prompt.

- "Configure" on page 5-13
- "Exit" on page 5-3
- "Help" on page 5-2
- "Ping" on page 5-2
- "Show" on page 5-3

These five items will be covered below.

Help

The help command displays instructions on how to access help on the CLI.

Syntax:

FSM726# Help

FSM726# ?

To access `Help` on specific command, you enter a question mark behind the command in question, then a list of available options will be presented to you. For example, suppose you want to know the available options to the command cos. You would enter `cos ?`.

Ping

The `ping` command is used to check network connectivity. It lets you send a small packet to a particular host. Once the host receives the packet, it will return the packet to its source. The time the packet takes for this round trip is recorded in milliseconds. If the destination host is not available, an error message is returned.

Syntax

FSM726# ping <IP address>

Where

`<IP Address>` = the IP address of the destination host

Exit

The `exit` command moves you up one level in the CLI structure. For example, when you are in configuration mode, and the prompt looks like `FSM726(config)#`. By entering exit at the prompt, you will exit the configuration mode and be taken back to the root level, where the prompt looks like `FSM726#`. When you enter the exit command at the root level, you will return to the CMI.

Syntax

FSM726# exit

Show

You can use the `show` command to view system configuration. The information that can be shown falls into the following categories:

- DiffServ – DiffServ settings. See “Show DiffServ” on page 5-4.
- Dot1x – Shows 802.1x settings. See “Show Dot1x” on page 5-4.
- Interfaces – Interface status & configuration. See “Show Interfaces” on page 5-4.
- IP – IP information. See “Show IP” on page 5-5.
- Mac-address-table – the MAC address table and other related items, such as aging timers and static addresses. See “Show Mac-Address-Table” on page 5-5.
- Mirror – Mirroring settings. See “Show Mirror” on page 5-7.
- Multimedia – IGMP settings. See “Show Multimedia” on page 5-7.
- Running-config – Current operating configuration. See “Show Running-Config” on page 5-7.
- SNMP – SNMP related information. See “Show SNMP” on page 5-8.
- Spanning-tree – the Spanning Tree topology. See “Show Spanning Tree” on page 5-9.
- System – System-related settings. See “Show System” on page 5-10.
- Trunking – Trunking information. See “Show Trunking” on page 5-11.
- VLAN – VLAN information. See “Show VLAN” on page 5-11.

Show DiffServ

Use the `show diffserv` command to view the priority associated with each DSCP value.

Syntax

FSM726# show diffserv

An example of the partial output is shown below.

```
DSCP  Priority

==== ========

    0 normal

    1 normal

    2 normal

    3 normal

    4 normal

    5 normal

    6 normal
```

Show Dot1x

Use the `show dot1x` command to show the authentication server IP, shared secret, and the Reauthentication Timer value.

Each port is listed with the 802.1x state, which can be forced authorized, forced unauthorized (deny client to access network), or auto detected. The Reauthentication Timer value specifies the time interval between the authentication server's checks of users connected to the network. The default time interval is 3600 seconds.

Show Interfaces

The `show interface` command displays such information as port statistics, duplex, speed, and other port-related information.

Syntax

FSM726# show interface Ethernet <x/y>

Where

`<x/y>` = x is the stack number (always 1 in FSM726), y is the port number

An example of the display output is shown below.

```
FastEthernet1/23 is Up
  Hardware is Fast Ethernet
  Auto-duplex (Full), Auto Speed (100), 100BaseTX/FX
  pvid is: 1
  cos is normal
  broadcast rate limit is 1488100 packets/second
  input:  63994 Bytes, 489 Unicast Packets, 83 Non-unicast Packets
        0 Packet Discards, 0 Packet Errors
        0 Undersized Packets, 0 Oversized Packets
  output: 223115 Bytes, 484 Unicast Packets, 4 Non-unicast Packets
        0 Packet Discards, 0 Packet Errors
```

Show IP

The `show IP` s IP information

Syntax

FSM726# show ip

An example of the display output is shown below.

```
IP Assignment Mode: Manual
IP address: 169.254.224.1
Subnet mask: 255.255.0.0
```

Show Mac-Address-Table

The `show mac-address-table` command displays a variety of information on the status and content of the MAC-address-table.

Aging Time

The `show mac-address-table aging-timer` command is used to display the aging timer of the mac-address-table.

Syntax

FSM726# show mac-address-table aging-timer

Dynamic

The `show mac-address-table dynamic` command displays the dynamically learned MAC addresses.

Syntax

FSM726# show mac-address-table dynamic

An example of the display output is shown below.

```
Destination Address  Address Type  Destination Port
-------------------  ------------  ----------------
00.06.5b.69.3d.be       Dynamic       FastEthernet1/23
```

Multicast-Static

The `show mac-address-table multicast-static` command displays the static multicast addresses

Syntax

FSM726# show mac-address-table multicast-static

Static

The `show mac-address-table static` command displays configured static addresses.

Syntax

FSM726# show mac-address-table static

Show Mirror

The `show mirror` command displays mirroring configurations of the switch. Primarily, it shows which ports are mirroring and being mirrored.

Syntax

FSM726# show mirror

An example of the output is shown below.

```
Port Mirroring is: Enabled
  Source: 1/23
  Monitor: 1/1
```

Show Multimedia

The `show multimedia` command displays IGMP and HPO status, indicating whether they are enabled or disabled

Syntax

FSM726# show multimedia

Show Running-Config

The `show running-config` command displays the current running configuration. It displays a great deal of information, including system information, interface status of each port, VLAN configuration, DiffServ, and SNMP configuration among other things.

Syntax

FSM726# show running-config

A partial example of the display output is shown below.

```
snmp-server name Not Defined
snmp-server location Wiring Closet #1
snmp-server contact Tom
!
snmp-server community public RO
snmp-server community Tom WO
snmp-server host-authorization
!
```

```
vlan database
 vlan 1 Default
 exit
!
interface Ethernet 1/1
 cos Normal
 description Not Defined
 no shutdown
 speed 100
 duplex full
 flow-ctrl
 negotiation auto
 switchport access vlan untagged 1
 switchport access native 1
 mirror--
 mirror monitor
 spanning-tree port-priority 128
 spanning-tree cost 19
 no spanning-tree fastlink
 exit
interface Ethernet 1/2
 cos Normal
 description Not Defined
 no shutdown
 speed 100
 duplex full
 flow-ctrl
 negotiation auto
 switchport access vlan untagged 1
 switchport access native 1
 spanning-tree port-priority 128
 spanning-tree cost 19
 no spanning-tree fastlink
 exit
 --More--
```

Show SNMP

The `show snmp` command displays system information that will be reported to an SNMP agent, including the Contact and the Location.

Syntax

FSM726# show snmp

Show Spanning Tree

The `show spanning tree` command displays the status and topology of the spanning-tree configuration, as well as spanning-tree state of each port.

Brief

The `show spanning-tree brief` command gives a brief summary of the spanning-tree status.

Syntax

FSM726# show spanning-tree brief

An example of the display output is shown below.

```
VLAN1

  Spanning tree enabled protocol IEEE
  ROOT ID    Priority 32768
             Address 0009.5b36.b007
             Hello Time 2 sec  Max Age 20 sec  Forward Delay  15 sec
 Bridge ID  Priority 32768
             Address: 0009.5b36.b007
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Port                    Designated
Name    Prio Cost  Sts  Cost  Bridge ID
------- ---- ----  ---  ----  --------------
Fa1/1   128  19    BLK  0     0009.5b36.b007
Fa1/2   128  19    BLK  0     0009.5b36.b007
Fa1/3   128  19    BLK  0     0009.5b36.b007
Fa1/4   128  19    BLK  0     0009.5b36.b007
…
Fa1/22  128  19    BLK  0     0009.5b36.b007
Fa1/23  128  19    FWD  0     0009.5b36.b007
Fa1/24  128  19    BLK  0     0009.5b36.b007
Gi1/25  128  4     BLK  0     0009.5b36.b007
Gi1/26  128  4     BLK  0     0009.5b36.b007
```

Interface

The `show spanning-tree interface` command displays the spanning tree state of a particular port.

Syntax

FSM726# show spanning-tree interface ethernet <x/y>

Where

`<x/y>` = x is the stack number (always 1 in the case with FSM726), and y is the port number.

An example of the display output is shown below:.

```
Interface Fa1/23 (port 23) in Spanning tree is FORWARDING
  Port path cost 128, Port priority 19
  Designated root has priority 32768, address 0009.5b36.b007
  Designated bridge has priority 32768, address 0009.5b36.b007
```

Show System

The `show system` command displays system-related data.

Syntax

FSM726# show system

An example of the display output is shown below.

```
System Uptime: 0 Days  1 hr.  42 min.  15 sec.
System Description: FSM726 Managed Switch
System name: Switch #1
System contact: Tom
System location: Closet #2
MAC Address: 00:09:5b:36:b0:07
IP Assignment Mode: Manual
IP Address: 169.254.224.1
Network Mask: 255.255.0.0
Gateway Address: 169.254.224.5
Web Access is: Enabled
Telnet Access is: Enabled
Password is: Disabled
User Authentication Mode is Local
```

RADIUS Server IP Address: 0.0.0.0
Shared Secret is:
Hardware Version: RA
Boot ROM Version: 1.2 (2495)
Software Version: 1.0.4 (2505)
Next Boot from: Last Saved
TFTP Server IP Address: 0.0.0.0
TFTP Path/Filename:
IP Filtering is: Disabled

Show Trunking

The `show trunking` command displays the trunking state of the switch. The FSM726 is capable of forming four trunks, so shown in the display are the ports that belongs to each trunk.

Syntax

FSM726# show trunking

An example of the display output is shown below.

```
Trunk Id     Ports
--------     ----------------------------
 1           Fa1/9,Fa1/10
 2           Fa1/1,Fa1/2
 3           Fa1/17,Fa1/18
 4
```

Show VLAN

The `show VLAN` command displays VLAN configuration and status of the switch.

Brief

The `show vlan brief` command displays a quick summary of each VLAN configured.

Syntax

FSM726# show vlan brief

An example of the display output is shown below.

```
VLAN Name                        Status   Ports
```

```
---- ------------------------------- --------- ------------------------------
1    Netgear                         active    Untagged:
                                               Fa1/4,Fa1/5,Fa1/7,Fa1/11,
                                               Fa1/12,Fa1/13,Fa1/14,Fa1/15,
                                               Fa1/19,Fa1/20,Fa1/21,Fa1/22,
                                               Fa1/23
3    Company                         active
                                               Tagged:
                                               Gi1/25, Gi1/26
```

VLAN

The `show vlan` command displays information on membership of individual VLANs.

Syntax

FSM726# show vlan [cr | VLAN index #]

Where

`<cr>` = a carriage return. The command show vlan lists the VLANs configured on the switch.

`<VLAN index #>` = The VLAN ID. Adding the VLAN ID to the show vlan command displays the port that belongs to that particular VLAN. For example, show vlan 1 displays the ports that belong to VLAN 1.

An example of the display output is shown below:.
Untagged port members: 4,5,7,11-15,19-23
Tagged port members: none

COS-PVID

The `show vlan cos-pvid` displays the PVIDs and the CoS settings of each port.

Syntax

FSM726# show vlan cos-pvid

An example of the display output is shown below:

```
Port     PVID   Priority
------------------------
1:1      1      Normal
1:2      1      Normal
```

1:3	1	Normal
1:4	1	Normal
1:5	1	Normal

Configure

The information that can be configured falls into the following categories:

- DiffServ – DiffServ settings. See "DiffServ" on page 5-13
- Dot1x – 802.1x settings. See "Dot1x" on page 5-14.
- Exit – takes you out of configuration mode. See "Exit" on page 5-15.
- Lacp – Link Aggregation Control Protocol. See ...
- Interface – select an Interface to configure. See "Interface" on page 5-15.
- Mac-address-table – configure the MAC address table. See "Mac-address-table" on page 5-21.
- Multimedia – IGMP and traffic optimization settings. See "Multimedia" on page 5-22.
- No – negate a command or its defaults. See "No " on page 5-23.
- SNMP-server – modify SNMP parameters. See "SNMP Server" on page 5-23.
- Spanning-tree – the Spanning Tree topology. See "Spanning Tree" on page 5-26.
- System – System-related settings. See "System" on page 5-27.
- VLAN – configure VLAN parameters. See "VLAN" on page 5-34

Entering the command `configure` at the root prompt takes you into configuration mode. When you're in configuration mode, the prompt changes to:

FSM726(config)#

It is in this mode where the vast majority of configuration is performed. To exit the configuration mode and return to root prompt, use the `exit` command.

DiffServ

DiffServ divides traffic into one of 64 classes using the packet's DSCP value. This allows for greater differentiation of traffic priority than port-based traffic prioritization.

Syntax

FSM726(config)# diffserv <DSCP> <priority>

Where

`<DSCP>` = The DSCP value, which ranges from 0-63

`<Priority>` = The priority associated with the defined DSCP value. The available options are `normal` and `high`

For example, suppose you want to set DSCP 33 to high, the command to do so would be:

FSM726(config)# diffserv 33 high

Dot1x

The RADIUS Server IP Address must be configured first before enabling 802.1x. Otherwise Port-Based Authentication will not take effect. You can also set a RADIUS server shared secret.

The Re-authentication Timer allows the user to specify the time interval between authentication server's checks of users connected to the network. The default time interval is 3600 seconds and the range is from 1 - 65535 seconds.

```
Commands:
  diffserve          Set DiffServe settings
  dot1x              Set 802.1x settings
  exit               Exit from configure mode
  interface          Select an interface to configure
  mac-address-table  Configure the MAC address table
  multimedia         Set IGMP and High Priority Optimization
  no                 Negate a command or set its defaults
  snmp-server        Modify SNMP parameters
  spanning-tree      Spanning Tree Subsystem
  system             System Settings
  vlan               Configure VLAN parameters

Not Defined(config)# dot1x ?
Commands:
  server-ip          Set the RADIUS server's IP
  shared-secret      Set the RADIUS shared secret
  timeout            Set 802.1x timer
```

Figure 6-1: Config Dox1x commands

Syntax

FSM726(config)# dot1x 123.123.123.12

Exit

The `exit` command takes you out of the CLI mode by one level. For example, when you are in configuration mode, and the prompt looks like `FSM726(config)#`. By entering `exit` at the prompt, you will exit the configuration mode and be taken back to the root level, where the prompt looks like `FSM726#`. When you enter the `exit` command at the root level, you will return to the Main Menu of the switch.

Syntax

FSM726(config)# exit

Interface

The `interface` command allows you to configure each network interface of the switch. Items such as the speed, duplex, and negotiation are configured in this mode. The command to enter the interface mode is

Syntax

FSM726(config)# interface ethernet <x/y>

Where

`<x/y>` = x is the stack number, and y is the port number, which ranges from 1-26. Since FSM726 is not stackable, the value of x is always 1.

For example, suppose you want to configure port 8 on the switch, the command to do so would be:

```
FSM726(config)# interface ethernet 1/8
```

When the interface command is properly entered, you will be taken to the Interface Configuration Mode, where the prompt changes from `FSM726(config)#` to `FSM726(config-if)#.`

When you are done configuring one particular interface and wish to configure another interface, you must exit the Interface Configuration Mode by using the `exit` command. You then have to re-enter Interface Configuration Mode by specifying another interface, again, using the `interface` command

When you're in interface configuration mode, you will be able to configure the following items.

CoS (Class or Service)

Class of Service (CoS) 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.

Syntax

FSM726(config-if)# cos <normal/high>

Where

`<normal/high>` = the priority given to the port. When set to high, traffic from and destined for this port will take priority over traffic from other ports.

Description

This command allows you to assign a name or description to a port.

syntax

FSM726(config-if)# description <description>

where

`<description>` = the description you wish to give to this particular interface

Duplex

Syntax

FSM726(config-if)# duplex <duplex operation>

Where

`<duplex operation>` = one of three modes. auto, full, or half.

Exit

This command takes you out of Interface Configuration Mode and back to Configuration Mode.

Syntax

FSM726(config-if)# exit

Flow Control

This command enables flow control on this particular port.

Syntax

FSM726(config-if)# flow-ctrl

Help

The `help` command displays instructions on how to access help on the CLI.

Syntax

FSM726(config-if)# Help

To access Help on a specific command, you enter a question mark behind the command in question, then a list of available options will be presented to you. For example, suppose you want to know the available options to the command `cos`. You would enter `cos ?`.

Mirror

You can designate a port for monitoring traffic from one or more other ports or of a single VLAN configured on the switch. The switch monitors the network activity by copying all traffic from the specified monitoring sources to the designated monitoring port, to which a network analyzer can be attached

Syntax

FSM726(config-if)# mirror [source | monitor]

Where

`[source | monitor]` = Setting this particular port to be a mirror source or a mirror monitor

Use the no command to disable mirror.

Negotiation

This command lets you enable speed and duplex auto-negotiation.

Syntax

FSM726(config-if)# negotiation auto

No

The `No` command negates one of your previously given commands.

Syntax

FSM726(config-if)# no <commands>

Where

`<command>` = the command which you wish to negate.

For example, suppose you previously turned on flow control on this particular interface by using the `flow-ctrl` command, and you changed your mind and wish to turn it off. The command to do so would be

no flow-ctrl

Another example:

Suppose you have configured this particular interface to e a mirror source with the mirror source command. To disable the port as a port mirror, use the `no mirror source` command.

Type

The type command let you select whether to use the RJ-45 interface or the GBIC interface on your gigabit ports (port 25 & 26). If a GBIC module is present, you may wish to use gbic mode; however, if no GBIC module is present, the switch defaults to the RJ-45, also known as twisted-pair (TP).

Syntax

FSM726(config-if)# type <interface type>

Where

`<interface type>` = Options for this field include `gbic` and `tp`.

Shutdown

The `shutdown` command let you shutdown this particular interface. You can reverse this command by using the `no shutdown` command.

Syntax

FSM726(config-if)# Shutdown

Spanning Tree

The `spanning-tree` command lets you configure the variables of the port that affects its spanning-tree operation, items such as port cost and priority is configured through this command.

Syntax

FSM726(config-if)# spanning-tree [cost <1-65535> | port-priority <0-255> | fastlink]

Where

`Cost <1-65535>` = the cost of the port, ranges from 1-65535

`port-priority <0-255>` = the priority of the port, ranges from 0-255

`fastlink` = enables Fastlink, a mode that bypasses the listening & learning phase of Spanning Tree

Speed

Syntax

FSM726(config-if)# speed <speed>

Where

`<speed>` = the speed of the port. The options are 10, 100, 1000, or auto (for automatic speed configuration).

Switchport

The `switchport` command lets you configure VLAN access mode of this particular port.

- VLAN

syntax

FSM726(config-if)# switchport access vlan [tagged <VLAN Membership> | untagged <VLAN membership>]

Where:

`tagged <VLAN Membership>` = setting the VLAN membership to tagged mode. VLAN Membership ranges from 1-4094

`untagged <VLAN Membership>` = setting the VLAN membership to untagged mode. VLAN Membership ranges from 1-4094

For example, suppose this particular port belongs in VLAN 64 and 32. You wish to configure it so that it operates in tagged mode in VLAN 64, but in untagged mode in VLAN 32, the command to do so would be:

FSM726(config-if)# switchport access vlan tagged 64

FSM726(config-if)# swtichport access vlan untagged 32

- Native

All untagged packets entering the switch will by default be tagged with the ID specified by the port's PVID. This command allows you to specify the PVID for each port. The PVID values ranges from 1-4094. Following industry standards, PVID 1 is the default PVID

Syntax

FSM726(config-if)# switchport access native <PVID value>

where

`<PVID Value>` = the PVID value assigned for this particular port.

Trunking

Port Trunking is a feature that allows multiple links between switches to work as one virtual link or 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 ports 1 to 8, ports 9 to 16, ports 17 to 24, or port 25 and port 26 (using an FSM726 as an example), on the same switch unit. Up to four trunks can be enabled at the same time. Spanning Tree will treat trunked ports as a single virtual port.

Syntax

FSM726(config-if)# trunking [add <trunk #> | remove <trunk #>]

Where

`add <trunk #>` = adding this particular port to a trunk. The trunk number ranges from 1-4.

`remove <trunk #>` = removing this particular port from a trunk. The trunk number ranges from 1-4.

For example, to add this particular port to trunk 4 by entering

FSM726(config-if)# trunking add 4

By the same token, to remove this port from trunk 4, you would enter

FSM726(config-if)# trunking remove 4

Mac-address-table

The `mac-address-table` command lets you configure the operation and maintenance of the MAC address table. The aging timers and static entries are configured through this command.

Aging-Timer

Syntax

FSM726(config)# mac-address-table aging-timer <aging time>

Where

`<aging time>` = the maximum time where a MAC address will stay in the MAC address table. This number ranges from 10-1,000,000 seconds.

Static

The Static Addresses Table, allows the administrator to specify Media Access Control (MAC) addresses for specific ports that will not be purged from the bridge table by the aging function.

Syntax

FSM726(config)# mac-address-table static <mac-address> <ethernet interface number>

Where

`<mac-address>` = The MAC address you wish to keep on the table regardless of aging timers. The MAC address is a 48-bit string, expressed in hexadecimal with a colon separating every 8 bits. For example, 00:2d:3f:22:11:54.

`<ethernet interface number>` = The Ethernet interface associated with the MAC address you specified. The interface number is expressed in x/y format, where x is the stack number (always 1 in the case with FSM726), and y is the port number.

Multicast-Static

You can use this menu to configure permanently reachable multicast groups. The `Static Multicast` command let you create individual groups by entering the MAC address of static group

Syntax

FSM726(config)# mac-address-table multicast-static <mac-address> ethernet <interface number>

Where

`<mac-address>` = the MAC address you wish to place into the static multicast group.

`<interface number>` = the Ethernet interface associated with the static multicast group.

For example, if you want to add port 5 to static multicast group aa:aa:aa:10:30:3f, the command to do so would be

FSM726(config)# mac-address-table multicast static aa:aa:aa:10:30:3f ethernet 1/5

Disable

The `disable` command disables the switch's dynamic address learning capability.

Syntax

FSM726(config)# mac-address-table disable

Multimedia

In networks where multimedia applications generate multicast traffic, Internet Group Multicast Protocol (IGMP) can greatly reduce unnecessary bandwidth usage by limiting traffic forwarding that is otherwise broadcast to the whole network to only those ports that need it. Enabling IGMP will allow the switch to detect IGMP queries, report packets, and manage IP multicast traffic through the switch.

IGMP

The `multimedia igmp` command enables Internet Group Management Protocol on the switch.

Syntax

```
FSM726(config)# multimedia igmp
```

HPO

The `multimedia hpo` command enables High Priority Optimization (HPO). This means that as traffic flows through the switch, if there is a conflict between maximizing high priority traffic or ensuring flow control, the switch will favor the high priority traffic. Use the no hpo command to optimize for flow control.

Syntax

FSM726(config)# multimedia hpo

No

The `No` command negates one of your previously given commands.

Syntax

FSM726# no <commands>

Where

`<command>` = the command which you wantwant to negate.

SNMP Server

SNMP (Simple Network Management Protocol) enables you to manage the switch through the use of a network management station running an SNMP server. Items such as trap settings, community, and hosts are configured through the `snmp-server` command.

Community

You can create up to eight different community strings with combinations of privileges. These community strings need to be set prior to setting host access, as the host table depends on the existence of community strings

Syntax.

FSM726(config)# snmp server community <name> [ro | rw |wo | trap]

Where

`<name>` = the name of the community

`[ro | rw |wo |trap]` = the privilege associated with this community.

`ro` = read only.
`rw` = read-write access
`wo` = read-only
`trap` = trap allowed

Contact

You can use the `contact` command to specify contact information for the switch.

Syntax

FSM726(config)# snmp-server contact <contact info>

Where

`<contact info>` = the contact information associated with this switch.

Location

You can use the `location` command to describe the location of the switch.

Syntax

FSM726(config)# snmp-server location <location info>

Where

`<location info>` = the location of this switch.

Name

Use the `name` command to give a name to the switch. This is done to make the switch easier to identify.

Syntax

FSM726(config)# snmp-server name <switch name>

Where

`<switch name>` = the name you wantwant to give to the switch

Host

The `host` command is used to specify hosts to receive SNMP notifications.

Syntax

FSM726(config)# snmp-server host <host name> <host IP address> <community string>

Where

`<host name>` = the name of the host that is to receive SNMP notifications.

`<host IP address>` = The IP address of the host specified

`<community string>` = the community which the host belongs to

Host Authorization

The `host-authorization` command enables SNMP host authorization.

Syntax

FSM726(config)# snmp-server host-authorization

Trap

The `trap` command enables SNMP trap. s IP is not in the SNMP host table.

Syntax

FSM726(config)# snmp-server trap

Spanning Tree

Spanning Tree Protocol (STP) ensures that only one path at a time is active between any two network nodes. There are maybe more than two physical path between any two nodes for redundant paths; STP ensures only one physical path is active and the others are blocked. STP will prevent an inadvertent loop in a network, which can disable your network due to a “Broadcast storm”, the result of a broadcast message traveling through the loop again and again.

Forward Time

Use the `forward-time` to set the STP forward interval.

Syntax

FSM726(config)# spanning-tree forward-time <interval>

Where

`<interval>` = the STP forward interval. This number ranges from 4 – 30 seconds.

Hello Time

Use the `hello-time` command to set the STP hello interval.

Syntax

FSM726(config)# spanning-tree hello-time <interval>

Where

`<interval>` = the STP hello interval. This number ranges from 1 – 10 seconds.

Max-Age

Use the `max-age` command to set the STP maximum age interval.

Syntax

FSM726(config)# spanning-tree max-age <interval>

Where

`<interval>` = the STP max age interval. This number ranges from 6 – 40 seconds.

Priority

Use the `priority` command to set the STP priority

Syntax

FSM726(config)# spanning-tree priority <priority>

Where

`<priority>` = is the STP priority. This number ranges from 0 – 65535.

System

The `system` command configures important system items such as IP addresses, password security, and firmware upgrade.

Config-TFTP

The `config-tftp` command is used to configure and control the mechanism to load or save the configuration file via TFTP.

Syntax

FSM726(config)# system config-tftp [save | load] <IP address> <path & filename>

Where

`[save | load]` = Choose `save` if you wish to save your configuration file to the TFTP server, load if you wish to load the configuration file from the TFTP server.

<IP address> = the IP of the TFTP server where the configuration file is stored (if you are loading a configuration file from the TFTP server) or destined for (if you are saving your configuration file to the TFTP server).

`<path & filename>` = The path and file name of the configuration file

config-tftp ip

The `config-tftp ip` command lets you set the IP address of the TFTP server for configuration file save/load.

Syntax

FSM726(config)# system config-tftp ip <IP address>

Where

`<IP address>` = the IP address of the TFTP server.

Config-tftp Path/File

The `config-tftp path/file` command lets you configure the path and the filename of the configuration file to be loaded/saved.

Syntax

FSM726(config)# system config-tftp path/file <path&filename>

Where

`<path&filename>` = the path and the filename of the file

IP

The `IP` command lets you set the IP address of the switch.

Syntax

FSM726(config)# system ip <IP address>

Where

`<IP address>` = the IP address of the switch.

IP-Filter

The purpose of IP filtering is to prevent unauthorized personnel from gaining access to the switch. This is accomplished by allowing only certain IP addresses to be able to access the management. This command enables IP filtering on the switch. The No command will disable it.

Syntax

FSM726(config)# system ip-filter

IP-filter address

The `IP-filter address` allows you to enter and remove IP address from the approved list. Use the No command to remove an IP address.

Syntax

FSM726(config)# system ip-filter address <IP-address>

Where

`<IP address>` = an IP address that is authorized to access the management.

IP-Mode

The `IP-Mode` command sets the IP assignment mode of the switch. There are three modes available to the user.

Manual – The user manually enter IP related information

BootP – Bootstrap Protocol, which allows the FSM726 switch to discover its own IP address from a BootP server on the network

DHCP – The switch accepts DHCP broadcast from a DHCP server and automatically configure IP related information

Syntax

FSM726(config)# system ip-mode [manual | bootp | DHCP]

Mask

Use the `Mask` command to set the network mask.

Syntax

FSM726(config)# system mask <network mask>

Where

`<network mask>` = network mask of your network

Gateway

Use the `Gateway` command to set the default gateway

Syntax

FSM726(config)# system gateway <default gateway>

Where

`<default gateway>` = the IP address of the default gateway

Save

The `save` command is used to save the configuration to NVRAM once you have made changes.

Syntax

FSM726(config)# system save

Restore

The `restore` command is used to restore all configurations back to factory default value. Please note that this command will cause the switch to reset itself.

Syntax

FSM726(config)# system restore

Web

Use this command enable/disable the web configuration interface. Use the `No` command to disable the web interface.

Syntax

FSM726(config)# system web

Telnet

Use this command to enable/disable configuration via telnet. Use the `No` command to disable the Telnet access.

Syntax

FSM726(config)# system telnet

Username

Use the `username` command to create a new user for the switch.

Syntax

FSM726(config)# system username <username>

Where

`<username>` = the user name you wish to set up for accessing the switch. Please note that this field is case sensitive.

Password

Use this command to set a password for the switch

Syntax

FSM726(config)# system password <password>

Where

`<password>` = the password you wish to set for the switch.

Firmware boot

The firmware command is used to upgrade the firmware through a variety of options. The `boot` command is used to configure the way in which the switch will boot after a firmware upgrade. Once the IP address of the TFTP and the path location of the new software image file is properly configured (Please see section 17 & 18), the user can choose one of three options to boot the switch after the firmware has been upgraded.

- Net option:

  This option allows you to try out a new image before upgrading. It requires a TFTP filename and a server IP address to retrieve the specified image from the given IP address.

  The new image will not overwrite the one in non-volatile memory.

- Net & save option

  This option requires the same setup as the Net option, i.e. TFTP server and a new image. However, it copies the image to non-volatile memory directly and then the system boots from non-volatile memory

Warning: The previous image in non-volatile memory will be lost when the procedure completes.

- Last Saved option

  The system will boot from non-volatile memory. This option will automatically show up after the 'Net & save' option is selected and the unit is reset.

Syntax

FSM726(config)# system firmware boot [net-tftp | net-and-save | last saved]

Firmware TFTP-IP

The `Firmware TFTP-IP` command is used to specify the IP location of the TFTP server where the new software image is stored.

Syntax

FSM726(config)# System firmware tftp-ip <IP address>

Where

`<IP address>` = the IP address of the TFTP server where the new firmware image is stored.

Firmware TFTP-File

The `Firmware TFTP-File` command is used to specify the path and the filename of the new firmware image.

Syntax

FSM726(config)# System firmware tftp-file <path&filename>

Where

`<path&filename>` = the path and the filename of the new firmware image

RADIUS

For enhanced security, you can choose to have authentication done through the RADIUS server if one is present on your network.

- Authen-Mode

  The `authen-mode` command configures the method in which the user is authenticated.

Syntax

FSM726(config)# system radius authen-mode [local | local-then-remote | remote]

Where

`Local` = authentication is performed locally and not through an external RADIUS server

`Local-then-remote` = Authentication is performed locally first, then by an external RADIUS server

`Remote` = Authentication is performed by a remote server and not locally.

- Server-IP

  The `Server-IP` command is used to set the IP address of the RADIUS server

Syntax

FSM726(config)# system radius server-ip <IP-address>

Where

`<IP address>` = IP address of the RADIUS server

- Shared-Secret

  The `shared-secret` command lets you set the RADIUS shared secret

Syntax

FSM726(config)# system radius shared-secret <shared secret>

Where

`<shared secret>` = the RADIUS shared secret

Reset

Use the reset command to reboot the switch.

Syntax

FSM726(config)# system reset

Stat-Reset

Use the `Stat-Reset` command to reset all of the statistics counters in the switch.

Syntax

FSM726(config)# system stat-reset

VLAN

The `config VLAN` command is used to configure VLAN database parameters.

Syntax

```
FSM726(config)# VLAN ...
```

Appendix A
Virtual Local Area Network

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

<u>Easy to do network segmentation</u>
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.

<u>Easy to manage</u>
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.

<u>Increased performance</u>
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

VLAN Behavior in a 700 Series Managed Switch

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 that port's respective Port Configuration 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. Port VLAN membership settings are changed in the Primary VLAN page.

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 and VLAN will mean that packets leaving the switch from that port and VLAN will be Untagged. Inversely, a 'T' for a given port and VLAN will mean that packets leaving the switch from that port and VLAN will be tagged with the respective VLAN ID in which it participated in.

Two examples of for setting up VLANs will be given. Example 1 will step through a simple two-group VLAN setup. Example 2 will step through a more elaborate setup illustrating all possible scenarios for a comprehensive understanding of tagged VLANs.

Example 1

This example shows the basics of setting up a VLAN.

In the VLAN Administration page, add a new VLAN to the list, shown below as "First" with a VLAN ID value of 2.

In the VLAN Membership page, use the space bar to modify the matrix until the desired ports are all members of the selected VLAN as either tagged or untagged ports.

To allow untagged packets to participate in the ‘First’ VLAN, make sure to change the Port VLAN IDs for the relevant ports. Access the PVID Settings page then use the space bar to add an ‘X’ indicating which Port VLAN ID is assigned to which port.

Example 2

This example demonstrates several scenarios of VLAN use and how the switch will handle VLAN and non-VLAN traffic.

1. Setup the following VLANs:
2. Configure the VLAN membership. Each image below shows a different VLAN to be setup. Be sure to set all of them as follows.
3. Setup the Port VLAN IDs as follows.

   Note: Port 01 PVID is set to 2. This must be done in the port specific page since there is no VLAN with ID 2

   The specific ports above have the following Port VLAN ID settings (The Port VLAN ID settings for each port are configured in the VLAN Ports page):

Port 01: 2	Port 05: 5	Port 09: 10	Port 13: 10
Port 02: 1	Port 06: 1	Port 10: 10	Port 14: 15
Port 03: 1	Port 07: 1	Port 11: 10	Port 15: 1
Port 04: 1	Port 08: 1	Port 12: 10	Port 16: 1

The following scenarios will produce results as described below:

If an untagged packet enters Port 4, the switch will tag it with a VLAN tag value of 1. Since Port 4 does not have membership with VLAN ID 1 (default), the packet will be dropped.

If a tagged packet with a VLAN tag value 5 enters Port 4, the packet will have access to Ports 5 and 1. If the packet leaves Port 5 and/or 1, it will be stripped of its tag becoming an untagged packet as it leaves the switch.

If an untagged packet enters Port 1, the switch will tag it with a VLAN tag value of 2. It will then be dropped since Port 1 has no membership with VLAN ID 2.

If a tagged packet with a VLAN tag value 10 enters Port 9, it will have access to Ports: 1, 10, 11, and 12. If the packets leave Ports 1 or 10, they will be tagged with a VLAN ID value of 10. If the packet leaves Ports 11 or 12, it will leave as an untagged packet.

If a tagged packet with a VLAN tag value 1 enters Port 9, it will be dropped since Port 9 does not have membership with VLAN ID 1.

Appendix B
Cabling Guidelines

This appendix provides specifications for cables used with a NETGEAR 700 Series Switches.

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-B-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 B-1 illustrates straight-through twisted pair cable.

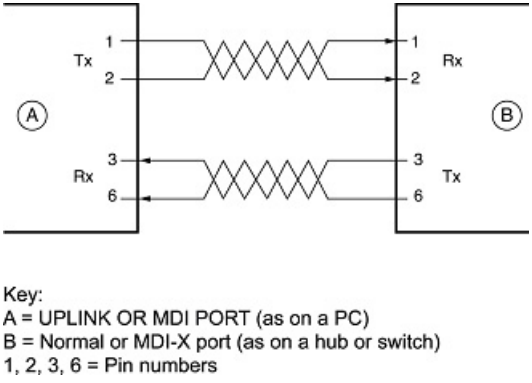


Figure B-1: Straight-Through Twisted-Pair Cable

Figure B-2 illustrates crossover twisted pair cable.

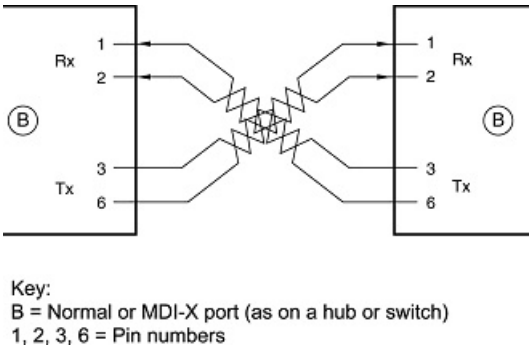


Figure B-2: Crossover Twisted-Pair Cable

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.

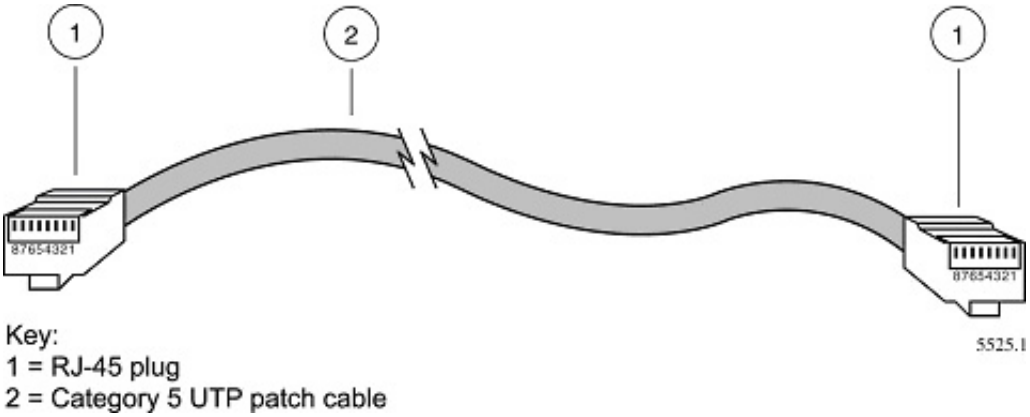


Figure B-3: Category 5 UTP Cable with Male RJ-45 Plug at Each End

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

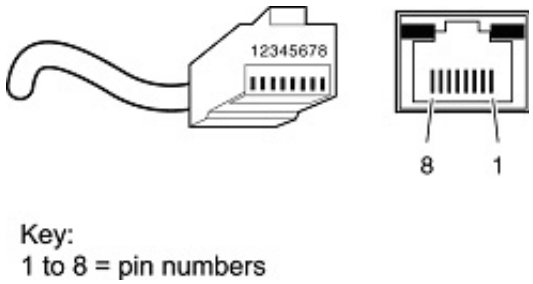


Figure B-4: RJ-45 Plug and RJ-45 Connector with Built-in LEDs

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

Table-B-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-B-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 C
802.1x Port-Based Authentication Overview

This appendix provides an overview of802.1x security and configuration.

Understanding 802.1x Port Based Network Access Control

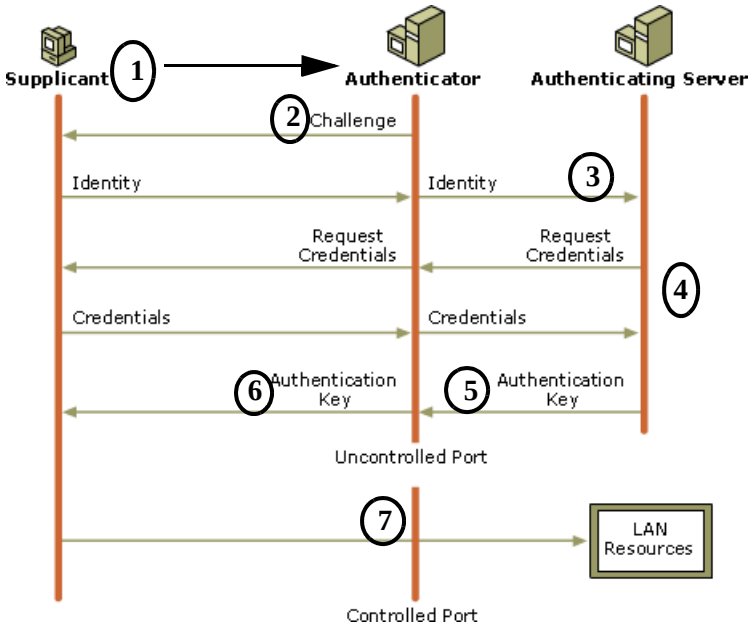
802.1x is well on its way to becoming an industry standard, and provides an effective wired and wireless LAN security solution. Windows XP implements 802.1x natively, and the 700 Series Switches supports 802.1x. The 802.11i committee is specifying the use of 802.1x to eventually become part of the 802.11 standard.

With 802.11 WEP, all wireless access points and client wireless adapters on a particular wireless LAN must use the same encryption key. Each sending station encrypts data with a WEP key before transmission, and the receiving station decrypts it using an identical key. This process reduces the risk of someone passively monitoring the transmission and gaining access to the data transmitted over the wireless connections.

However, a major problem with the 802.11 wireless standard is that the keys are cumbersome to change. If you don't update the WEP keys often, an unauthorized person with a sniffing tool can monitor your network for less than a day and decode the encrypted messages. In order to use different keys, you must manually configure each access point and wireless adapter with new keys.

Products based on the 802.11 standard alone offer system administrators no effective method to update the keys. This might not be too much of concern with a few users, but the job of renewing keys on larger networks can be a monumental task. As a result, companies either don't use WEP at all or maintain the same keys for weeks, months, and even years. Both cases significantly heighten the wireless LAN's vulnerability to eavesdroppers.

IEEE 802.1x offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.



1. The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client.
2. The access point replies with an EAP-request identity message.
3. The client sends an EAP-response packet containing the identity to the authentication server.
4. The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or other EAP authentication type.
5. The authentication server will either send an accept or reject message to the access point.
6. The access point sends an EAP-success packet (or reject packet) to the client.
7. If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic.

Initial 802.1x communications begin with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

The basic 802.1x protocol provides effective authentication and can offering dynamic key management using 802.1x as a delivery mechanism. If configured to implement dynamic key exchange, the 802.1x authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1x implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

It's important to note that 802.1x doesn't provide the actual authentication mechanisms. When using 802.1x, you need to choose an EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS), which defines how the authentication takes place.

The important part to know at this point is that the software supporting the specific EAP type resides on the authentication server and within the operating system or application software on the client devices. The 700 Series Switches acts as a “pass through” for 802.1x messages. As a result, you can update the EAP authentication type as newer types become available and your requirements for security change.

Glossary

Use the list below to find definitions for technical terms used in this manual.

10BASE-T
The IEEE specification for 10 Mbps Ethernet over Category 3, 4, or 5 twisted-pair cable.

100BASE-FX
The IEEE specification for 100 Mbps Fast Ethernet over fiber-optic cable.

100BASE-TX
The IEEE specification for 100 Mbps Fast Ethernet over Category 5 twisted-pair cable.

1000BASE-SX
The IEEE specification for 1000 Mbps Gigabit Ethernet over fiber-optic cable.

1000BASE-T
The IEEE specification for 1000 Mbps Gigabit Ethernet over Category 5 twisted-pair cable.

802.1x
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.
The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

ARP
Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address.
A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is

also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto-negotiation
A feature that allows twisted-pair ports to advertise their capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.

Auto Uplink
Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

Backbone
The part of a network used as a primary path for transporting traffic between network segments.

Bandwidth
The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

Baud
The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

Broadcast
A packet sent to all devices on a network.

Broadcast storm
Multiple simultaneous broadcasts that typically absorb all the available network bandwidth and can cause a network to fail. Broadcast storms can be due to faulty network devices or network loops.

CA
A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5
Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).
This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Capacity planning

Determining whether current solutions can satisfy future demands. Capacity planning includes evaluating potential workload and infrastructure changes.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic_commerce because they guarantee that the two parties exchanging information are really who they claim to be.

Class of Service

A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

Collision

A term used to describe two colliding packets in an Ethernet network. Collisions are a part of normal Ethernet operation, but a sudden prolonged increase in the number of collisions can indicate a problem with a device, particularly if it is not accompanied by a general increase in traffic.

DHCP

An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

DMZ

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you'll willing to risk open access.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.
Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name
A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL
Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Dynamic Host Configuration Protocol
DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

EAP
Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.
EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

Endstation
A computer, printer, or server that is connected to a network.

Ethernet
A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

Fast Ethernet
An Ethernet system that is designed to operate at 100 Mbps.

Fault isolation
A technique for identifying and alerting administrators about connections (such as those associated with switch ports) that are experiencing congestion or failure, or exceeding an administrator-defined threshold.

Forwarding
The process of sending a packet toward its destination using a networking device.

Filtering
The process of screening a packet for certain characteristics, such as source address, destination address, or protocol. Filtering is used to determine whether traffic is to be forwarded, and can also prevent unauthorized access to a network or network devices.

Flow control
A congestion- control mechanism. Congestion is caused by devices sending traffic to already overloaded port on a switch. Flow control prevents packet loss and temporarily inhibits devices from generating more traffic until the period of congestion ends.

Full-duplex
A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

Gigabit Ethernet
An Ethernet system that is designed to operate at 1000 Mbps (1 Gbps).

Half-duplex
A system that allows packets to transmitted and received, but not at the same time. Contrast with full-duplex.

IEEE
Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF
Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IGMP
Internet Group Management Protocol, the standard for IP multicasting in the Internet. IGMP is used to establish host memberships in multicast groups on a single network. (See IP multicast)

IP
Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).

Ranges of addresses are assigned by Internic, an organization formed for this purpose.

IP multicast
Sending data to distributed servers on a multicast backbone. For large amounts of data, IP Multicast is more efficient than normal Internet transmissions, because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

ISP
Internet service provider.

Internet Protocol
The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN
A communications network serving users within a limited area, such as one floor of a building.

Load balancing
The ability to distribute traffic across various ports of a device, such as a switch, to provide efficient, optimized traffic throughout the network.

local area network
LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

Loop
An event that occurs when two network devices are connected by more than one path, thereby causing packets to repeatedly cycle around the network and not reach their destination.

MAC
Media Access Control. A protocol specified by the IEEE for determining which devices have access to a network at any one time.

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps
Megabits per second.

MD5

MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.
When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See also Auto-negotiation.

Multicast

A single packet sent to a specific group of end stations on a network.

NAT

A technique by which several hosts share a single IP address for access to the Internet.

NetBIOS

Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.

netmask

Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation

A technique by which several hosts share a single IP address for access to the Internet.

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

Port monitoring
The ability to monitor the traffic passing through a port on a device to analyze network characteristics and perform troubleshooting.

Port speed
The speed that a port on a device uses to communicate with another device or the network.

Port trunking
The ability to combine multiple ports on a device to create a single, high-bandwidth connection.

Protocol
A set of rules for communication between devices on a network.

Quality of Service
A term to describe delay, throughput, bandwidth, and other factors that measure the service quality provided to a user.

RADIUS
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.
Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

RIP
A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

SNMP
Simple Network Management Protocol. An IETF standard protocol for managing devices on a TCP/IP network.

Segment
A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

Spanning Tree
A technique that detects loops in a network and logically blocks the redundant paths, ensuring that only one route exists between any two LANs.

Spanning Tree Protocol (STP)
A protocol that finds the most efficient path between segments of a multi-looped, bridged network. STP allows redundant switches and bridges to be used for network resilience, without the broadcast storms associated with looping. If a switch or bridge falls, a new path to a redundant switch or bridge is opened.

Subnet Mask
Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

Switch
A device that interconnects several LANs to form a single logical LAN that comprises of several LAN segments. Switches are similar to bridges, in that they connect LANs of a different type; however they connect more LANs than a bridge and are generally more sophisticated.

TFTP
Trivial File Transfer Protocol. Allow you to transfer files (such as software upgrades) from a remote device using the local management capabilities of the switch.

TLS
Short for Transport Layer Security, TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.
The TLS protocol is made up of two layers. The TLS Record Protocol ensures that a connection is private by using symmetric data encryption and ensures that the connection is reliable. The second TLS layer is the TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before data is transmitted or received. Based on Netscape's SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

Telnet
A TCP/IP application protocol that provides a virtual terminal service, allowing a user to log into another computer system and access a device as if the user were connected directly to the device.

Traffic prioritization
Giving time-critical data traffic a higher quality of service over other, non-critical data traffic.

UTP
Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

Unicast
A packet sent to a single end station on a network.

VLAN
Virtual LAN. A logical association that allows users to communicate as if they were physically connected to a single LAN, independent of the actual physical configuration of the network.

WAN

A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

wide area network

WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.
If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Index

Numerics

802.1x Port-Based Authentication 3-16, 4-25

A

Address Aging 3-26
Admin field 3-9
Advanced Security 3-16, 4-20, 4-25
Advanced Tools 4-21
Advanced> Spanning Tree 4-35
Advanced Options 4-19
Advantages of VLANs A-1
Auto MDI/MDI-X D-2
Auto Uplink D-2

B

Bridge Priority 3-24
Broadcast Control 3-21, 4-21

C

Cat5 cable D-2
Class of Service 4-21
CLI Configure 5-13
CLI Configure Aging-Timer 5-21
CLI Configure Community 5-23
CLI Configure Contact 5-24
CLI Configure DiffServ 5-13
CLI Configure Disable 5-22
CLI Configure Exit 5-15
CLI Configure Forward Time 5-26
CLI Configure Hello Time 5-26
CLI Configure Host 5-25
CLI Configure Host Authorization 5-25
CLI Configure HPO 5-23
CLI Configure IGMP 5-23
CLI Configure Interface 5-15
CLI Configure Interface CoS (Class or Service) 5-16
CLI Configure Interface Description 5-16
CLI Configure Interface Duplex 5-16
CLI Configure Interface Help 5-17
CLI Configure Interface Mirror 5-17
CLI Configure Interface Negotiation 5-17
CLI Configure Interface No 5-18
CLI Configure Interface Shutdown 5-18
CLI Configure Interface Spanning Tree 5-19
CLI Configure Interface Speed 5-19
CLI Configure Interface Switchport 5-19
CLI Configure Interface Trunking 5-20
CLI Configure Interface Type 5-18
CLI Configure Location 5-24
CLI Configure mac-address-table 5-21
CLI Configure Max-Age 5-26
CLI Configure Multicast-Static 5-22
CLI Configure Multimedia 5-22
CLI Configure Name 5-24
CLI Configure No 5-23
CLI Configure Priority 5-27
CLI Configure SNMP Server 5-23
CLI Configure Spanning Tree 5-26
CLI Configure Static 5-21
CLI Configure System 5-27
CLI Configure System Config-TFTP 5-27
CLI Configure System config-tftp ip 5-27
CLI Configure System Config-tftp Path/File 5-28
CLI Configure System Firmware boot 5-31
CLI Configure System Firmware TFTP-File 5-32
CLI Configure System Firmware TFTP-IP 5-32
CLI Configure System Gateway 5-29
CLI Configure System IP 5-28
CLI Configure System IP-Filter 5-28
CLI Configure System IP-filter address 5-29
CLI Configure System IP-Mode 5-29
CLI Configure System Mask 5-29
CLI Configure System Password 5-31
CLI Configure System RADIUS 5-32
CLI Configure System Reset 5-33

CLI Configure System Restore 5-30
CLI Configure System Save 5-30
CLI Configure System Stat-Reset 5-34
CLI Configure System Username 5-31
CLI Configure System Web 5-30
CLI Configure Trap 5-25
CLI Exit 5-3
CLI Help 5-2
CLI Manual Syntax 5-1
CLI Ping 5-2
CLI Show 5-3
CLI Show DiffServ 5-4
CLI Show Interfaces 5-4
CLI Show IP 5-5
CLI Show MAC Aging Time 5-6
CLI Show MAC Multicast-Static 5-6
CLI Show MAC Static 5-6
CLI Show Mac-Address-Table 5-5
CLI Show Mirror 5-7
CLI Show Multimedia 5-7
CLI Show Running-Config 5-7
CLI Show SNMP 5-8
CLI Show Spanning-Tree Brief 5-9
CLI Show Spanning-Tree Interface 5-10
CLI Show System 5-10
CLI Show Trunking 5-11
CLI Show VLAN 5-11, 5-12, 5-34
CLI Show VLAN Brief 5-11
CLI Show VLAN COS-PVID 5-12
CMI 3-3
COM Port Selection 3-2
Command Menu Interface 3-3
Configuration Manager 4-30
console port 3-1
conventions
  typography 1-2
Cost 3-25, 4-37
crossover cable D-2

D

Device Reset 4-18
Differentiated Service 3-20
Differentiated Service Code Points 3-20
DiffServ 3-20
Direct Console Access 3-1
Disable Advanced Alerting 4-20, 4-22
Documentation updates 1-2
DSCP 3-20

E

Enable/Disable IGMP 3-27
Entering the CLI 5-1
Ethernet Oversize Packet Rate 4-6
Ethernet Oversize Packets 4-6
Ethernet Undersize Packet Rate 4-6
Ethernet Undersize Packets 4-6

F

Fastlink 3-25
Fastlink in STP mode 3-25, 4-37
Flow Control 3-10
Forward Delay 3-24, 4-36

G

GBIC 3-10, 4-15

H

Hello Time 3-24, 4-36
How to Use This Document 1-1
HyperTerminal 3-2

I

Inbound Discard Rate 4-5
Inbound Discards 4-6
Inbound Error Rate 4-5

Inbound Errors 4-6
Inbound Non-unicast Packet rate 4-5
Inbound Non-unicast Packets 4-6
Inbound Octet Rate 4-5
Inbound Octets 4-6
Inbound Unicast Packet Rate 4-5
Inbound Unicast Packets 4-6
IP Configuration 3-8, 4-13

L

Last Saved option 3-19, 4-29

M

MAC 4-21
MAC > Address Aging 4-38
MAC Address Manager 3-25
MAC Address Table 3-6
MAC> Address Aging 4-38
MAC> Static Addresses 4-38
Main Menu> System 3-5
Management Access 1-1
Max Age 3-24, 4-36
MDI/MDI-X D-2
MDI/MDI-X wiring D-7
Multimedia Support 3-27, 4-39
Multimedia Support> Static Multicast Groups 4-40
Multimedia Support>Enable/Disable IGMP 4-39

N

Net & save option 3-18, 4-29
Net option 3-18, 4-29
non-volatile memory 2-1
NVRAM 2-1, 4-17

O

Outbound Discard Rate 4-6
Outbound Discards 4-6
Outbound Error Rate 4-6
Outbound Errors 4-6
Outbound Non-unicast Packet Rate 4-6
Outbound Non-unicast Packets 4-6
Outbound Octet Rate 4-5
Outbound Octets 4-6
Outbound Unicast Packet Rate 4-5
Outbound Unicast Packets 4-6

P

Passwords 4-18
Port Configuration 3-9, 4-14
Port Mirroring 3-14, 4-20, 4-22
Port Priority 3-20
Port Selection 4-8
Port Settings 4-10
Port Trunking 3-15, 4-20
Port Trunking 4-23
Primary VLAN 4-33
Priority 3-25, 4-37
Product updates 1-2

R

RADIUS 4-20
Rate/Duplex field 3-9
Refresh Rate 4-8
Restore Factory Defaults 4-17
RS-232 serial port 2-1

S

Save Configuration 4-16
Security 3-12
Set-Up 3-7
Set-Up> GBIC 3-10
SNMP 1-3, 3-29, 4-40
SNMP> Community Table 4-41
SNMP> Host Table 3-30

SNMP> Host Table 4-41
SNMP> Trap Setting 4-42
SNMP> Trap Settings 3-30
Spanning Tree 3-23
Spanning Tree > Port Setting 4-36
Spanning Tree >Bridge Settings 4-35
Spanning Tree Protocol 4-21
Spanning Tree> Bridge Settings 3-23
State field 3-9
Static Addresses 3-26
Static Multicast Administration 3-27
Static Multicast Membership 3-28
Statistics 3-5, 4-8
Statistics Rest 3-6
STP 4-21
Support for Standard MIBs 3-29, 4-40
Switch Statistics 4-5
System Configuration 4-12
system tools 3-11

T

TIP 3-2
Tools Menu 4-16
Traffic Management 3-19, 4-21, 4-31
typographical conventions 1-2

V

Virtual Cable Tester 3-15, 4-20, 4-23
Virtual Terminal Protocols 1-3
VLAN 4-21, A-1
VLAN Port 4-34
VLAN Ports 3-22
VLANS 4-32

W

Web Based Management 4-2
Web site 1-2
Why the Document was Created 1-1

Z

ZTerm 3-2