8275 Model 416 High Performance Ethernet
Workgroup Switch

User's Guide

Release 1.2

GC30-4026-02

8275 Model 416 High Performance Ethernet
Workgroup Switch

User’s Guide

Release 1.2

GC30-4026-02

Note

Before using this information and the product it supports, be sure to read “Appendix A. Safety Information” on page 93 and “Appendix B. Notices” on page 103.

Third Edition (December 1999)

This edition applies to Release 1.2 of the IBM 8275 Model 416 High Performance Ethernet Workgroup Switch.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers’ comments appears at the back of this publication. If the form has been removed, address your comments to:

Department CGF
Design & Information Development
IBM Corporation
PO Box 12195
Research Triangle Park NC 27709
U.S.A.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

About this guide

This guide briefly describes the features and capabilities of the 8275 Model 416 High Performance Ethernet Workgroup Switch. However, its primary purpose is to describe how to use the capabilities offered by the switch to configure, obtain status information, and monitor performance of the switch in your network.

Who should use this guide

This guide is intended for the network administrator or person responsible for integrating, maintaining and monitoring the switch in your network. The person responsible for coordinating installation and service for the switch will also find this manual useful.

How this guide is organized

This guide contains the following chapters and appendixes:

- "Chapter 1. Introduction" on page 1 describes the functions and capabilities of the switch.
- "Chapter 2. Accessing the switch" on page 19 describes the various physical methods of accessing the switch.
- "Chapter 3. Configuring your switch" on page 25 describes initial configuration of IP information.
- "Chapter 4. Using the Terminal Interface" on page 31 describes the using functions of the terminal interface.
- "Chapter 6. Using the SNMP Interface" on page 85 contains information about using SNMP to manage the switch.
- "Chapter 5. Using the Web Interface" on page 81 introduces the Web interface.
- "Chapter 7. Troubleshooting and Obtaining Service" on page 89 gives suggestions for solving problems obtaining service.
- "Appendix A. Safety Information" on page 93 contains translated safety instructions to observe when performing troubleshooting procedures.
- "Appendix B. Notices" on page 103 lists important notices about the use of this product.
- "Appendix C. Cable Pinout Diagrams" on page 109 describes and illustrates pinout diagrams for Ethernet and null-modem cable connectors.
- "Appendix D. Interface Conventions for the Console" on page 113 describes the definitions and functions of special keys and commands that are used by the terminal interface.
- "Appendix E. Introduction to Virtual LANs (VLANs)" on page 117 briefly introduces concepts and terminology about virtual local area Networks (VLANs).

Accessing the softcopy library

Softcopy versions of 8275-416 product documentation are available from either the Documentation CD-ROM (shipped with the product) or the IBM Networking Products Web site. To access product documentation shipped on the CD-ROM, follow the instructions in the booklet that accompanies the CD-ROM. Visit the following Web site to access the 8275-416 documentation at:

```
http://www.ibm.com/networking/support/docs.nsf/8275docs?OpenView
```

Online support

To obtain support information, including technical tips, current product information, and code updates and fixes for the switch, visit the IBM Networking Tech Support page at:

`http://www.ibm.com/networking/support`

You may also subscribe to receive e-mail notifications about code updates, tips, and FAQs for your switch.

Obtaining service

If you need assistance in troubleshooting or you need service for your 8275-416, call IBM at:

- 1-800-772-2227 in the United States
- 1-800-426-7378 (1-800-IBM-SERV) in Canada.
- In other locations, contact your place of purchase.

Refer to your IBM Warranty for information concerning service for the product.

Summary of Changes

Changes in this revision are indicated with revision bars in the left margin and reflect:

- The addition of the 2-Port 1000BASE-SX Gigabit Feature Module
- The addition of these functions:
  - Trunking
  - Self-learning IP
  - Port-based and fast spanning tree
  - Enable/disable Web mode configuration from SNMP
  - Enable/disable broadcast storm suppression trap
- New terminal interface panels in Chapter 4 to reflect new function for Release 1.2.
- General editorial changes

Chapter 1. Introduction

This chapter briefly describes the functions, capabilities, and benefits of the 8275 Model 416 High Performance Ethernet Workgroup Switch. This information helps you to plan for and use the switch in your network.

Product overview

Fast Ethernet switching continues to evolve from high-end backbone applications to desktop-switching applications. The switch provides a low-cost and powerful Layer 2 switch solution. It is an attractive base switch offering with the following key functions:

- High-performance, Layer 2, managed switch
- 16 base ports (10/100BASE-TX), expandable from 18 to 32 ports, depending on the combination of the following optional feature modules:
  - 8-Port 10/100BASE-TX
  - 8-Port 100BASE-FX
  - 4-Port 100BASE-FX
  - 2-Port 1000BASE-SX
- Robust management support; VT100 terminal interface, Web interface, SNMP
- Backplane performance 10 gigabits per second Ethernet switching
- Desktop and segment switching infrastructure
- Affordable migration to higher-performance networks

As a network administrator, you have a choice of three easy-to-use management methods: VT100 terminal interface, Web-based, and Simple Network Management Protocol (SNMP). These management methods enable you to configure, manage, and control the switch locally or from anywhere on the network.

The Spanning Tree Protocol (STP) provides fault tolerance on the network.

Switch functions

This section describes the functional support included in the switch:

- Layer 2 switching
- Virtual local area networks (VLANs)
- Management and user interface
- Self-learning IP
- Link aggregation (trunking)
- Fast spanning tree mode
- Security
- Reliability and serviceability
- Performance
- Flow Control
- Year 2000 (Y2K) compliance

Layer 2 switching

The 8275-416 is a Layer 2 Ethernet switch in which frame forwarding is based on MAC addresses and VLAN membership. The switch supports the IEEE 802.1D (1998) and 802.1Q standards.

802.3x flow control

The switch supports 802.3x flow control, which, when enabled, allows the transmission of data frames to be inhibited for a specified period of time. The default for 802.3x flow control is *Disabled*. 802.3x flow control is valid only when the port is in full-duplex mode.

Broadcast storm recovery

The switch detects broadcast storms and automatically blocks broadcast traffic to minimize the impact of the broadcast storm on the rest of the network. You can enable or disable this function at a switch level. For all broadcast frames received by the switch, the broadcast storm recovery operation depends on port speed and is described as follows:

1. If the Broadcast Storm Recovery Mode is *Enable*, and if the broadcast traffic on a 10 Mbps Ethernet port exceeds 20% of the link speed, then the switch blocks the broadcast traffic on the port until the broadcast traffic is returned to 10% or below.
2. If the Broadcast Storm Recovery Mode is *Enable*, and if the broadcast traffic on a 100 Mbps Ethernet port exceeds 5% of the link speed, then the switch blocks the broadcast traffic on the port until the broadcast traffic is returned to 2.5% or below.
3. Broadcast Storm Recovery is not supported on 1000 Mbps Ethernet ports.
4. If Broadcast Storm Recovery Mode is *Disable*, the switch does not block the broadcast traffic on the Ethernet port.
5. The switch issues a trap message when traffic exceeds a port's broadcast threshold and when it returns to or below the port's recovery threshold.

Forwarding database

The switch port MAC addresses are stored in the forwarding database. An address learned by the switch is removed from the forwarding database after a period of time if no frames have been received from that address. The default value for the aging period is 300 seconds (5 minutes), but it can be configured by the user. The time values range from 10 seconds to 600 seconds.

The switch forwarding database stores 12 000 entries. When the database is full, no new entries are learned until an existing entry ages out. All frames with unknown destination addresses are multicast to all ports in the appropriate VLAN.

Virtual local area networks (VLANs)

The switch supports VLANs. "Appendix E. Introduction to Virtual LANs (VLANs)" on page 117 provides an introduction to VLANs. It describes concepts and terminology, as well as, the benefits of using VLANs. The switch is manageable only through the ports which are members of the Default VLAN (VLAN 1).

Figure 36 on page 54 and Figure 37 on page 55 show examples of the panels and descriptions of the parameters used to configure VLANs.

Self Learning IP

Self Learning IP is a configurable function of the switch that learns where IP addresses are in the network so that packets normally sent from one host to another through a router can bypass the router and be sent directly to the destination host address. Self Learning IP is most effective when the switch is used to "front" the router (the switch is positioned logically between the router and the networks to which it belongs). Because of this strategic vantage point in the network (Figure 1 on page 3), the switch has visibility to all packets flowing to and from the router, as well as between any two switch ports. The switch monitors the traffic to determine if a Layer 2 shortcut can be used instead of subjecting the packet to Layer 3 router processing which can be relatively lengthy.

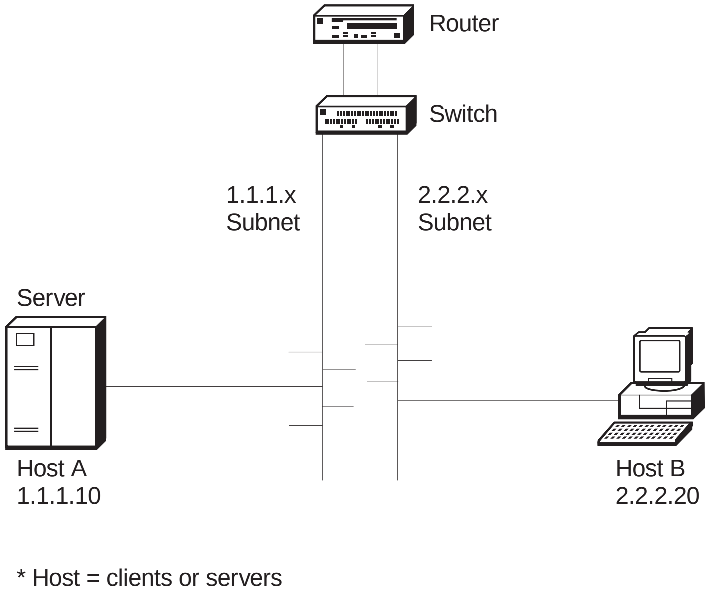


Figure 1. Self-Learning IP in the network

The Self Learning IP function essentially:

- Learns the network structure, classifying attached devices as routers or hosts.
- Maintains knowledge of network structure, aging out unused devices over time.
- Expedites packet flow through the network by circumventing the router whenever possible.

Device learning and classification is accomplished by watching ARP replies that flow naturally through the switch with the addition of active probing to determining whether a device is a router or a host. When an IP packet enters the switch, the Self Learning IP function compares the destination MAC address against the list of known routers, then checks if the destination IP address is a known host. If both tests pass, the packet is automatically re-addressed to the destination IP host device and is sent out the appropriate switch port.

A Router Table and Host Table are used to manage information learned about router and host devices, respectively. To keep this network information current, the Router Table entries are refreshed every 5 minutes while Host Table entries are checked every 3 minutes. Devices which are no longer active are dropped from their table; devices may be relearned at a later time as conditions change.

To use the Self Learning IP function, the switch must be configured with the following:

- IP information (see Network Connectivity Configuration Menu in Chapter 4).

  Note: For the Self Learning IP function to work, the IP information must include a default gateway for the network.

- Enable the Self Learning IP function (see the Switch Configuration Menu in Chapter 4).

Once Self Learning IP is enabled, the following information is available:

- Self Learning IP statistics for the switch (see Switch Detailed Statistics Menu in Chapter 4).
- IP and MAC addresses of routers learned (see Self Learning IP Router Table Menu in Chapter 4).
- Host IP statistics (see Self Learning IP Host Address Menu in Chapter 4).

Note that the Packets Switched count included in the Switch Detailed Statistics Menu may not reflect the absolute latest value. The information used for updating this count is obtained as individual Host Table entries are refreshed, so while this value can change over time, it does not necessarily update at the same frequency as other statistics on the menu.

While intended as an autonomous feature, Self Learning IP is affected by certain changes in switch configuration. If Self Learning IP is enabled and the switch IP address is reset, the Self Learning IP function is automatically disabled. The Self Learning IP Router and Host Tables are cleared whenever there is a link aggregation configuration change (see Link aggregation (trunking) in this chapter), forcing router and host devices to be relearned.

Link aggregation (trunking)

Link aggregation, also called *trunking* allows 802.3 MAC interfaces to be grouped together logically to appear as one super-link. The super-link or Link Aggregation Group (LAG) has access to the combined bandwidth of all links.

The Sun Trunking™ 1.0 specification is supported for the 10/100BASE-TX and 100BASE-FX ports. All members of the trunk must support Sun Trunking™ 1.0. For information about configuring trunks, see “Trunk management menu” on page 58. Up to 8 trunks can be configured.

Advantages of trunking are:

- Fault tolerance: Failure of one or more of the links in the LAG are handled gracefully. If a link of the LAG fails, the flows mapped to that link are dynamically reassigned to the remaining links of the LAG.
- Redundancy: Link aggregation also provides automatic, point-to-point redundancy between two devices (switch-to-switch).

Fast spanning tree mode

The IEEE 802.1D spanning tree protocol (STP) is designed to prevent loops in Ethernet networks. To achieve this objective the STP does not allow switches to forward data frames on a link immediately after the link is activated. The STP first listens for spanning tree BPDUs from other switches, then determines whether to put the link into forwarding state. When a default IEEE spanning tree timer value of 15 seconds is used for the forward delay timer, a link can start forwarding traffic 30 seconds after it becomes active on the network.

In networks with shared media hubs, there is a trend to attach network stations (or hosts) directly to multi-port bridges (otherwise known as switches). Unfortunately, the 802.1D spanning tree protocol has not been changed to accommodate this trend. So, when a network station is ready to send data, the switch does not allow the network station to communicate on the network until STP puts the port in forwarding state. The 30 second delay forces the network station users to wait longer before accessing the network. Even worse, some higher level protocols running on the network station may time out, generate error messages or not work at all.

The 802.1D standard specifies that when a link comes up on the network, the spanning tree state is set to “Listening”. After the forward delay timer expires, the spanning tree state is set to “Learning”, and after another forward delay timer interval the state is set to “Forwarding”. The forward delay timer is set for the entire network by the root bridge. The default value for this timer is 15 seconds.

With the Fast Spanning Tree function, the transition from “Listening” to “Learning” and the transition from “Learning” to “Forwarding” takes approximately 6 to 8 seconds. The forward delay timer behavior reverts to the 802.1D standard (15 seconds) after a port goes into forwarding state or blocking state.

Fast Spanning Tree mode is configurable by port. The default is the standard 802.1D protocol. When a port is configured in Fast Spanning Tree mode, it takes approximately 6 to 8 seconds before traffic can be forwarded on the link. Spanning tree can also be disabled on the port. For details about configuring ports for Fast Spanning Tree mode, see the Port Configuration Menu in Chapter 4.

Management and user interfaces

Note: The switch is manageable using the Ethernet network only through the ports which are members of the Default VLAN (VLAN 1).

You have a choice of these easy-to-use management methods:

- A VT100 terminal interface allows you to fully manage the switch using a standard terminal or terminal emulator connected over the network using Telnet or connected to the switch’s serial port (EIA 232).

  “Chapter 2. Accessing the switch” on page 19 describes how to access the switch using this interface and “Chapter 4. Using the Terminal Interface” on page 31 instructs you about using this interface.
- A Web-based interface enables you to manage the switch through standard Web browsers. There must be a physical path between the Web browser and the switch over the Ethernet network to use this method of connectivity.

  “Chapter 2. Accessing the switch” on page 19 describes how to access the switch using this interface and “Chapter 5. Using the Web Interface” on page 81 instructs you about using this interface.
- The switch has a Simple Network Management Protocol (SNMP) agent that the network administrator can access with a standard network manager. The following MIBs (Management Information Base) are supported:
  - MIB II (RFC 1213)
  - 8275-416 Enterprise MIB
  - RMON MIB (RFC 1757)
  - Bridge MIB (RFC 1493)
  - IEEE 802.3 Ethernet (RFC 1643)
- The switch interoperates with the following SNMP Managers:
  - Any standard MIB browser (SNMPv1)
  - IBM Nways® Manager for Windows NT® (V2.0 or later)
  - IBM Nways Manager for HP-UX (V2.0 or later)
  - IBM Nways Manager for AIX® (V2.0 or later)

Security

User access security can be implemented using the following functions of the 8275-416:

- User Accounts: The switch supports up to six accounts (one user with read/write status and five with read-only status) for terminal interface and Web access. Access to the switch configuration panels is password protected. Only one user name with read/write status is allowed to be configured, which prevents potential conflicts in configuration changes. The default Read/Write user name is: *admin*, and the default password consists of blanks (no password). If you lose the password, contact your IBM service representative.
- SNMP read/write protection based on community name.

Reliability and serviceability

The switch:

- Provides a comprehensive power-on self-test (POST) that ensures that all of its components are functioning correctly.
- Controls a seven-segment LED that allows you to follow the boot sequence.
- Allows you to download software upgrades using any of the management methods.
- Allows you to implement parallel paths for network traffic through the use of spanning tree protocol (STP), which provides a level of fault tolerance and ensures that:
  - Redundant paths are disabled when the main paths are operational
  - Redundant paths are enabled if the main paths fail
- Allows you to configure a port to “see” traffic going into and out of another port on the switch (port monitoring).
- Provides statistics for all ports.

Performance

High performance, Layer 2 switching for the switch consists of:

- Switching for up to 32 ports
- Supporting up to 12 000 end stations
- Processing 64-byte packets at the following rates:
  - 14 880 packets per second to 10-Mbps ports.
  - 148 800 packets per second to 100-Mbps ports
- Detecting broadcast storms and preventing them from impacting the network (Broadcast Storm Recovery).

Year 2000 (Y2K) Compliance

The 8275-416 is Y2K compliant.

When used in accordance with its associated documentation, it is capable of correctly processing and/or receiving date data within and between the 20th and 21st centuries providing all other products (for example, hardware, software, and firmware) used with the switch properly exchange accurate date data.

For additional information about Year 2000 related topics, visit:

`http://www.ibm.com/year2000`

Hardware

Cabling requirements

Ethernet cables are ***not*** provided and must be separately purchased. You can order them through your IBM representative.

Table 1 shows cable type and length requirements. Cable requirements depend on the speed of the network. Cables and connecting hardware must meet the standards specified in the ANSI/TIA/EIA 856-A or CSA T529 standards.

Table 1. Ethernet cable requirements

Ethernet Type	Cable Requirements	Max. Cable Length
10BASE-T	Category 3, 4 or 5 100-ohm STP/UTP cable	100 m (328 ft)
100BASE-TX	Category 5, 100-ohm STP or UTP cable and connecting hardware	100 m (328 ft)
100BASE-FX	62.5-micron multimode fiber (MMF) cabling	2 km (6561 ft) at full-duplex; 412 m (1352 ft) at half-duplex
1000BASE-SX	50/125-micron or 62.5-micron multimode fiber (MMF) cabling	550 m (1804 ft) at full-duplex.

10/100BASE-TX

10BASE-T connections are MDX ports and operate correctly with standard Category 3, 4, or 5 100-ohm UTP or STP cable and connecting hardware, as specified in the ANSI/TIA/EIA 856-A or CSA T529 standards when connected to MDI ports. When connecting to other MDX ports, such as ports of other 8275-416 switches, you must use crossover cables.

Do not use telephone extension cables in 10/100BASE-TX networks. The wire pairs in those cables are not twisted and the cables do not meet other requirements for use in a 10BASE-T network.

For connections to 10/100BASE-TX networks, you can use only Category 5 STP or UTP cables.

100BASE-FX

For connection to 100BASE-FX networks, you can use only 62.5/125 MMF cabling with MTRJ connectors.

1000BASE-SX

For connection to 1000BASE-SX networks, you can use 62.5/125 µm or 50/125 µm multi-mode fiber (MMF) cabling with SC fiber optic connectors.

Front panel

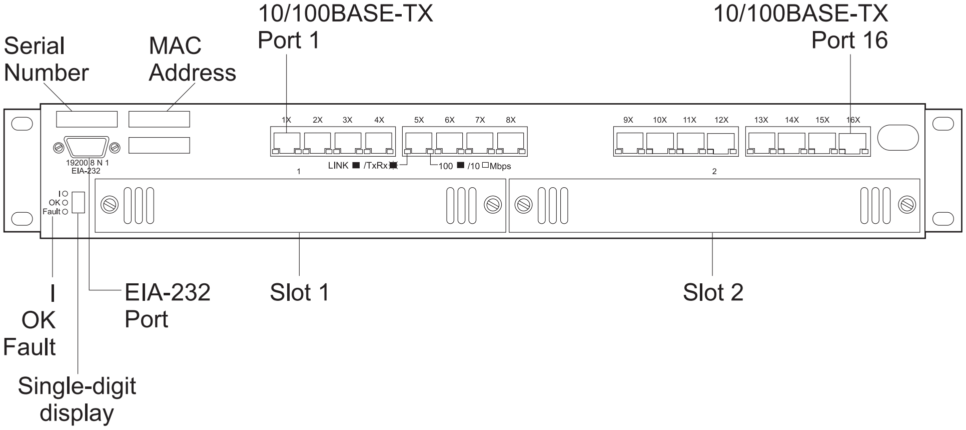


Figure 2. Front panel of the switch.

Switch LEDs

Switch LEDs are located at the lower left corner of the front panel (left of the single-digit display) and are identified with a vertical bar (I), OK, and Fault. The LED identified with the vertical bar and the OK LED are Green; the Fault LED is amber. The states of the LEDs are *on*, *off*, or *blinking*. They are explained later in this chapter.

Single-Digit Display

The single-digit display is located at the lower left corner of the front panel as shown in Figure 3 on page 10. During diagnostics, the character displayed indicates the diagnostic test being executed. Once the switch is operational, the character displayed is its unit ID (Table 3 on page 11).

Serial Port (EIA 232)

The serial port is a standard DB-9 male connector that provides an EIA 232 serial interface (sometimes referred to as the out-of-band management port). Use a null-modem serial cable when connecting to a workstation (“Appendix C. Cable Pinout Diagrams” on page 109). Use a VT100 terminal emulator program to configure your terminal’s attached COM port as follows:

- 19200 baud
- 8 data bits
- 1 stop bit
- No parity
- Hardware flow control OFF

See “Chapter 2. Accessing the switch” on page 19 for more information about connectivity.

Ethernet 10/100BASE-TX Ports

The switch has 16 Ethernet 10/100BASE-TX ports. Each port has two LEDs located at the lower right and left of the connector. Status indications of the Port LEDs are explained later in this chapter.

Feature Module Slots 1 and 2

These feature modules are available to expand port connections for your switch:

- 8-Port 10/100BASE-TX Ethernet Feature Module, P/N 30L6661
- 8-Port 100BASE-FX Ethernet Feature Module, P/N 30L6662

- 4-Port 100BASE-FX Ethernet Feature Module, P/N 31L4054
- 2-Port 1000BASE-SX Ethernet Feature Module, P/N 30L6663

Switch LED status

Switch LEDs are shown in Figure 3 and LED status is explained in the table that follows:

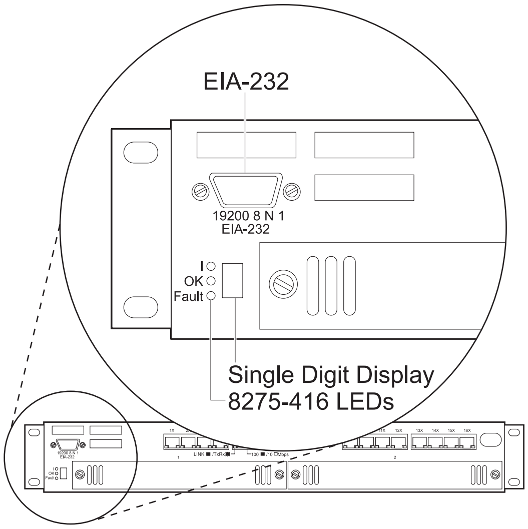


Figure 3. LEDs for the switch.

Table 2. LED status for the switch.

LEDs			Explanation
I (Green)	**OK (Green)**	**Fault (Yellow)**	
Off	Off	Off	No power is present, or there is a power supply failure. The switch is ***not*** operational.
On	On	Off	The switch is operational.
On	Blinking	Off	Configuration file or Operational Code file transfer is in process. ***Do not*** power-off or reset the switch.
On	Off	On	There is a hardware fault. The switch is ***not*** operational.
On	Off	Blinking	Diagnostics are in process. The switch is ***not*** yet operational.

Note: Any other state of the LEDs indicates an LED failure.

Single-digit display

The single-digit display (shown in Figure 3 on page 10) displays characters while diagnostics are running after power is applied to the switch. At the successful completion of diagnostics, the unit number appears in the display (for example, “1” indicates Unit Number 1). Table 3 gives the meaning of other digits that can be displayed and the corrective actions required.

Table 3. Problem indications on the single-digit display when the Fault LED is ON.

Character	Problem	Corrective Action
d	Board RAM problem	Replace the switch.
3	Detected an unsupported feature module.	Remove the feature module and update the operational code, or the feature module is not fully seated in its connector.
4	PIF fault on the feature module or base board.	If feature module Fault LED is On, remove the feature module. If no feature module Fault LED is On, replace the switch.
5 or 6	Non-volatile memory problem.	Replace the switch.
7	Switch memory problem.	Replace the switch.
8	Base board loopback problem.	Replace the switch.
9 or a	Feature module loopback problem.	• 9 = Feature module in Slot 1 has the fault; remove this feature module. • a = Feature module in Slot 2 has the fault; remove this feature module.

Base ports LEDs

The switch has 16 base 10/100BASE-TX ports. LED status for these 16 base ports are shown in Figure 4 and they are explained in Table 4.

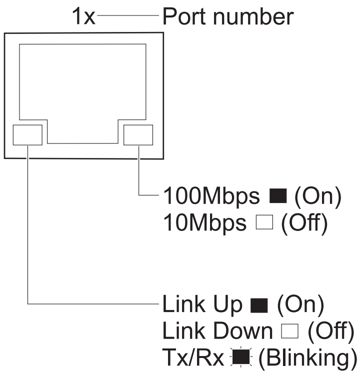


Figure 4. LEDs for the base 10/100BASE-TX ports on the switch

Table 4. Status of LEDs for 16 base 10/100BASE-TX ports

LED	Color	State	Explanation
Right Ethernet Port LED	Green	ON	Indicates a 100-Mbps port.
		OFF	Indicates a 10-Mbps port.
Left Ethernet Port LED	Green	ON	The link is up.
		OFF	The link is down.
		Blinking	Transmitting (Tx) and Receiving (Rx) traffic.

Feature module LEDs

Each feature module has an OK and a Fault LED located at the left side of the faceplate. The OK LED is green and the Fault LED is yellow. LED locations are shown in Figure 5, Figure 6 on page 14, Figure 7 on page 15, and Figure 8 on page 16; LED status of the feature modules are explained in Table 5, Table 6 on page 14, Table 7 on page 15, and Table 8 on page 16.

Status LEDs for the 8-port 10/100BASE-TX Ethernet feature module

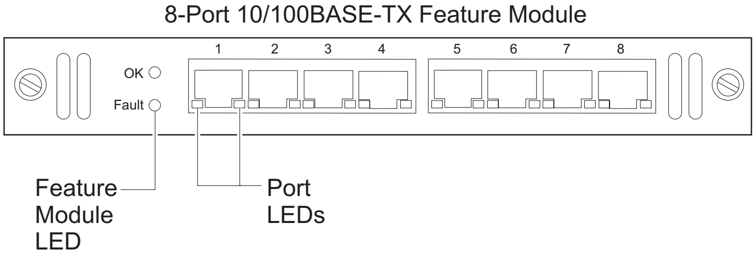


Figure 5. LEDs for the 8-port 10/100BASE-TX feature module.

Table 5. Status of LEDs for 8-port 10/100BASE-TX feature module

LED	Color	State	Explanation
OK	Green	ON	There is power to feature module.
		OFF	There is no power to feature module, no power to the switch, or the module has failed.
Fault	Yellow	ON	There is a module fault.
		OFF	There is no module fault.
Right Ethernet Port LED	Green	ON	Indicates a 100-Mbps port.
		OFF	Indicates a 10-Mbps port.
Left Ethernet Port LED	Green	ON	The link is up.
		OFF	The link is down.
		Blinking	Transmitting (Tx) and Receiving (Rx) traffic.

Status LEDs for the 8-port 100BASE-FX Ethernet feature module

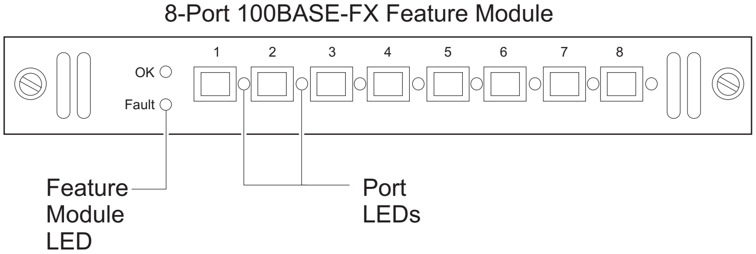


Figure 6. LEDs for the 8-port 100BASE-FX feature module.

Table 6. Status of LEDs for 8-port 100BASE-FX feature module

LED	Color	State	Explanation
OK	Green	ON	There is power to the feature module.
		OFF	There is no power to the feature module, no power to the switch, or the module has failed.
Fault	Yellow	ON	There is a module fault.
		OFF	There is no module fault.
Port LED	Green	ON	Link is up.
		OFF	Link is down.
		Blinking	Transmitting (Tx) and receiving (Rx) traffic.

Status LEDs for the 4-port 100BASE-FX Ethernet feature module

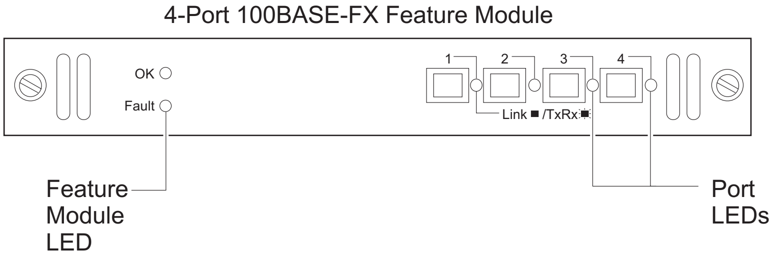


Figure 7. LEDs for the 4-port 100BASE-FX feature module.

Table 7. Status of LEDs for 4-port 100BASE-FX feature module

LED	**Color**	**State**	**Explanation**
OK	Green	ON	There is power to the feature module.
		OFF	There is no power to the feature module, no power to the switch,or the module has failed.
Fault	Yellow	ON	There is a module fault.
		OFF	There is no module fault.
Port LED	Green	ON	Link is up.
		OFF	Link is down.
		Blinking	Transmitting (Tx) and receiving (Rx) traffic.

Status LEDs for the 2-port 1000BASE-SX Ethernet feature module

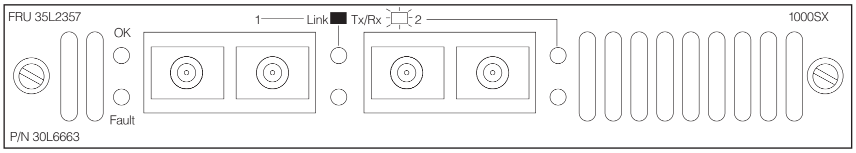


Figure 8. LEDs for the 2-port 1000BASE-SX feature module.

Table 8. Status of LEDs for 2-port 1000BASE-SX feature module

LED	Color	State	Explanation
OK	Green	ON	There is power to the feature module.
		OFF	There is no power to the feature module, no power to the switch,or the module has failed.
Fault	Yellow	ON	There is a module fault.
		OFF	There is no module fault.
Port LED	Green	ON	Link is up.
		OFF	Link is down.
		Blinking	Transmitting (Tx) and receiving (Rx) traffic.

Physical characteristics

Table 9 summarizes the physical characteristics for the switch:

Table 9. Summary of physical characteristics for the switch

Characteristic	Specification
Physical Dimensions	**Height** 63.0 mm (2.48 in.) 1.5 EIA rack units **Width** 440.0 mm (17.16 in.) **Depth** 355.6 mm (14 in.)
Weight (estimate)	6.0 kg (13 lb)
Minimum Service Clearance	**Front** 15.3 mm (6 in.) for cooling, cables, and to view LEDs **Sides** 50 mm (2 in.) for cooling **Rear** 15.3 mm (6 in.) for cooling and power cord
Environment	**Operating Temperature** 10° - 40° C (50° - 104° F) **Operating Humidity** 8% - 80% **Storage Temperature** 1° - 60° C (33.8° - 140° F) **Storage Humidity** 8% - 80% **Shipment Temperature** -40°C - 60°C (-40°F - 140°F) **Shipment Humidity** 5% - 100%

Chapter 2. Accessing the switch

This chapter explains the types of connections that you can use to physically access the switch. Once the connection is established, you will configure the IP information (either through the terminal interface or through DHCP or BootP), and then choose which user interface you want to use to manage it. Therefore, all interfaces support configuring the switch and obtaining information from it, thus providing greater flexibility in how you manage your switch.

Types of Connectivity

There are two connection methods used to physically access the switch:

- Out-of-band connectivity, which provides access to the switch through the EIA 232 port.
- In-band connectivity, which provides access to the switch from a remote station using the Ethernet network

Table 10 outlines the user interfaces that are available depending on your method of connection.

Table 10. Connection methods and available user interfaces

Type of Connection	Available User Interface
Out-of-band	Terminal interface via the EIA 232 port (terminal directly attached, or remotely attached to modem)
In-band	• Terminal interface via Telnet • SNMP-based management interface • Web-based management interface

Out-of-band connection

Out-of-band connection lets you access your switch through the serial EIA 232 port. It can be either through a locally attached PC running VT100 terminal emulation software, or through a remotely attached PC running VT100 terminal emulation software connected to a modem.

Locally attached terminal

To establish out-of-band connectivity using a locally attached terminal, make the physical connections and set up using the following procedure:

1. Attach one end of a null-modem cable to the EIA 232 port of the switch as shown in Figure 9 on page 20, and the other end to the COM port of your PC (see “Appendix C. Cable Pinout Diagrams” on page 109).

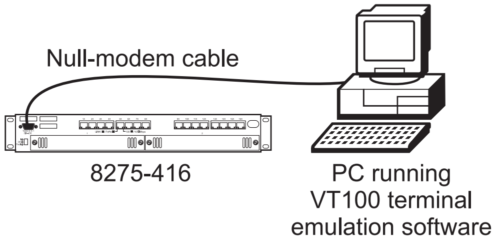


Figure 9. Out-of-band connectivity - locally attached terminal

2. Configure the VT100 terminal emulation application as follows:
   - Baud rate: 19200
   - Parity: None
   - Data bits: 8
   - Stop bits: 1
   - Flow control: None
3. Log in to the terminal interface. The terminal interface requires you to log in with a user name and password. The user name can have either Read/Write or Read Only status. The default Read/Write user name is *admin* and the password consists of blanks (no password). The default Read Only user name is *guest* and the password consists of blanks (no password).
4. See “Appendix D. Interface Conventions for the Console” on page 113 for a description of terminal interface key definitions. You may need to configure your terminal emulation application to enable the use of these keys.

Remotely attached terminal

To establish out-of-band connectivity using a remotely attached terminal, make the physical connections using the following procedure:

1. Unpack the modem and install it according to the manufacturer’s instructions.
2. Attach one end of the serial cable (not provided) to the EIA 232 port of the switch and the other end to your modem as shown in Figure 10.

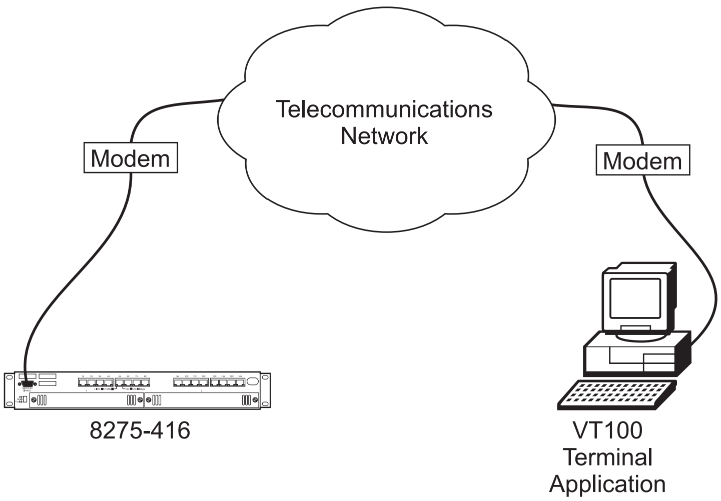


Figure 10. Out-of-band connectivity - remotely attached terminal

3. Set up the modem that is attached to the switch by following these steps:
   a. Configure the modem to use the same settings as those on your switch.
      - Baud rate: 19200

   - Parity: None
   - Data bits: 8
   - Stop bits: 1
   - Flow control: None

b. Configuration command syntax varies from modem to modem. Make sure that the modem has the following characteristics:
   - Asynchronous mode
   - Disable modem response
   - Disable flow control (for example, AT \Q)
   - Disable echo (for example, AT Q1)
   - Autoanswer mode on second ring (for example, AT SO=2)
   - Dumb mode - (No response in/out AT commands). This enables it to act as a “pass thru” device (setting the modem to dumb mode [])

c. Set up the remote modem and terminal.

d. After configuring the modem, save the configuration.

e. Establish a modem link as described in the modem user documentation.

f. Login to the terminal interface. The terminal interface requires you to login with a user name with read/write or read-only status and a password. The default read/write user name is *admin* and the password consists of blanks (no password). The default read-only user name is *guest* and the password consists of blanks (no password).

g. See “Appendix D. Interface Conventions for the Console” on page 113 for a description of terminal interface key definitions. You may need to configure your terminal emulation application to enable use of these keys.

4. To use in-band connectivity, you must configure the switch with IP information (IP address, subnet mask, and default gateway), and the port being used to access the switch must be on the Default VLAN (VLAN 1). You can configure IP information initially by using either of these methods:
   - DHCP or BootP
   - Terminal interface via the EIA 232 port.

   To configure the IP information, see “Chapter 3. Configuring your switch” on page 25 for details.

In-band connection – Telnet, Web, SNMP

Note: To use in-band connectivity, you must configure the switch with its IP information (IP address, subnet mask, and default gateway), and have a path available through the Default VLAN (VLAN 1). See “Chapter 3. Configuring your switch” on page 25 for configuring BootP or DHCP and IP information for your switch.

In-band connectivity allows access to the switch using the data network (as shown in Figure 11 on page 22).

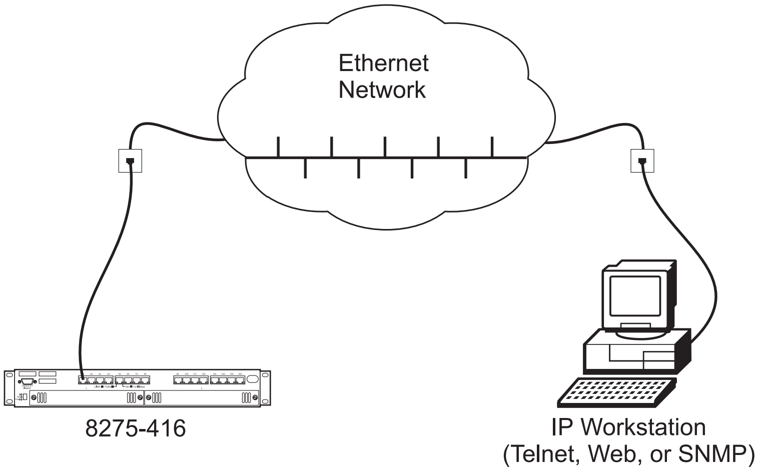


Figure 11. In-band connection

Terminal Interface – Telnet

Telnet console management can be performed through an Ethernet port (in-band connection). You must configure an IP address before using Telnet console management (Refer to “Chapter 3. Configuring your switch” on page 25 for initially configuring IP information for your switch.

You can use any Telnet application that emulates a VT100 terminal to establish a Telnet console management session. Up to five concurrent Telnet sessions are supported. For security, the Telnet session can be automatically logged off after a certain time of inactivity. You can configure the time of inactivity from 0 to 160 minutes; the default is 5 minutes.

The terminal interface is menu-driven and can be used to manage the switch through the EIA 232 port or a Telnet session. For security, a login user ID and password are required. Multiple user IDs and associated passwords can be created. Two levels of access privileges are supported: read/write and read only.

See “Appendix D. Interface Conventions for the Console” on page 113 for a description of the terminal keys. You may need to configure your terminal application to enable use of these keys.

See “Chapter 4. Using the Terminal Interface” on page 31 for a description of the terminal interface panels.

SNMP-Based Management Interface

The switch has an SNMP agent that supports SNMP Version 1 which allows it to be managed by any SNMP-based application (for example, Nways Campus Manager which supports the MIBs that the switch supports). See “Chapter 6. Using the SNMP Interface” on page 85 for details about the MIBs supported by the switch.

Web-Based Management Interface

The switch has a Web server that supports HTTP 1.1 or later, and HTML 4.0 or later. Your Web browser must support HTTP 1.1 or later, HTML 4.0 or later, and JavaScript© 1.2.

You can use the Web interface to access and change switch parameters. Menus similar to those available through the terminal interface are also displayed by the Web browser. To access the switch from a Web browser, you must have configured the IP information for the switch. You will need a valid login user ID and password. The accepted user IDs and passwords are the same as those configured for the terminal interface.

The is no specific logout command to end a Web session. The Web session will be automatically logged off after a period of inactivity. The inactivity timeout value that is configured for the Telnet session is used by the Web interface.

See “Chapter 5. Using the Web Interface” on page 81 for starting and using the Web interface.

Chapter 3. Configuring your switch

After hardware installation, you must configure the IP information for your switch in order to manage the switch using in-band connection.

First, you need to decide how you will access your switch. See “Chapter 2. Accessing the switch” on page 19 for details about in-band and out-of-band connection. It is assumed that when you come to this chapter you will already have established physical connectivity.

Configuring IP information

IP information can be initially assigned through either:

- DHCP or BootP (the default), or
- Terminal interface through the EIA 232 serial port

Remote configuration using DHCP or BootP

You can configure your switch from remote locations using DHCP (Dynamic Host Configuration Protocol) or BootP. BootP (documented in RFC 951 and RFC 1542) is a bootstrap protocol used by a diskless workstation to learn its IP address, the location of its boot file, and the boot server name. The switch supports “reserved” or static DHCP, documented in RFC 1541. The DHCP or BootP server must be available through the Default VLAN (VLAN 1).

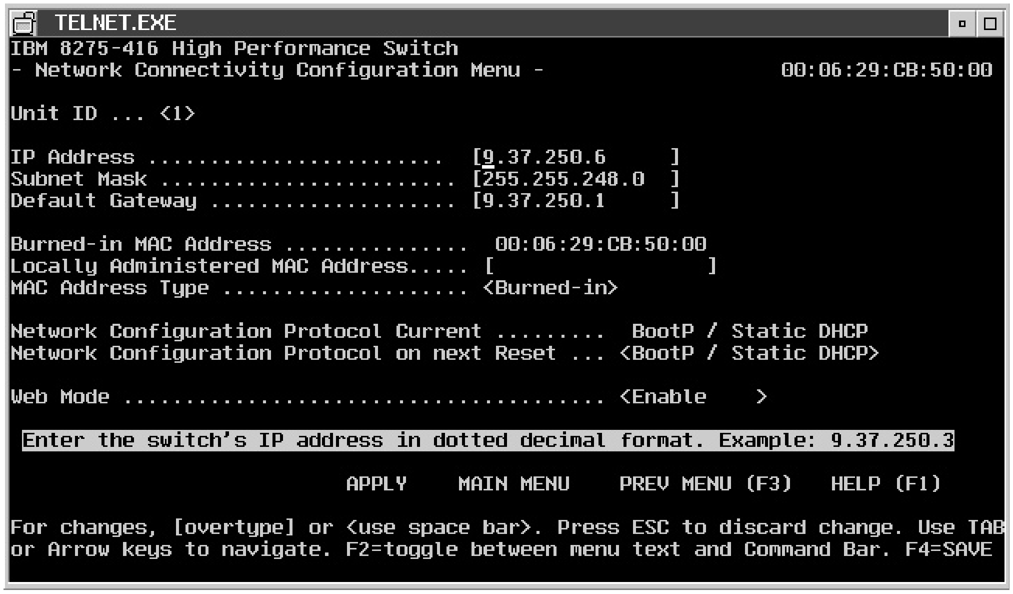
To configure the IP information remotely using DHCP or BootP:

1. Select **Management Menu** from the Main Menu on the terminal interface.
2. Select **Network Connectivity Configuration Menu** from the Management Menu, then specify *BootP / Static DHCP* for the Network Configuration Protocol Current parameter. If you are not using BootP or DHCP, set the *Network Configuration Protocol Current* parameter with a value of *None* to reduce network traffic. You must reset the switch to activate the change.

Manual configuration using the terminal interface

To manually configure the IP information:

1. Log onto the terminal interface using the read/write user ID and password.
2. Select the **Management Menu** from the Main Menu.
3. Select **Network Connectivity Configuration Menu** from the Management Menu, then specify IP address, Subnet Mask, and Default Gateway. Also, ensure that *None* is specified for Network Configuration Protocol Current.



```
IBM 8275-416 High Performance Switch
- Network Connectivity Configuration Menu -              00:06:29:CB:50:00

Unit ID ... <1>

IP Address ........................  [9.37.250.6      ]
Subnet Mask ....................... [255.255.248.0   ]
Default Gateway ................... [9.37.250.1      ]

Burned-in MAC Address ...............  00:06:29:CB:50:00
Locally Administered MAC Address..... [                 ]
MAC Address Type ................... <Burned-in>

Network Configuration Protocol Current .........  BootP / Static DHCP
Network Configuration Protocol on next Reset ... <BootP / Static DHCP>

Web Mode ..................................... <Enable    >

 Enter the switch's IP address in dotted decimal format. Example: 9.37.250.3

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 12. Configuring BootP/static DHCP and network connection (IP information).

IP Address
Unique IP address of your switch. Each IP parameter is made up of four decimal numbers. The numbers range from 0 to 255. The default for all IP parameters consists of “0”s (that is, 0.0.0.0).

Subnet Mask
The subnet mask for the LAN.

Default Gateway
Identifies the address of the default router if the switch is a node outside the IP range of the LAN.

Burned-in MAC Address
The default MAC address.

Locally Administered MAC Address
This is an additional parameter that you can configure. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (B‘0’) or locally administered (B‘1’).
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (B‘0’) or a group address (B‘1’).
- A locally administered address must have bit 6 On (B‘1’) and bit 7 Off (B‘0’).

MAC Address Type
Specifies if the burned-in MAC address or the locally-administered MAC address should be used. The burned-in MAC address is the default MAC address type.

Network Configuration Protocol Current
Specifies the network configuration protocol currently being used. Possible values are:

- BootP / Static DHCP: the switch periodically sends requests to a BootP or DHCP server until a response is received.
- None: the switch will be manually configured with IP information as specified on the Network Connectivity Configuration Menu.

Network Configuration Protocol on Next Reset
When you select BootP/Static DHCP (the default), the switch periodically

sends requests to a BootP or DHCP server until a response is received. You must specify None, if you want to manually configure the switch with the appropriate IP information. When this value is modified, you need to issue a Save and then reset the switch in order for the new value to take effect.

Web mode

Used to enable or disable access to the switch through the Web interface. When enabled, you can login to the switch from the Web interface. When disable is selected, you cannot login to the switch's Web server. Specifying Disable provides for more secure access to the switch. The default is Enable.

Note: Disabling the Web interface will not disable Web sessions that are in progress; no new Web sessions will be started.

Configuration Changes

This section describes how to make configuration changes, apply them, and retain the changes across a power cycle of the switch. It also provides you with specific information about making configuration changes using the terminal interface, Web interface, and SNMP interface.

You make configuration changes by entering data for one or more items. Configuration changes made by one user are also seen by other users who request the same data. Be aware that information displayed may be old data if you do not request the latest information before making any changes.

After you have make a configuration change and it is accepted:

- Selecting APPLY causes the change on the current panel to be applied but **not** retained across a reset or power cycle.
- Selecting SAVE causes the change on the current panel to be applied and all applied changes are retained across a reset or power cycle.

Making configuration changes using the terminal interface

This section provides information about making configuration changes, applying the changes, and retaining the changes across a power cycle when using the terminal interface.

Applying the configuration changes

On the terminal interface menus, field entries that can modified are enclosed in either square brackets ([ ]) or angle brackets (< >).

Square brackets identify an item that you can change by typing in text. As soon as you begin typing, the current value of the field is erased and is replaced by the new text. You cannot perform insert or overwrite in the field. You can use the following special keys while you are editing text fields:

- **Arrow keys**: These are ignored when you are editing a text field. On a field where you have made no modifications, use arrow keys to move the cursor to the appropriate field indicated by the direction of the arrow key.
- **Backspace**: Removes a character in front of the cursor.
- **Delete**: Gives the same result as the Back Space.
- **Enter**: The text is accepted and the cursor moves to the next field. On a text field where you have made no modifications, Enter moves the cursor to the next field.
- **Esc**: Stops editing the field and restores the original data.

- **Space Bar**: Is an allowable key to enter text.
- **Tab**: Performs the same function as the Enter key.
- **F4**: Save. Causes the configuration data to be saved and also applied if not already done.

Angle brackets identify an item that can be changed by selecting the desired option. The following special keys are used while selecting a configuration option:

- **Arrow keys**: The text is accepted and the cursor moves to the appropriate field indicated by the direction of the arrow key pressed. On a field where you have made no modifications, arrow keys move the cursor to the appropriate field.
- **Enter**: The text is accepted and the cursor moves to the next field. On a field where you have made no modifications, Enter moves the cursor to the next field.
- **Esc**: Stops modifying the field and restores the original data.
- **Space Bar**: Displays the next possible value for this field. Use it to cycle through the available options to select the desired value.
- **Tab**: Performs the same function as the Enter key.
- **F4**: Save. Causes the configuration data to be saved and also applied if not already done.

When processing data entered in a text field, all leading and trailing white-space characters are ignored (such as, space, Tab, Esc).

Once a configuration change is made and is accepted (the cursor is no longer on the field that was modified), the change is not put into effect until you select APPLY.

Saving the configuration changes

Note: To help remind you that a configuration change needs to be applied, APPLY always appears on the Command Bar.

When you select APPLY, the following actions occur:

1. All configuration changes that you made are checked for correct syntax.
2. If you entered invalid configuration data (for example, data value that is out of the supported range), an error message is displayed identifying the field that contained the error. Errors are reported one field at a time. All data must be valid before it can be applied.
3. When the data has been checked and you have corrected any errors, UNSAVED DATA is displayed in the upper right corner of the panel.

If you make configuration changes and then exit a panel without applying the changes, your changes may be lost. For example, the following results in losing any changes made on the panel:

- You make configuration changes on the current panel and you select any of the following commands:
  - MAIN MENU
  - PREV MENU

Note: Configuration changes are not automatically retained across a reset or a power cycle. To retain changes, you must select the Save command as described in the following section.

Saving the configuration changes across a reset or power cycle

To save configuration changes across a reset or power cycle, perform one of the following actions:

- Select **F4** (Save).
- Select **Save Applied Changes** on the System Utilities Menu.

If you select SAVE without previously having selected APPLY for recently made configuration changes, the changes are automatically applied.

If you request a switch reset without saving your configuration changes, you are prompted to save them. Reply **yes** to save the changes or **no** if you do not want to save them.

You are next prompted if you want to reset the switch. If you reply **yes**, the switch is reset regardless of whether you saved the changes or not.

Making configuration changes using the Web interface

This section provides information on making configuration changes, getting the changes put into effect, and retaining the changes across a power cycle when using the Web Interface.

On the Web pages, field entries that can be modified are displayed in a box with a white background. Depending on the field being modified, you can modify the text by either:

- Typing in the appropriate text over existing text (overwriting). If the data typed in is incorrect, the data entered is rejected and the original data is displayed.
- Selecting an option from one of the items displayed when the pull-down menu is selected. All items in a pull-down menu are correct.

Until you select **APPLY** or **SAVE**, you can restore any modified values to their original values by selecting the **Undo**.

Applying Configuration Changes

After you have modified the fields, select the **APPLY** or **SAVE** to process the changes. Selecting **APPLY** makes the changes take effect but the changes are not automatically retained across a reset or power cycle. Selecting **SAVE** makes the changes take effect and also results in the changes being retained across a reset or power cycle.

Before the Web Browser sends the request to the switch, the data for the fields changed are verified. If any field is invalid, an error message is displayed identifying the field that contains the error. Invalid data errors are reported one field at a time. All configuration changes must be valid before any of the changes are sent.

If you make configuration changes and then change the page without applying or saving the changes, the changes are not processed.

Saving configuration changes across a reset or power cycle

To save configuration changes to be retained across a reset or power cycle, select **SAVE**. Configuration changes can be permanently saved by either of these actions:

- Selecting **SAVE**.
- Going to the System Utilities Menu and selecting **Save All Applied Changes.**

Making configuration changes using SNMP

This section provides information on making configuration changes, getting the changes put into effect, and retaining the changes across a power cycle when using the SNMP interface.

You make configuration changes using SNMP by issuing SNMP Set commands to MIB objects that the switch supports as read/write.

Applying configuration changes

When the SNMP Set is received, the switch checks the data to ensure that it is valid. If it is invalid, the SNMP error code BADVALUE is returned in the SNMP Set Response. Otherwise, the configuration change is applied.

Saving configuration changes across a reset or power cycle

Configuration changes made using SNMP Set commands are not automatically retained across a reset or power cycle. To get these changes retained across a reset or power cycle, issue an SNMP Set to the **swDevCtrlSaveConfiguration** object supported by the switch private MIB.

Managing the configuration file

Your switch's configuration is written to a configuration file. Having this file available at a remote location would allow you to restore a corrupted switch configuration. System utilities allow you to upload files from the switch and download files to the switch.

From the System Utilities panel, you can select to **Upload File From Switch** or **Download File to Switch** to process a configuration file; just specify *Config File* as the file type on either panel. The switch must have a path available through Default VLAN (VLAN 1).

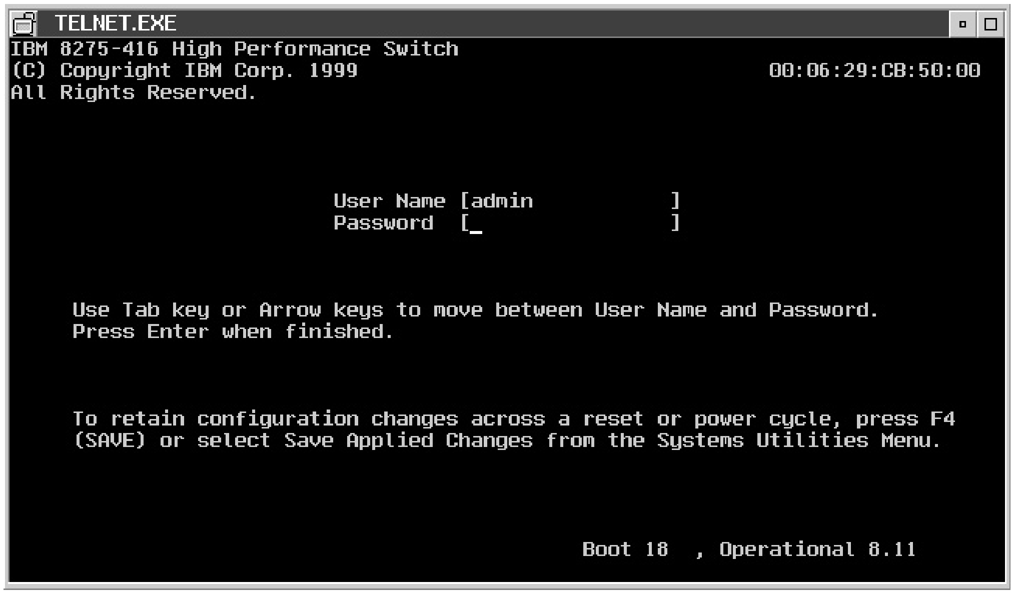
Chapter 4. Using the Terminal Interface

This chapter describes the switch terminal interface. The terminal interface panels are automatically refreshed every few seconds to provide you with current information.

Note: The panels shown in this chapter are intended to be representative and should not be assumed to be entirely accurate because they are subject to change before final shipment of the product.

Login panel

The Login panel is the first panel displayed when initializing the terminal interface. Figure 13 shows the Login panel; you need an approved user name and password to login.



```
IBM 8275-416 High Performance Switch
(C) Copyright IBM Corp. 1999                                 00:06:29:CB:50:00
All Rights Reserved.



                          User Name [admin           ]
                          Password  [_               ]



     Use Tab key or Arrow keys to move between User Name and Password.
     Press Enter when finished.



     To retain configuration changes across a reset or power cycle, press F4
     (SAVE) or select Save Applied Changes from the Systems Utilities Menu.



                                              Boot 18  , Operational 8.11
```

Figure 13. Login panel for terminal interface

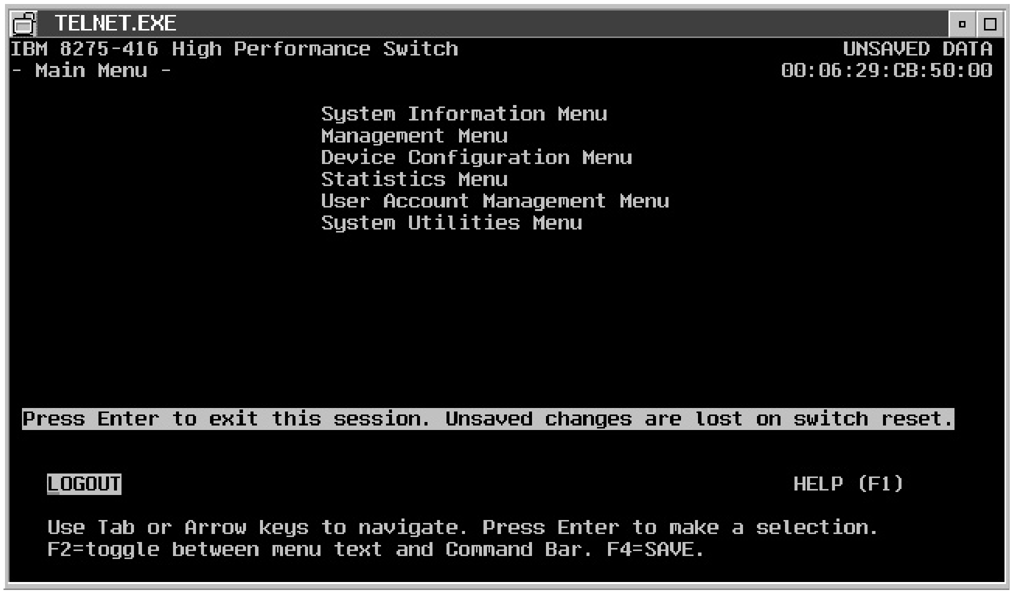
User Name
Can be up to 8 alphanumeric characters in length. The value is not case sensitive. The default is **admin** for a read/write user, and **guest** is the default for a read only user.

Password
Can be up to 8 alphanumeric characters in length. The value is not case sensitive. The default is no password.

The terminal interface provides a way to log out. From the Main Menu, select **LOGOUT** or select **System Utilities Menu**, then select **Logout**. When you have finished using the terminal interface, ensure you have saved all configuration changes before logging out.

The Main Menu

Following a successful login, the Main Menu appears (Figure 14). Information following in this section is arranged in the order of topics on the Main Menu.



```
IBM 8275-416 High Performance Switch                              UNSAVED DATA
- Main Menu -                                                00:06:29:CB:50:00

                         System Information Menu
                         Management Menu
                         Device Configuration Menu
                         Statistics Menu
                         User Account Management Menu
                         System Utilities Menu








 Press Enter to exit this session. Unsaved changes are lost on switch reset.


   LOGOUT                                                      HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 14. Main menu for terminal interface

System Information Menu
Allows access to information that is maintained about the switch.

Management Menu
Contains selections associated with managing the switch.

Device Configuration
Contains selections associated with configuring the switch.

Statistics Menu
Contains selections for access to statistical data that is gathered for the switch.

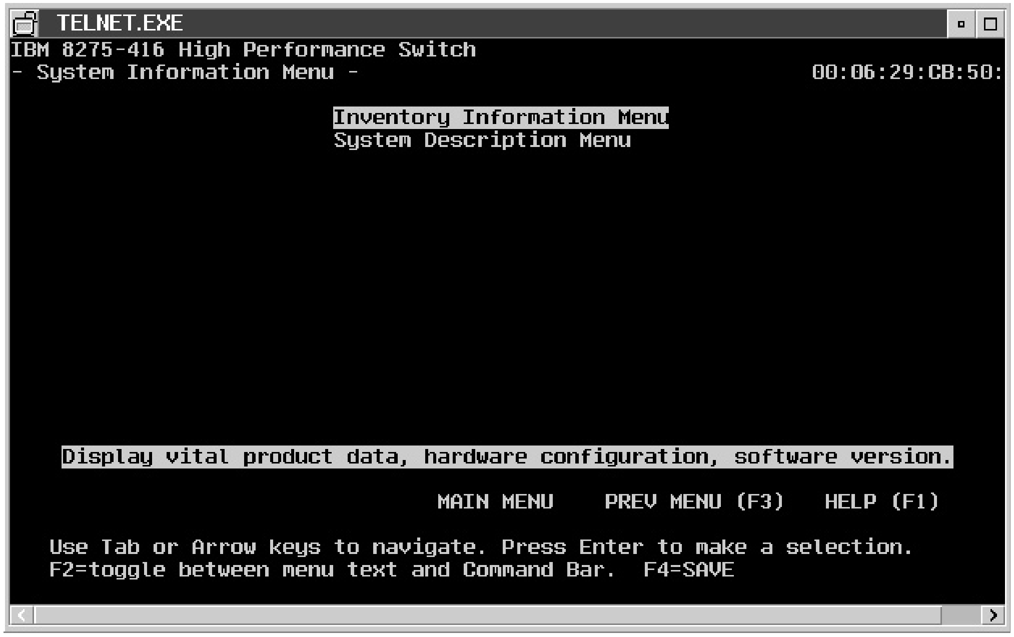
User Account Management
Allows you to define users and passwords and their level of access.

System Utilities
Allows selection of the utilities available with the switch.

System information

The switch manages information about its installed hardware and software. System information contains read-only and read/write fields. The read-only fields are written when the switch is manufactured. Through configuration you can change only the read/write fields: *System Name*, *System Location* and *System Contact*. Changes to these fields must be saved to be effective. A reset is not necessary for the changes to be effective.

To access system information, select **System Information Menu** on the Main Menu. By selecting **Inventory Information Menu** and **System Description Menu**, you can view information about your switch. Figure 15 on page 33 shows your system information options.

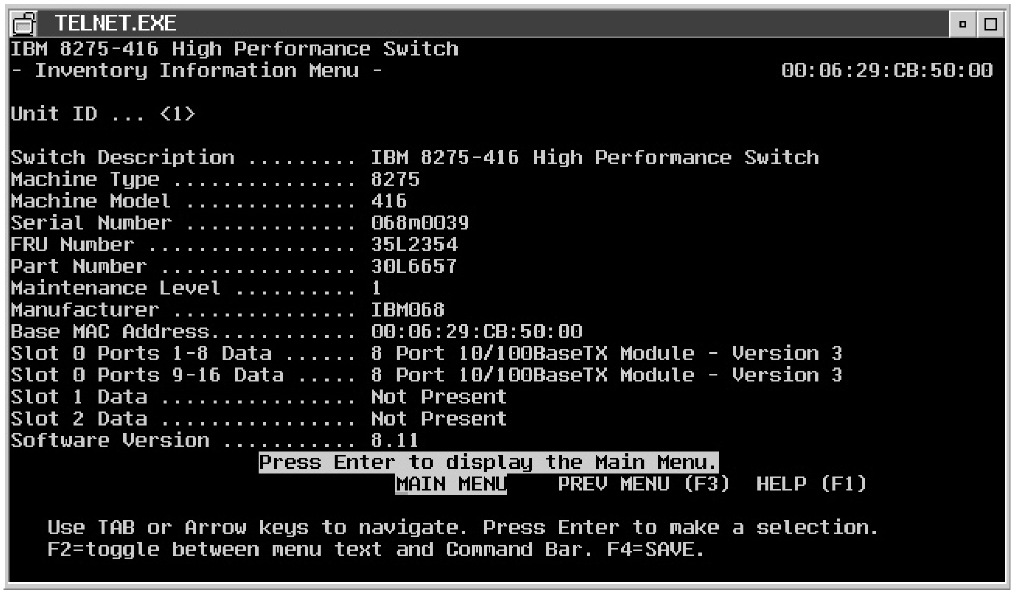


```
IBM 8275-416 High Performance Switch
- System Information Menu -                                00:06:29:CB:50:

                         Inventory Information Menu
                         System Description Menu




    Display vital product data, hardware configuration, software version.

                                 MAIN MENU    PREV MENU (F3)   HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 15. System information menu

Inventory information

Figure 16 shows the Read-Only inventory information available for your switch.

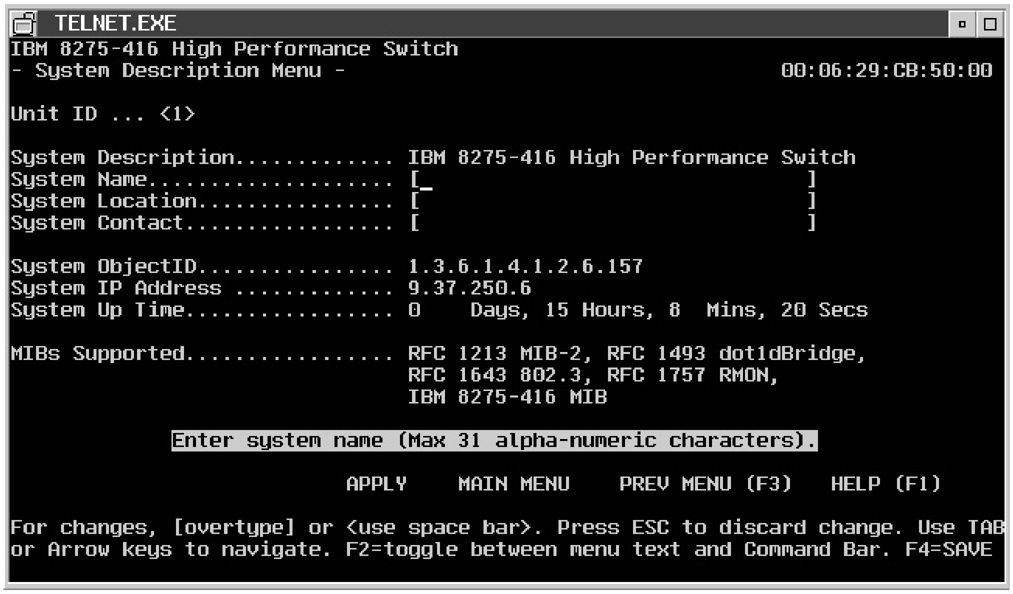


```
IBM 8275-416 High Performance Switch
- Inventory Information Menu -                           00:06:29:CB:50:00

Unit ID ... <1>

Switch Description ......... IBM 8275-416 High Performance Switch
Machine Type ............... 8275
Machine Model .............. 416
Serial Number .............. 068m0039
FRU Number ................. 35L2354
Part Number ................ 30L6657
Maintenance Level .......... 1
Manufacturer ............... IBM068
Base MAC Address............ 00:06:29:CB:50:00
Slot 0 Ports 1-8 Data ...... 8 Port 10/100BaseTX Module - Version 3
Slot 0 Ports 9-16 Data ..... 8 Port 10/100BaseTX Module - Version 3
Slot 1 Data ................ Not Present
Slot 2 Data ................ Not Present
Software Version ........... 8.11
                    Press Enter to display the Main Menu.
                               MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use TAB or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 16. Inventory information menu

System description

Figure 17 on page 34 shows the system information for your switch.



```
IBM 8275-416 High Performance Switch
- System Description Menu -                                 00:06:29:CB:50:00

Unit ID ... <1>

System Description............ IBM 8275-416 High Performance Switch
System Name................... [_                               ]
System Location............... [                                ]
System Contact................ [                                ]

System ObjectID............... 1.3.6.1.4.1.2.6.157
System IP Address ............ 9.37.250.6
System Up Time................ 0    Days, 15 Hours, 8  Mins, 20 Secs

MIBs Supported................ RFC 1213 MIB-2, RFC 1493 dot1dBridge,
                               RFC 1643 802.3, RFC 1757 RMON,
                               IBM 8275-416 MIB

             Enter system name (Max 31 alpha-numeric characters).

                          APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 17. System description menu

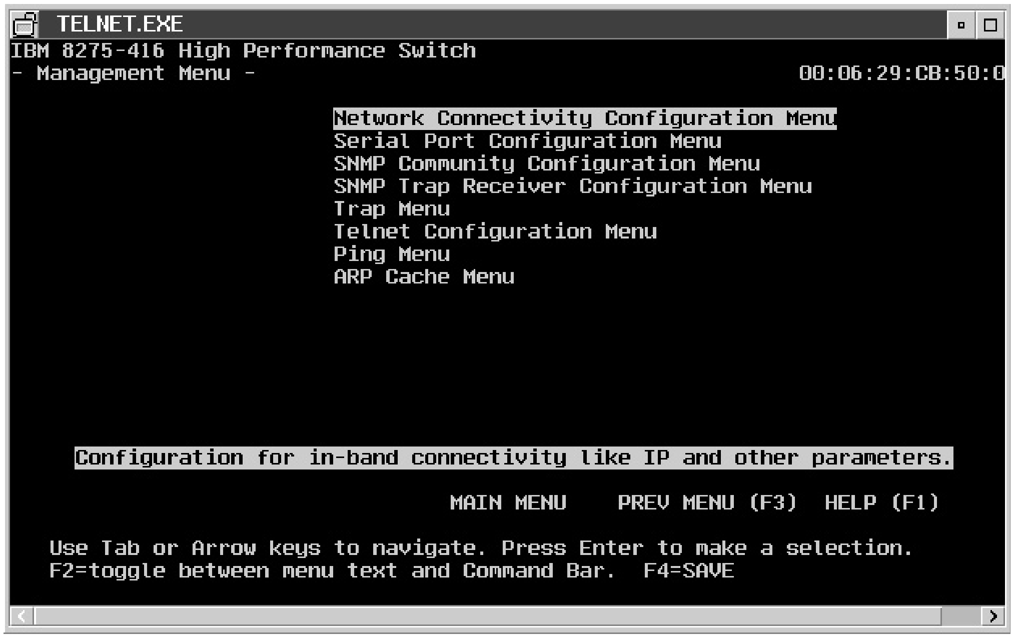
System Name
The name assigned to the switch. Specify up to 31 alphanumeric characters. The default is blank.

System Location
Indicates the physical location of the switch. Specify up to 31 alphanumeric characters. The default is blank.

System Contact
Identifies the person responsible for your network (for example, you network administrator) Specify up to 31 alphanumeric characters. The default is blank.

Management

Select **Management Menu** on the Main Menu (Figure 18) to use the management functions of the switch.

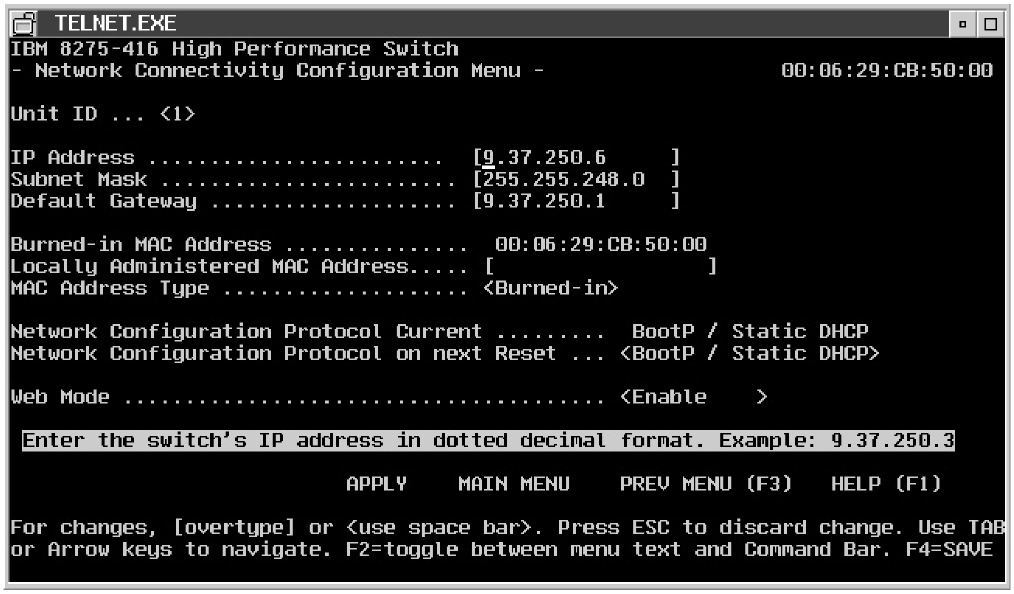


```
IBM 8275-416 High Performance Switch
- Management Menu -                                         00:06:29:CB:50:0

                         Network Connectivity Configuration Menu
                         Serial Port Configuration Menu
                         SNMP Community Configuration Menu
                         SNMP Trap Receiver Configuration Menu
                         Trap Menu
                         Telnet Configuration Menu
                         Ping Menu
                         ARP Cache Menu



     Configuration for in-band connectivity like IP and other parameters.

                                  MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 18. Management menu

Configuring network connection for the switch

To configure the IP information, select **Management Menu** from the Main Menu, then select **Network Connectivity Configuration Menu** from the Management Menu. The Network Connectivity Configuration Menu appears as shown in Figure 19.



```
IBM 8275-416 High Performance Switch
- Network Connectivity Configuration Menu -                 00:06:29:CB:50:00

Unit ID ... <1>

IP Address .......................  [9.37.250.6     ]
Subnet Mask ....................... [255.255.248.0  ]
Default Gateway ................... [9.37.250.1     ]

Burned-in MAC Address ...............  00:06:29:CB:50:00
Locally Administered MAC Address..... [                 ]
MAC Address Type ................... <Burned-in>

Network Configuration Protocol Current .........  BootP / Static DHCP
Network Configuration Protocol on next Reset ... <BootP / Static DHCP>

Web Mode ....................................... <Enable    >

 Enter the switch's IP address in dotted decimal format. Example: 9.37.250.3

                          APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 19. Network connection configuration

You must configure the following IP information to establish in-band connectivity to the switch:

IP Address
Unique IP address for your switch. Each IP parameter is made up of four decimal numbers. The numbers range from 0 to 255. The default for all IP parameters consists of zeros (that is, 0.0.0.0).

Subnet Mask
The subnet mask for the LAN.

Default Gateway
Identifies the address of the default router if the switch is a node outside the IP range of the LAN.

Burned-in MAC Address
The burned-in MAC address is the default MAC address used.

Locally Administered MAC Address
This is an additional parameter that you can configure. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (B‘0’) or locally administered (B‘1’).
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (B‘0’) or a group address (B‘1’).
- A locally administered address must have bit 6 On (B‘1’) and bit 7 Off (B‘0’).

MAC Address Type
Specifies if the burned-in MAC address or the locally-administered MAC address should be used. The burned-in MAC address is the default MAC address type.

Network Configuration Protocol Current
Specifies the network configuration protocol currently being used. Possible values are:

- BootP / Static DHCP: the switch periodically sends requests to a BootP or DHCP server until a response is received.
- None: the switch will be manually configured with IP information as specified on the Network Connectivity Configuration Menu.

Network Configuration Protocol on next Reset
When you select BootP/Static DHCP (the default), the switch periodically sends requests to a BootP or DHCP server until a response is received. You must specify None, if you want to manually configure the switch with the appropriate IP information. When this value is modified, you need to issue a Save and then reset the switch in order for the new value to take effect.

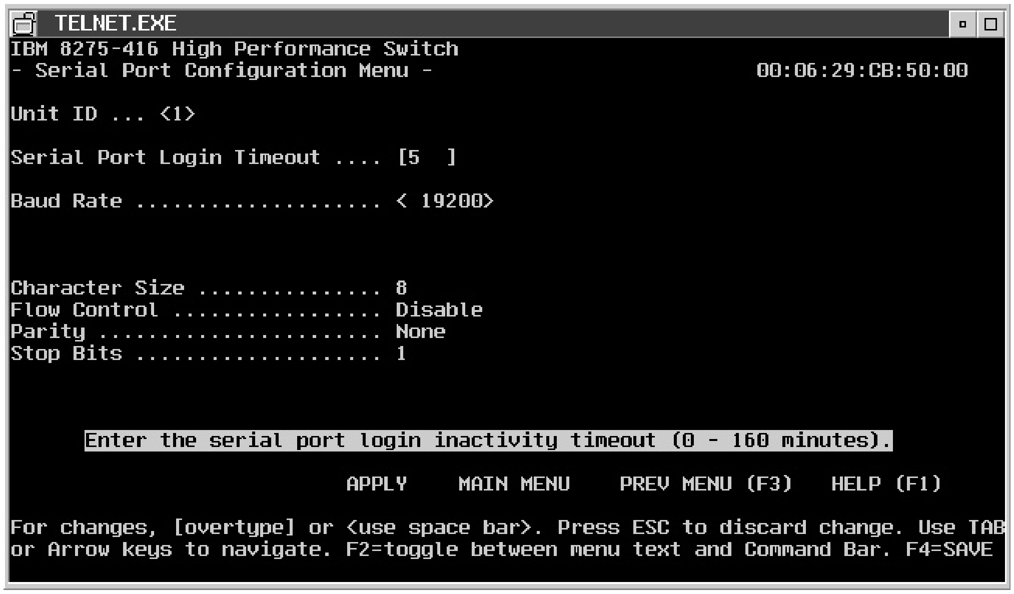
Web mode
Used to enable or disable access to the switch through the Web interface. When enabled, you can login to the switch from the Web interface. When disable is selected, you cannot login to the switch’s Web server. Specifying Disable provides for more secure access to the switch. The default is Enable.

Note: Disabling the Web interface will not disable Web sessions that are in progress; no new Web sessions will be started.

Configuring serial port

The switch allows you to access the switch through the serial EIA 232 port. This type of connectivity is called out-of-band connection. See “Chapter 2. Accessing the switch” on page 19 for descriptions of ways to access the switch.

On the Main Menu, select **Management Menu**. From the Management Menu, select **Serial Port Configuration Menu**. Figure 20 shows the parameters to configure the serial EIA 232 port.



```
IBM 8275-416 High Performance Switch
- Serial Port Configuration Menu -                          00:06:29:CB:50:00

Unit ID ... <1>

Serial Port Login Timeout .... [5  ]

Baud Rate ................... < 19200>



Character Size ............... 8
Flow Control ................. Disable
Parity ....................... None
Stop Bits .................... 1



      Enter the serial port login inactivity timeout (0 - 160 minutes).

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 20. Serial port configuration

You specify Login Timeout and Baud Rate:

Serial Port Login Timeout
Specifies the maximum connect time without console activity. The value is in a range from 0 to 160 minutes. A value of 0 indicates that a console can be connected indefinitely. The default value is 5 minutes.

Baud Rate
Specifies the communication rate of the terminal interface. Values can be 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200. The default value is 19200.

Configuring for DHCP or BootP

If you do not want to manually configure the switch with IP information, the switch can obtain the IP information from a BootP or DHCP server. The switch must be accessible through a port which is a member of the Default VLAN ID 1. When BootP or DHCP is enabled, the switch periodically sends out requests until a response is received from either a DHCP or BootP server. The IP information in the BootP or DHCP response overlays any existing IP information in switch. The new IP information is not retained across a reset until you select **Save**.

Note: If you configure a switch with an IP address, then DHCP frames will effectively be ignored (that is, the configured IP address will have priority over the address received via DHCP). However, BootP frames will have priority over a configured IP address. A difference between BootP and DHCP frames is that DHCP frames have 0xFFFFFFFFFFFF as the destination MAC address, while BootP frames have the switch’s individual MAC address as the destination address.

Configuring the DHCP

To configure the DHCP server for static DHCP, you must specify an IP address that will be assigned to the switch. This IP address is mapped to the switch’s MAC address. The static DHCP does not obtain an IP address from a pool of addresses on a DHCP server unless one is explicitly set up for a given MAC address. For example, In Windows NT®, you must set up a reservation for the switch's MAC address. Assign an IP address from the pool of current addresses. Configure the router, IP address, and subnet mask for the switch's MAC address. The switch supports no other DHCP options.

Configuring the BootP

For BootP, the BootP server must have the appropriate information configured for the switch. A newly installed switch broadcast a BootP request over IP when it is powered on or reset. The BootP server, using information from its BOOTPTAB file, provides the switch with configuration information.

The following is an example of a BOOTPTAB file entry containing configuration information for the switch:

```
8275_416_Switch_1:ht=ethernet:ha=0004ac6b0980:\
         ip=10.1.7.7:gw=10.1.1.1:\
         sm=255.255.255.0

8275_416_Switch_2:ht=ethernet:ha=0004ac6b09C0:\
         ip=10.1.7.8:gw=10.1.1.1:\
         sm=255.255.255.0
```

Where:

ht	hardware type
ha	host hardware address
ip	host IP address
gw	gateway address list
sm	subnet mask

Configuration information obtained from the BootP server is not saved unless you select **SAVE**. Next, configure the Network Configuration Protocol.

Configuring the switch for DHCP or BootP

If you are using DHCP or BootP, you must configure the appropriate information for the switch. To do so, configure the Network Configuration Protocol as follows:

1. On the Main Menu, select **Management Menu**.
2. On the Management Menu, select **Network Connectivity Configuration Menu**, then complete the network connection information shown in Figure 19 on page 35.

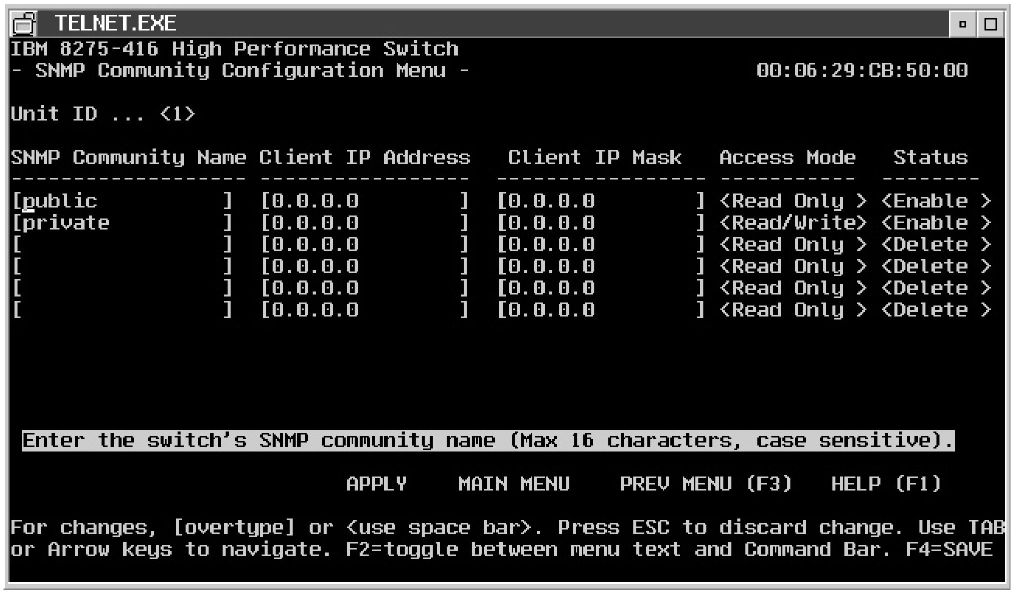
Configuring the SNMP community

The switch has an SNMP agent that complies with SNMP Version 1 (SNMPv1). For more about the SNMP specification, see the appropriate SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on your SNMP configuration. SNMP configuration for the switch includes configuring the trap receiver and SNMP community parameters, which are described in the following text.

If you do not use the default community information, you must configure the SNMP agent with a community name for the switch. A community name is a name associated with the switch and with a set of SNMP managers allowed to manage it with a specified privileged level. You can add, change or delete communities. The switch does not have to be reset for changes to take effect. Up to six communities are simultaneously supported.

Community names in the SNMP community table must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

To configure your SNMP communities, select **SNMP Community Configuration Menu** from the Management Menu. Figure 21 shows SNMP community information you need to specify.



```
IBM 8275-416 High Performance Switch
- SNMP Community Configuration Menu -                   00:06:29:CB:50:00

Unit ID ... <1>

SNMP Community Name Client IP Address   Client IP Mask   Access Mode   Status
------------------- -----------------  ----------------- -----------  --------
[public          ]  [0.0.0.0        ]  [0.0.0.0        ] <Read Only > <Enable >
[private         ]  [0.0.0.0        ]  [0.0.0.0        ] <Read/Write> <Enable >
[                ]  [0.0.0.0        ]  [0.0.0.0        ] <Read Only > <Delete >
[                ]  [0.0.0.0        ]  [0.0.0.0        ] <Read Only > <Delete >
[                ]  [0.0.0.0        ]  [0.0.0.0        ] <Read Only > <Delete >
[                ]  [0.0.0.0        ]  [0.0.0.0        ] <Read Only > <Delete >





 Enter the switch's SNMP community name (Max 16 characters, case sensitive).

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 21. SNMP community configuration

SNMP Community Name
This name identifies each SNMP community; the name can be up to 16 characters, and it is case-sensitive. A *public* community means users have read only access. A *private* community is for users who have read/write access. Two communities have default values. The default names are Public and Private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.

Client IP Address
This attribute is an IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is logical-ANDed with the Client IP Mask and the result must match the Client IP Address. The default value is 0.0.0.0.

Note: If the Client IP Mask is set to 0.0.0.0, a Client IP Address of 0.0.0.0 matches all IP addresses.

Client IP Mask
This attribute is a mask to be logical-ANDed with the requesting entity's IP address before comparison with the Client IP Address. If the result matches with Client IP Address then the address is an authenticated IP address. For example, if the Client IP Address is 9.47.128.0 and the corresponding Client IP Mask is 255.255.255.0, a range of incoming IP addresses would match, that is, the incoming IP addresses could be a value in the following range: 9.47.128.0 to 9.47.128.255.

To have a specific IP address be the only authenticated IP address, set the Client IP Address to the required IP address and set the Client IP Mask to 255.255.255.255. The default for the Client IP Mask is 0.0.0.0.

Access Mode

This value can be read-only or read/write. A community with a read-only access allows for switch information to be displayed. A community with a read/write access allows for configuration changes to be made and for information to be displayed.

A community name with read-only access is restricted from viewing SNMP community and SNMP trap receiver information.

Status

This attribute has the following values: Enable, Disable and Delete on the terminal and Web interface and Active, Inactive, and Delete on SNMP.

A community status of Enable/Active means that the community is active, allowing SNMP managers associated with this community to manage the switch according to its access right.

A community status of Disable/Inactive means that the community is not active; no SNMP requests using this community will be accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable/Active.

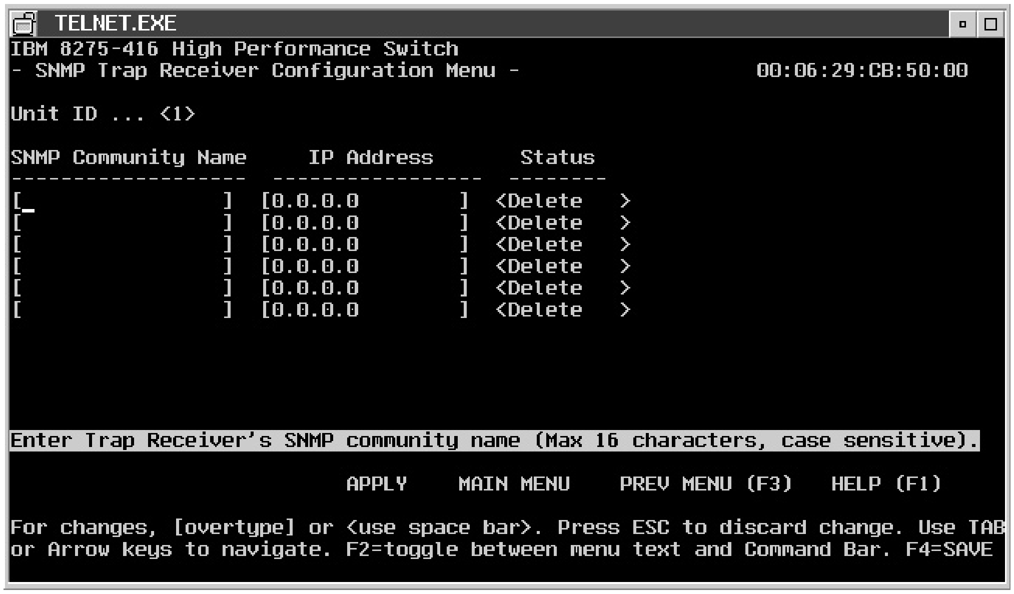
A community status of Delete means that this name will be removed from the table. The default Status values for the default private and public community names are both Enable/Active. The default value is Delete/Inactive for the 4 undefined community names.

Configuring the trap receiver

Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Up to six simultaneous trap receivers are supported.

IP Addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is kept and processed and all duplicate entries are ignored.

To configure trap receivers, select **SNMP Trap Receiver Configuration Menu** on the Management Menu. Figure 22 on page 41 shows the parameters you need to specify.



```
IBM 8275-416 High Performance Switch
- SNMP Trap Receiver Configuration Menu -                00:06:29:CB:50:00

Unit ID ... <1>

SNMP Community Name     IP Address       Status
-------------------  -----------------  --------
[_               ]  [0.0.0.0        ]  <Delete   >
[                ]  [0.0.0.0        ]  <Delete   >
[                ]  [0.0.0.0        ]  <Delete   >
[                ]  [0.0.0.0        ]  <Delete   >
[                ]  [0.0.0.0        ]  <Delete   >
[                ]  [0.0.0.0        ]  <Delete   >




Enter Trap Receiver's SNMP community name (Max 16 characters, case sensitive).

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 22. SNMP trap receiver configuration

Trap receiver parameters are:

SNMP Community Name
This is the SNMP community name of the remote network manager; the name can be up to 16 characters, and is case-sensitive. The default value for the 6 undefined community names is Delete.

IP Address
Each IP address parameter is four decimal numbers. The numbers range from 0 to 255. The default IP address is 0.0.0.0.

Status
The status for trap receivers can be Enabled, Disabled, or Deleted. Trap receivers with Enabled status are active and the SNMP agent sends traps to them. Trap receivers with Disabled status are inactive and the SNMP agent does not send traps to them. Trap receivers with a Deleted status are removed from the table.

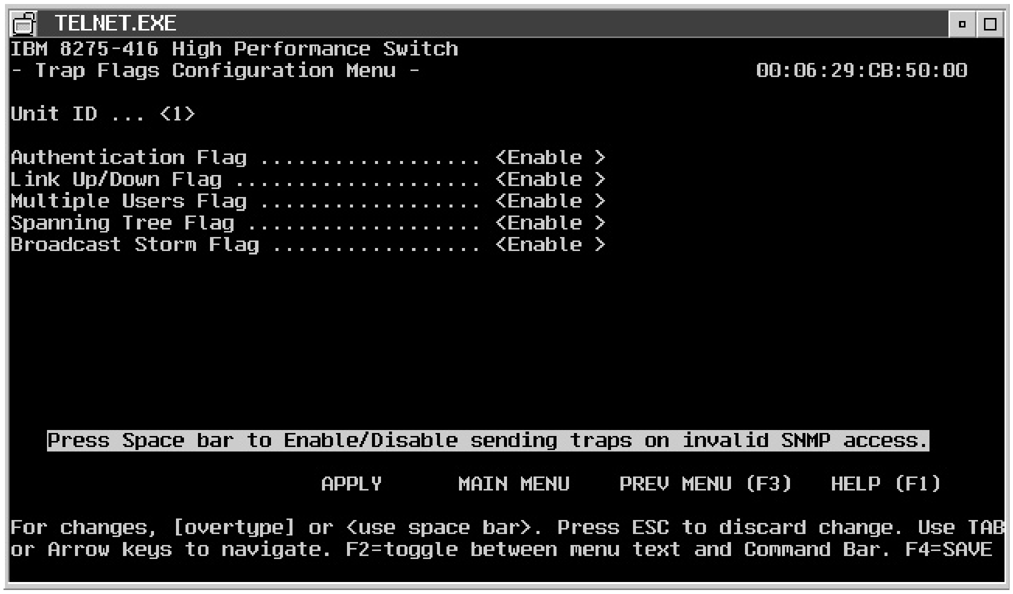
Configuring traps

Configuring trap conditions

You can optionally configure which traps that the switch should generate. You do this by selecting a status for the trap condition, that is, if it is either enabled or disabled. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. Otherwise, no condition is detected and no trap is sent. The default Status value for all Trap Conditions is Enabled. The switch does not have to be reset to implement the changes. Cold start traps are always generated; there are no associated trap conditions.

To configure trap conditions, select **Trap Menu** from the Management Menu. From the Trap Menu, select **Trap Flag Configuration Menu**, then enable or disable trap flags.

Figure 23 on page 42 shows the trap flags that you can set.



```
IBM 8275-416 High Performance Switch
- Trap Flags Configuration Menu -                             00:06:29:CB:50:00

Unit ID ... <1>

Authentication Flag .................. <Enable >
Link Up/Down Flag .................... <Enable >
Multiple Users Flag .................. <Enable >
Spanning Tree Flag ................... <Enable >
Broadcast Storm Flag ................. <Enable >








   Press Space bar to Enable/Disable sending traps on invalid SNMP access.

                         APPLY      MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 23. Trap flags configuration

These are the trap conditions that can be enabled/disabled:

Authentication Flag
Enable/Disable authentication Flag.

Link Up/Down Flag
Enable/Disable Link Up/Link Down traps for the entire switch. When set to Enable, the Link Up/Down traps will be sent only if the Link Trap flag setting associated with the port (Port Configuration Menu) is set to Enable.

Multiple Users Flag
Enable/Disable Multiple User traps. When the value is set to Enable, a Multiple User Trap is sent whenever someone logs in to the terminal interface (EIA 232 or Telnet) and there is already an existing terminal interface session.

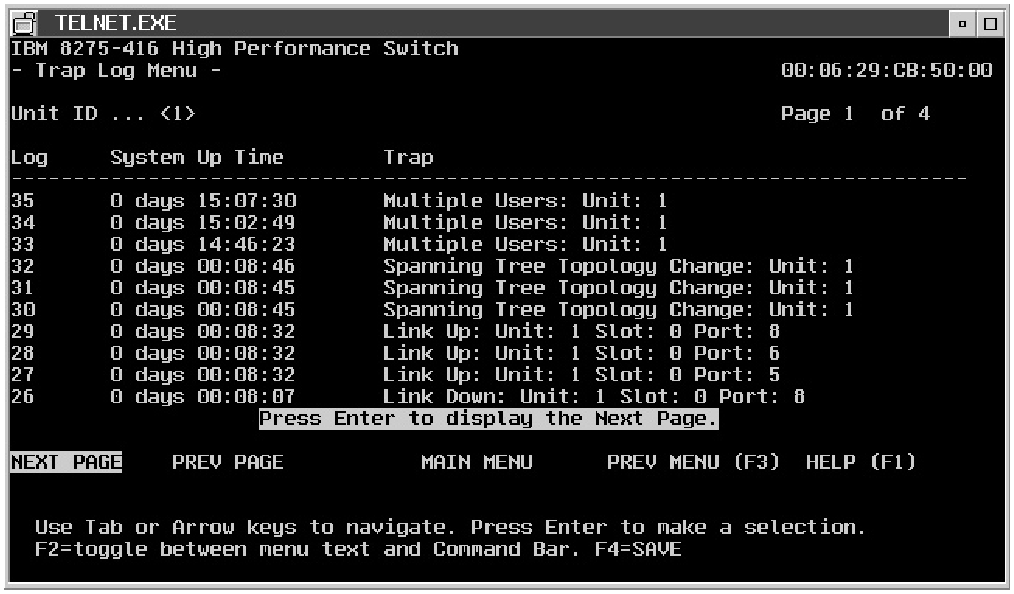
Spanning Tree Flag
This flag enables the sending of new root traps and topology change notification traps. See “Appendix E. Introduction to Virtual LANs (VLANs)” on page 117 for more information.

Broadcast Storm Flag
This flag enables or disables the broadcast storm trap. You must also enable Broadcast Storm Recovery Mode (see the Switch Configuration Menu). The default is Disable. When this value is set to Enable and Broadcast Storm Recovery mode is set to Enable, the Broadcast Storm Start/End traps are sent when the switch enters and leaves Broadcast Storm Recovery.

Trap log

The switch maintains a Trap Log; it contains a maximum of 256 entries that wrap. Trap Log information is not retained across a switch reset.

Select **Trap Menu** from the Management Menu, then select **Trap Log Menu** from the Trap Menu. Figure 24 on page 43 shows the entries in the trap log.



```
IBM 8275-416 High Performance Switch
- Trap Log Menu -                                                00:06:29:CB:50:00

Unit ID ... <1>                                                  Page 1  of 4

Log     System Up Time        Trap
-----------------------------------------------------------------------------
35      0 days 15:07:30       Multiple Users: Unit: 1
34      0 days 15:02:49       Multiple Users: Unit: 1
33      0 days 14:46:23       Multiple Users: Unit: 1
32      0 days 00:08:46       Spanning Tree Topology Change: Unit: 1
31      0 days 00:08:45       Spanning Tree Topology Change: Unit: 1
30      0 days 00:08:45       Spanning Tree Topology Change: Unit: 1
29      0 days 00:08:32       Link Up: Unit: 1 Slot: 0 Port: 8
28      0 days 00:08:32       Link Up: Unit: 1 Slot: 0 Port: 6
27      0 days 00:08:32       Link Up: Unit: 1 Slot: 0 Port: 5
26      0 days 00:08:07       Link Down: Unit: 1 Slot: 0 Port: 8
                    Press Enter to display the Next Page.

NEXT PAGE    PREV PAGE           MAIN MENU      PREV MENU (F3)  HELP (F1)


  Use Tab or Arrow keys to navigate. Press Enter to make a selection.
  F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 24. Trap log

Each entry contains:

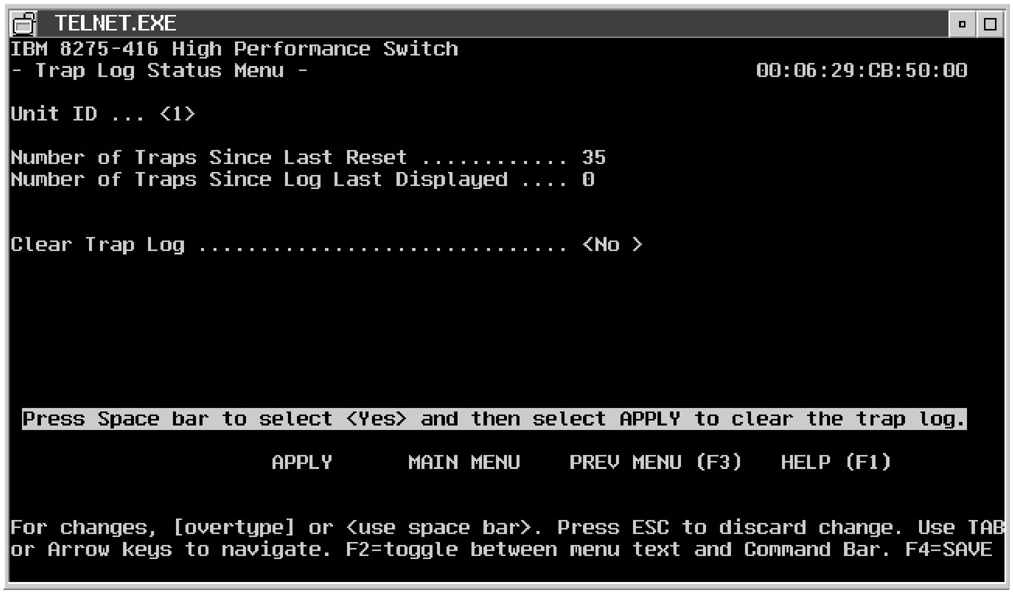
System Up Time
This entry shows how long the system has been up when the trap occurred.

Trap This entry is the name of the trap condition, which can be:
- Cold Start
- Authentication Failure
- Link Up
- Link Down
- Multiple Users
- New Spanning Tree Root
- Spanning Tree Topology Change
- Broadcast storm start/end

Checking trap log status

To check how many traps have been generated, select **Trap Menu** from the Management Menu, then select **Trap Log Status Menu** from the Trap Menu.

You can choose to clear the trap log on this panel (Figure 25 on page 44).



```
IBM 8275-416 High Performance Switch
- Trap Log Status Menu -                                00:06:29:CB:50:00

Unit ID ... <1>

Number of Traps Since Last Reset ............ 35
Number of Traps Since Log Last Displayed .... 0


Clear Trap Log ............................. <No >







 Press Space bar to select <Yes> and then select APPLY to clear the trap log.

                     APPLY      MAIN MENU    PREV MENU (F3)   HELP (F1)


For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

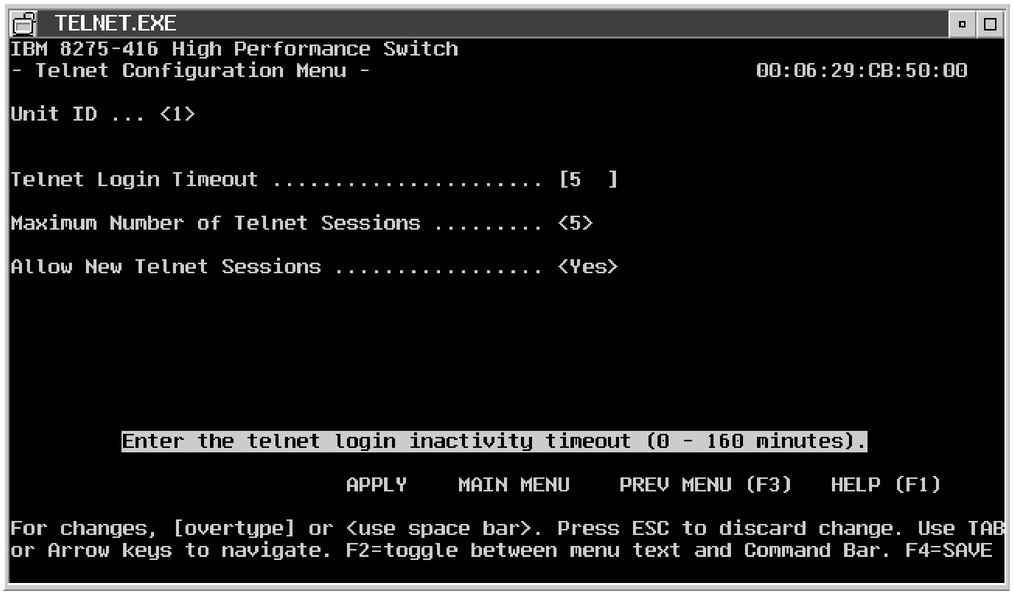
Figure 25. Trap log status

You can perform this operation on this panel:

Clear Trap Log
Specify Yes or No. *Yes* causes the contents of the Trap Log to be erased. *No* causes the trap log to continue logging trap information after the last entry.

Configuring Telnet

You can manage the switch remotely using a Telnet connection. “Chapter 2. Accessing the switch” on page 19 describes setting up a Telnet connection. To configure for Telnet, select **Management Menu** from the Main Menu, then from the Management Menu, select **Telnet Configuration Menu** (Figure 26).



```
IBM 8275-416 High Performance Switch
- Telnet Configuration Menu -                           00:06:29:CB:50:00

Unit ID ... <1>


Telnet Login Timeout ...................... [5  ]

Maximum Number of Telnet Sessions ......... <5>

Allow New Telnet Sessions ................. <Yes>







         Enter the telnet login inactivity timeout (0 - 160 minutes).

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 26. Telnet configuration

The following parameters are for configuring a Telnet session with the switch:

Telnet Login Timeout
A session is active as long as the session has not remained idle for the value set. Specify a decimal value from 0 to 160 minutes. A value of 0 indicates that a Telnet session remains active indefinitely. The default is 5 minutes.

Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

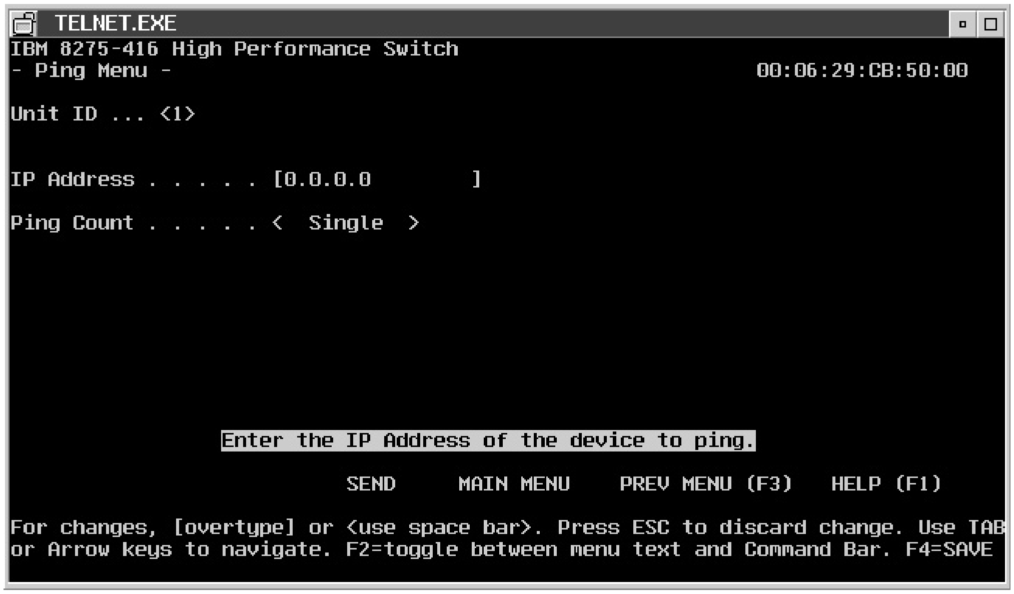
Maximum Number of Telnet Sessions
Specify a decimal value from 0 to 5. If the value is 0, no Telnet session can be established. The default value is 5.

Allow New Telnet Sessions
Specify Yes or No. *Yes* means that new Telnet sessions can be established until there are no more sessions available. *No* means that no new Telnet sessions are to be established. Any already established session remains active until the session is ended or an abnormal network error ends it. The default value is Yes.

Ping

The switch provides a ping utility that you can use to check connectivity between devices in a network. To use ping, the switch must be configured correctly for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the Default VLAN (VLAN 1) (as long as there is a physical path between the switch and the workstation). The terminal interface allows you to send one ping, three pings or a continuous ping (one every second) to the target station.

To use Ping, select **Management Menu** from the Main Menu. Then select **Ping Menu** from the Management Menu (Figure 27).



```
IBM 8275-416 High Performance Switch
- Ping Menu -                                               00:06:29:CB:50:00

Unit ID ... <1>


IP Address . . . . . [0.0.0.0        ]

Ping Count . . . . . <  Single  >









                 Enter the IP Address of the device to ping.

                           SEND     MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 27. Ping

You must supply this information:

IP Address
The IP address of the target station. The value is 4 decimal bytes ranging from 0 to 256. The default is 0.0.0.0.

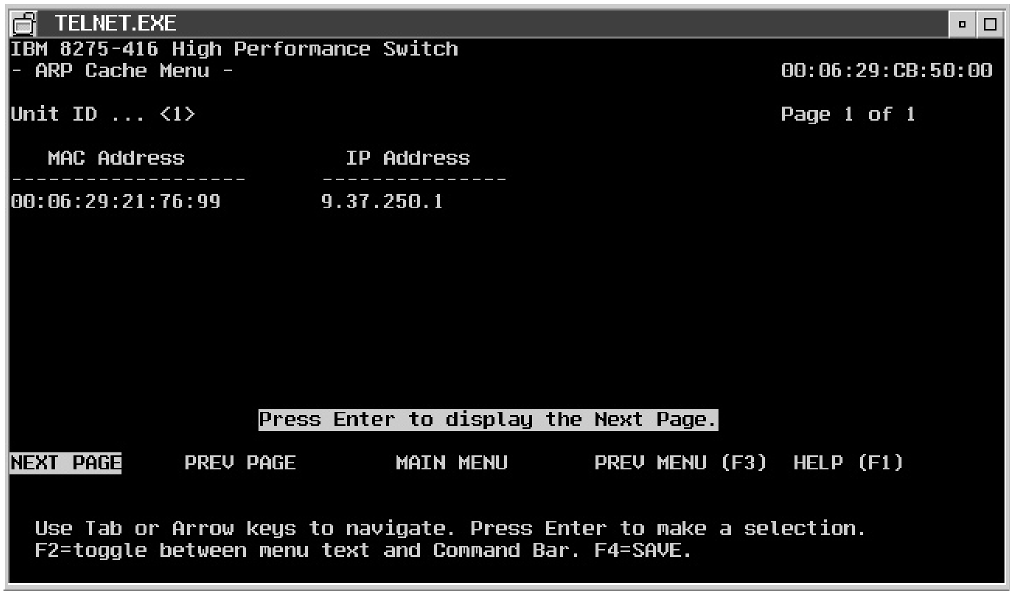
Ping Count
You can select one of these values; the default value is single:
- Single–one ping is sent to target station.
- Multiple–three pings are sent to the target station.
- Continuous–a ping is sent every second.

Command
Send is the only command. To stop sending pings, press any key that moves the cursor from the current field.

ARP cache

Select **Management Menu** from the Main Menu. Then select **ARP Cache Menu** from the Management Menu to displays the ARP cache for the switch.

This is used to check connectivity between the switch and other devices. The ARP cache identifies the MAC addresses of the IP stations communicating with the switch. Figure 28 shows ARP Cache information.

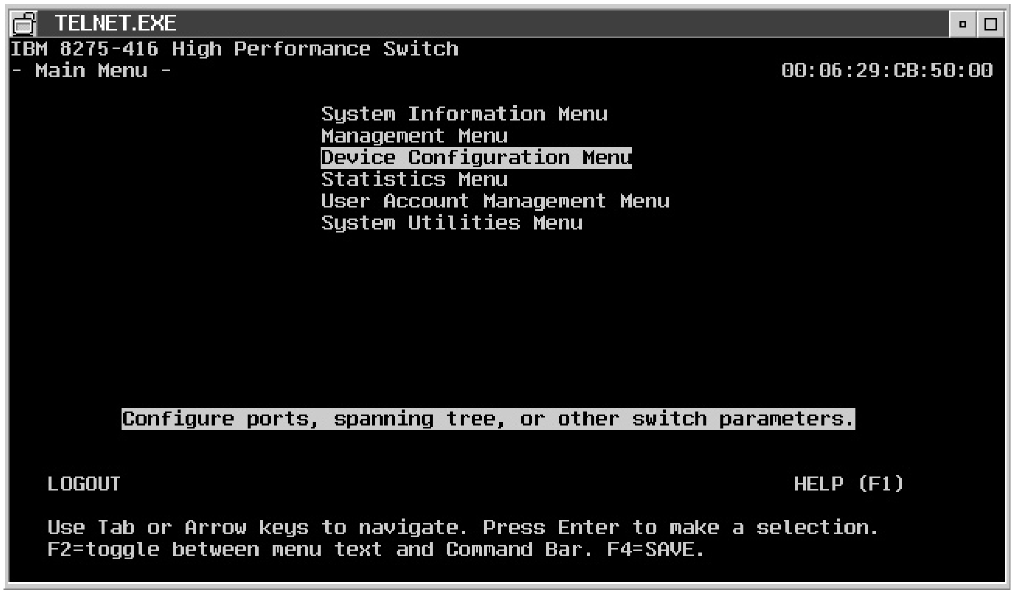


```
IBM 8275-416 High Performance Switch
- ARP Cache Menu -                                           00:06:29:CB:50:00

Unit ID ... <1>                                              Page 1 of 1

   MAC Address              IP Address
-------------------      ---------------
00:06:29:21:76:99        9.37.250.1







                    Press Enter to display the Next Page.

NEXT PAGE     PREV PAGE       MAIN MENU       PREV MENU (F3)  HELP (F1)


  Use Tab or Arrow keys to navigate. Press Enter to make a selection.
  F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 28. ARP cache

Device configuration

To configure the switch, select **Device Configuration Menu** on the Main Menu. Figure 29 shows your options.

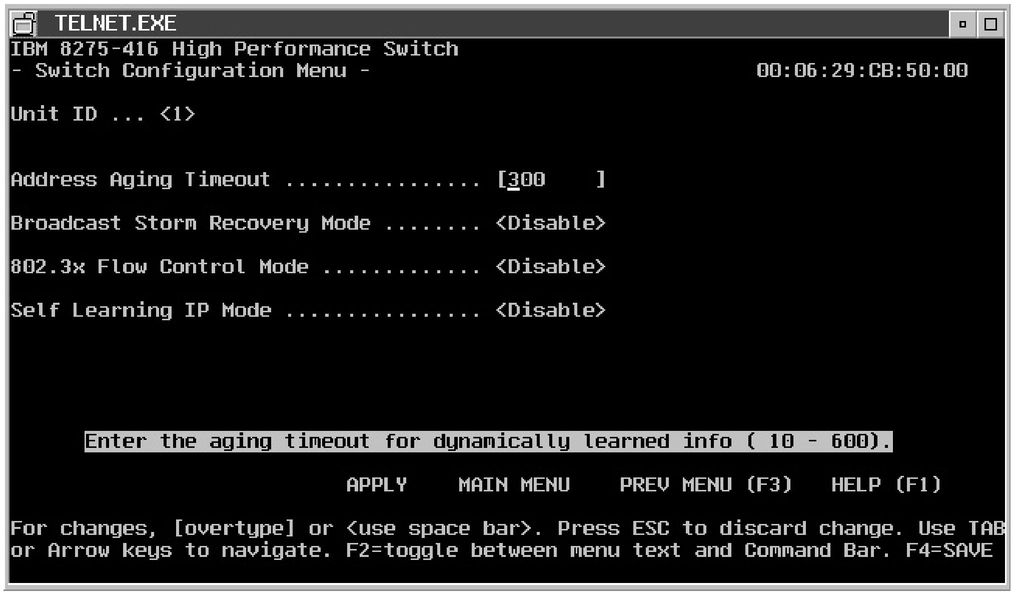


```
IBM 8275-416 High Performance Switch
- Main Menu -                                                   00:06:29:CB:50:00

                         System Information Menu
                         Management Menu
                         Device Configuration Menu
                         Statistics Menu
                         User Account Management Menu
                         System Utilities Menu




         Configure ports, spanning tree, or other switch parameters.

   LOGOUT                                                      HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 29. Device configuration

Configuring the switch

The switch allows you to set a time after which the address will timeout, and to enable/disable broadcast storm recovery and 802.3x flow control. To set these values, select **Device Configuration Menu** from the Main Menu and then select **Switch Configuration Menu** (Figure 30).



```
IBM 8275-416 High Performance Switch
- Switch Configuration Menu -                                 00:06:29:CB:50:00

Unit ID ... <1>


Address Aging Timeout ................ [300    ]

Broadcast Storm Recovery Mode ........ <Disable>

802.3x Flow Control Mode ............. <Disable>

Self Learning IP Mode ................ <Disable>




      Enter the aging timeout for dynamically learned info ( 10 - 600).

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 30. Switch configuration

The value you specify is:

Address Aging Timeout

Indicates the timeout period (in seconds) for aging out dynamically learned forwarding information. The range is 10 to 600 (seconds). The default is 300 (seconds).

Broadcast Storm Recovery Mode

When you specify Enable for Broadcast Storm Recovery and the broadcast traffic on any Ethernet port exceeds 20 percent of the link speed, the switch blocks (discards) the broadcast traffic until the broadcast traffic returns to 10 percent or less.

When you specify Disable for Broadcast Recovery Mode, then the switch will not block any broadcast traffic on any Ethernet port. The default is Disable.

802.3x Flow Control Mode

Indicates if 802.3x flow control is enabled for the switch. The default is Disable. This value applies to only full-duplex mode ports.

Self Learning IP Mode

Indicates that the self-learning IP mode is enabled or disabled. Disable is the default.

Note: For the Self Learning IP function to work, the IP information must include a default gateway for the network.

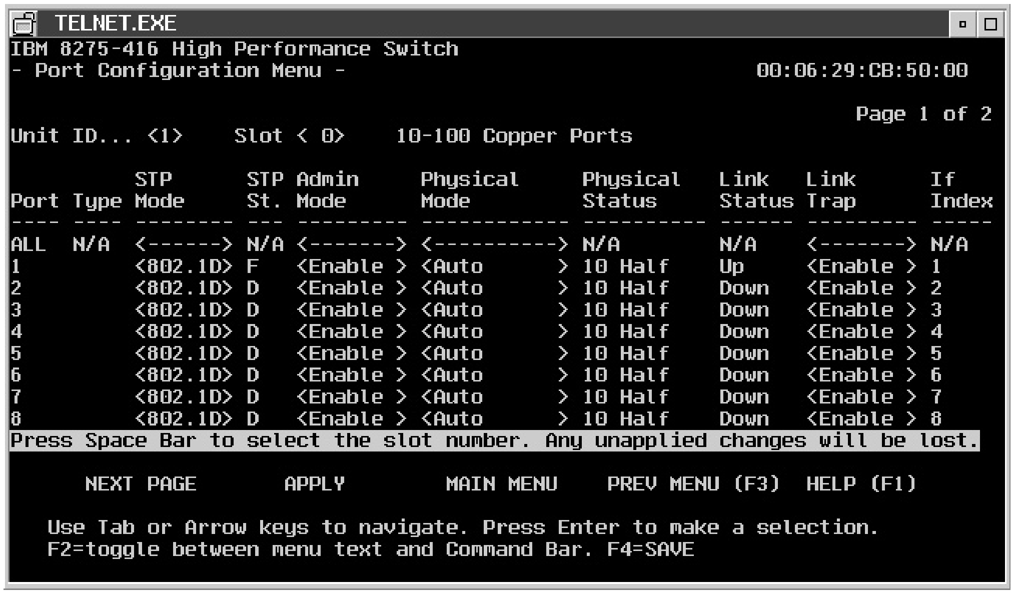
When you specify Enable, self-learning IP entries can be viewed on the second panel (Page 2 of 2) of the **Switch Detailed Statistics Menu** (see “Switch detailed statistics” on page 64).

Configuring ports

The switch is shipped from the factory with default port settings that allow it to automatically determine the port type and speed.

See “Chapter 3. Configuring your switch” on page 25 for details about making and saving configuration changes.

To configure the ports, select **Device Configuration Menu** from the Main Menu, then select **Port Configuration Menu** from the Device Configuration Menu (Figure 31 on page 49).



```
IBM 8275-416 High Performance Switch
- Port Configuration Menu -                                 00:06:29:CB:50:00

                                                                    Page 1 of 2
Unit ID... <1>    Slot < 0>    10-100 Copper Ports

          STP      STP Admin     Physical     Physical   Link   Link      If
Port Type Mode     St. Mode      Mode         Status     Status Trap      Index
---- ---- -------- --- --------- ------------ ---------- ------ --------- -----
ALL  N/A  <------> N/A <-------> <----------> N/A        N/A    <-------> N/A
1         <802.1D> F   <Enable > <Auto      > 10 Half    Up     <Enable > 1
2         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 2
3         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 3
4         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 4
5         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 5
6         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 6
7         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 7
8         <802.1D> D   <Enable > <Auto      > 10 Half    Down   <Enable > 8
Press Space Bar to select the slot number. Any unapplied changes will be lost.

      NEXT PAGE       APPLY        MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 31. Port configuration

You can select or change the following values:

Slot This is a read/write field. The 16 base ports are associated with slot 0. A feature module in Slot 1 or Slot 2 can have 2, 4, or 8 ports associated with each of them, depending on the feature module that is installed.

Port You can use the *All* option to change the value for all ports in this slot. You can specify Enable or Disable for the Admin Mode and Link Trap fields.

Note that when All is specified and you specify Disable in the Admin Mode field, you lose in-band connection to the switch.

Indicates the port number.

The feature slots are Slot 1 and Slot 2. Available feature modules have 2, 4, and 8 ports.

Type This is a read only field. It indicates whether a port currently belongs to a trunk or is enabled for monitoring. Type values are:

- Trnk: indicates that this port belongs to a trunk.
- Mntr: indicates that this port is enabled for port monitoring.

STP Mode

This is a configurable parameter. It specifies the spanning tree protocol mode for the port. STP mode values are:

- 802.1D (the default)
- Fast, indicates you want to use the fast spanning tree mode
- Off, indicates the STP mode is turned off for a particular port

STP St. (STP state)

This is a read-only field. It contains a single letter to indicate the current spanning tree protocol state, which can be:

- D: disabled
- B: blocking
- l: listening
- L: learning
- F: forwarding
- X: indicates port is diagnostically disabled

Admin Mode
This is a configurable value and indicates if the port is enabled or disabled. The default for all ports is Enabled.

Physical Mode
This is a configurable value and indicates the speed and duplex setting for the port. The value of Auto (autodetect) is valid only for 10/100BASE-TX ports.

- Auto: automatically negotiates the speed and duplex setting
- 100 Half: 100BASE-T half-duplex
- 100 Full: 100BASE-T full duplex
- 10 Half: 10BASE-T half duplex
- 10 Full: 100BASE-T full duplex
- 100FX Half: 100BASE-FX half duplex
- 100FX Full: 100BASE-FX full duplex
- 1000SX Full: 1000BASE-SX full duplex

Physical Status
Indicates the port speed and duplex. This is a read-only field.

Link Status
Indicates if the port link is up or down. This is a read-only field.

Link Trap
This is a configurable value and can be Enabled or Disabled. It allows you to enable or disable link status traps by port. This parameter is only valid when Link Up/Down Flag is enabled on the Trap Flags Configuration Menu.

IfIndex
This is a read-only field. When using SNMP, the interface index (ifIndex) is used to identify the specific interface being addressed. The ifIndex is determined by MIB II.

Configuring port monitoring

You can select any of the Ethernet ports as a probe to monitor forwarded traffic (not local traffic) with an external network analyzer. The selected probe port can monitor (mirror) traffic from one port. The selected probe port also receives and transmits network traffic (tagged frames) which allows a device connected to the probe port to be managed over the network (in-band connectivity). However, the device must be 802.1Q aware to be remotely managed by the switch.

The monitoring port forwards frames with a VLAN membership which matches the monitored port. The monitoring port transmits all frames as tagged. The monitoring port does not participate in Spanning Tree Protocol (STP) and is always in a forwarding state when the link is up. The monitoring port does not forward local traffic, and it does not participate in GVRP.

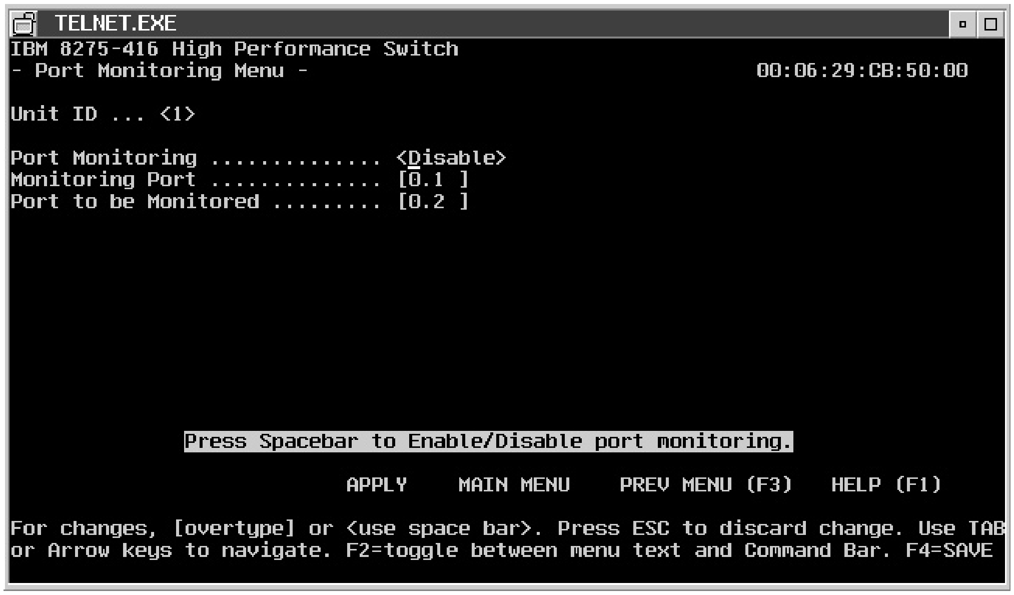
Port Monitoring Operation

1. The monitoring port transmits all frames as tagged; therefore, a network analyzer is remotely manageable only if it is 802.1Q-aware.
2. The monitoring port is unable to transmit frames outside of its VLAN membership. Therefore, if the monitored port has ingress filtering disabled, any frames received or forwarded on that port, and which are not affiliated with a VLAN with which the monitored port is a member, will not be transmitted out of the monitoring port.
3. The monitoring port always transmits frames with the NCFI bit set. Therefore, frames not transmitted not on the monitored port due to untagging and a set NCFI bit cannot be detected and filtered by the monitoring port. In this case, the

monitoring port will transmit these frames, even though they are not transmitted by the monitored port. The existence of such frames in a network is expected to be a rare occurrence.

4. Frames not forwarded by the monitored port will not be monitored. These include:
   - Local frames
   - 802.3x PAUSE frames
   - Frames dropped due to ingress rules
   - Frames dropped due to forwarding rules

From the Main Menu, select **Device Configuration Menu** and then, select **Port Monitoring Menu** from the Device Configuration Menu (Figure 32).



```
IBM 8275-416 High Performance Switch
- Port Monitoring Menu -                                   00:06:29:CB:50:00

Unit ID ... <1>

Port Monitoring .............. <Disable>
Monitoring Port .............. [0.1 ]
Port to be Monitored ......... [0.2 ]










              Press Spacebar to Enable/Disable port monitoring.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 32. Port monitoring

Specify values for the following parameters:

Port Monitoring
Used to *Enable* or *Disable* the port monitoring function. The default is Disable.

Monitoring Port
This is the ***slot.port*** that the *monitored* data is sent to. This is the ***slot.port*** that a Network Analyzer is attached to. The slot can be 0, 1 or 2. The default is 0. The port range is 1 to 16 for Slot 0; 1 to 2, 1 to 4, or 1 to 8 for Slots 1 and 2.

When Port Monitoring is Enabled, make sure that the monitoring port is connected to a network analyzer and not to the network itself to avoid potential problems.

Port to be Monitored
This is the port from which data is captured and sent to the monitoring port (the port under analysis). The port range is 1 to 16 for Slot 0; 1 to 2, 1 to 4, or 1 to 8 for Slots 1 and 2.

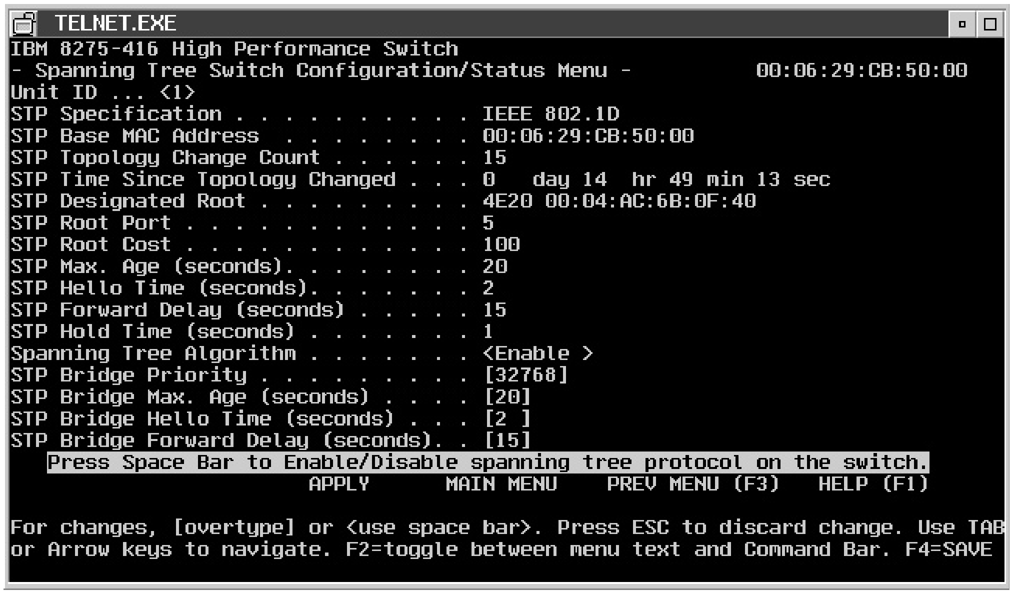
Configuring spanning tree protocol (STP)

Spanning tree switch configuration/status

The switch participates in Spanning Tree Protocol (STP). STP allows you to configure redundant paths in the switch topology. The switch automatically blocks redundant paths to prevent loops (that is, make it fault tolerant). If an active path is broken and a backup path is available, the switch finds the redundant path and enables it. Without STP, a path failure means loss of connectivity for the affected part of the network.

The switch complies with the IEEE 802.1D standard. Refer to the IEEE 802.1D document for STP specifications. The switch supports one Spanning Tree Protocol (STP) for the entire switch.

To configure the Spanning Tree Protocol for the switch, select **Device Configuration Menu** from the Main Menu, then select **Spanning Tree Switch Configuration/Status Menu** or **Spanning Tree Port Configuration/Status Menu** from the Device Configuration Menu (Figure 33).



```
IBM 8275-416 High Performance Switch
- Spanning Tree Switch Configuration/Status Menu -          00:06:29:CB:50:00
Unit ID ... <1>
STP Specification . . . . . . . . . . IEEE 802.1D
STP Base MAC Address  . . . . . . . . 00:06:29:CB:50:00
STP Topology Change Count . . . . . . 15
STP Time Since Topology Changed . . . 0   day 14  hr 49 min 13 sec
STP Designated Root . . . . . . . . . 4E20 00:04:AC:6B:0F:40
STP Root Port . . . . . . . . . . . . 5
STP Root Cost . . . . . . . . . . . . 100
STP Max. Age (seconds). . . . . . . . 20
STP Hello Time (seconds). . . . . . . 2
STP Forward Delay (seconds) . . . . . 15
STP Hold Time (seconds) . . . . . . . 1
Spanning Tree Algorithm . . . . . . . <Enable >
STP Bridge Priority . . . . . . . . . [32768]
STP Bridge Max. Age (seconds) . . . . [20]
STP Bridge Hello Time (seconds) . . . [2 ]
STP Bridge Forward Delay (seconds). . [15]
   Press Space Bar to Enable/Disable spanning tree protocol on the switch.
                        APPLY      MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 33. Spanning tree switch configuration/status

The following section lists and describes the STP configuration functions and related parameters.

Spanning Tree Algorithm
: Indicates if the switch participates in Spanning Tree Protocol. A status of Enable means that the switch participates in the STP. Disable means that the switch does not participate in the STP. The default is Disable.

Bridge Priority
: Decimal value that indicates the priority of the switch. The range is 0 to 65535. The lower the value, the higher the priority. The bridge with the lowest priority value becomes the root (IEEE 802.1D). The default is 32768.

Maximum Age Time
: When the switch is root, Maximum Age Time is the time in seconds during which the configuration message used by the Spanning Tree Algorithm is discarded. The range is 6 to 40 seconds. The default is 20 seconds.

Hello Time

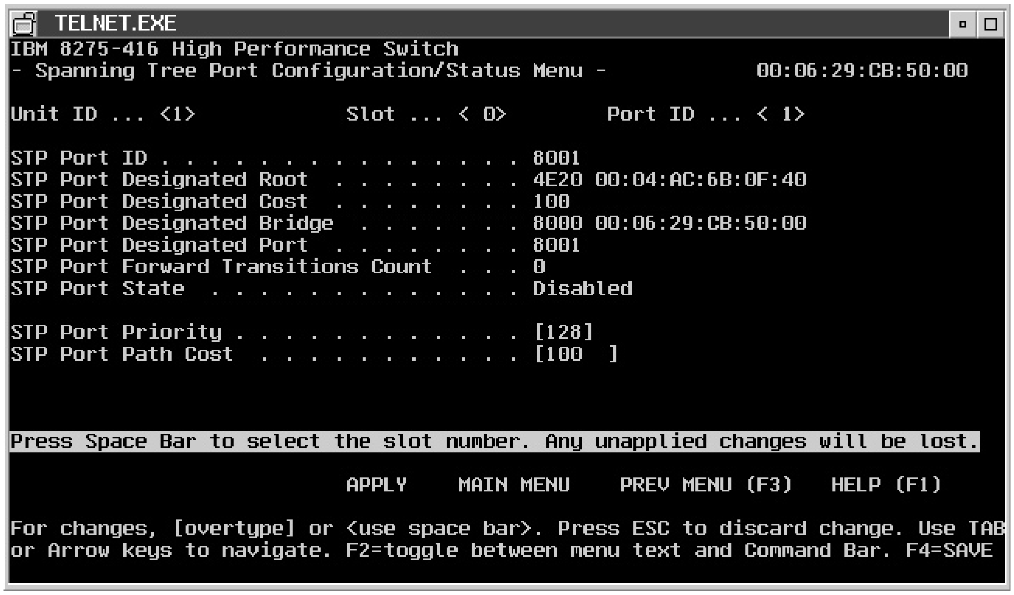
When the switch is root, Hello Time is the time in seconds that the switch waits before sending the next configuration message. The range is 1 to 10 seconds. The default is 2 seconds.

Forward Delay Time

This value specifies the time spent in “Listening and Learning” mode before forwarding packets. The range is 4 to 30 seconds. The default is 15 seconds.

Spanning tree port configuration/status

You can configure the Spanning Tree Protocol by ports. Select **Device Configuration Menu** from the Main Menu. Then select **Spanning Tree Port Configuration/Status Menu** from the Device Configuration Menu (Figure 34).



```
IBM 8275-416 High Performance Switch
- Spanning Tree Port Configuration/Status Menu -          00:06:29:CB:50:00

Unit ID ... <1>            Slot ... < 0>       Port ID ... < 1>

STP Port ID . . . . . . . . . . . . . . . . 8001
STP Port Designated Root  . . . . . . . . . 4E20 00:04:AC:6B:0F:40
STP Port Designated Cost  . . . . . . . . . 100
STP Port Designated Bridge  . . . . . . . . 8000 00:06:29:CB:50:00
STP Port Designated Port  . . . . . . . . . 8001
STP Port Forward Transitions Count  . . . . 0
STP Port State  . . . . . . . . . . . . . . Disabled

STP Port Priority . . . . . . . . . . . . . [128]
STP Port Path Cost  . . . . . . . . . . . . [100  ]



Press Space Bar to select the slot number. Any unapplied changes will be lost.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 34. Spanning tree port configuration/status

The parameter values are:

Port Priority

Decimal value which indicates the priority of port on the switch. The range is 0 to 255. The default is 128.

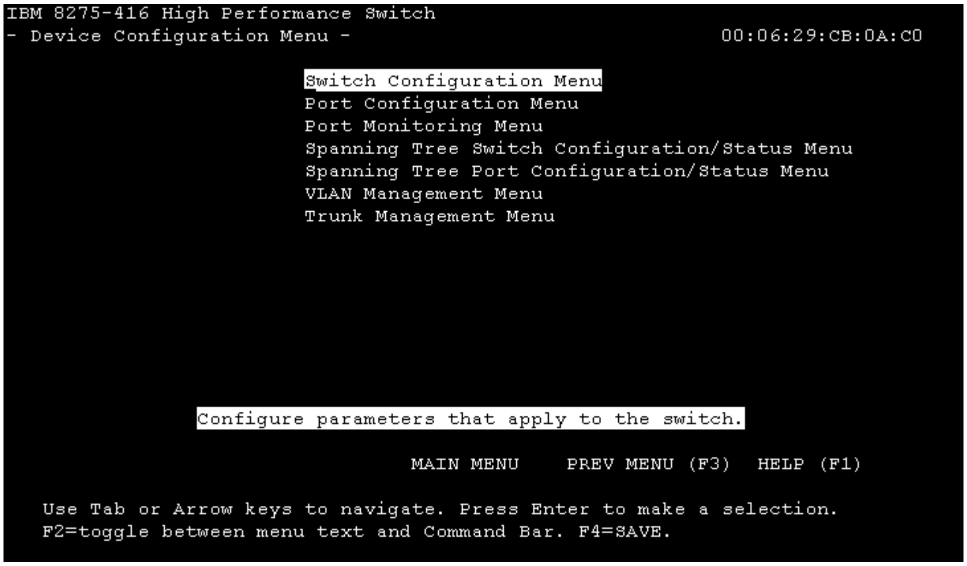
Port Path Cost

This output is automatically calculated. The cost represents the shortest distance from any switch to the root switch interval for the unit announcing its presence on the network. The range is 1 to 65535. The port path cost defaults to 0, which means that the path cost will be assigned dynamically depending upon the detected speed of the port. A value of 100 is assigned to 10 Mbps ports, and a value of 19 is assigned to 100 Mbps ports.

VLAN management

“Appendix E. Introduction to Virtual LANs (VLANs)” on page 117 provides an introduction to the terminology and concepts for VLANs. It is helpful to review this material before you define values for the parameters associated with configuring VLANs.

From the Main Menu, select **Device Configuration**, and then select **VLAN Management Menu** to begin configuring VLANs for your switch (Figure 35).

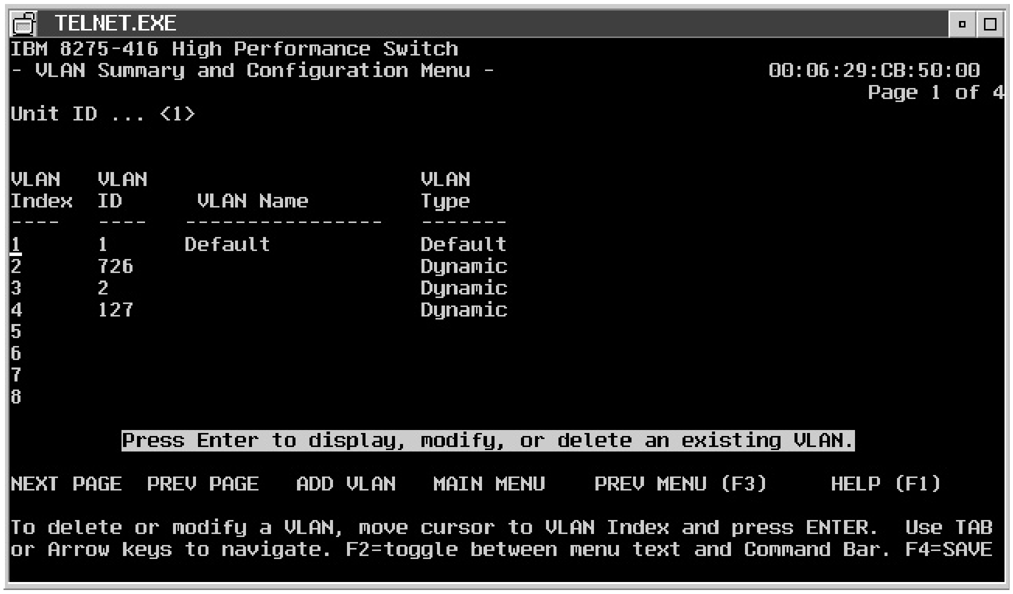


```
IBM 8275-416 High Performance Switch
- Device Configuration Menu -                          00:06:29:CB:0A:C0

                         Switch Configuration Menu
                         Port Configuration Menu
                         Port Monitoring Menu
                         Spanning Tree Switch Configuration/Status Menu
                         Spanning Tree Port Configuration/Status Menu
                         VLAN Management Menu
                         Trunk Management Menu







                Configure parameters that apply to the switch.

                                  MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 35. VLAN management menu

VLAN summary and configuration

From the VLAN Management Menu, select **VLAN Summary and Configuration Menu** to begin configuring your VLANs (Figure 36). Note that there are four panels on which you can define a total of 32 VLANs.



TELNET.EXE

```
IBM 8275-416 High Performance Switch
- VLAN Summary and Configuration Menu -                   00:06:29:CB:50:00
                                                                  Page 1 of 4
Unit ID ... <1>


VLAN   VLAN                      VLAN
Index  ID      VLAN Name         Type
----   ----   ----------------   -------
1      1      Default            Default
2      726                       Dynamic
3      2                         Dynamic
4      127                       Dynamic
5
6
7
8

         Press Enter to display, modify, or delete an existing VLAN.

NEXT PAGE  PREV PAGE   ADD VLAN   MAIN MENU    PREV MENU (F3)     HELP (F1)

To delete or modify a VLAN, move cursor to VLAN Index and press ENTER.  Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 36. VLAN summary and configuration

The parameters for this panel are:

Unit ID

Selects the unit for which data is to be displayed or configured. In a non-stacked environment the Unit ID is 1.

VLAN Index
Sequential number of defined VLANs. You can configure 8 VLANs on each of 4 pages for up to 32 VLANs.

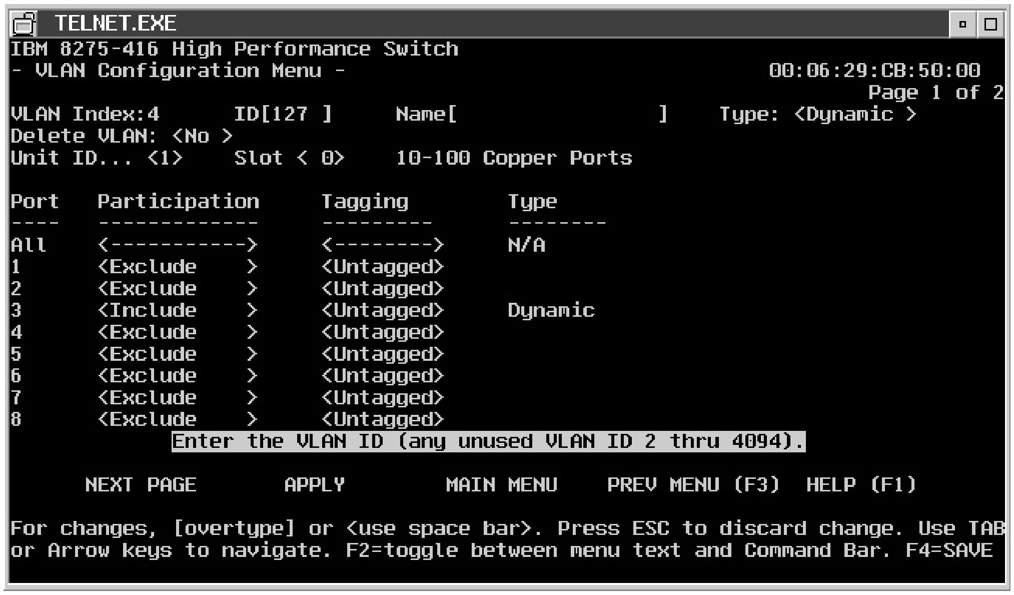
VLAN ID
VLAN identifier. It can be any number from 2 to 4094 (ID 1 is reserved for the default VLAN).

VLAN Name
An alphanumeric character string of up to 16 characters which identifies the VLAN. The default name is blank. The name for VLAN ID 1 is always *Default*.

VLAN Type
The type can be the Default VLAN, a static VLAN (one that is permanently configured and defined), or a dynamic VLAN (one that is created by GVRP registration). A VALN maked as “Dynamic” can be made “Static” by toggling in the *Type* field when the VLAN is being modified.

Adding or Modifying a VLAN

If you want to add a VLAN, move the cursor to the ADD VLAN command at the bottom of the panel and press Enter. To modify an existing VLAN, move the cursor to the line containing the VLAN and press Enter. You will be presented the VLAN Configuration Menu (Figure 37).



```
IBM 8275-416 High Performance Switch
- VLAN Configuration Menu -                                  00:06:29:CB:50:00
                                                                     Page 1 of 2
VLAN Index:4      ID[127 ]     Name[                ]    Type: <Dynamic >
Delete VLAN: <No >
Unit ID... <1>    Slot < 0>    10-100 Copper Ports

Port   Participation     Tagging       Type
----   -------------     ---------     --------
All    <----------->     <-------->     N/A
1      <Exclude    >     <Untagged>
2      <Exclude    >     <Untagged>
3      <Include    >     <Untagged>     Dynamic
4      <Exclude    >     <Untagged>
5      <Exclude    >     <Untagged>
6      <Exclude    >     <Untagged>
7      <Exclude    >     <Untagged>
8      <Exclude    >     <Untagged>
             Enter the VLAN ID (any unused VLAN ID 2 thru 4094).

      NEXT PAGE       APPLY        MAIN MENU    PREV MENU (F3)  HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 37. VLAN Configuration Menu

The parameters for this panel are:

Port This value is not selectable. Indicates by slot ID and port number which port is controlled by the fields on this line.

Slot ID
This value is not configurable. Indicates by slot ID and port number which port is controlled by the fields on this line.

Participation
Determines the degree of participation of this port in this VLAN. The values can be:

- Include: Indicates this port is always a member of this VLAN. This is equivalent to registration fixed.

- Exclude: Indicates this port is never a member of this VLAN. This is equivalent to registration forbidden.
- Autodetect: Specifies the port is to be dynamically registered in this VLAN by GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal.

Tagging
Indicates the tagging behavior for this port in the VLAN. The values can be:

- Tagged: Specifies to transmit traffic for this VLAN as tagged frames.
- Untagged: Specifies to transmit traffic for this VLAN as untagged frames.

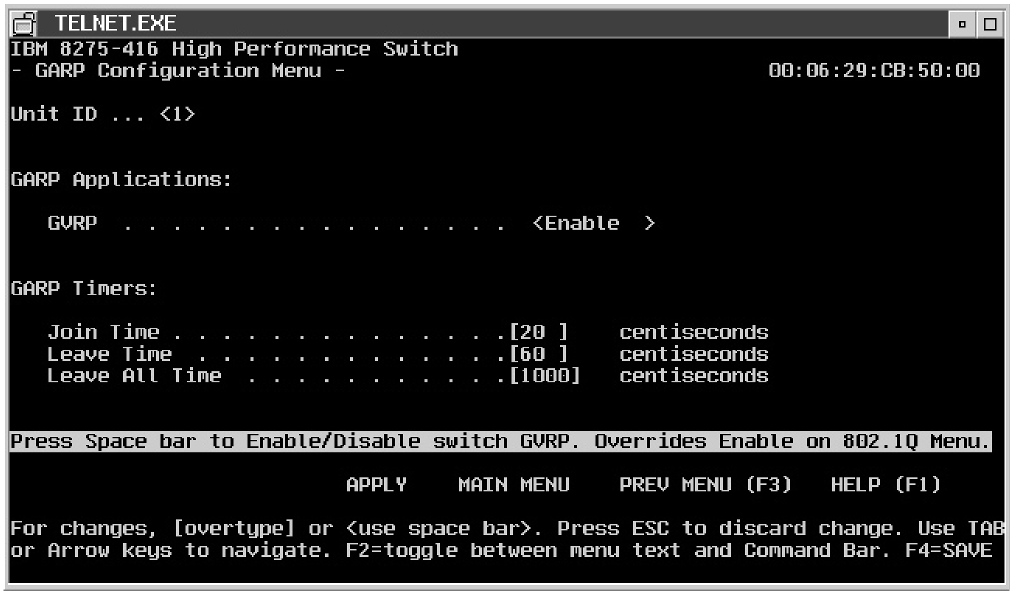
Type This value is not configurable. Indicates the port type. The values can be:

- Static: Indicates that the port is configured to be statically included in this VLAN.
- Dynamic: Indicates that this port is to be dynamically registered in this VLAN by GVRP.
- Monitor: Indicates that this is a monitoring port.
- blank (no text): Indicates that this port is excluded from being a member of this VLAN.

If a monitoring port is configured, its VLAN membership always follows the VLAN membership of the port being monitored. However, the VLAN Configuration Menu always displays the monitoring port's actual configuration; this configuration will take effect when the port is no longer a monitoring port.

Generic Attributes Registration Protocol (GARP) configuration

See Figure 38 for the GARP configuration parameters.



```
IBM 8275-416 High Performance Switch
- GARP Configuration Menu -                                  00:06:29:CB:50:00

Unit ID ... <1>


GARP Applications:

   GVRP  . . . . . . . . . . . . . . . .  <Enable  >


GARP Timers:

   Join Time . . . . . . . . . . . . . . .[20 ]    centiseconds
   Leave Time  . . . . . . . . . . . . . .[60 ]    centiseconds
   Leave All Time  . . . . . . . . . . . .[1000]   centiseconds


Press Space bar to Enable/Disable switch GVRP. Overrides Enable on 802.1Q Menu.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 38. GARP configuration

GVRP Used to enable or disable GVRP (GARP VLAN Registration Protocol). The default is Disabled.

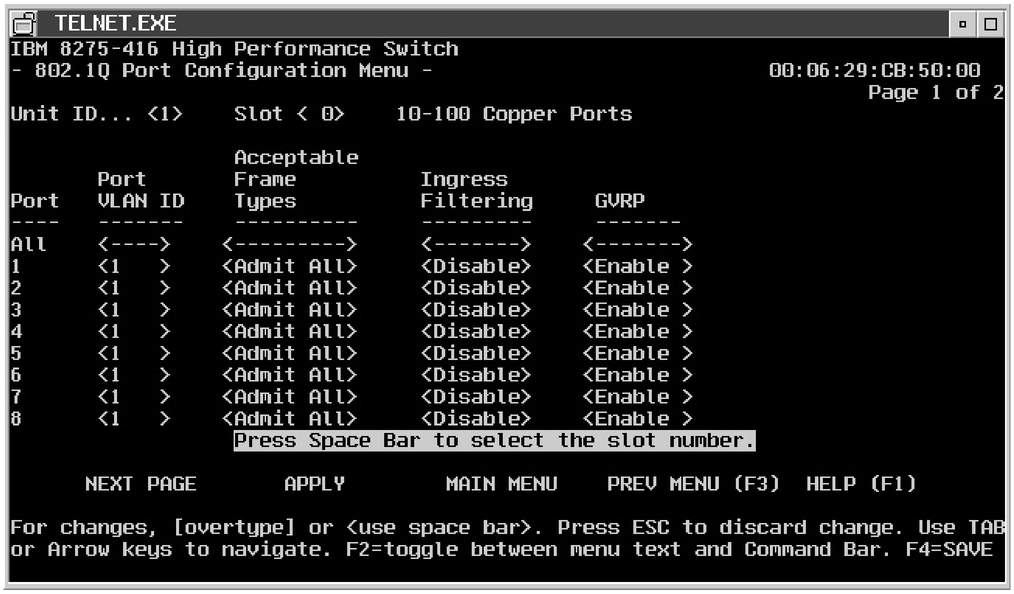
GARP Timers

- Join Time: Specifies the interval between the transmission of GARP PDUs registering (or reregistering) membership for a VLAN or multicast group. This value applies per port and per GARP. The value can be from 10 to 100 centiseconds (0.1 to 1.0 seconds). The default is 20 centiseconds (0.2 seconds).

- Leave Time: Specifies the period of time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Values can be from 200 to 6000 centiseconds (2.0 to 60 seconds). The default is 60 centiseconds (0.6 seconds).
- Leave All Time: Controls how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be shortly unregistered. Participants will need to rejoin in order to maintain registration. This value applies per port and per GARP participation. The value can be from 200 to 6000 centiseconds (2.0 to 60 seconds). The default is 60 centiseconds (0.6 seconds).

802.1Q port configuration

See Figure 39 for parameters used to configure your 802.1Q ports.



```
IBM 8275-416 High Performance Switch
- 802.1Q Port Configuration Menu -                          00:06:29:CB:50:00
                                                                  Page 1 of 2
Unit ID... <1>    Slot < 0>    10-100 Copper Ports

                  Acceptable
       Port       Frame          Ingress
Port   VLAN ID    Types          Filtering     GVRP
----   -------    ----------     ---------     -------
All    <---->    <--------->     <------->    <------->
1      <1   >    <Admit All>     <Disable>    <Enable >
2      <1   >    <Admit All>     <Disable>    <Enable >
3      <1   >    <Admit All>     <Disable>    <Enable >
4      <1   >    <Admit All>     <Disable>    <Enable >
5      <1   >    <Admit All>     <Disable>    <Enable >
6      <1   >    <Admit All>     <Disable>    <Enable >
7      <1   >    <Admit All>     <Disable>    <Enable >
8      <1   >    <Admit All>     <Disable>    <Enable >
                  Press Space Bar to select the slot number.

      NEXT PAGE       APPLY        MAIN MENU    PREV MENU (F3)  HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 39. 802.1Q port configuration

Port Indicates by a slot ID and port number which port is controlled by the fields on this line. *All* specifies all ports on all slots.

Port VLAN ID
Indicates the VLAN ID that this port will assign to untagged frames or priority-tagged frames received on this port. The value must be the ID of an existing VLAN. The default is 1.

Acceptable Frame Types
Specifies the frames that will be passed through this port. The values can be *VLAN only* or *Admit All*. For VLAN only, untagged frames or priority frames received on this port are discarded. For Admit All, untagged frames or priority frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the 802.1Q VLAN Specification.

Ingress Filtering
Indicates that ingress filtering is enabled or disabled. The default is

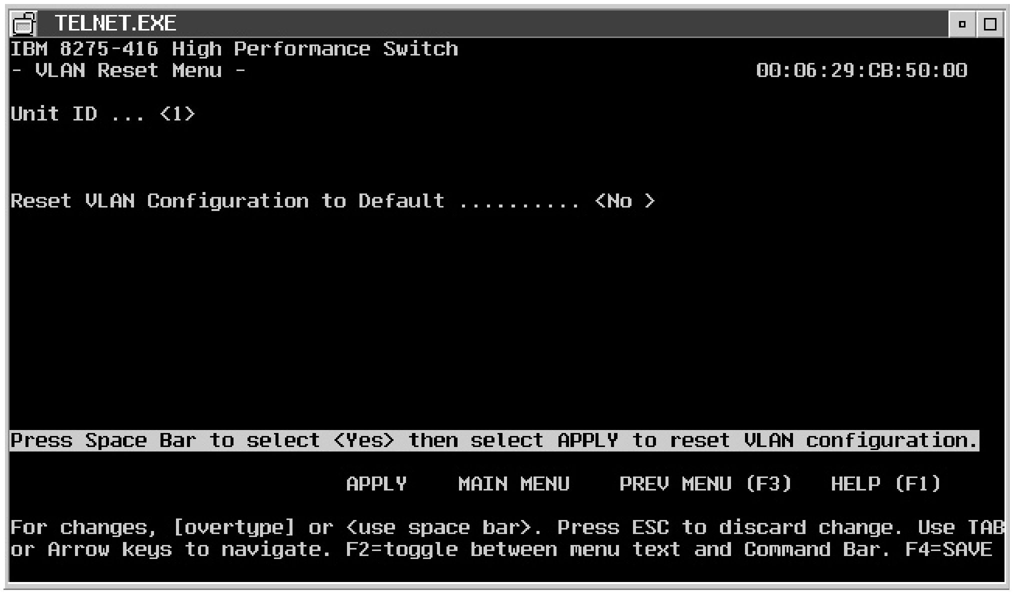
Disabled. If disabled is specified, frames received with VLAN IDs which do not match the VLAN membership of the receiving port are admitted and forwarded to ports which are members of that VLAN.

GVRP Indicates that GVRP is enabled or disabled. The default is Disabled.

VLAN reset

This function allows you to reset VLAN configuration parameters to those default parameters provided by the factory.

See Figure 40 for an example of the panel used to reset a VLAN.



```
IBM 8275-416 High Performance Switch
- VLAN Reset Menu -                                           00:06:29:CB:50:00

Unit ID ... <1>


Reset VLAN Configuration to Default .......... <No >










Press Space Bar to select <Yes> then select APPLY to reset VLAN configuration.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

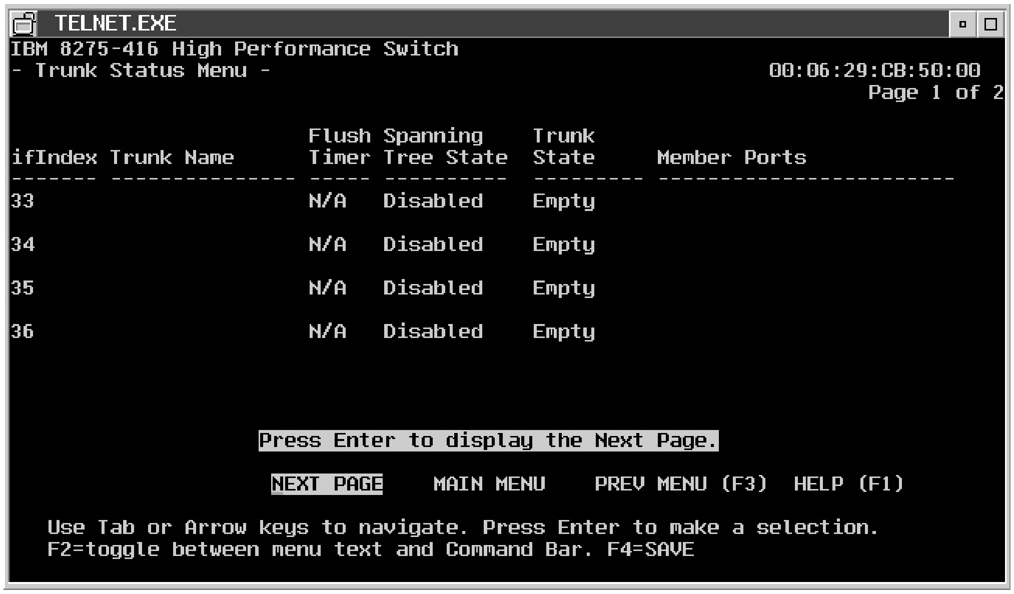
Figure 40. VLAN reset

Trunk management menu

Link aggregation, also called trunking, allows multiple 802.3 MAC interfaces to be grouped together logically to appear as one super-link. The super-link or Link Aggregation Group (LAG) has access to the combined bandwidth of all links. Link aggregation also provides automatic, point-to-point redundancy between two devices (switch-to-switch). Each link in the trunk must be running at the same link speed and in full-duplex mode (half-duplex mode is not supported).

Configuring a trunk

To configure (or create) a trunk, select **Device Configuration** on the Main Menu, then select **Trunk Management**. The Trunk Status Menu (Figure 41 on page 59) is displayed; it consist of two panels; Page 1 of 2 and Page 2 of 2. You can define up to four trunks on each of these panels for a total of 8 trunks. To Configure a trunk, complete the configuration information on the Trunk Status Menu, then move the cursor to the ifIndex field, press Enter, and the Configure Trunk Menu (Figure 42 on page 60) is displayed. Complete the configuration information on the Configure Trunk Menu.



```
IBM 8275-416 High Performance Switch
- Trunk Status Menu -                                   00:06:29:CB:50:00
                                                               Page 1 of 2

                        Flush Spanning    Trunk
ifIndex Trunk Name      Timer Tree State  State     Member Ports
------- --------------- ----- ----------  --------- -----------------------
33                      N/A   Disabled    Empty

34                      N/A   Disabled    Empty

35                      N/A   Disabled    Empty

36                      N/A   Disabled    Empty



                    Press Enter to display the Next Page.

                     NEXT PAGE    MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 41. Trunk status menu

ifIndex
Trunk interface number (ifIndex) values are fixed at 33 to 40. The interface number is assigned by the switch and in a range above the numbers of the ports (for example, ifIndex 33 to 36 is shown on panel 1of 2, and 37 to 40 is shown on panel 2 of 2). This field is not configurable.

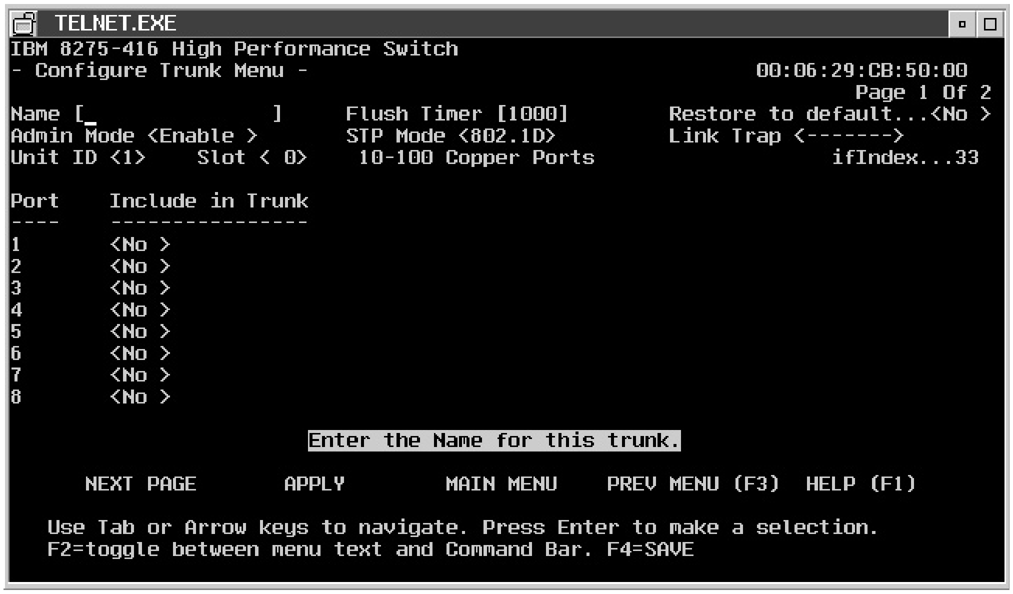
Trunk Name
Defines the unique name for the trunk. You can use up to 15 alphanumeric characters. There is no default trunk name.

Flush Timer
Specifies the time that all trunk ports will be disabled during trunk transitions. This is done to ensure that frames are not misordered when flows are re-assigned to new ports. “N/A” indicates the trunk is not configured. The range of values is 100 to 4000 milliseconds (0.1 second to 4 seconds). The default is 1000 milliseconds (1 second).

Spanning Tree State
Specifies that spanning tree is either Enabled or Disabled for the trunk.

Trunk State
Specifies whether the trunk is Empty, LinkUp, or LinkDown. Empty indicates the trunk is not configured.

Member Ports
Defines the port numbers associated with a specific trunk.



```
TELNET.EXE
IBM 8275-416 High Performance Switch
- Configure Trunk Menu -                                     00:06:29:CB:50:00
                                                                     Page 1 Of 2
Name [_             ]     Flush Timer [1000]        Restore to default...<No >
Admin Mode <Enable >      STP Mode <802.1D>         Link Trap <------->
Unit ID <1>    Slot < 0>    10-100 Copper Ports                  ifIndex...33

Port    Include in Trunk
----    ----------------
1       <No >
2       <No >
3       <No >
4       <No >
5       <No >
6       <No >
7       <No >
8       <No >

                        Enter the Name for this trunk.

      NEXT PAGE       APPLY        MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 42. Configure trunk menu

Name Defines the unique name for the trunk. You can use up to 15 alphanumeric characters. There is no default trunk name.

Flush Timer
This value should match your network hold-time (that is, the time that the switch holds a frame before forwarding or discarding it). The range is 100 to 4000 milliseconds (0.1 second to 4 seconds). The default is 1000 milliseconds (1 second).

Restore to Default
You can select yes or no. The default is No.

Admin Mode
Indicates whether the trunk group is Enabled or Disabled. The default is Enable.

STP Mode
This is the value specified for STP Mode on the Port Configuration Menu. It specifies the spanning tree protocol (STP) mode for the port; values are:

- 802.1D: the default
- Fast: indicates fast STP mode for this port
- Off: indicates STP is turned off for this port

Link Trap
Indicates whether link traps are Enabled or Disabled; Enable is the default.

Port This field is not configurable. For Slot 0, indicates the number of the port (ports 1 to 8 are listed on the first panel (page 1 of 2) and ports 9 to 16 are listed on the second panel (page 2 of 2)). For Slots 1 and 2, indicates the number of the port (ports 1 and 2, 1 to 4, or 1 to 8 are listed on the first panel) if the feature module is installed.

Include in Trunk
Indicates whether the port is included in trunk. You can specify No or Yes; No is the default.

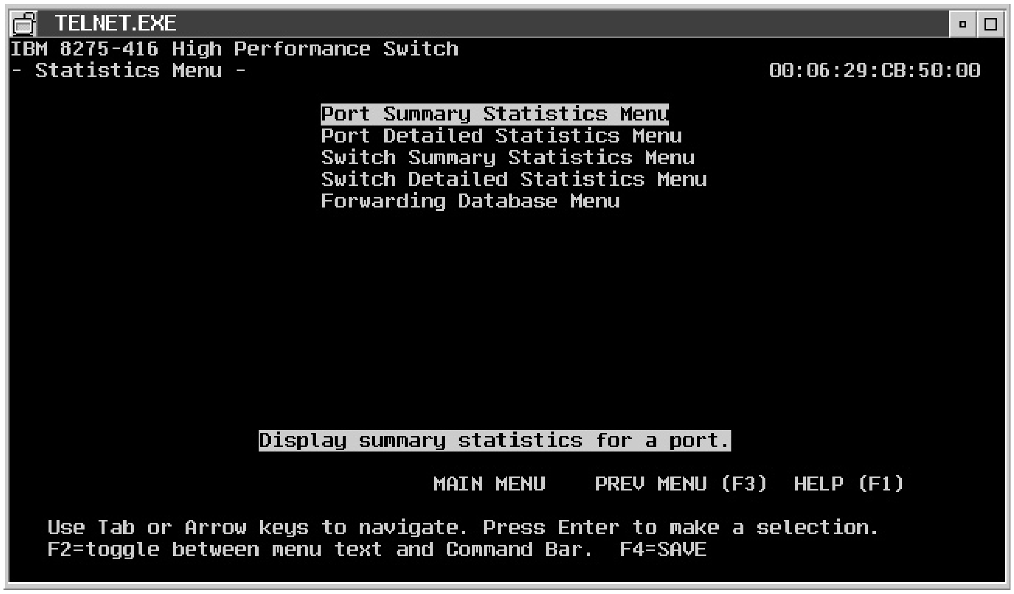
Statistics

To access statistics, select **Statistics Menu** on the Main Menu. Traffic statistics are kept by port. Details and summaries of packets broadcast, transmitted, and switched, as well as error packets and discarded packets are the types of statistics kept for your switch.

Figure 43 shows the types of statistics that you can select to view from the Statistics Menu.

After making your selection, the panels containing statistics will refresh every few seconds. All counters may not update every few seconds. Even though the refresh rate is every few seconds, some counters will not change. For example, the Self-Learning Statistics counters update on an as needed basis whenever a host gets updated.

Note: A description for each statistic may be obtained by pressing Help on the associated Web statistics panel.

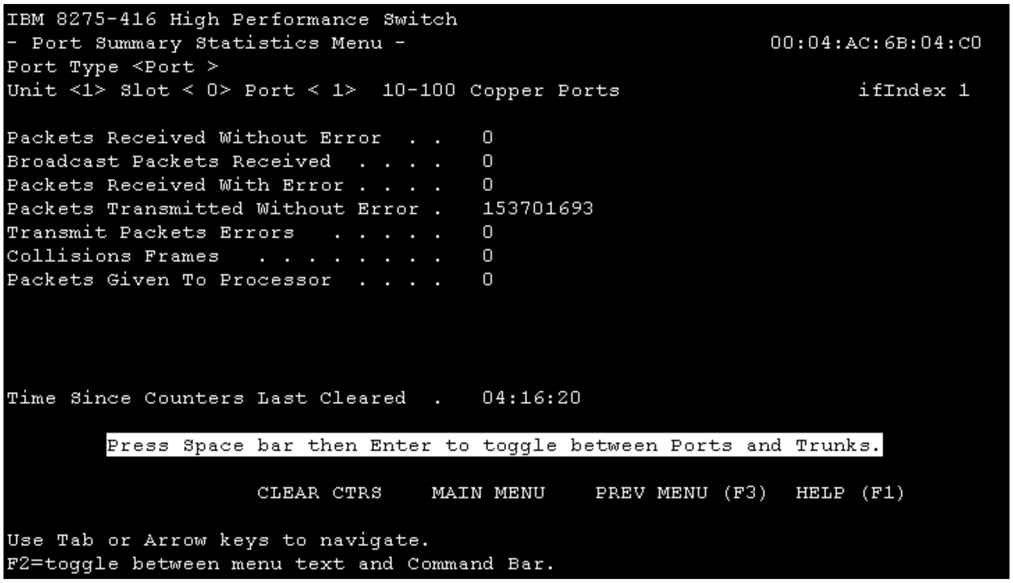


```
IBM 8275-416 High Performance Switch
- Statistics Menu -                                           00:06:29:CB:50:00

                         Port Summary Statistics Menu
                         Port Detailed Statistics Menu
                         Switch Summary Statistics Menu
                         Switch Detailed Statistics Menu
                         Forwarding Database Menu

                    Display summary statistics for a port.

                                  MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 43. Statistics Menu

Port summary statistics

To view a summary of port statistics, select **Port Summary Statistics Menu** from the Statistics Menu. See Figure 44 on page 62 for a summary of port statistics that are collected.

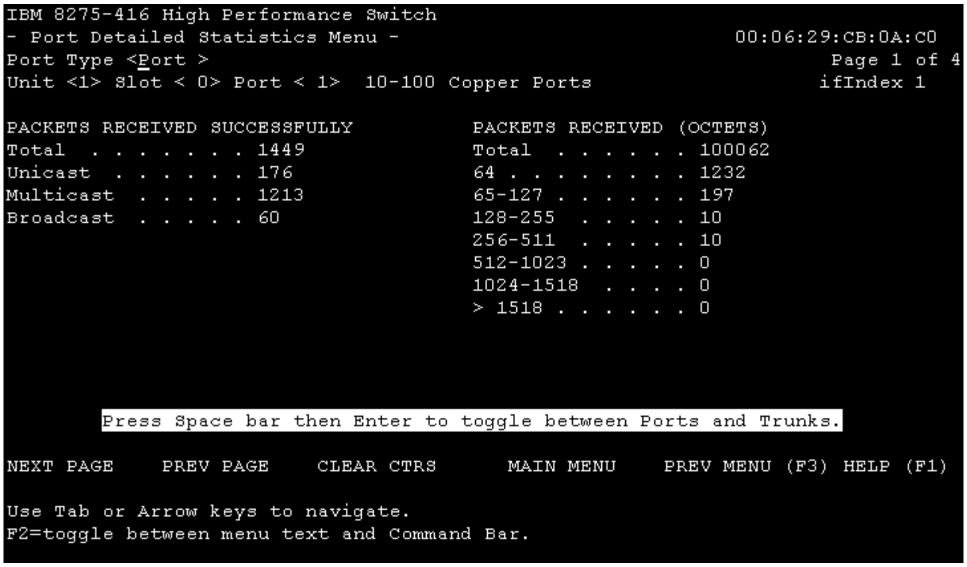


```
IBM 8275-416 High Performance Switch
- Port Summary Statistics Menu -                           00:04:AC:6B:04:C0
Port Type <Port >
Unit <1> Slot < 0> Port < 1>  10-100 Copper Ports                 ifIndex 1

Packets Received Without Error  . .   0
Broadcast Packets Received  . . . .   0
Packets Received With Error . . . .   0
Packets Transmitted Without Error .   153701693
Transmit Packets Errors   . . . . .   0
Collisions Frames   . . . . . . . .   0
Packets Given To Processor  . . . .   0




Time Since Counters Last Cleared  .   04:16:20

        Press Space bar then Enter to toggle between Ports and Trunks.

                    CLEAR CTRS    MAIN MENU    PREV MENU (F3)  HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 44. Port summary statistics

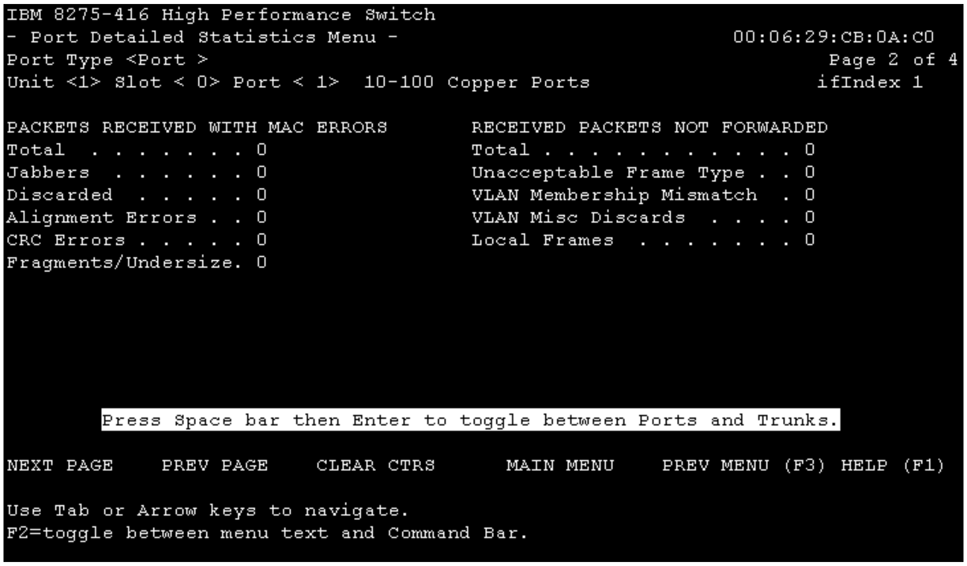
Port detailed statistics

To view detailed port statistics, select **Port Detailed Statistics Menu** from the Statistics Menu. Detailed port statistics can be viewed on four consecutive panels (Figure 45, Figure 46 on page 63, Figure 47 on page 63, and Figure 48 on page 64). To view the next panel, move the cursor to NEXT PAGE (at the bottom of each panel) and press Enter.



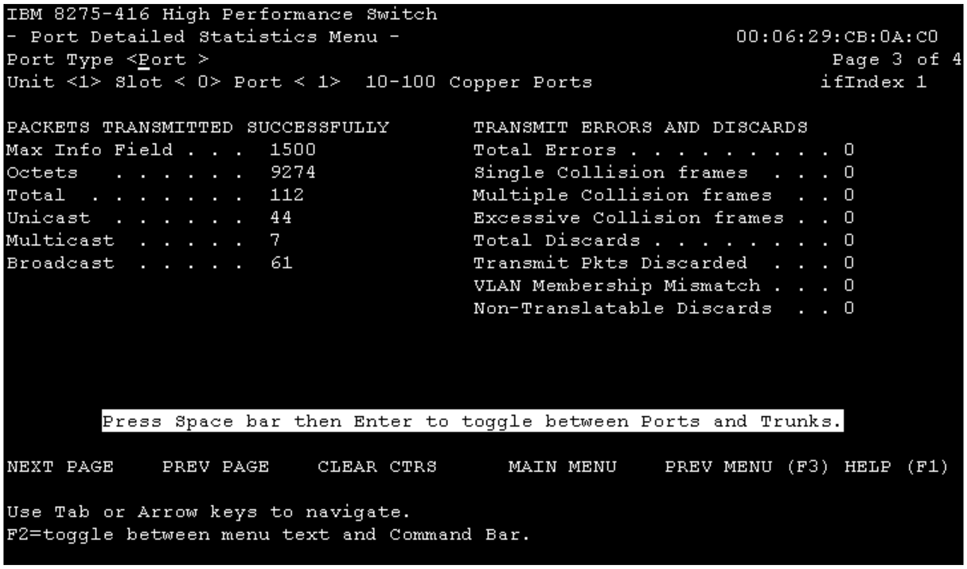
```
IBM 8275-416 High Performance Switch
- Port Detailed Statistics Menu -                        00:06:29:CB:0A:C0
Port Type <Port >                                                Page 1 of 4
Unit <1> Slot < 0> Port < 1>  10-100 Copper Ports               ifIndex 1

PACKETS RECEIVED SUCCESSFULLY          PACKETS RECEIVED (OCTETS)
Total  . . . . . . . 1449              Total  . . . . . . 100062
Unicast  . . . . . . 176               64 . . . . . . . . 1232
Multicast  . . . . . 1213              65-127 . . . . . . 197
Broadcast  . . . . . 60                128-255  . . . . . 10
                                       256-511  . . . . . 10
                                       512-1023 . . . . . 0
                                       1024-1518  . . . . 0
                                       > 1518 . . . . . . 0



        Press Space bar then Enter to toggle between Ports and Trunks.

NEXT PAGE    PREV PAGE    CLEAR CTRS      MAIN MENU    PREV MENU (F3) HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 45. Port detailed statistics (Page 1 of 4)



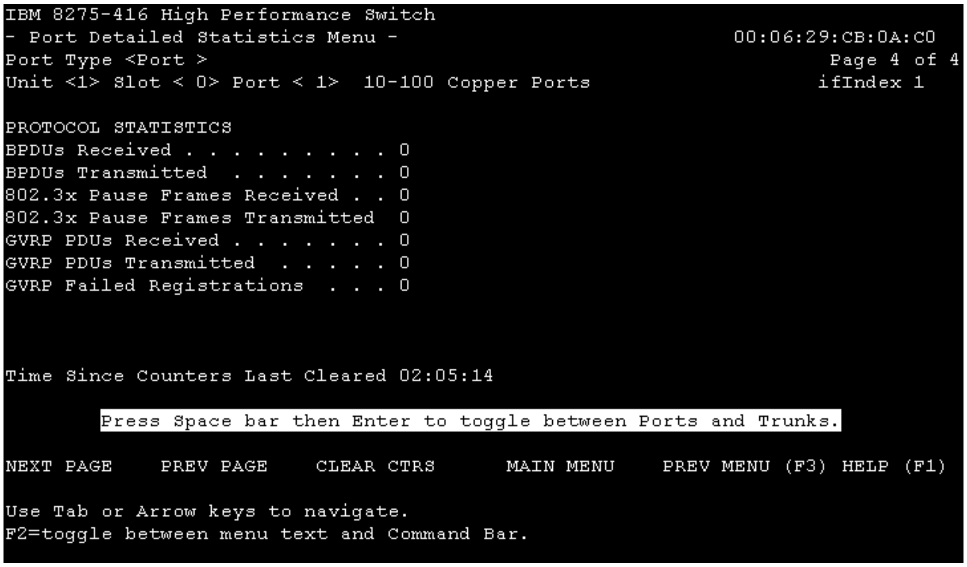
```
IBM 8275-416 High Performance Switch
- Port Detailed Statistics Menu -                            00:06:29:CB:0A:C0
Port Type <Port >                                                    Page 2 of 4
Unit <1> Slot < 0> Port < 1>  10-100 Copper Ports                   ifIndex 1

PACKETS RECEIVED WITH MAC ERRORS       RECEIVED PACKETS NOT FORWARDED
Total  . . . . . . . 0                 Total . . . . . . . . . . . 0
Jabbers  . . . . . . 0                 Unacceptable Frame Type . . 0
Discarded  . . . . . 0                 VLAN Membership Mismatch  . 0
Alignment Errors . . 0                 VLAN Misc Discards  . . . . 0
CRC Errors . . . . . 0                 Local Frames  . . . . . . . 0
Fragments/Undersize. 0




        Press Space bar then Enter to toggle between Ports and Trunks.

NEXT PAGE    PREV PAGE    CLEAR CTRS      MAIN MENU    PREV MENU (F3) HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 46. Port detailed statistics (Page 2 of 4)



```
IBM 8275-416 High Performance Switch
- Port Detailed Statistics Menu -                            00:06:29:CB:0A:C0
Port Type <Port >                                                    Page 3 of 4
Unit <1> Slot < 0> Port < 1>  10-100 Copper Ports                   ifIndex 1

PACKETS TRANSMITTED SUCCESSFULLY       TRANSMIT ERRORS AND DISCARDS
Max Info Field . . .  1500             Total Errors . . . . . . . . . 0
Octets   . . . . . .  9274             Single Collision frames  . . . 0
Total  . . . . . . .  112              Multiple Collision frames  . . 0
Unicast  . . . . . .  44               Excessive Collision frames . . 0
Multicast  . . . . .  7                Total Discards . . . . . . . . 0
Broadcast  . . . . .  61               Transmit Pkts Discarded  . . . 0
                                       VLAN Membership Mismatch . . . 0
                                       Non-Translatable Discards  . . 0



        Press Space bar then Enter to toggle between Ports and Trunks.

NEXT PAGE    PREV PAGE    CLEAR CTRS      MAIN MENU    PREV MENU (F3) HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 47. Port detailed statistics (Page 3 of 4)

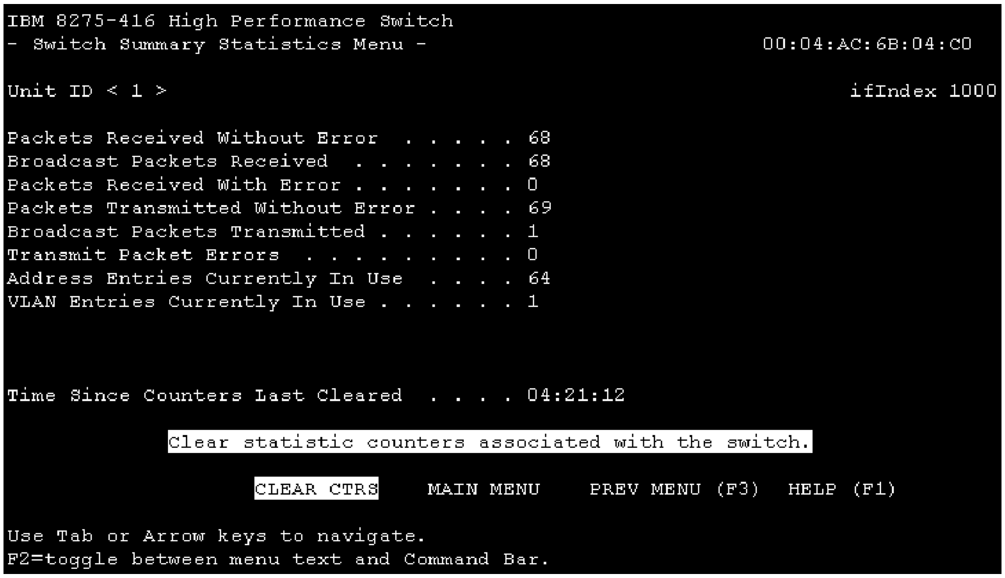


```
IBM 8275-416 High Performance Switch
- Port Detailed Statistics Menu -                          00:06:29:CB:0A:C0
Port Type <Port >                                                  Page 4 of 4
Unit <1> Slot < 0> Port < 1>  10-100 Copper Ports                   ifIndex 1

PROTOCOL STATISTICS
BPDUs Received . . . . . . . . . 0
BPDUs Transmitted  . . . . . . . 0
802.3x Pause Frames Received . . 0
802.3x Pause Frames Transmitted  0
GVRP PDUs Received . . . . . . . 0
GVRP PDUs Transmitted  . . . . . 0
GVRP Failed Registrations  . . . 0



Time Since Counters Last Cleared 02:05:14

        Press Space bar then Enter to toggle between Ports and Trunks.

NEXT PAGE    PREV PAGE    CLEAR CTRS      MAIN MENU    PREV MENU (F3) HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 48. Port detailed statistics (Page 4 of 4)

Switch summary statistics

To view a summary of switch statistics, select **Switch Summary Statistics Menu** from the Statistics Menu. See Figure 49 for a summary of the switch statistics that are collected.



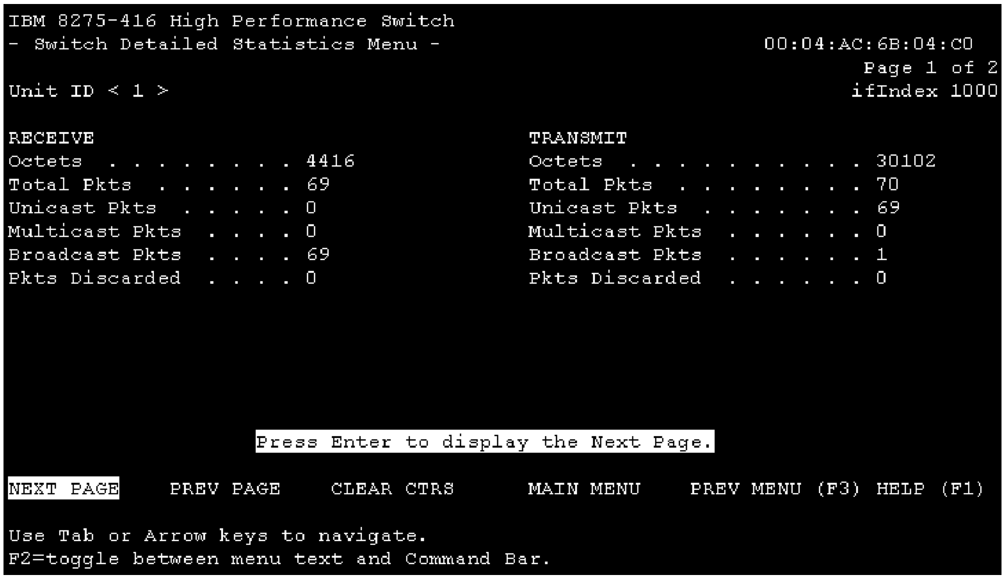
```
IBM 8275-416 High Performance Switch
- Switch Summary Statistics Menu -                            00:04:AC:6B:04:C0

Unit ID < 1 >                                                       ifIndex 1000

Packets Received Without Error  . . . . . 68
Broadcast Packets Received  . . . . . . . 68
Packets Received With Error . . . . . . . 0
Packets Transmitted Without Error . . . . 69
Broadcast Packets Transmitted . . . . . . 1
Transmit Packet Errors  . . . . . . . . . 0
Address Entries Currently In Use  . . . . 64
VLAN Entries Currently In Use . . . . . . 1



Time Since Counters Last Cleared  . . . . 04:21:12

             Clear statistic counters associated with the switch.

                    CLEAR CTRS    MAIN MENU    PREV MENU (F3)  HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 49. Switch summary statistics

Switch detailed statistics

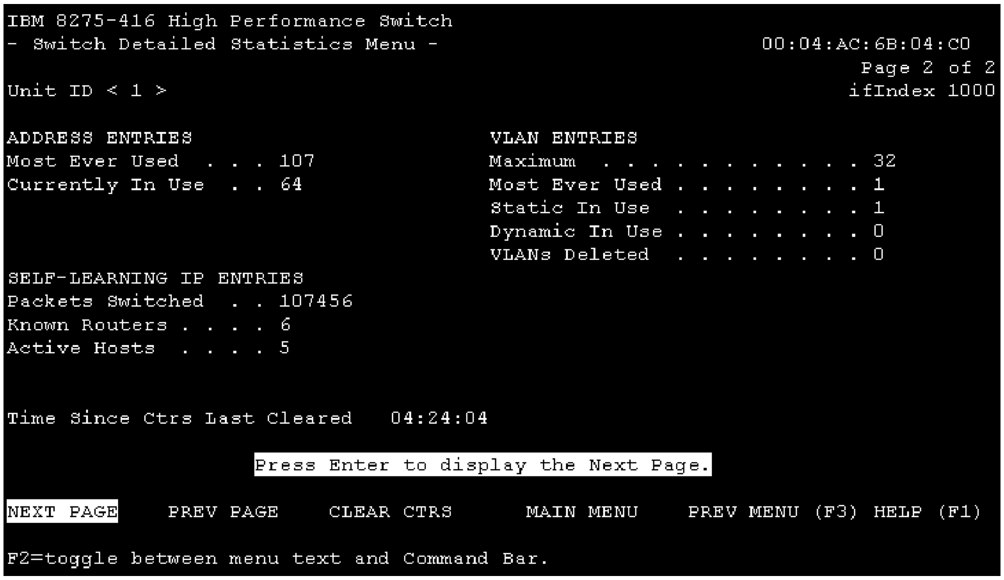
To view detailed switch statistics, select **Switch Detailed Statistics Menu** (Page 1 of 2) from the Statistics Menu. See Figure 50 on page 65 for the detailed switch statistics that are collected.

To view Self Learning IP statistics, select **Switch Detailed Statistics Menu** (Page 2 of 2) from the Statistics Menu. See Figure 51 for an example of the statistics that are collected for Self Learning IP.



```
IBM 8275-416 High Performance Switch
- Switch Detailed Statistics Menu -                        00:04:AC:6B:04:C0
                                                                 Page 1 of 2
Unit ID < 1 >                                                   ifIndex 1000

RECEIVE                                   TRANSMIT
Octets  . . . . . . . . 4416              Octets  . . . . . . . . . . 30102
Total Pkts  . . . . . . 69                Total Pkts  . . . . . . . . 70
Unicast Pkts  . . . . . 0                 Unicast Pkts  . . . . . . . 69
Multicast Pkts  . . . . 0                 Multicast Pkts  . . . . . . 0
Broadcast Pkts  . . . . 69                Broadcast Pkts  . . . . . . 1
Pkts Discarded  . . . . 0                 Pkts Discarded  . . . . . . 0




                    Press Enter to display the Next Page.

NEXT PAGE    PREV PAGE    CLEAR CTRS      MAIN MENU    PREV MENU (F3) HELP (F1)

Use Tab or Arrow keys to navigate.
F2=toggle between menu text and Command Bar.
```

Figure 50. Switch detailed statistics



```
IBM 8275-416 High Performance Switch
- Switch Detailed Statistics Menu -                        00:04:AC:6B:04:C0
                                                                 Page 2 of 2
Unit ID < 1 >                                                   ifIndex 1000

ADDRESS ENTRIES                        VLAN ENTRIES
Most Ever Used  . . . 107              Maximum  . . . . . . . . . . . 32
Currently In Use  . . 64               Most Ever Used . . . . . . . . 1
                                       Static In Use  . . . . . . . . 1
                                       Dynamic In Use . . . . . . . . 0
                                       VLANs Deleted  . . . . . . . . 0
SELF-LEARNING IP ENTRIES
Packets Switched  . . 107456
Known Routers . . . . 6
Active Hosts  . . . . 5


Time Since Ctrs Last Cleared   04:24:04

                    Press Enter to display the Next Page.

NEXT PAGE    PREV PAGE    CLEAR CTRS      MAIN MENU    PREV MENU (F3) HELP (F1)

F2=toggle between menu text and Command Bar.
```

Figure 51. Self Learning IP statistics

Packets switched
8-byte value containing the total number of packets directly switched by the self-learning IP function since it was enabled. The count is all inclusive for the switch, regardless of the routers or hosts involved. The value starts at 0 whenever the function is enabled and continues to increment until you reset the function or the switch.

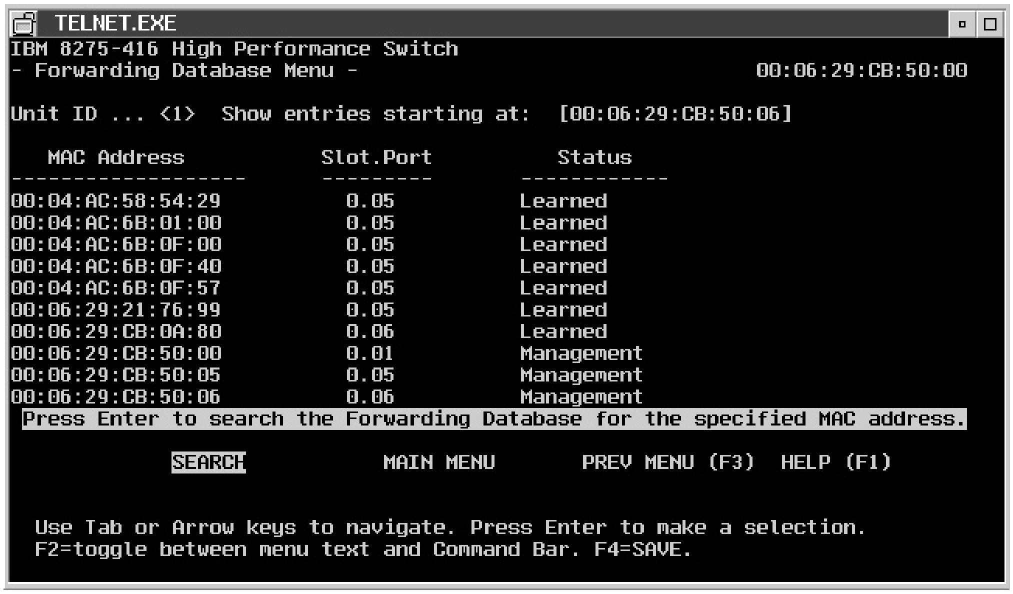
Known routers
Current number of known routers identified by the self-learning IP function

since it was enabled. You cannot clear this counter. The value starts at 0 when the function is enabled and changes over time as routers are learned and age-out.

Active Hosts
Current number of hosts (IP addresses) identified by the self-learning IP function since it was last enabled. You cannot clear this counter. The value starts at 0 when the function is enabled and changes over time as hosts are learned and age out, reflecting the dynamic nature of host traffic as it traverses the switch.

Forwarding database information

To view forwarding database information, select **Forwarding Database Menu** from the Statistics Menu. See Figure 52 for the forwarding database information.

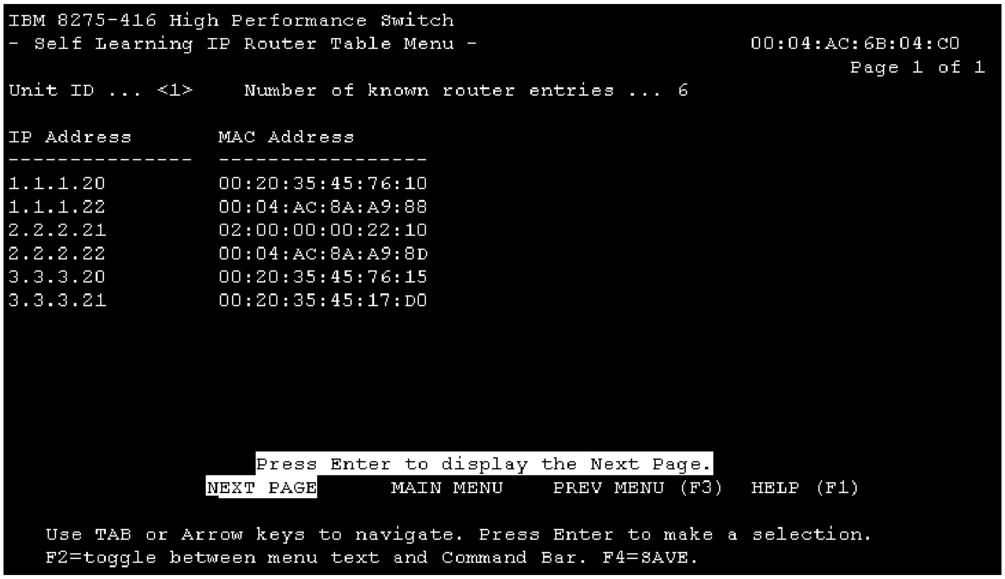


```
IBM 8275-416 High Performance Switch
- Forwarding Database Menu -                              00:06:29:CB:50:00

Unit ID ... <1>  Show entries starting at:  [00:06:29:CB:50:06]

   MAC Address           Slot.Port          Status
-------------------      ---------       ------------
00:04:AC:58:54:29          0.05          Learned
00:04:AC:6B:01:00          0.05          Learned
00:04:AC:6B:0F:00          0.05          Learned
00:04:AC:6B:0F:40          0.05          Learned
00:04:AC:6B:0F:57          0.05          Learned
00:06:29:21:76:99          0.05          Learned
00:06:29:CB:0A:80          0.06          Learned
00:06:29:CB:50:00          0.01          Management
00:06:29:CB:50:05          0.05          Management
00:06:29:CB:50:06          0.06          Management
 Press Enter to search the Forwarding Database for the specified MAC address.

             SEARCH           MAIN MENU       PREV MENU (F3)  HELP (F1)


  Use Tab or Arrow keys to navigate. Press Enter to make a selection.
  F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 52. Forwarding database information

Self Learning IP router table menu

To view statistics about known routers whenever the Self Learning IP function is enabled, select **Statistics Menu** from the Main Menu, then select **Self Learning IP Router Table Menu**. See Figure 53 on page 67 for the router statistics.



```
IBM 8275-416 High Performance Switch
- Self Learning IP Router Table Menu -                       00:04:AC:6B:04:C0
                                                                   Page 1 of 1
Unit ID ... <1>    Number of known router entries ... 6

IP Address        MAC Address
---------------   -----------------
1.1.1.20          00:20:35:45:76:10
1.1.1.22          00:04:AC:8A:A9:88
2.2.2.21          02:00:00:00:22:10
2.2.2.22          00:04:AC:8A:A9:8D
3.3.3.20          00:20:35:45:76:15
3.3.3.21          00:20:35:45:17:D0






                    Press Enter to display the Next Page.
                NEXT PAGE      MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use TAB or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 53. Self Learning IP router table menu

The description of the information collected is:

Number of known router entries
Current number of known routers identified by the Self Learning IP function since it was enabled. This is the same value that is found on the Switch Detailed Statistics Menu.

IP Address
The IP address of the router.

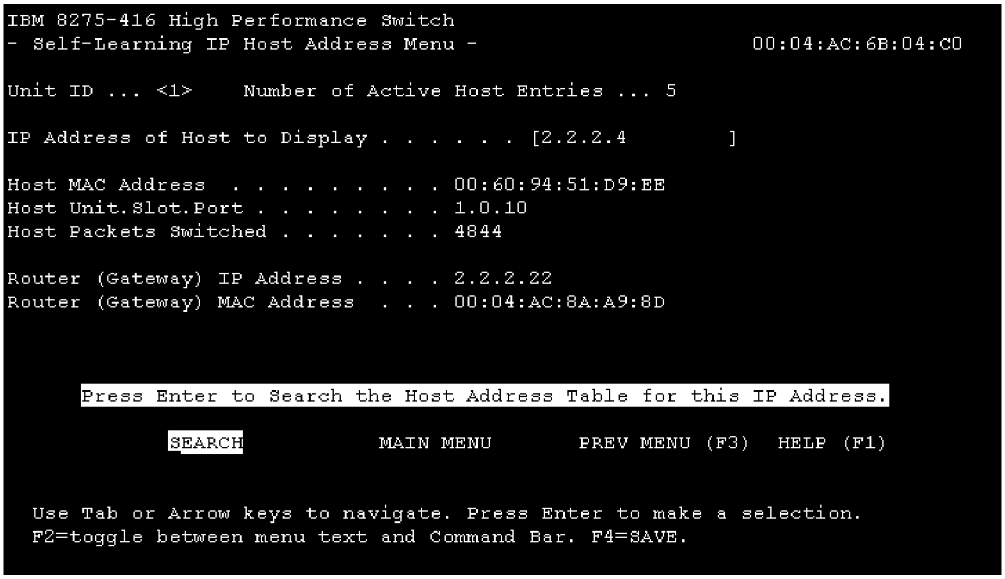
MAC Address
The MAC address of the router.

Notes:

1. The table is displayed in the order of increasing IP addresses.
2. The table can contain up to 32 entries, with up to 11 entries per page; up to 3 pages.
3. Only the number of pages that contain data are displayed.

Self Learning IP host address menu

To view information about IP host addresses that are collected when the Self Learning IP function is enabled, select **Statistics Menu** from the Main Menu, then select **Self Learning IP Host Address Menu**. See Figure 54 on page 68 for the host IP statistics.



```
IBM 8275-416 High Performance Switch
- Self-Learning IP Host Address Menu -                    00:04:AC:6B:04:C0

Unit ID ... <1>    Number of Active Host Entries ... 5

IP Address of Host to Display . . . . . . [2.2.2.4        ]

Host MAC Address  . . . . . . . . . 00:60:94:51:D9:EE
Host Unit.Slot.Port . . . . . . . . 1.0.10
Host Packets Switched . . . . . . . 4844

Router (Gateway) IP Address . . . . 2.2.2.22
Router (Gateway) MAC Address  . . . 00:04:AC:8A:A9:8D



      Press Enter to Search the Host Address Table for this IP Address.

             SEARCH          MAIN MENU       PREV MENU (F3)  HELP (F1)


  Use Tab or Arrow keys to navigate. Press Enter to make a selection.
  F2=toggle between menu text and Command Bar. F4=SAVE.
```

Figure 54. Self Learning IP host address menu

Number of active host entries
Current number of hosts (IP addresses) identified by the Self Learning IP function since it was last enabled. This is the same value that is displayed on the Switch Detailed Statistics Menu.

IP Address of Host to Display
You specify the IP address of the host for which you want to view information.

Host MAC Address
MAC address associated with the host’s IP address.

Host Unit.Slot.Port
Unit, slot, and port number for this host. If the port is part a trunk, then this line is labeled “Trunk ifIndex” and the value is the ifIndex for this trunk.

Host Packets Switched
The number of IP packets destined for this host’s IP address that were switched directly to this host address, bypassing the router, since the host was last learned by the self-learning IP function.

Router (Gateway) IP Address
The IP address of the router to which this host communicates when sending IP traffic to a different subnet (as viewed by the self-learning IP function).

Router (Gateway) MAC Address
The MAC address of the router to which this host communicates when sending IP traffic to a different subnet (as viewed by the self-leaning IP function).

Notes:

1. When the panel is first displayed, the lines for the Host MAC Address, Router MAC Address, Host Unit.Slot.Port, and Host Packets Switched are blank. After the IP Address is entered and Apply is selected, these lines appear.
2. If the specified Host IP address is not found, the message “Information for <IP address> is not available” where <IP address> is the value that was entered for “IP Address of Host to Display”.

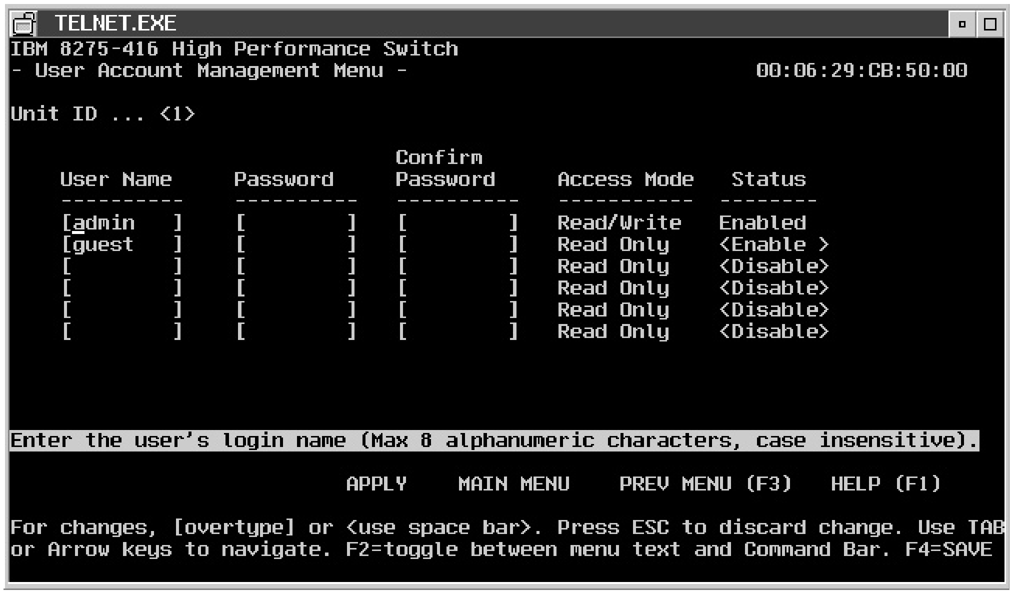
3. The latest value for the Host Packets Switched count is shown whenever the host information is displayed or manually refreshed. Changes in the count value are also reflected in the Packets Switched value on the Switch Detailed Statistics Menu.

User account management

On the Main Menu, select **User Account Management Menu** to use the functions for managing user accounts.

Defining user accounts

On the User Account Management Menu, select User Accounts Menu. Figure 55 shows the User Accounts Menu where you specify user names, passwords, and access mode.



```
IBM 8275-416 High Performance Switch
- User Account Management Menu -                              00:06:29:CB:50:00

Unit ID ... <1>

                          Confirm
    User Name     Password     Password     Access Mode    Status
    ----------    ----------   ----------   -----------    --------
    [admin   ]    [        ]   [        ]   Read/Write     Enabled
    [guest   ]    [        ]   [        ]   Read Only      <Enable >
    [        ]    [        ]   [        ]   Read Only      <Disable>
    [        ]    [        ]   [        ]   Read Only      <Disable>
    [        ]    [        ]   [        ]   Read Only      <Disable>
    [        ]    [        ]   [        ]   Read Only      <Disable>



Enter the user's login name (Max 8 alphanumeric characters, case insensitive).

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 55. User account management

The switch allows you to add and delete users and set user passwords for the switch. You are to provide the following information:

User Name
User name can be up to eight alphanumeric characters and is not case sensitive. Up to six user names (accounts) can be defined; one with read/write access mode and five with read only access mode.

Password
The password can be up to eight alphanumeric characters and is not case sensitive. A blank password indicates no password. The default value is blank.

Confirm Password
The confirm password can be up to eight alphanumeric characters and is not case sensitive. You should use the same password as defined in the Password field. A blank confirm password indicates no password. The default value is blank.

Access Mode
This value is not configurable. User access mode can be:

Read/Write
Only one user can be defined with read/write access mode per switch. This user can change the status of other users, add and delete users, change passwords and change configurations, and use system utilities.

Read Only
Up to five users can be defined with read only access mode per

switch. When Read only users are logged in, the message READONLY appears at the top right corner of all panels.

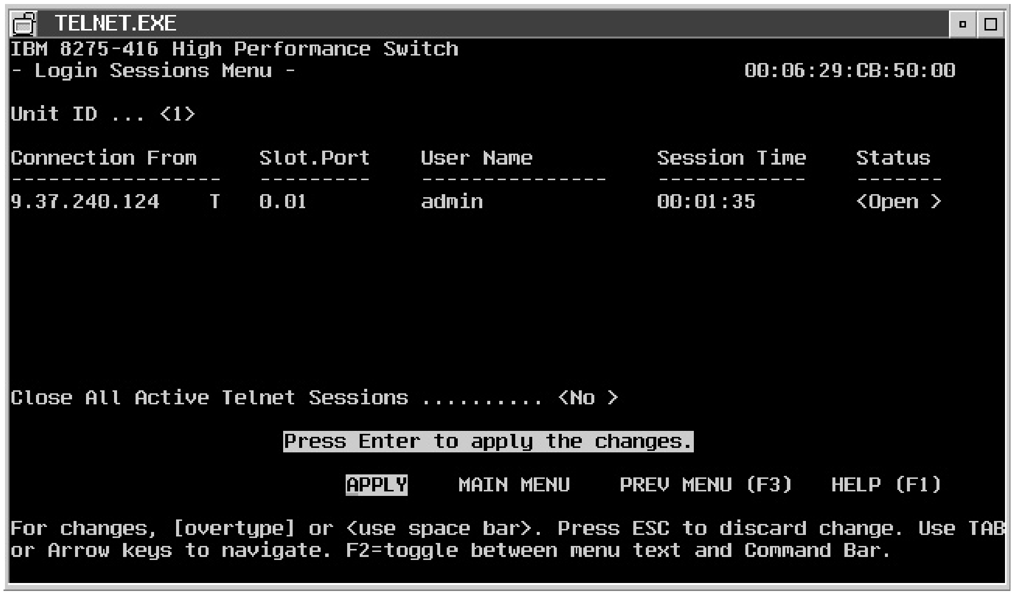
A user with read only access is restricted from accessing the SNMP Community Configuration menu, SNMP Trap Receiver Configuration menu, User Account Management menu, and System Utilities menu. When a read only user tries to modify a configuration parameter on a menu, the data is not accepted and is not processed.

Status

Status applies to Read only user names; status can be Enable, Disable or Delete. Enable means that the user name is authorized to access the switch. Disable means that the user name is not allowed to access the switch. Delete means the user will be removed from the list upon an apply or save. The status of the read/write user name is always Enabled.

Managing login sessions

On the User Account Management Menus, select **Login Sessions Menu** (Figure 56), which allows you to close a single session or close all active Telnet sessions.



```
IBM 8275-416 High Performance Switch
- Login Sessions Menu -                                 00:06:29:CB:50:00

Unit ID ... <1>

Connection From     Slot.Port    User Name          Session Time    Status
-----------------   ---------    ---------------    ------------    -------
9.37.240.124    T   0.01         admin              00:01:35        <Open >







Close All Active Telnet Sessions .......... <No >

                      Press Enter to apply the changes.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar.
```

Figure 56. Login session management

These fields are read-only:

- Connection From (the letter “T” at the right of the IP address indicates that this is a Telnet session)
- Slot.Port
- User Name
- Session Time (the time shown indicates how long this session has been active)

These fields are configurable

Status

Specifies that the individual session is Open or Closed. Toggle to the selection (Open or Closed), press Enter, then Apply your selection.

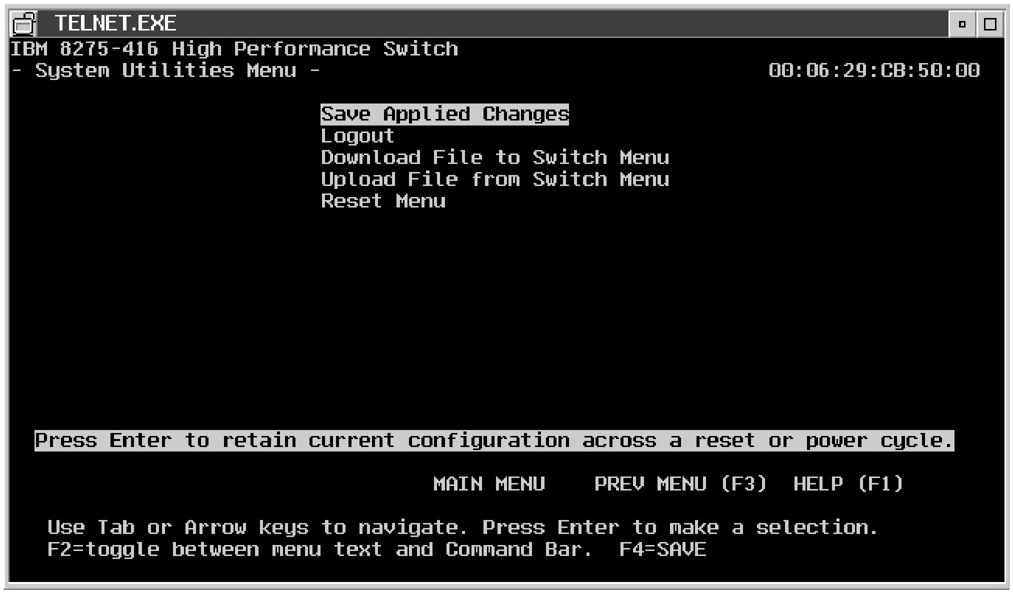
Close All Active Telnet Sessions
Specifies if all Telnet sessions are to be Closed or not. Toggle to the selection (Yes or No) , press Enter, then Apply your selection.

System utilities

The system utilities can be used only by users with read/write access. You can use the system utilities by selecting **System Utilities Menu** on the Main Menu. Figure 57 shows the available utilities.

Saving applied changes

To permanently save configuration changes either select **F4** to save or go to the System Utilities Menu and select **Save Applied Changes**, as shown in Figure 57.

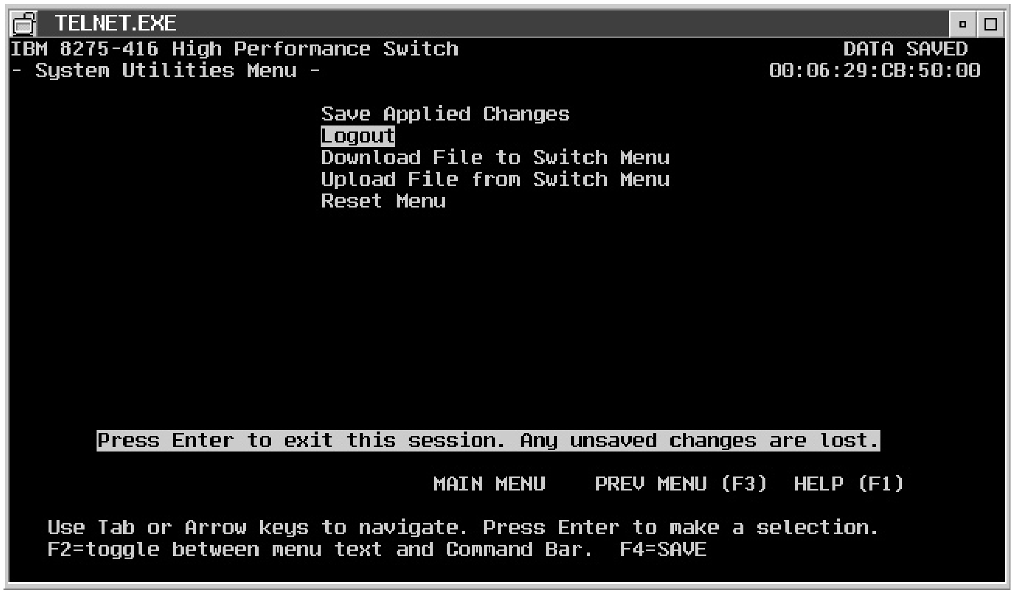


```
IBM 8275-416 High Performance Switch
- System Utilities Menu -                                        00:06:29:CB:50:00

                         Save Applied Changes
                         Logout
                         Download File to Switch Menu
                         Upload File from Switch Menu
                         Reset Menu

  Press Enter to retain current configuration across a reset or power cycle.

                                  MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 57. Save applied changes

Logging out

When you have finished using the terminal interface, ensure you have saved and applied all configuration changes before you log out. The terminal interface provides an orderly way to log out. One way is to use the **LOGOUT** command on the Main Menu. Another way to log out is to select **System Utilities Menu** from the Main menu, then select **Logout** as shown in Figure 58 on page 73.



```
TELNET.EXE
IBM 8275-416 High Performance Switch                                DATA SAVED
- System Utilities Menu -                                     00:06:29:CB:50:00

                         Save Applied Changes
                         Logout
                         Download File to Switch Menu
                         Upload File from Switch Menu
                         Reset Menu




       Press Enter to exit this session. Any unsaved changes are lost.

                                  MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 58. Logout utility

Handling files

To upload or download a file, select **System Utilities Menu** from the Main Menu. Then make the appropriate selection from the System Utilities Menu.

The switch can download or upload files. Downloading is the transfer of files from a remote server into the switch. Uploading is the transfer of files from the switch to a remote server.

You can retrieve configuration settings from the switch as a binary file and send a binary configuration file to the switch. This allows you to back up the configuration or to easily update the configuration of multiple switches. Additionally, you can provide a configuration file to IBM support personnel for problem determination.

The last-saved configuration used by the switch is retained after a code update or a reset.

The switch displays result messages to indicate the status of a file transfer. Table 11 and Table 12 on page 74 show the messages along with explanations for each.

Downloading code or configuration to the switch

Table 11. Messages - while downloading files

Message	Explanation
`TFTP in progress...`	The switch has initiated the file transfer with the TFTP server.
`Can't start...previous transfer is not complete yet!`	Another TFTP operation is still taking place. Only one TFTP operation can occur at a given time. This includes both download and upload operations. Wait until the previous operation completes.
`TFTP receive complete...storing in flash...`	For Code only: The file has been successfully transferred to the switch and passed all the verification tests. It is now being stored permanently in flash memory.

Table 11. Messages - while downloading files (continued)

Message	Explanation
`TFTP receive complete... updating configuration`	For Configuration only: The switch has received the file and will verify its integrity. The file will be stored in flash if it passes the integrity checks. The switch will reset itself after storing the file in order for the newly loaded configuration to take effect.
`File transfer operation completed successfully.`	The file has successfully been stored in flash. The switch must be reset now for the new code to become operational.
`File failed CRC check!`	The switch received the file, but detected a CRC error. Because the file is corrupted, it will not be stored in flash. Try obtaining another copy of the file.
`This file is not intended for this product!`	The switch received the file, but detected that the file was not meant for the switch. The file will not be stored in flash. If this is for a code update, obtain the correct software image from the IBM Web site. If this is for configuration, make sure that the configuration file originated from a 8275-416 switch.
`Failure while storing in flash!`	The switch successfully received the file, and began storing the image in flash; however, an error occurred during the process. For code only, the flash is most likely corrupt now and new code will have to be downloaded via the bootcode utility function. For configuration, retry the download. If the file transfer still fails, contact your IBM service representative.
`File transfer failed!`	A general error occurred. The most likely cause for this message is when the switch cannot complete the TFTP operation. This may happen if you have not entered the correct IP address for the TFTP server, or if an IP address has not been set up on the switch. Check to see if your IP addresses are configured correctly. Also, make sure that you can ping the TFTP server from the Ping Menu. This error could also occur if you entered an incorrect path or file name. Check to make sure these fields match the file location on the TFTP server.

Uploading trap log, error log, configuration or system trace from the switch

Table 12. Messages - while uploading files

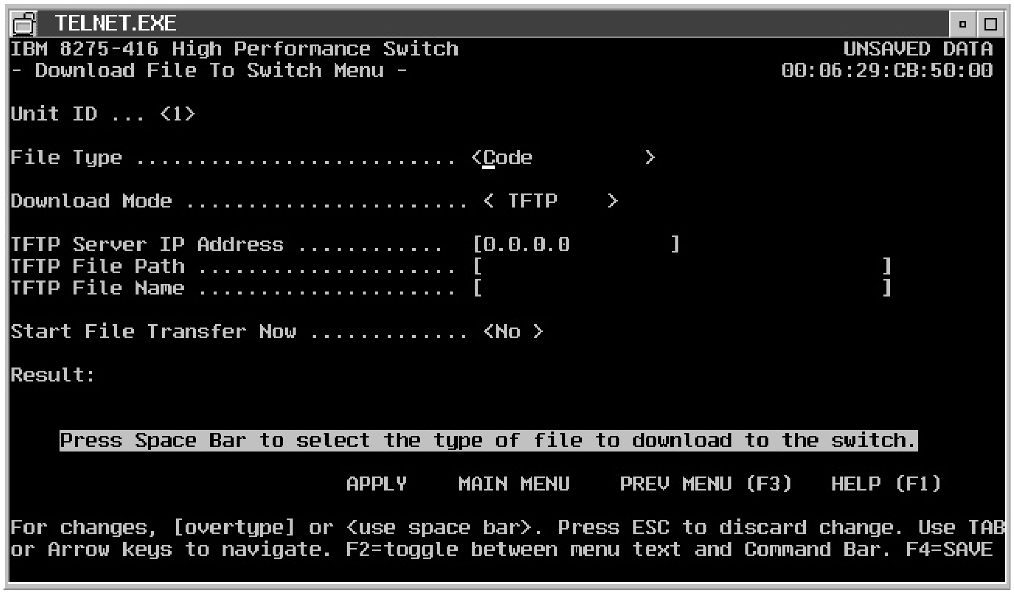
Message	Explanation
`TFTP in process...`	The switch has initiated the file transfer with the TFTP server.
`Can't start...previous transfer is not complete yet!`	Another TFTP operation is still taking place. Only one TFTP operation can occur at a given time. This includes both download and upload operations. Wait until the previous operation completes.
`Error while preparing file for transfer.`	Before uploading a file, the switch must prepare that file for transfer. This message means that there was a problem either in reading the information required for making the file, or there was a problem creating the file. Contact your IBM service representative.

Table 12. Messages - while uploading files (continued)

Message	Explanation
`File transfer failed!`	A general error occurred. The most likely cause of this message is when the switch cannot complete the TFTP operation. This may happen if you have not entered the correct IP address for the TFTP server, or if an IP address has not been set up on the switch. Check to see if your IP addresses are configured correctly. Also, make sure that you can ping the TFTP server from the Ping Menu. This error could also occur if you entered an incorrect path or file name. Check to make sure these fields match the file location on the TFTP server.
`File transfer completed successfully`	The switch successfully sent the file to the TFTP server.

Downloading a file to the switch

Downloading is the transfer of files from a remote server into the switch. The download operation is initiated by selecting **Download File to Switch Menu** on the System Utilities Menu (Figure 59). While the download is in process, you may see messages displayed. Table 11 on page 73 shows messages that can appear during the download process.

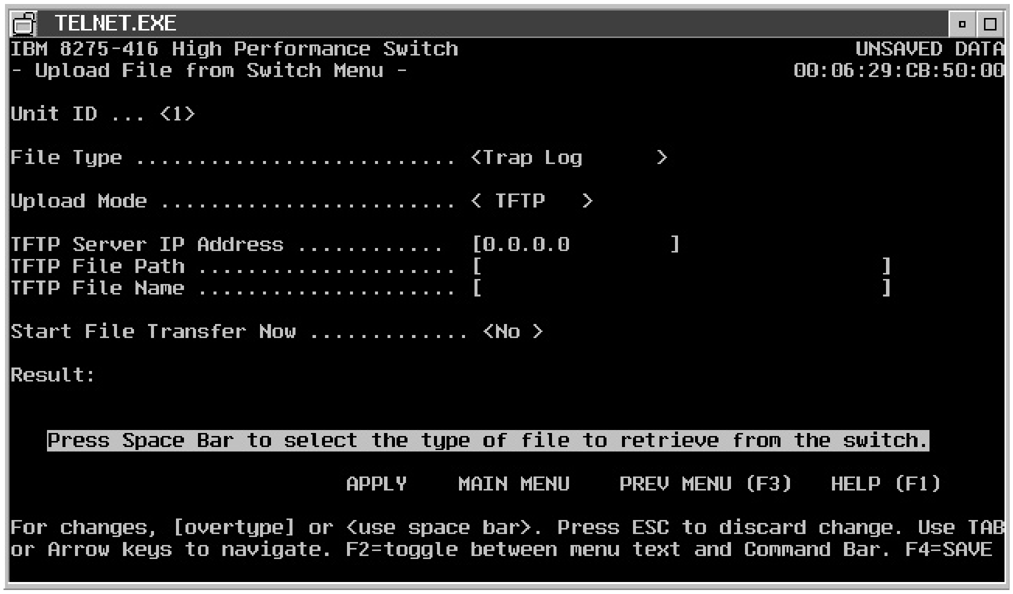


```
IBM 8275-416 High Performance Switch                            UNSAVED DATA
- Download File To Switch Menu -                             00:06:29:CB:50:00

Unit ID ... <1>

File Type ......................... <Code        >

Download Mode ...................... < TFTP    >

TFTP Server IP Address ...........  [0.0.0.0        ]
TFTP File Path .................... [                                ]
TFTP File Name .................... [                                ]

Start File Transfer Now ............ <No >

Result:


    Press Space Bar to select the type of file to download to the switch.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 59. Downloading a file to the switch

Uploading a file from the switch

Uploading is the transfer of files from the switch to a remote server (Figure 60 on page 76).



```
IBM 8275-416 High Performance Switch                              UNSAVED DATA
- Upload File from Switch Menu -                               00:06:29:CB:50:00

Unit ID ... <1>

File Type .......................... <Trap Log      >

Upload Mode ........................ < TFTP   >

TFTP Server IP Address ............  [0.0.0.0        ]
TFTP File Path ..................... [                                ]
TFTP File Name ..................... [                                ]

Start File Transfer Now ............. <No >

Result:


   Press Space Bar to select the type of file to retrieve from the switch.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 60. Uploading a file from the switch

The following parameters apply to uploading and downloading of files.

File Type
The file types are:

For Download
- Code (the default)
- Configuration

For Upload
- Configuration
- Error log
- System trace
- Trap log (the default)

Upload or Download Mode
The mode is either XMODEM or TFTP. XMODEM is valid only when the file transfer is initiated by the serial EIA 232 port. The default value is XMODEM.

Start Transfer Now
Enter Yes or No. The value is No whenever the panel is initially displayed.

File Name
The file name can be up to 16 alphanumeric characters. The switch remembers the last file name used. The default value is blank.

File path can be appended to the file name if the string is less than 17 characters. Otherwise, the File Path field will need to be used and the File Name will be appended to the File Path as is. An example would be File Path set to ***c:|tftp|code|*** and File Name set to ***e1r1v1.opr***.

Note: File Name, File Path, and TFTP Server IP Address are applicable only if the Transfer Mode is TFTP.

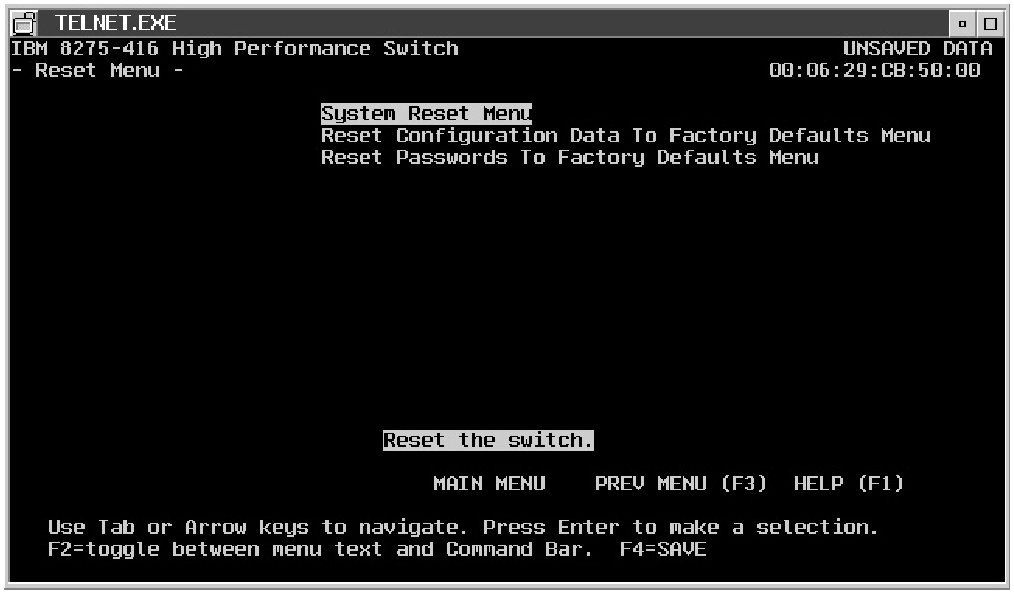
File Path
The directory path where the file is located or where it is to be uploaded to. The switch remembers the last file path used. The default value is blank.

TFTP Server IP Address
The IP address of the server where the file is located. It is valid only when the Transfer Mode is TFTP. The address is 4 decimal bytes ranging from 0 to 255. The default value is zeros.

Reset utility

You can reset the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted for confirmation if you want the reset to proceed. A successful reset is indicated by the LEDs on the switch.

After selecting Reset Menu from the System Utilities Menu, you are given the choice of the resets you can request as shown Figure 61.

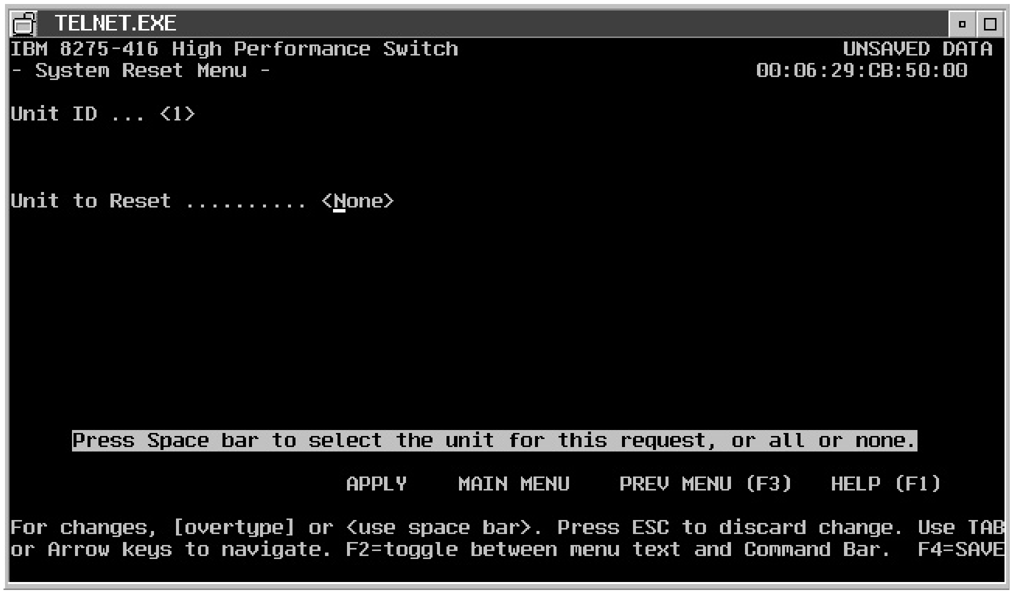


```
IBM 8275-416 High Performance Switch                             UNSAVED DATA
- Reset Menu -                                                00:06:29:CB:50:00

                         System Reset Menu
                         Reset Configuration Data To Factory Defaults Menu
                         Reset Passwords To Factory Defaults Menu








                              Reset the switch.

                                  MAIN MENU    PREV MENU (F3)  HELP (F1)

   Use Tab or Arrow keys to navigate. Press Enter to make a selection.
   F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 61. System Reset menu

System reset menu

Reset the system by indicating the particular unit as shown in Figure 62 on page 78. You must identify the switch to reset. *None* is the default.



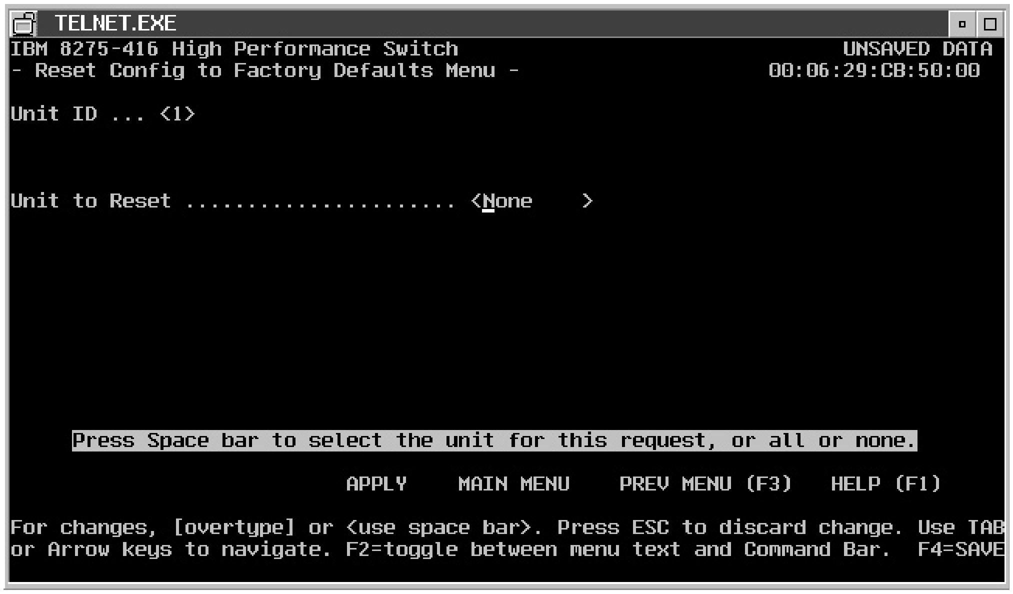
```
IBM 8275-416 High Performance Switch                              UNSAVED DATA
- System Reset Menu -                                        00:06:29:CB:50:00

Unit ID ... <1>


Unit to Reset .......... <None>









     Press Space bar to select the unit for this request, or all or none.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 62. System reset menu

Resetting configuration data to factory default values

You can reset the configuration to factory default values without powering off the switch. The factory defaults are not restored until the switch is reset. The switch is automatically reset when this command is processed. You are prompted to confirm that you want the reset to proceed.

Reset the configuration data to the factory defaults by indicating the particular unit as shown in Figure 63. You must identify the switch to reset. *None* is the default.



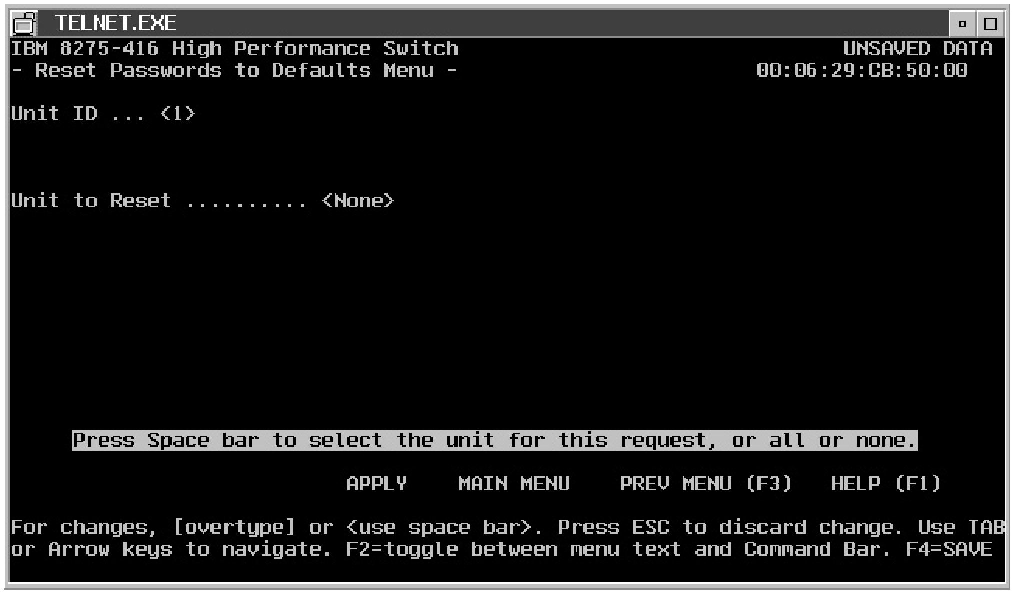
```
IBM 8275-416 High Performance Switch                              UNSAVED DATA
- Reset Config to Factory Defaults Menu -                     00:06:29:CB:50:00

Unit ID ... <1>


Unit to Reset ...................... <None    >









     Press Space bar to select the unit for this request, or all or none.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar.  F4=SAVE
```

Figure 63. Reset configuration data to factory defaults

Resetting passwords to factory default values

You can reset user passwords to factory default values without powering off the switch. The factory defaults are not restored until the switch is reset. The switch is automatically reset when this command is processed. You are prompted to confirm that you want the reset to proceed.

Reset the passwords by indicating the particular unit as shown in Figure 64. You must identify the switch to reset. None is the default.



```
TELNET.EXE
IBM 8275-416 High Performance Switch                             UNSAVED DATA
- Reset Passwords to Defaults Menu -                           00:06:29:CB:50:00

Unit ID ... <1>


Unit to Reset .......... <None>









     Press Space bar to select the unit for this request, or all or none.

                           APPLY    MAIN MENU    PREV MENU (F3)   HELP (F1)

For changes, [overtype] or <use space bar>. Press ESC to discard change. Use TAB
or Arrow keys to navigate. F2=toggle between menu text and Command Bar. F4=SAVE
```

Figure 64. Reset passwords to factory defaults

Chapter 5. Using the Web Interface

You can manage your switch through your Web browser and Internet connection. This is referred to as Web-based management. To access the switch, your Web browser must support:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.2, or later

This chapter explains how to access the switch Web-based management panels to configure and manage your switch.

It is important to note that there are equivalent functions in the Web interface as in the terminal interface (that is, there are usually the same menus to accomplish a task). For example, when you log in, there is a Main Menu with the same functions available, and so on. The Web login session will be automatically logged off based on the Telnet timeout settings. There are several differences between the Web and terminal interface. For example, on the Web interface the entire forwarding database can be displayed, and the terminal interface only displays 10 entries starting at specified addresses.

So, if you have read “Chapter 3. Configuring your switch” on page 25 and “Chapter 4. Using the Terminal Interface” on page 31, navigating the Web interface will not be difficult. This chapter is a brief introduction to the Web interface.

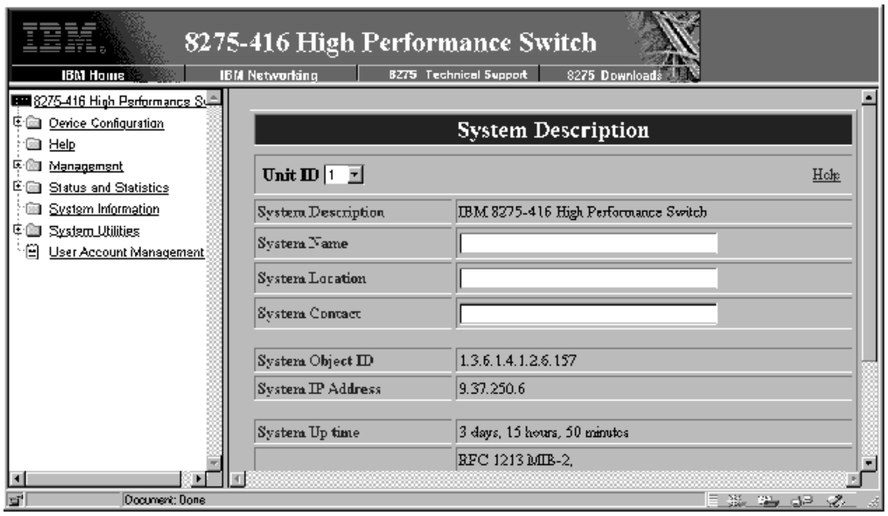
Configuring for Web Access

To have Web access to the switch:

- Configure the switch for in-band connectivity (see “Chapter 2. Accessing the switch” on page 19).
- Enable Web mode (see “Configuring network connection for the switch” on page 35.)

Web Page Layout

A Web interface panel for the switch Web page consists of three frames (Figure 65 on page 82). Frame 1, across the top, appears a banner graphic of the switch. Frame 2, at the bottom-left displays a hierarchical-tree view. The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. You can think of the folders and subfolders as branches and the configuration and status HTML pages as leafs. Only the selection of a leaf (not a folder or subfolder) will cause Frame 2 to display a new HTML page. A folder or subfolder has no corresponding Frame 3 HTML page. Frame 3, the bottom-right frame, displays the currently selected device configuration status or the user configurable information that you have selected from the tree view of Frame 2, or both. You can resize each of these frames. There are no fixed-sized frames.



System Description

Unit ID 1

System Description	IBM 8275-416 High Performance Switch
System Name	
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.2.6.157
System IP Address	9.37.250.6
System Up time	3 days, 15 hours, 50 minutes
	RFC 1213 MIB-2,

Figure 65. Web interface panel–example

Starting the Web Interface

Note: You must configure the IP address of the switch before using the Web interface.

Follow these steps to bring up the switch Web interface:

1. Enter the IP address of the switch in the Web browser address field.
2. When the Login panel is displayed, enter the appropriate User Name and Password. The User Name and associated password are the same ones used for the terminal interface. Click on the **Login** button. The navigation tree is displayed in Frame 2, and the System Description Menu is displayed in Frame 3.
3. Make your selection by clicking on the appropriate item in the navigation tree in Frame 2.

Note: There is an inactivity timeout associated with a Web session. The timeout value is the same one that is used for Telnet sessions.

Commands

The following command buttons are used throughout the Web interface panels for the switch:

Undo Restores any changes made on the panel to their original value since the last Apply or Save.

Save Implements and saves the changes you just made. Some settings may require you to reset the system in order for them to take effect.

Apply Implements the changes you just made. Some settings may require you to reset the system for them to take effect.

Refresh
The Refresh button that appears next to the Apply button in Web interface panels refreshes the data on the panel.

Restart
Refreshes the list and displays the data starting at the beginning of the list.

Next Displays the next set of information in the list.

Chapter 6. Using the SNMP Interface

The switch has an SNMP agent that supports SNMPv1. This allows it to be managed by any SNMP-based application that supports the MIBs supported by the switch. The switch SNMP agent communicates with:

- Any standard MIB Browser (SNMPv1)
- IBM Nways Manager for Windows NT® V2.0 or later
- IBM Nways Manager for HP-UX V2.0 or later
- IBM Nways Manager for AIX® V2.0 or later

The SNMP-based application must specify the appropriate community name that the switch is configured to support. Real-time trap messages can be configured to be sent to designated trap receivers. All configuration information on the switch has read/write access via SNMP. All status information is also available via SNMP.

Refer to “Chapter 4. Using the Terminal Interface” on page 31 for details about configuring SNMP and SNMP trap receiver.

MIBs supported

Refer to the various SNMP RFCs that are supported because the SNMP specification is not described in this chapter. MIBs supported by the switch are shown in Table 13.

Table 13. MIBs Supported by the Switch.

MIBs Supported
MIB-II (RFC 1213)
Definitions of Managed Objects for Bridges (RFC 1493)
IEEE 802.3 Ethernet MIB (RFC 1643)
RMON MIB (RFC 1757)
IBM 8275-416 MIB

The latest 8275-416 MIBs can be obtained from our Web site at:

`http://www.ibm.com/networking/support`

Note: Exceptions to the 8275-416 support for the MIBs listed in Table 13 are described in the sections that follow in this chapter.

MIB II (RFC 1213)

The following are 8275-416 exceptions to the support of MIB II groups:

Address Translation (AT) Group
All the objects are read-only; none are read/write.

Interface Groups
For Ethernet ports, ifAdminStatus is a read-only object instead of read/write. To modify the status of a port interface via SNMP, swPortCtrlAdminMode in the 8275-416 private MIB must be used. There is no explicit ifAdminStatus associated for the Management Interface via MIB-II or any other MIB or access method.

IP Group

- ipNetToMediaTable is read-only; not read/write
- ipAddrTable is not supported
- ipRouteTable is not supported

EPG Group
Not supported.

The switch automatically collects and provides information for the MIB II groups that it supports. There are no additional configuration parameters to enable or disable this support.

Definitions of managed objects for bridges (RFC 1493)

RFC 1493 defines objects for managing MAC bridges based on IEEE 802.1D-1990 standard between local areas network (LAN) segments. The following objects are 8275-416 exceptions to definitions of managed objects for bridges:

dot1dStp
dot1dStpPortEnable is a read-only object. To modify the administrative state of an interface via SNMP, use swPortCtrlAdminMode in the 8275-416 private MIB.

dot1dSr Group
Not supported.

dot1dStatic Group
Not supported.

dot1dTP
Not supported.

dot1dTpLearnedEntryDiscards
Not supported.

IEEE 802.3 Ethernet MIB (RFC 1643)

RFC 1643 defines objects for managing Ethernet-like objects. The following objects are 8275-416 exceptions to IEEE 802.3 Ethernet MIB.

dot3StatsTable Group
The following objects are not supported:

- dot3StatsSQETestErrors
- dot3StatsDeferredTransmissions
- dot3StatsLateCollisions
- dot3StatsInternalMacTransmitErrors
- dot3StatsCarrierSenseErrors
- dot3StatsInternalMacReceiveErrors
- dot3StatsEtherChipSet

dot3CollTable Group
Not supported.

dot3Tests Group
Not supported.

dot3Errors Group
Not supported.

The switch automatically collects and provides information for the IEEE 802.3 Ethernet MIB groups that it supports. There are no additional configuration parameters to enable or disable this support.

Remote monitoring (RMON) MIB (RFC 1757)

The RMON MIB defines objects that allow a device to act like a network traffic analyzer monitoring flows and gathering data for all traffic on the network with varying degrees of detail. It is recommended that a Remote Monitor application be used to manipulate RMON MIB objects. Unexpected results can occur if an SNMP MIB browser is used to manipulate RMON MIB objects.

Note: The switch only supports up to 10 history buckets per history instance.

IBM 8275-416 switch enterprise MIB

Many of the items needed to obtain information from a switch are not available in standard MIBs. A private MIB for the switch (referred to as the IBM 8275-416 Switch Enterprise MIB) was created for these items.

The following objects in the 8275-416 MIB are not supported by this version of code:

- swPortMonitorNetworkConnection
- swDevTrapConsole

Whenever the above objects are accessed, the switch will return an SNMP GetResponse-PDU[2] error-status = no SuchName(2)

Port ifIndex values

When you use SNMP, the interface index (ifIndex) is sometimes used to identify the specific interface being addressed. On the switch, each Ethernet port is an interface and so is the IP agent being used to manage it (which is also referred to as the Management Interface).

The total number of ifIndex values in the switch is the number of installed ports plus 1. The “1” is for the Management Interface. The port ifIndex values for the switch ports start with 1 and increment by 1 for each port physically in the box. Each ifIndex value maps, one for one, with an Ethernet port. Example scenarios:

- If there are 32 ports (16 base ports, 8 ports in slot 1, 8 ports in slot 2)
  - ifIndex 1 is slot 0, port1
  - ifIndex 9 is slot 0, port 9
  - ifIndex 17 is slot 1, port 1
  - ifIndex 25 is slot 2, port 1
- If there are 24 ports (16 base ports, 8 ports in slot 2)
  - ifIndex 1 is slot 0, port 1
  - ifIndex 9 is slot 0, port 9
  - ifIndex 25 is slot 2, port 1
- If there are 28 ports (16 base ports, 4 ports in slot 1 and the ports are on the right side of the card, 8 ports in slot 2)
  - ifIndex 1 is slot 0, port 1
  - ifIndex 9 is slot 0, port 9
  - ifIndex 21 is slot 1, port 1
  - ifIndex 25 is slot 2, port 1

The management interface will always have an ifIndex of 1000.

Chapter 7. Troubleshooting and Obtaining Service

Diagnosing Problems

This chapter contains procedures that help you to troubleshoot problems with your switch and its connections to other devices.

Be sure you read “Appendix A. Safety Information” on page 93 before proceeding.

Obtaining Software

To obtain support information, including technical tips, current product information, and code updates and fixes for the switch, visit the IBM Networking Tech Support page at:

```
http://www.ibm.com/networking/support
```

You can also subscribe to receive e-mail notifications about code updates, tips, and FAQs for your switch.

Troubleshooting in a Network

The switch terminal interface, Web interface, and SNMP management agent give you access to important statistics and other information about the network. To obtain these statistics, see “Chapter 4. Using the Terminal Interface” on page 31 and “Chapter 5. Using the Web Interface” on page 81 and select the appropriate panels.

Start of Troubleshooting Process

If one or more devices (such as workstations) connected to a switch are unable to communicate with other devices in the network, use the following steps to start the troubleshooting process:

1. Locate the switch to which the device is connected. Use the network sketch, the label on the cable connected to the device, or other network records to help you locate the switch.
2. Have available any documentation associated with the feature modules that are installed on the switch.
3. If you have an EIA 232 console session set up, (see “Chapter 2. Accessing the switch” on page 19), you can use it to determine if diagnostics have been completed correctly.
4. Observe the LEDs on the front panel of the switch. The location of these LEDs is shown in Figure 3 on page 10 with explanations of the LED status conditions in the accompanying table. Ignore the feature module LEDs at this time. Review this information before proceeding with the troubleshooting process.
5. If the LED status are not OK, locate the symptom that best describes the communication problem and the LED status you observed in Table 14 on page 90. Then go the section that contains the recommended actions for resolving the problem and follow that procedure.

Choosing a Troubleshooting Procedure

Use Table 14 to determine which troubleshooting procedure you should use. Unless otherwise stated, references to the OK and Fault LEDs are those on the switch.

Table 14. Troubleshooting Symptoms and Actions

Symtom and LED State	Action
The Fault LED and the OK LED are Off, and the fan is not running	Go to “Procedure A”
The Fault LED is blinking.	Diagnostics are still in progress...Wait
The Fault LED is On and there is a “1” in the single-digit display.	Go to “Procedure E” on page 92
The Fault LED is On and there is a character other than a “1” displayed in the single-digit display.	Go to “Procedure B”
None of the devices connected to the switch can communicate, the Fault LED is Off and the Power (I) LED is On.	Go to “Procedure C” on page 91
A single device connected to the switch is having trouble communicating.	Go to “Procedure D” on page 91
A feature module Fault LED is On.	Remove and replace the feature module.

Note: The term *segment* refers to a single cable or interconnected cables between a port and the device at the other end.

Procedure A

Use this procedure if all LEDs are Off:

1. Verify that the ac power outlet to which the switch power supply is connected is active. If an uninterruptible power supply (UPS) is being used to provide ac power, ensure that the UPS is working correctly.
2. Verify that the power cord is installed correctly.
3. If the preceding conditions are satisfied, the power supply is defective. See “Obtaining Service” on page 92.

Procedure B

Use this procedure if the Fault LED is On, and there is a character other than a “1” in the single-digit display:

1. Reset the switch by disconnecting the power cord from the outlet, waiting 10 seconds, and reconnecting the power cord to the outlet. If this corrects the problem, resume using the switch.
2. One or more faulty feature modules can cause this symptom, and the remaining ports might continue to operate.
   a. If you have feature modules, remove them.
   b. Reset the switch.
   c. If the switch comes up, reinstall the feature modules one at a time, and reset the switch to determine the failing feature module.
3. If the problem is not corrected, the switch is defective. See “Obtaining Service” on page 92.

Procedure C

Use this procedure if all devices connected to the switch are having communication problems, the Fault LED is Off and the OK LED is On:

1. Reset the switch by disconnecting the power cord from the outlet, waiting 10 seconds, and reconnecting the power cord to the ac outlet.
   - If the problem goes away, resume using the switch.
   - If the status LEDs indicate a failure, go to "Procedure B" on page 90.
   - If the problem persists, check all the configuration parameters.
   - If the problem has still not been resolved, go to "Procedure D" and try to get individual ports working.

Procedure D

Use this procedure if one device connected to the switch is having a communication problem, the Fault LED is Off, the OK LED is On and other attached devices can communicate through the switch:

1. If the port LED is Off (left LED On 10/100BASE-TX port and single port LED On 100BASE-FX port):
   - Check the cable and the attached device.
   - Check the configuration settings to ensure they are OK.
2. If the port Link LED is On:
   a. Go to the Port Configuration Menu. Check that the port is administratively enabled, has not been diagnostically disabled, has link up, and is in spanning tree forwarding state.
   b. Go to the Port Monitoring Menu. Check that the port is not a monitoring port.
   c. Go to the VLAN Management Menu. Check that the port is a member of the VLAN over which traffic from this device would transverse (this is usually VLAN 1). See "Appendix E. Introduction to Virtual LANs (VLANs)" on page 117 for more details.
   d. Try pinging the attached device from another device in the same VLAN. (The switch is a member of VLAN 1; all ports are in VLAN 1 by default.)
   e. If ping is received, go to Step 5.
   f. If the ping is not received, go to Step 3.
3. Restart the communications program on the failed connected device.
   - If the communications program appears to start without errors, observe the port LED on the switch port. If it is On it might have gone away. Check the port configuration parameters for possible causes of the failure.
   - If the problem persists, go to Step 4.
4. For each device that is having a communication problem, connect its segment to another identically configured Ethernet port on the switch. Try each of the remaining ports to determine if the problem will go away.
   - If the problem goes away, the problem might be in the switch. See "Obtaining Service" on page 92.
   - If the problem persists, continue with Step 5.
5. The problem does not appear to be in the switch and the cables and devices connected to the switch. The problem might be in the network applications or other software running on the devices that are having the communication problem. Refer to the networking software documentation for software problem determination procedures, or consult your network administrator for assistance.

Procedure E

Any port failing Power-On self test diagnostics will be “diagnostically disabled” when the switch becomes operational. Ports not failing diagnostics will be unaffected and will initialize to their configured state. This fault tolerant feature allows the switch to provide levels of connectivity even in the event of hardware failures. A quick glance at the Fault LEDs allows you to determine if the switch has diagnostically disabled any ports.

If a “1” appears in the single-digit display and any Fault LED is on solid, ports have been diagnostically disabled. If a console is connected to the switch through the EIA 232 port, a list of problem ports is printed on the console immediately after diagnostics and before entering operational code. You can also examine the Port Configuration Menu accessible from the Device Configuration Menu. Any ports with an “x” in the “STP St” column have been diagnostically disabled. To isolate this problem:

1. Ensure that the feature modules are seated.
2. Reset the switch.
3. Replace any feature module if its LED is On; the feature module is defective.
4. Replace the switch if the its Fault LED is On; the switch is defective.

Obtaining Service

There are no user-serviceable parts inside the switch chassis. All feature modules are replaceable by the user.

If you need assistance in troubleshooting or you need service for your 8275–416, call IBM at:

- 1 800 772 2227 in the United States
- 1 800 426 7378 (1 800 IBM-SERV) in Canada.
- In other locations, contact your place of purchase.

Refer to your IBM Warranty for information concerning service for the product, or contact the place where you purchased the product.

Appendix A. Safety Information

Reference to Safety Booklet

Danger: Before you begin to install this product, read the safety information in *Caution: Safety Information—Read This First*, SD21-0030. This booklet describes safe procedures for cabling and plugging in electrical equipment.

Gevaar: Voordat u begint met de installatie van dit produkt, moet u eerst de veiligheidsinstructies lezen in de brochure *PAS OP! Veiligheidsinstructies—Lees dit eerst,* SD21-0030. Hierin wordt beschreven hoe u electrische apparatuur op een veilige manier moet bekabelen en aansluiten.

Danger: Avant de procéder à l’installation de ce produit, lisez d’abord les consignes de sécurité dans la brochure *ATTENTION: Consignes de sécurité—A lire au préalable,* SD21-0030. Cette brochure décrit les procédures pour câbler et connecter les appareils électriques en toute sécurité.

Perigo: Antes de começar a instalar este produto, leia as informações de segurança contidas em *Cuidado: Informações Sobre Segurança—Leia Isto Primeiro,* SD21-0030. Esse folheto descreve procedimentos de segurança para a instalação de cabos e conexões em equipamentos elétricos.

危險：安裝本產品之前， 請先閱讀 "Caution: Safety Information--Read This First" SD21-0030 手冊中所提供的安全注意事項。 這本手冊將會說明使用電器設備的纜線及電源的安全程序。

Opasnost: Prije nego sto pŏcnete sa instalacijom produkta, pročitajte naputak o pravilima o sigurnom rukovanju u Upozorenje: Pravila o sigurnom rukovanju - Prvo pročitaj ovo, SD21-0030. Ovaj privitak opisuje sigurnosne postupke za priključrivanje kabela i priključivanje na električno napajanje.

Upozornění: než zahájíte instalaci tohoto produktu, přečtěte si nejprve bezpečnostní informace v pokynech „Bezpečnostní informace“ č. 21-0030. Tato brožurka popisuje bezpečnostní opatření pro kabeláž a zapojení elektrického zařízení.

Fare! Før du installerer dette produkt, skal du læse sikkerhedsforskrifterne i *NB: Sikkerhedsforskrifter—Læs dette først* SD21-0030. Vejledningen beskriver den fremgangsmåde, du skal bruge ved tilslutning af kabler og udstyr.

Gevaar Voordat u begint met het installeren van dit produkt, dient u eerst de veiligheidsrichtlijnen te lezen die zijn vermeld in de publikatie *Caution: Safety Information - Read This First*, SD21-0030. In dit boekje vindt u veilige procedures voor het aansluiten van elektrische appratuur.

VAARA: Ennen kuin aloitat tämän tuotteen asennuksen, lue julkaisussa *Varoitus: Turvaohjeet—Lue tämä ensin*, SD21-0030, olevat turvaohjeet. Tässä kirjasessa on ohjeet siitä, miten sähkölaitteet kaapeloidaan ja kytketään turvallisesti.

Danger : Avant d’installer le présent produit, consultez le livret *Attention: Informations pour la sécurité — Lisez-moi d’abord*, SD21-0030, qui décrit les procédures à respecter pour effectuer les opérations de câblage et brancher les équipements électriques en toute sécurité.

Vorsicht: Bevor mit der Installation des Produktes begonnen wird, die Sicherheitshinweise in *Achtung: Sicherheitsinformationen—Bitte zuerst lesen,* IBM Form SD21-0030, lesen. Diese Veröffentlichung beschreibt die Sicherheitsvorkehrungen für das Verkabeln und Anschließen elektrischer Geräte.

Κίνδυνος: Πριν ξεκινήσετε την εγκατάσταση αυτού του προϊόντος, διαβάστε τις πληροφορίες ασφάλειας στο φυλλάδιο *Caution: Safety Information-Read this first,* SD21-0030. Στο φυλλάδιο αυτό περιγράφονται οι ασφαλείς διαδικασίες για την καλωδίωση των ηλεκτρικών συσκευών και τη σύνδεσή τους στην πρίζα.

Vigyázat: Mielôtt megkezdi a berendezés üzembe helyezését, olvassa el a *Caution: Safety Information— Read This First,* SD21-0030 könyvecskében leírt biztonsági információkat. Ez a könyv leírja, milyen biztonsági intézkedéseket kell megtenni az elektromos berendezés huzalozásakor illetve csatlakoztatásakor.

Pericolo: prima di iniziare l’installazione di questo prodotto, leggere le informazioni relative alla sicurezza riportate nell’opuscolo *Attenzione: Informazioni di sicurezza — Prime informazioni da leggere, SD21-0030,* in cui sono descritte le procedure per il cablaggio ed il collegamento di apparecchiature elettriche.

危険：　導入作業を開始する前に、安全に関する
小冊子SD21-0030　の「最初にお読みください」
(Read This First)の項をお読みください。
この小冊子は、電気機器の安全な配線と接続の
手順について説明しています。

위험: 이 제품을 설치하기 전에 반드시
"주의: 안전 정보-시작하기 전에"
(SD21-0030)　에 있는 안전 정보를
읽으십시오.

ОПАСНОСТ
Пред да почнете да го инсталирате овој продукт, прочитајте ја информацијата за безбедност:
"Предупредување: Информација за безбедност: Прочитајте го прво ова", SD21-0030.
Оваа брошура опишува безбедносни процедури за каблирање и вклучување на електрична опрема.

Fare: Før du begynner å installere dette produktet, må du lese sikkerhetsinformasjonen i *Advarsel: Sikkerhetsinformasjon — Les dette først*, SD21-0030 som beskriver sikkerhetsrutinene for kabling og tilkobling av elektrisk utstyr.

Uwaga:
Przed rozpoczęciem instalacji produktu należy zapoznać się z instrukcją:
"Caution: Safety Information - Read This First", SD21-0030.
Zawiera ona warunki bezpieczeństwa przy podłączaniu do sieci elektrycznej i eksploatacji.

Perigo: Antes de iniciar a instalação deste produto, leia as informações de segurança *Cuidado: Informações de Segurança — Leia Primeiro*, SD21-0030. Este documento descreve como efectuar, de um modo seguro, as ligações eléctricas dos equipamentos.

ОСТОРОЖНО: Прежде чем инсталлировать этот продукт, прочтите Инструкцию по технике безопасности в документе "Внимание: Инструкция по технике безопасности -- Прочесть в первую очередь", SD21-0030. В этой брошюре описаны безопасные способы каблирования и подключения электрического оборудования.

Nebezpečenstvo: Pred inštaláciou výrobku si prečítajte
bezpečnosté predpisy v
Výstraha: Bezpeč osté predpisy - Prečítaj ako prvé,
SD21 0030. V tejto brožúrke sú opísané bezpečnosté
postupy pre pripojenie elektrických zariadení.

Pozor: Preden zaènete z instalacijo tega produkta
preberite poglavje: 'Opozorilo: Informacije
o varnem rokovanju-preberi pred uporabo,"
SD21-0030. To poglavje opisuje pravilne
postopke za kabliranje,

Peligro: Antes de empezar a instalar este producto, lea la información de seguridad en *Atención: Información de Seguridad — Lea Esto Primero,* SD21-0030. Este documento describe los procedimientos de seguridad para cablear y enchufar equipos eléctricos.

Varning — livsfara: Innan du börjar installera den här produkten bör du läsa säkerhetsinformationen i dokumentet *Varning: Säkerhetsföreskrifter— Läs detta först,* SD21-0030. Där beskrivs hur du på ett säkert sätt ansluter elektrisk utrustning.

危險：

開始安裝此產品之前，請先閱讀安全資訊。

注意：

請先閱讀 - 安全資訊 SD21-0030

此冊子說明插接電器設備之電纜線的安全程序。

Safety Notice

Danger: Double-pole/neutral fusing in the power supply. Power might present in the product unless the power cord is unplugged.

⚠

Cuidado: Fusível bipolar/neutro na fonte de alimentação. Pode haver energia presente no produto, a menos que o cabo de alimentação esteja desconectado.

⚠

Waarschuwing:

Dubbelpool/neutraal zekering in de voedingseenheid. Er kan spanning in het product aanwezig zijn zolang de stekker in het stopcontact zit.

⚠

Pas på!

Strømforsyningsenheden; er sikret til brug ved 110 og 220 volt. Der kan være; spænding; i produktet, medmindre netledningen er trukket ud.

⚠

VAARA: Virtalähde on varustettu kaksinapaisella sulakkeella, jossa on myös maanapa. Tuotteessa voi olla jännite, jos verkkojohtoa ei ole irrotettu.

⚠

ATTENTION : L’un des deux fusibles est sur le neutre. L’alimentation é lectrique est protégée e par fusibles sur les deux pô les (phase et neutre). Pré sence de courant possible sauf si le cordon d’alimentation est débranché.

⚠

Achtung: Zweipolige bzw. Neutralleiter-Sicherung im Netzteil. Netzstecker ziehen, um sicherzustellen, daß; keine Spannung am Gerät; anliegt.

⚠

Attenzione: L’alimentatore contiene fusibili su fasi/neutro. Puoò essere presente tensione nell’apparecchiatura se il cavo di alimentazione è collegato.

Advarsel: Topolet/nøytral; sikring i strømforsyningsenheten.; Det kan være; strø.m; i maskinen hvis ikke nettkabelen er dratt ut .

Cuidado:

Protecção (por fusíveis) bipolar com neutro na fonte de alimentação. A menos que o cabo de alimentação esteja desligado, o produto pode estar sob tensão.

Precaución: Hay una fusión de doble polo/neutro en la fuente de alimentación. El producto podría estar cargado eléctricamente a menos que el cable de alimentación esté desconectado.

VARNING: Nätaggregatet är dubbelpoligt avsäkrat. Det kan finnas stråm i produkten sövida inte när 228;tkabeln urkopplad.

تحــذيــر: القطب الثنائي\محايد الانصهار في مصدر الطاقة .
يمكن أن تكون الكهرباء موجودة في المنتج ما لم يتم فصل سلك
الكهرباء.

Предупреждение: Дублирано - фаза/нула свързване в енергийното захранване. Възможно е наличие на ел.енергия в уреда, докато захранващият кабел не е изваден от контакта.

Opasnost: Energetski izvor opremljen je osiguračima na faznom i nultom priključku. Uređaj moze ostati pod naponom sve dok se priključni kabel ne odvoji od utičnice.

注意：电源中装有双柱式/中性保险丝。除非未插入电源线，否则产品带电。

注意：電源供應器內含雙極/中性熔絲 (Double-pole/neutral fusing)。未將電源線自插座拔掉前，本產品內部可能有電存在。

Pozor: V napájecím zdroji je dvoupólové jištění (pojistka ve středním vodiči). Dokud není napájecí šňůra odpojená od sítě, může být zařízení pod napětím.

Προσοχή: Ασφάλεια δύο πόλων/ουδέτερου στην πηγή ρεύματος. Ενδέχεται να υπάρχει ηλεκτρική ισχύς στο προϊόν εάν δεν έχει αποσυνδεθεί το καλώδιο ρεύματος.

זהירות: נתיך דו-קוטבי/נייטרלי באספקת הכוח.
יש לנתק את כבל הכוח כדי למנוע זרם חשמל
במוצר.

Figyelem: A tápegységben kétpólusú biztosíték található. A termék kikapcsolt állapotban is feszültség alatt állhat, kivéve, ha a tápkábel ki van húzva.

注意：
この電源は、２極／中性線にヒューズを使用しています。
電源コードを抜いていない状態では電圧がかかっています。

주의: 전원 공급 장치에 양극/중성의 퓨즈가 있습니다. 전원 코드가 연결되지 않아도 제품 내에 전원이 잔류할 수 있습니다.

⚠

Uzmanību: Divpolu/neitrālā apvienotā strāvas apgāde. Iespējams, ka produktā ir elektriskā strāva, ja strāvas vada kontaktdakša nav izrauta no ligzdas.

⚠

Dėmesio: Įrenginyje yra atvirų dvigubų kontaktų su įtampa. Jeigu įrenginys neišjungtas, kai kurios dalys gali būti su įtampa.

⚠

Опасност: Во единицата за напојување има двополен осигурувач. Доколку кабелот за напојување не е исклучен, во производот може да биде присутна електрична енергија.

⚠

Uwaga: W zasilaczu zamontowany jest bezpiecznik. Dopóki kabel zasilający nie zostanie odłączony w urządzeniu może występować napięcie.

⚠

Pericol: O siguranţă neutră/două capete este în sursa de alimentare. Tensiunea poate să fie prezentă în produs dacă nu este scos din priză cablul de alimentare.

⚠

Осторожно: Источник питания с двухполюсным предохранителем. Устройство может быть под напряжением, пока вы не выдернете шнур из розетки.

⚠

Опасност: Извор напајања је опремљен осигурачима на фазном и нултом прикључку. У уређају може бити присутан напон осим ако је прикључни кабл одвојен од утичнице.

⚠

Výstraha: Poistky sú na oboch póloch napájacieho zdroja. Pokiaľ nie je odpojená šnúra zo siete, zariadenie môže byť pod napätím.

⚠

Nevarnost: Pri napajalniku je zagotovljeno varovanje polov in nevtralnega vodnika. Napetost je lahko prisotna na izdelku, če priključnega kabla ne potegnemo iz vtičnice.

⚠

Dikkat: Güç kaynağı çift kutuplu, topraklı sigorta içerir. Güç kablosu prizden çekilmedikçe üründe elektrik bulunabilir.

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

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

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A Emission Compliance Statement

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

Avis de conformité aux normes d’Industrie Canada

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

European Norm (EN) Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived from commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

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

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richlinie 89/336)

Dieses Gerät ist berechtigt in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland Informationssysteme GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Gerät erfüllt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse A.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: “Warnung: dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.”

EN 50082-1 Hinweis: “Wird dieses Gerät in einer industriellen Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu vergrößern.”

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den IBM Handbüchern angegeben, zu installieren und zu betreiben.

Japanese Voluntary Control Council for Interference (VCCI) Statement

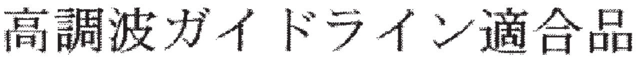
This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean Communications Statement

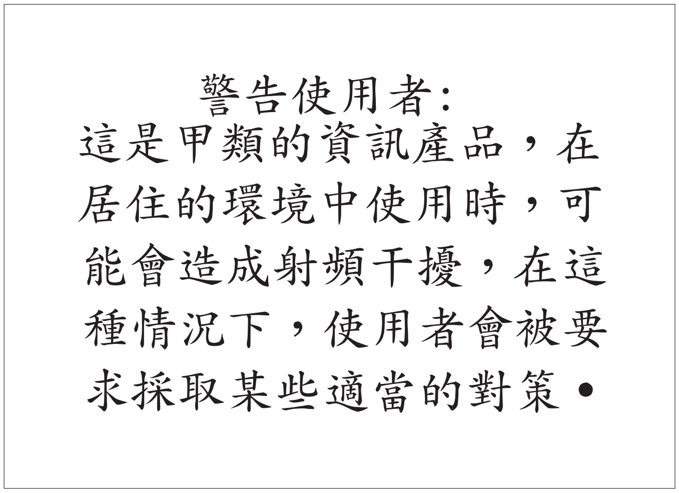
Please note that this device has been certified for business purpose with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for one of residential use.

Power line harmonics compliance



高調波ガイドライン適合品

Taiwanese Class A Warning Statement



警告使用者:

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

Class 1 Laser Statement

Class 1 Laser Product

Laser Klasse 1

Laser Klass 1

Luokan 1 Laserlaite

Appareil à Laser de Classe 1

To IEC 825-1:1993

Class 1 LED Statement

Class 1 LED Product

LED Klasse 1

LED Klass 1

Luokan 1 Ledlaite

Appareil à LED de Classe 1

To IEC 825-1:1993

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States or other countries or both:

AIX
IBM
Nways

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others

Appendix C. Cable Pinout Diagrams

This appendix specifies Ethernet and null-modem cable pinouts.

Straight-Through 10BASE-T/100BASE-TX Cables

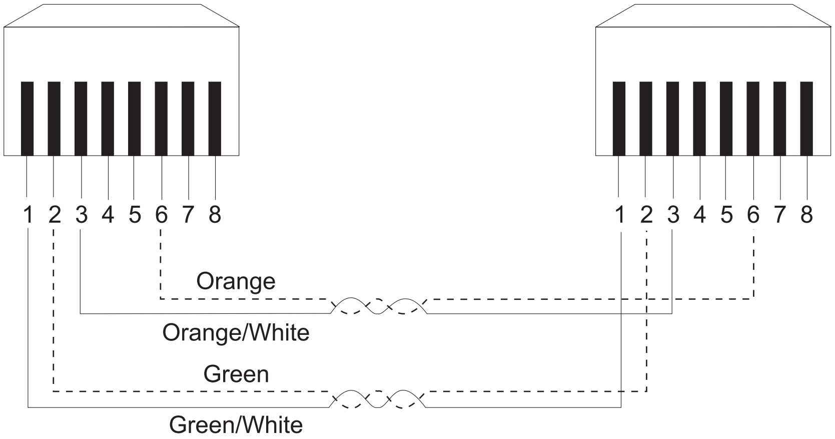


Figure 66. Straight-Through UTP Cable (RJ-45 to RJ-45), T568A

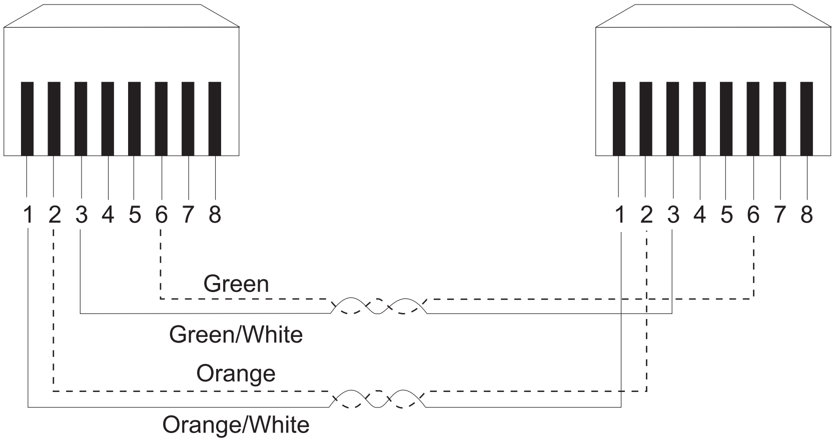


Figure 67. Straight-Through UTP Cable (RJ-45 to RJ-45), T568B

Straight-Through 10BASE-T/100BASE-TX Cables for STP

RJ-45 Pins		IBM Cabling System Data Connector Color Code
1	◄──────►	Red
2	◄──────►	Black
3	◄──────►	Green
6	◄──────►	Orange

Figure 68. Straight-Through STP Cable (RJ-45 to IBM Data Connector)

Crossover 10BASE-T/100BASE-TX Cables

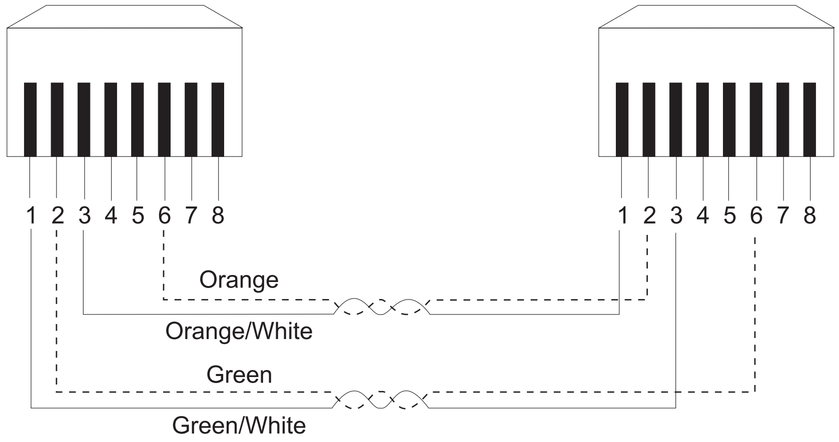


Figure 69. Crossover UTP Cable (RJ-45 to RJ-45), T568A

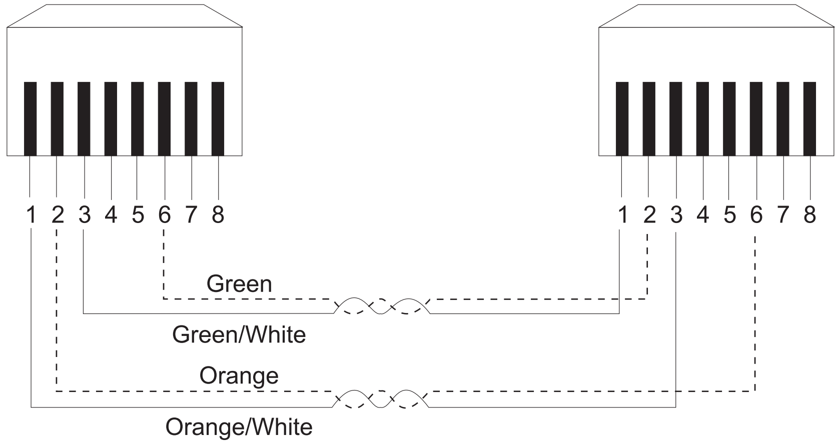


Figure 70. Crossover UTP Cable (RJ-45 to RJ-45), T568B

Crossover 10BASE-T/100BASE-TX Cables for STP

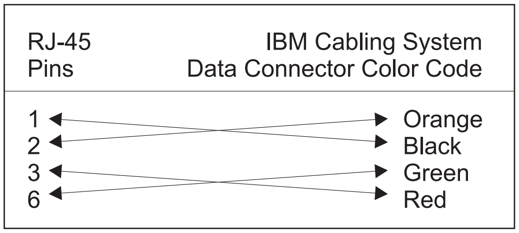
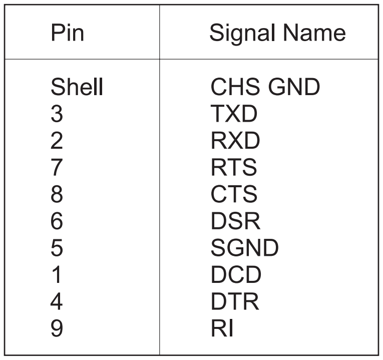


Figure 71. Crossover STP Cable (RJ-45 to IBM Data Connector Crossover)

EIA-232 Port



Pin	Signal Name
Shell	CHS GND
3	TXD
2	RXD
7	RTS
8	CTS
6	DSR
5	SGND
1	DCD
4	DTR
9	RI

Figure 72. Pinout of the EIA-232 Port

Null-Modem Cables

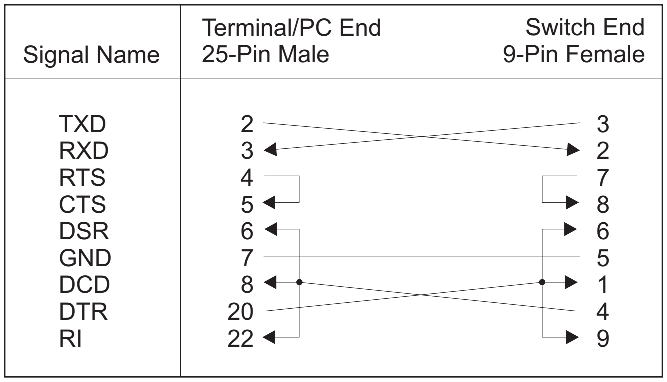


Figure 73. EIA-232 Null Modem Cable for Terminal with 25-Pin Connector

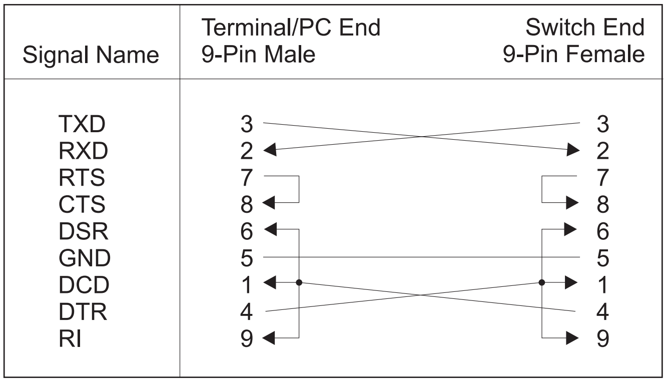


Figure 74. EIA-232 Null Modem Cable for Terminal with 9-Pin Connector

Appendix D. Interface Conventions for the Console

Table 15 summarizes the meaning of special keys and commands that can be used by the terminal interface. You may need to configure your VT100 terminal emulation application to recognize some of these keys.

Active keys are clearly identified at the lower portion of each panel in the terminal interface.

Table 15. Special Keys and Commands Used with the Terminal Interface

Special Keys/ Text/Commands	Description
Brackets	Identifies fields that can be modified. **Angle (< >)** Field entries surrounded by angle brackets identify an item that has a predifined set of options. Use the spacebar to toggle through the available values. If you press the Esc key before you move off the field, the current operational value is restored to the field. The change is not activated until Apply is selected. **Square ([ ])** Field entries surrounded by square brackets identify an item that can be changed by typing in text. Characters within a text field cannot be modified using the cursor keys. No insert or overwrite modes can be performed in the field. The text in the field is erased and replaced by the new text. If you press the Esc key before you move off the field, the current operational value is restored to the field The change is not activated until Apply is selected.
Arrow Keys	Use to move between items within the menu body, within the command Bar, between the menu body and command bar. Up and down arrow keys move the cursor between lines. Right and left arrow keys move the cursor between columns. Arrow keys are ignored when data is entered in a text field. **Right Arrow Key** The right arrow key moves the cursor to the next field to the immediate right. **Left Arrow Key** The left arrow key moves the cursor to the previous field to the immediate left. **Down Arrow Key** The down arrow key moves the cursor vertically down to the first character in the next row in the same position as the original row or wraps to the next section of the menu. **Up Arrow Key:** The up arrow key moves the cursor vertically up to the first character in the previous row in the same position as the original row or wraps to the next section of the menu.

Table 15. Special Keys and Commands Used with the Terminal Interface (continued)

Special Keys/ Text/Commands	**Description**
Tab	Used to move to the next field. • When navigating between fields, Tab is used to move forward to the next field and acts like the right arrow key. • When in a text field which has been modified, Tab performs the same function as the Enter key. When in a text field and no text has been changed, Tab moves you to the next field.
Shift-Tab	Not supported by VT100
Ctrl-Tab	Not supported by VT100
Back Space	Used to remove the character in front of the cursor when entering text enclosed in square brackets.
Blinking Text	Warning or confirmation messages
Cursor	The software does not have control over the cursor shape. Cursor shape is controlled by the terminal emulation.
Delete	Acts like the Backspace key in a text field
End	Not supported
Enter	Used to make a selection. If you are: • On a login panel and press Enter, the User ID and password are processed for login. • On a non-leaf menu option and press Enter, the selected menu is displayed. (A non-leaf menu is a panel that contains a list of menu names that can be selected.) • On the Unit ID or Slot ID and press Spacebar, the item toggles through the available values for that item. After a value is determined, pressing Enter updates the screen with the appropriate data for that unit ID and slot ID. • On a field being modified and press Enter, the text is accepted and undergoes syntax checking and the cursor is moved to the next modifiable field. • On a text field where no modifications have been made, Pressing Enter moves the cursor to the next field.
Esc	When modifying field data enclosed in square backets ([ ]) or angle brackets (< >), press Esc to stop modifying the field and go back to the original data.
Home Key	Not supported
Insert	Not supported
Spacebar	When the cursor is on a modifiable field indicated by angle brackets, use the space bar to toggle through the options for that field. When the cursor is on a modifiable field indicated by square brackets, the space bar may be an allowable key to enter text.

Table 15. Special Keys and Commands Used with the Terminal Interface (continued)

Special Keys/ Text/Commands	**Description**
Function keys	**F1** Takes you to the Help Menu. **F2** Toggles between the first item in the menu body and the Command bar. **F3** Takes you back to the previous menu. **F4** This is the Save key and is used to save changed configuration data. It is the same as going to the System Utilities Menu and selecting Save Configuration Changes. There is no undo after configuration changes have been saved. Pressing F4 after making configuration changes causes configuration changes to be automatically applied (F4 is used to Apply and Save configuration changes).
MAC Addresses	• MAC addresses are displayed and entered as 12 hexadecimal digits in canonical format. • Any alphabetic character (A-F) is displayed as uppercase. When you enter the MAC address, uppercase and lowercase characters are accepted. • Any illegal characters for a MAC address are not accepted.
Uppercase Words in the Menu	Identifies commands.
READ ONLY	When in the upper right corner of the panel, indicates that the current user has read-only access.
UNSAVED DATA	When in the upper right corner of panel, indicates that there are unsaved changes; and that any changes made since the last SAVE was issued will not be retained across a power cycle.
SAVING DATA	After a SAVE is issued, indicates the Save is in process.
DATA SAVED	Save operation has completed successfully.
NEXT PAGE	Command used to display next panel.
PREV PAGE	Command used to display previous panel.
LOGOUT	Command used to end this login session.
CLEAR CTRS	Command used to set to 0 the counters associated with this panel.
SEND	Command used to begin sending pings.
APPLY	Command used to cause configuration changes to take effect. Apply appears on the panel once a change has been made.
REFRESH	Command used to refresh the panel with the current status or configured values.
MAIN MENU	Command used to display the Main Menu.
PREV MENU	Command used to display the previous menu.
HELP	Command used to display the Help Menu.

Appendix E. Introduction to Virtual LANs (VLANs)

Virtual LANs

A VLAN is defined as a group of location and topology independent devices that communicate as if they are on the same physical LAN. This means that the LAN segments are not restricted by the hardware that physically connects them; the segments are defined by flexible user groups that you create using various network management tools.

With VLANs, you can define your network according to:

- **Departmental groups**: For example, you can have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups**: For example, you can have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**: For example, you can have one VLAN for users of e-mail and another VLAN for users of multimedia application services.

Benefits of VLANs

Implementing VLANs has three main advantages:

- It eases the change and movement of devices on IP networks.
- It helps to control broadcast traffic.
- It provides extra security.

How VLANs ease change and movement

With traditional IP networks, network administrators spend much of their time dealing with moves and changes. If users move to a different IP subnet, the IP addresses of each device must be updated manually.

With a VLAN setup, if a device in VLAN 1 is moved to a port in another part of the network, you only need to specify that the new port is in VLAN 1.

How VLANs control broadcast traffic

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices whether they require it or not. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other; therefore, limiting broadcast traffic to only those segments within the VLAN.

How VLANs provide extra security

Devices within each VLAN can communicate only with devices in the same VLAN.

Figure 75 on page 118 shows a network configured with three VLANs—one for each of the departments that access the network.

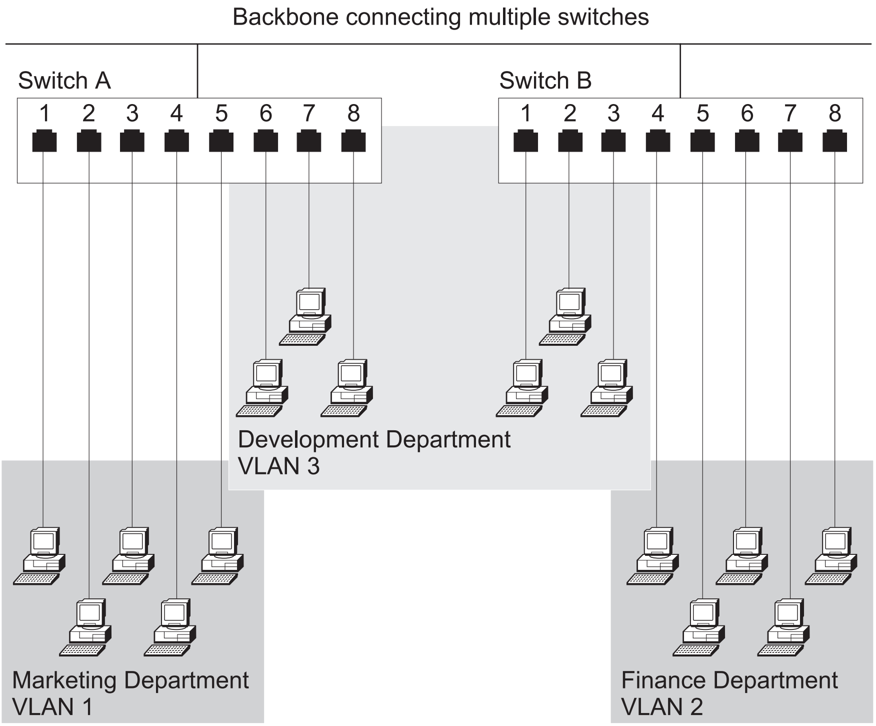


Figure 75. An Example of VLANs

The membership of VLAN 1 is restricted to ports 1, 2, 3, 4, and 5 of Switch A; membership of VLAN 2 is restricted to ports 4, 5, 6, 7, and 8 of Switch B while VLAN 3 spans both switches containing ports 6, 7, and 8 of Switch A and 1, 2, and 3 of Switch B.

In this simple example, each of these VLANs can be seen as a *broadcast domain*—physical LAN segments that are not constrained by their physical location.

VLANs and the switch

The switch supports VLANs that conform to the IEEE 802.1Q VLAN standard. This specifies a standard VLAN implementation that allows operation of VLANs across a multivendor network. This provides the services of traditional port-based VLANs, but also allows true interoperability with other devices that support the 802.1Q standard. In addition, the switch supports GVRP, a protocol that automates the registration of VLANs across networks.

The switch supports up to 32 user-configured VLANs (including the Default VLAN (VLAN 1)). A port may belong to multiple VLANs. This is useful if devices on a LAN segment belong to multiple VLANs.

Priority and traffic classes

The switch assigns a priority of “0” to untagged frames. Otherwise, the priority specified in the VLAN tag of the frame at the originating end-station is used to determine which of two priority queues is used for frame transmission. Frames with a priority of 0 to 3 are transmitted as low priority. Frames with a priority of 4 to 7 are transmitted at high priority. The mapping from user priority to traffic class is defined in table 7-2 of the IEEE P802.1D standard

Overview of IEEE 820.1Q VLAN support

The switch supports IEEE 802.1Q standards-based VLANs. This standard describes port-based VLANs as well as the methods to propagate VLAN memberships across compliant devices using GARP VLAN Registration Protocol (GVRP). Each frame contains information about the VLAN. This information is contained in a 4-byte tag that is inserted into each frame. This tag contains information concerning the VLAN that the device belongs to.

GVRP automates the configuration of VLAN information at the switch. When using devices that support GVRP, VLANs will automatically be created on the switch based on information being passed across the network from other GVRP-enabled devices in frames referred to as GVRP PDUs. This further eases change and movement as the administrator does not need to make any configuration changes at the switch, the change will automatically be detected and the necessary VLAN port membership changes made by the switch.

The switch provides configuration options that allow the use of devices that do not support tagging or GVRP. With proper configuration, both “legacy” devices and devices that support tagging or GVRP may be used on the same network.

These configuration options are described in the following sections.

Port VLAN ID (PVID)

The Port VLAN ID (PVID) specifies a VLAN ID for all untagged frames received on the port. Only one PVID can be configured per port. This setting is used to determine to which VLAN the untagged frames belong as they enter the switch. The specific use of this value will be discussed later in this appendix.

GARP VLAN registration protocol (GVRP)

The switch provides a feature that allows the automatic propagation of VLAN membership information across the network. This feature is facilitated by a new protocol called GARP VLAN Registration Protocol (GVRP) that is defined as a part of the IEEE 802.1Q standard. GVRP registration messages (PDUs) are sent across the network and received by GVRP-enabled devices (switches, adapters, and so on). This protocol allows devices to automatically join and leave VLANs. An advantage of this is that if a user moves from one network connection point to another, you would not have to manually reconfigure the switch ports to add the new switch port to the VLANs that the user belongs to.

GVRP messages are sent across the network with a group address of 0x0180C2000021. The GVRP PDUs use the the same DYAP/SSAP as Spanning Tree BPDUs. Older network analyzers often interpret these GVRP PDUs as Spanning Tree BPDUs. The switch allows you to disable the GVRP function on a switch basis or on an individual port basis.

Static versus dynamic VLANs

Two VLAN types, *static* and *dynamic* are associated with the switch. As the network administrator, you can manually configure static VLANs. Dynamic VLANs are created on the switch as a result of GVRP registration messages. Consequently, a dynamic VLAN is automatically removed from the switch if it is no longer being used by other devices in the network. You can convert a dynamic VLAN to a static VLAN. Once this is done, the VLAN will remain configured on the switch until you remove it.

For each static VLAN configured on the switch, you can define the mode of participation for each port. There are three modes of participation:

- Include (registration fixed)
- Exclude (registration forbidden)
- Autodetect (normal registration)

When a port is configured to be included in a VLAN, the port is always a member of the specified VLAN. This is similar to port-based VLANs from other legacy products. VLAN membership of these ports will propagate across the network if GVRP is enabled. Ports should be included in a VLAN whenever VLAN membership of a port is desired to be guaranteed.

A port that is configured to be Autodetected does not initially belong to the given VLAN. However, the port may join the VLAN if a GVRP PDU is received on that port declaring membership in that VLAN. Ports may be left in Autodetect mode if the devices on the segment connected to the port all support GVRP and thus will register their VLANs with the port.

A port that is configured to be excluded is prevented from being a part of the specified VLAN. You can disable GVRP on a specific port or set of ports to ensure that they never join a VLAN by receiving and propagating GVRP PDUs.

Configuration examples

The following section will discuss some common network configuration scenarios and how the switch should be configured to ensure proper operation.

Untagged device to untagged device

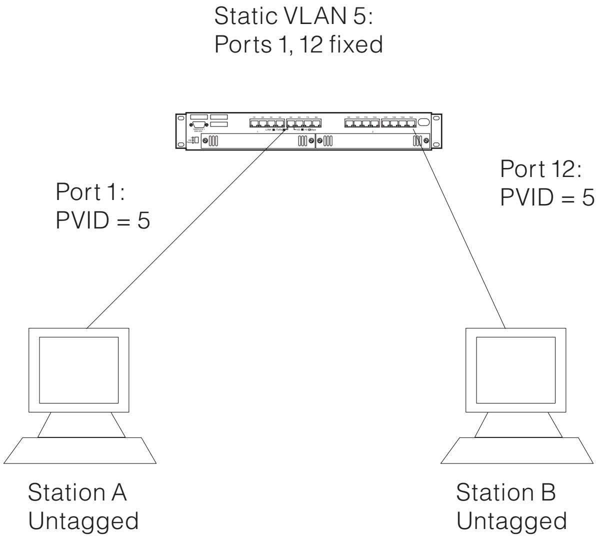


Figure 76. Untagged device to untagged device configuration

This configuration consists of two untagged “legacy” devices connected to the switch. In order for these devices to communicate, they must be members of the same VLAN. In this case, the PVID of the ports that the devices are connected to must be set to the VLAN that the devices are members of. In order to set the ports PVID, a VLAN must first be created with this VLAN ID. Additionally, both ports must be configured to untag frames for this VLAN.

After this configuration is complete, the frames from Station A will arrive at Port 1 untagged, and will then be tagged internally to the switch with the PVID (VLAN 5).

These frames will be sent to port 12 which is a member of the same VLAN. Because the port is set to untagged frames for this VLAN, the tag will be removed and the frame sent to Device B untagged.

802.1Q-compliant device (tagging and GVRP) to 802.1Q-compliant device (tagging and GVRP)

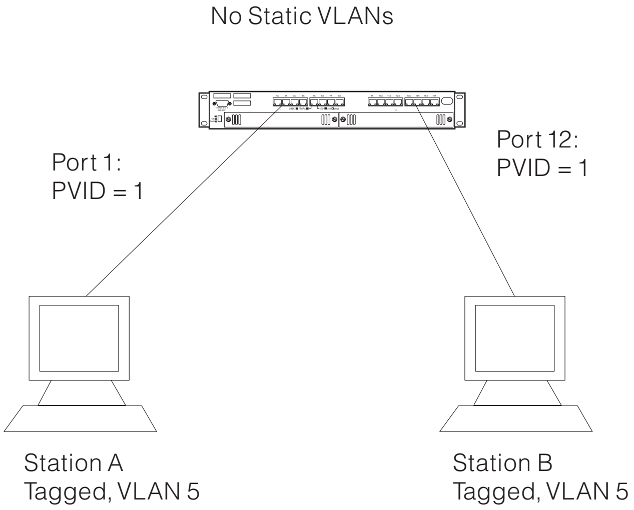


Figure 77. 802.1Q-compliant device (tagging and GVRP) to 802.1Q-compliant device (tagging and GVRP) configuration

In this configuration, both devices support tagging and GVRP. Both devices are configured to transmit tagged frames for VLAN 5. GVRP must be enabled for the switch and for all ports which must participate in GVRP.

When Station A attempts to communicate with Station B, VLAN 5 (that Station A is a member of) is registered at Port 1 by GVRP. Likewise, Station B registers its membership with VLAN 5 on Port 12. Note that this VLAN will be dynamic because the network administrator has not explicitly configured the VLAN on the switch. Frames arrive at Port 1 from Device A, tagged for VLAN 5. These frames are forwarded to Port 12. The frames will be transmitted out of Port 12 tagged for receipt at Station B. Note that all frames in dynamically-created VLANs are transmitted as tagged.

Untagged device to 802.1Q compliant device (tagging and GVRP)

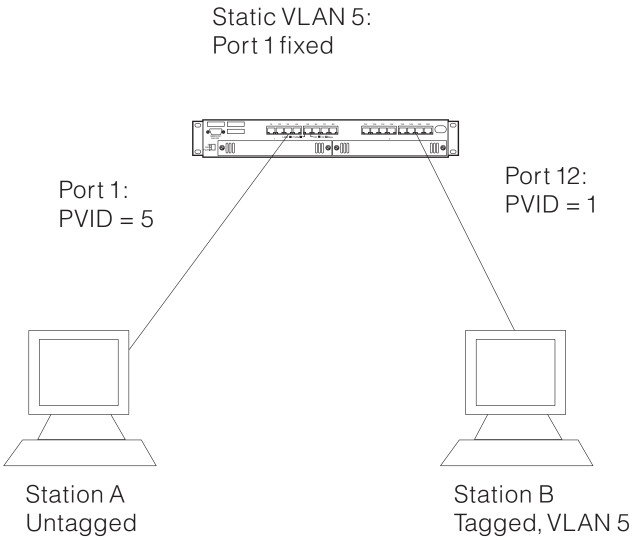


Figure 78. Untagged device to 802.1Q compliant device (tagging and GVRP) configuration

In this configuration, an untagged device, Station A, is attempting to communicate to a tagged device that is a member of the same VLAN. The network administrator first statically creates VLAN 5 on the switch to include Port 1 in this VLAN. Port 1 is configured to transmit frames untagged in VLAN 5 because Station A cannot comprehend tagged frames. Port 1 is configured with a PVID of 5 to ensure that untagged frames received on that port are assigned to VLAN 5.

Station B is also assigned to VLAN 5, and because it supports both tagging and GVRP it will automatically register its membership to VLAN 5. Because Station B resides off of Port 12, Port 12 must be configured to be either autodetected or always included in VLAN 5. Port 12 may be configured to transmit frames as either tagged or untagged because Station B is capable of handling both.

Frames from Station A arrive at Port 1 and are tagged with a VLAN ID equal to the PVID of Port 1 (VLAN 5). The frames are then switched to Port 12, where they are transmitted out of the switch either tagged or untagged, as configured. On the return path, frames tagged with VLAN 5 will arrive at Port 12, and will be received since the port is a member of VLAN 5. The frames will be switched to Port 1, and will be transmitted as untagged, as specified by the configuration of that port in that VLAN.

If any devices on a link cannot handle tagged frames, it would be best to configure the port to transmit frames as untagged in any VLAN in which those devices participate.

Untagged device to 802.1Q-compliant device (tagging only)

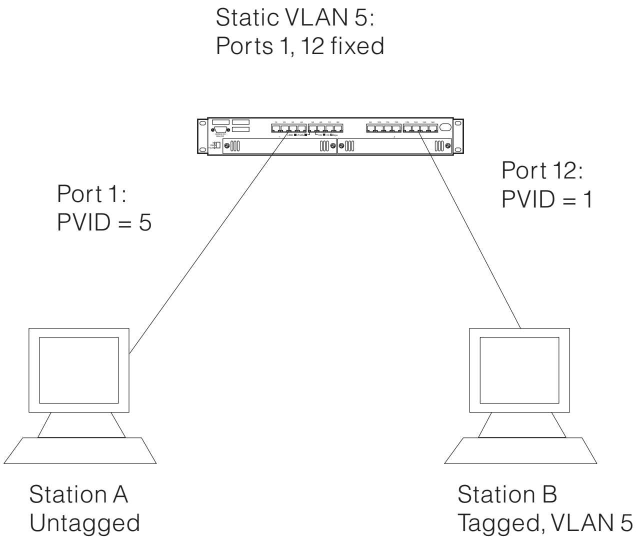


Figure 79. Untagged device to 802.1Q-compliant device (tagging only) configuration

The primary difference in this configuration is that Station B supports tagging, but not GVRP. As a result, VLAN membership information will not be propagated from Station B to the switch. Therefore, the network administrator must configure Port 12 to always be included in VLAN 5. If this is not done, Station B's frames will be dropped as they are received at the switch because the frame's VLAN tag does not match the port's VLAN membership set.

Once this configuration is complete, data flows as in the example above.

Using unique MAC addresses

All addresses in the network should be unique to ensure proper communication.

Duplicate VLAN configurations and oversubscription of switch resources

The 8275-416 allows you the flexibility of configuring VLANs with identical port memberships. However, duplicate VLANs can unnecessarily waste VLAN entries and be an indication that the network design needs to be reconsidered. Too many duplicate VLANs may also lead to an oversubscription of switch resources.

The 8275-416 always guarantees resources for all 32 ports in the Default VLAN (VLAN 1). Up to 31 additional VLANs may be configured or registered with the switch, with certain restrictions.

In a switch with no feature modules (that is, with only the 16 base ports which may potentially be members of any VLAN) up to 10 ports may be included or autodetected in *each* of the 31 available VLANs. Phrased alternatively, the switch supports *310 individual instances of port VLAN membership* distributed across non-Default VLANs in whatever fashion you choose. You can choose a configuration that "oversubscribes" the switch resources. However, unpredicted results may occur. You will be notified of potential oversubscriptions by the terminal interface message `Operation succeeded. WARNING: Resources exceeded!` A similar message appears if you are using the Web interface to configure your switch.

Oversubscription of switch resources due to dynamic VLAN registration cannot be predicted. Therefore, oversubscription will only be indicated during configuration if the number of *statically included* instances of port VLAN membership exceeds the threshold of 310.

The following configuration example indicates an acceptable configuration for an 8275-416 *with no feature modules*:

Table 16. Acceptable VLAN configurations with no feature modules

Configuration	Non-Default VLAN Port Instances
16 ports in Default VLAN (VLAN 1)*	Not counted
16 ports each in 2 other VLANs *	32
10 ports each in 12 other VLANs	120
8 ports each in 16 other VLANs	128
9 ports each in 1 other VLAN	9
* Duplicate VLANs	Total 289

As the Table 16 shows, port membership can be distributed in many ways across many VLANs, and still not exceed the limits of the switch.

The two feature modules on the 8275-416 *together* have the same restrictions as the base ports of the switch. The addition of feature modules does *not* increase the number of non-Default VLAN port instances that can be supported by either the base ports or the two feature modules together. However, the addition of feature modules *does* double the number of non-Default VLAN port instances that can be supported across the entire switch, with 310 port instances distributed across the base ports and 310 port instances distributed across the feature module slots.

The limitation only exist for the number of ports used in either the top or bottom of the switch. There is *no* limitation using base ports and feature module ports in the same VLAN.

Although duplicate VLAN configurations can waste switch resources, there are some instances where they are useful. For instance, security concerns may be addressed by having devices on the same LAN segments belonging to different VLANs, but the VLANs having the same port membership. Another use for duplicate VLAN configurations would be if a switch is placed in the core or in an intermediate level of a network. The 8275-416 functions best as an edge device as opposed to as a core switch.

Index

Glossary

AC. The Access Control field in frame header.

ACE. Address Copied Error. When a station reports this it indicates a problem with the station upstream rather than with itself, normally someone else on the Token Ring with this station’s address. An isolating error.

Application Layer. Layer seven, the uppermost part of the OSI network layer model. This layer contains the user and application programs.

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

Bandwidth. Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps. FDDI bandwidth is 100 Mbps. Token Ring bandwidth is 4/16 Mbps.

Bit. Either of the digits 0 or 1 when used in the binary numeration system. Eight bits equals a single byte. Broadcast . All good frames destined for the broadcast address, in other words sent out to all stations on the network. Some broadcasts are limited to the local network, and some broadcasts may cross onto other networks.

Broadcast. All good frames destined for the broadcast address, in other words, sent out to all stations on the network. Some broadcasts are limited to the local network, and some broadcasts may cross onto other networks.

Buffer. The space allocated to the storage of filtered packets as they are captured from the network. A probe only has a limited set of resources to hold buffer data. If one of the buffers uses all of the probe’s resources, it will stop the other buffers from capturing packets. To conserve resources, you can slice packets or assign maximum sizes to buffers.

Bytes. The total number of bytes making up a frame - includes FCS octets.

Client. Any application that retrieves and displays data from probes or agents.

Collision. The best estimate of the number of collisions on an Ethernet segment.

Community Name. Also known as Community String. SNMP uses community names to limit access to certain device management functions. The Community Name used when accessing a device determines which functions may be accessed.

CRC Align Error. An Ethernet packet between 64 and 1518 octets long inclusive (includes FCS octets) - not an integral number of octets in length or has a bad FCS.

CSMA/CD Carrier. Carrier Sense Multiple Access with Collision Detection. The Ethernet protocol that allows each device to create and send its own data packets. CSMA/CD is used to avoid excessive collisions between packets as they are randomly transmitted. A CSMA/CD device first listens for other carriers, if it detects no other carriers, it will then allow the data packet to be transmitted. If a collision is detected, the device stops transmitting, waits a random length of time, and begins transmitting again

Data Link Layer. The second layer of the OSI reference model. This layer is responsible for controlling message traffic.

Data Packet (Packet). A sequence of binary digits, including data and control signals that is transmitted across a LAN.

Default Gateway. The IP address of a device, usually a router or gateway, to which the probe directs all packets not destined for its subnet.

ED. Ending Delimiter - a distinctive byte marking the end of a frame or a token.

Forwarding. The process of sending a frame towards its destination by an intranet working device.

Fragment Packet. An Ethernet packet less than 64 octets long (excludes frame bits but includes FCS octets) - not an integral number of packets in length or has a bad FCS.

GARP. See Generic Attributes Registration Protocol.

GARP VLAN Registration Protocol (GVRP). The IEEE 802.1p protocol that enables workstations to request admission to a specific VLAN rather than to a multicast domain.

Generic Attributes Registration Protocol (GARP). A protocol defined by IEEE 802.1p. There are two versions: GARP Multicast Registration Protocol (GMRP) and GARP VLAN Registration Protocol (GVRP).

GARP Multicast Registration Protocol (GMRP). The IEEE 802.1p protocol that enables workstations to request membership in a multicast domain. This joining action is called a leaf-initiated join. GMRP provides a standard protocol for sending traffic to only those ports that have requested multicast traffic. It is compatible with 802.1Q because it operates on a port basis.

GVRP. See GARP VLAN Registration Protocol.

HDLC. High-Level Data Link Control. OSI bit-orientated protocol.

Host. A device or computer on an IP network to which you can connect.

Jabber Packet. An Ethernet packet longer than 1518 octets (excludes frame bits but includes FCS octets) - not an integral number of octets in length or has a bad FCS.

ICMP. Internet Control Message Protocol. Internet protocol that reports errors and provides other information relevant to IP packet processing.

IEEE. Institute of Electrical and Electronics Engineers.

IETF. Internet Engineering Task Force, whose responsibilities include specification of protocols and recommendation of Internet standards via the Request for Comment (RFC) process.

Long Packet. See oversize packet.

MIB. Management Information Base.

Multicast. Good packets directed to the multicast address. Does not include broadcast packets. Multicasts are similar to broadcasts but have a more limited scope, for example they may be directed to all bridges on a ring.

Oversize Packet. An Ethernet packet longer than 1518 octets (including FCS octets) but otherwise well formed.

Network Layer. The third layer of the OSI reference model. This layer is responsible for controlling message traffic.

Octet. A digital unit of information comprising eight binary digits (bits) equivalent to a byte.

OSI. Open Systems Interconnection, a body of standards set by the International Standards Organization to define the activities that must occur when computers communicate. In the OSI Reference Model there are seven layers, and each contains a specific set of rules to follow at that point in the communication.

Packet. A unit of information that contains data, origin information; and destination information, which is switched as a whole through a network.

PACMIB. Port Address Correlation MIB maps port to host data and gathers port statistics for 3Com CoreBuilder devices on your network.

Probe. Station (or agent) responsible for gathering network data on a remote segment and passing it up to a central management station (or client). Usually configured and controlled by the client.

PDN. Public Data Network.

Physical Layer. The first layer of the OSI network layer model. This layer manages the transfer of individual bits of data over wires, or whatever medium, that is used to connect workstations and peripherals.

Presentation Layer. The sixth layer of the OSI network layer model. This layer controls the formatting and translation of data.

Protocol. A set of rules and procedures that govern the exchange of data between two communicating systems.

Protocol Number. The port or program number as defined by the parent protocol. For example, if you are adding a TCP child protocol, the protocol number will be the TCP port number.

PSTN. Public switched telephone network.

RMON. Remote MONitoring. Subset of SNMP MIB II which allows monitoring and management capabilities by addressing up to ten different groups of information. Defined in IETF document RFC 1757.

RMON2. Extends the capability of RMON to include protocols above the MAC layer.

Short Packet. See undersize packets.

Station. Any machine connected to the network - for example a fileserver, PC, workstation, printer or probe.

Subnet Mask. A filtering system for IP addresses. It defines the portion of the IP address used to identify the subnet. The remaining portion is used to represent host information. Devices and routers use the mask to identify the subnet on which a probe resides.

System Descriptor. A free-form field on RMON devices used by vendors to supply basic information about the device.

Transport Layer. The fourth layer of the OSI network layer model. This is responsible for error checking and correction, and some message flow control.

Trigger. A trigger represents a sequence of events that may occur on a network. When these events occur, an alarm is triggered.

Undersize Packets. An Ethernet packet less than 64 octets long (excluding frame bits but including FCS octets) but otherwise well formed.

Virtual Circuit. Circuit-like service provided by the software protocols of a network, enabling two end points to communicate as though connected by a physical circuit. Network nodes provide the addressing information needed in the packets that carry the source data to the destination.

Readers' Comments — We'd Like to Hear from You

8275 Model 416 High Performance Ethernet Workgroup Switch
User's Guide

Publication No. GC30-4026-02

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name	Address
Company or Organization	
Phone No.	

Readers' Comments — We'd Like to Hear from You
GC30-4026-02

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL   PERMIT NO. 40   ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Department CGFA–Design and Information Development
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC, U.S.A.   27709-9990

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

Web sites:

8275-416 Documentation
`http://www.ibm.com/networking/support/docs.nsf/8275docs`

8275-416 Software Updates
`http://www.ibm.com/networking/support/downloads/8275`

8275-416 Product Support
`http://www.ibm.com/networking/support/8275`

GC30-4026-02