IBM

Ethernet Workgroup Switch 8275-217/225

Installation and Planning Guide

IBM

Ethernet Workgroup Switch 8275-217/225

Installation and Planning Guide

Note:

Before using this information and the product it supports, be sure to read the safety information under “Safety Information” on page xi and the general and emisssions notices in Appendix B, “Notices.” on page B-1

First Edition (March 1999)

This edition applies to the IBM Ethernet Workgroup Switch 8275-217/225.

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 and Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK NC 27709-9990
USA

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

Chapter 1. Introduction

Chapter 2. Installation

Chapter 3. Control Panel Management

Chapter 5. Using Web Management

Chapter 6. Troubleshooting and Service

Appendix A. Introduction to Virtual LANs (VLANs) and Spanning Tree Protocol (STP)

Appendix B. Notices

Figures

Tables

Safety Information

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.

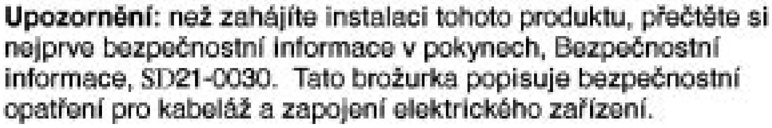
Gevarr: Voodrat u begint met de installatie van dit produkt, moet u eerst de veiligheidsinstructies lezen in de brochure *PAS OP! Veiligheidsinstructies–Lees dit eerst*, SD21-0030. Hierin wordt beschreven hoe u electrische apparatuur op een veilige manier moet bekabelen en aansluiten

Danger: Avant de procéder à l'nstallation 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 instaler deste produto, leia as informações de segurança contidas em *Cuidado: Informações Sobre Segurança–Leia 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 pöcnete sa instalacijom produkta, procitajte 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, SD21-0030. 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.

Gevarr: 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.

VARRA: Ennen kuin aloitat tämän tuotteen asennuksen, lue julkaisussa *Varoitus: Turvaohjeet–Lue tämä ensin,* SD21-0030, olevat turvaohjeet. Tässä kirjasessa on ohjeet siitä, mitensähkölaitteet kaapeloidaan ja kytketään turvallisesti.

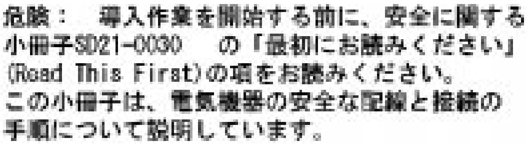
Danger : Avant d'installer le présent produit, consultez le livret *Attention : Informations pour la sécurité–Lisez-moi d'abord,* SD21-0030, qui décrit les procédures à respecter pour effectuer les opérations de câblage et brancher les équipments électriques en toute sécurité.

Vorsicht: Bevor mit der Installation des Produktes begonnen wird, die Sicherheitshinweise in *Achtung: Sicherheitsinformationen–Bitte zuerst lesen*. IBM Form SD21-0030. Diese Veröffentilchung beschreibt die Sicherheitsvorkehrungen für das Verkabien 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, miyen biztonsági intézkedéseket kell megtenni az elektromos berendezés huzalozásakor illetve csatlakoztatásakor.

Pericolo: prima di iniziare l'installazione di questo prodotto, leggere le informazioni relatie alla sicurezza riportate nell'opuscolo *Attenzione: Informazioni di sicurezza–Prime informazioni da leggere* 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 forst*, 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: Säkerhetsforeskrifter – Läs detta först*, SD21-0030. Där beskrivs hur du på ett säkert satt 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。

About This Manual

This manual explains how to install and configure the IBM Ethernet Workgroup Switch 8275-217/225.

Who Should Read This Manual

This manual is intended for use by installation technicians, network administrators, and service personnel.

How This Manual Is Organized

- Chapter 1, "Introduction," provides a functional product description and cabling requirements.
- Chapter 2, "Installation," describes installation and cabling procedures.
- Chapter 3, "Control Panel Management," describes how to use the Ethernet Workgroup Switch control panel.
- Chapter 4, "Using the Management Interface," describes how to use the EIA 232 management port through a local or remote connection.
- Chapter 5, "Using Web Management," describes how to use an Internet web browser to connect to and manage your Ethernet Workgroup Switch.
- Chapter 6, "Troubleshooting and Service," provides troubleshooting procedures, how to get help from IBM, and procedures for downloading new code.
- Appendix A, "Introduction to Virtual LANs (VLANs) and Spanning Tree Protocol (STP)," provides background and conceptual information about virtual LANs (VLANs) and spanning tree protocol (STP).
- Appendix B, "Notices," describes product notices and provides warranty information.

Prerequisite Publication

Caution: Safety Information—Read This First, SD21-0030.

Chapter 1. Introduction

This chapter describes the features of the IBM Ethernet Workgroup Switch 8275-217/225 and provides a functional overview that can help you integrate the Ethernet Workgroup Switch into your new or existing network.

The Ethernet Workgroup Switch is an intelligent, managed switch, designed for use in medium-sized workgroups or remote locations that are part of a large network.

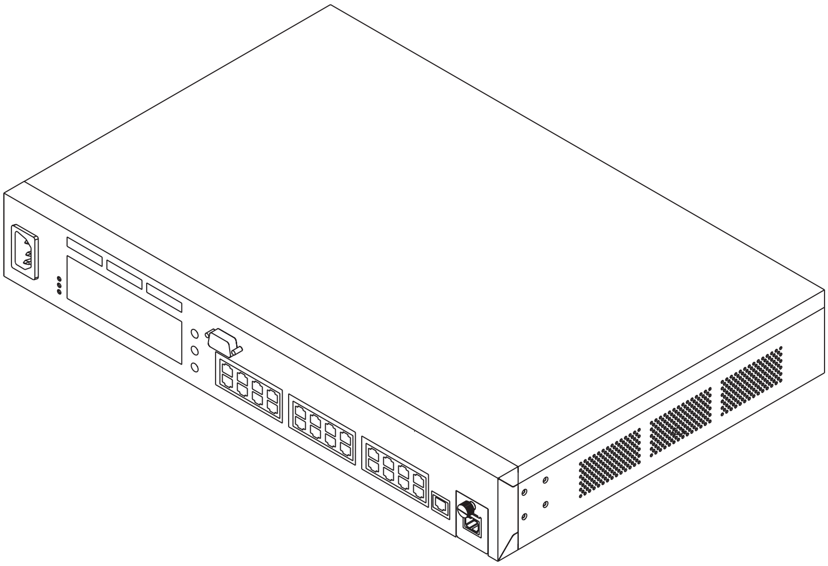


Figure 1-1. IBM Ethernet Workgroup Switch 8275-217/225

Product Features

The Ethernet Workgroup Switch contains the following features:

- Control Panel—A display console on the front panel of the Ethernet Workgroup Switch that allows you to monitor and manage the Ethernet Workgroup Switch and its ports. You can use the Control Panel to set device-level configuration values.

- Management Interface—An interface that allows you to issue management commands and retrieve data. You can access this interface by either:

  – VT100 terminal emulation, using a local or remote connection through the switch's EIA 232 management port (referred to as *out-of-band*).

  – Telnet (referred to as *in-band*).

- SNMP Network Management—The ability to act as an SNMP agent allowing the switch to be managed by a wide range of SNMP management programs such as Nways Workgroup Manager for Windows NT and Nways Manager for AIX - Campus Manager LAN.

- Web-Based Management—The ability to use an Internet browser to manage the Ethernet Workgroup Switch remotely using the World Wide Web.

- MAC Address Filtering—The ability to restrict access between certain users or segments. Network traffic can be controlled by selectively filtering addresses at the ports.

- Switch Security—The ability to use a password to prevent unauthorized personnel from changing switch configuration settings.

- Virtual LANs (VLANs)—The ability to effectively divide the Ethernet Workgroup Switch into as many as 31 separate domains. Packets are forwarded only between ports within the same domain.

- Software updates—The ability to download software upgrades to the Ethernet Workgroup Switch by using TFTP.

Functional Characteristics

Figure 1-2 and Figure 1-3 shows the indicators, ports, and keys on the front panel of the Ethernet Workgroup Switch Model 217 and Model 225 respectively.

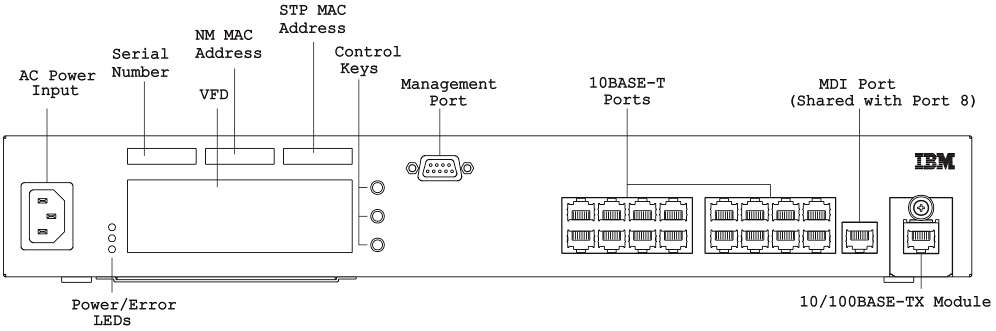


Figure 1-2. Front Panel of the Model 217

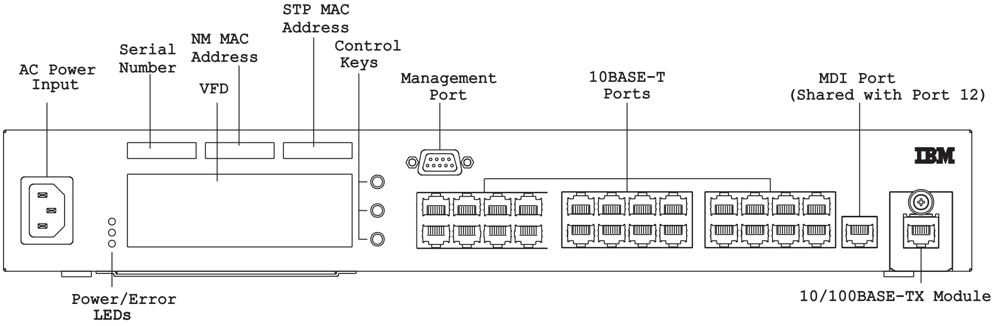


Figure 1-3. Front Panel of the Model 225

Figure 1-4 shows the rear panel of the Ethernet Workgroup Switch.

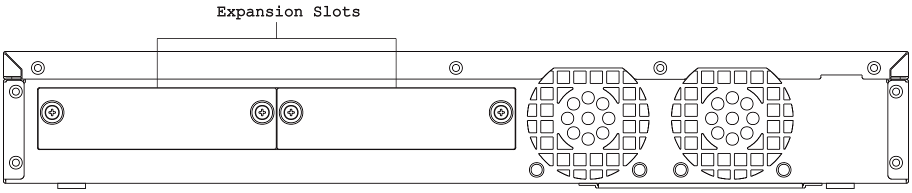


Figure 1-4.   Rear Panel

Control Panel

The control panel is an effective management tool for monitoring and configuring the Ethernet Workgroup Switch. The Control Panel provides overall utilization statistics that allow you to monitor all the ports at a glance as well as providing detailed error and configuration information by port. For more information about the control panel, see “Control Panel” on page 3-1.

Communication Ports

The following types of ports, shown in Figure 1-2 and Figure 1-4, are available on the Ethernet Workgroup Switch.

- Ethernet Ports – 16 10BASE-T ports on the Model 217 and 24 10BASE-T ports on the Model 225. These ports are located on the front panel (ports 1-16 on the Model 217/ports 1-24 on the Model 225) and use UTP/STP Category 3, 4, or 5 cables with RJ-45 connectors.

- Fast Ethernet Port – One 10/100BASE-TX auto-sensing port. This port is located on the front panel (port 17 on Model 217/port 25 on Model 225). If the port operates at 10 Mbps, you can use UTP/STP Category 3, 4, or 5 cables with RJ-45 connectors. If the port operates at 100 Mbps, you need to use a UTP/STP Category 5 cable with RJ-45 connectors.

- MDI Port – One shared port. One MDI port is shared with port 8 on Model 217/port 12 on Model 225. This port is located on the front panel and uses UTP/STP Category 3, 4, or 5 cables with RJ-45 connectors.

Management Port

The management port is an EIA 232 port that is used to configure the Ethernet Workgroup Switch. You can connect it directly to a local workstation or to a modem for a remote connection using Serial Line Internet Protocol (SLIP). Once connected you can manage the Ethernet Workgroup Switch. This is called *out-of-band management* (OOB).

Cables and Connectors

Cable and connector requirements differ depending on the port to which each cable connects.

Maximum Cable Lengths

Table 1-1 lists the maximum recommended cable lengths.

Table 1-1. Recommended Maximum Cable Lengths

Ethernet Type	Maximum Segment Length
10BASE-T 100BASE-TX	100 m (328 ft) 100 m (328 ft)
100BASE-FX	Half-duplex — 412 m (1352 ft) Full-duplex — 2000 m (6561 ft)

Cabling Requirements for 10BASE-T Ports

10BASE-T ports will operate correctly on any of the following cables:

- Category 3, 4, or 5 100-ohm UTP or STP cable and connecting hardware, as specified in the ANSI/TIA/EIA 568-A or CSA T529 standards.
- 150-ohm STP-A cable and components as specified in these standards.
- IBM Cabling System types 1, 6, and 9, 150-ohm STP or STP-A cable. If you are using 150-ohm cabling systems, impedance matching devices must be using in conjunction with the cable.
- Category 3, 4, or 5 100- and 120-ohm, balanced, shielded or unshielded cables and components, as specified in the ISO/IEC 11801 standard.
- 150-ohm, balanced, shielded cables and components, as specified in the ISO/IEC 11801 standard.
- Any link that meets the specifications of a Class D link. If you are using 150-ohm cabling systems, impedance-matching devices must be using in conjunction with the cable.

All devices connected to the cables must be grounded.

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

Cabling Requirements for 10/100BASE-TX Fast Expansion Module

For connection to 10BASE-T networks, you should use Category 3, 4, or 5 cables meeting the specifications outlined in “Cabling Requirements for 10BASE-T Ports”. For connection to 100BASE-TX networks, you can use only Category 5 cables. The large 10/100BASE-TX Fast Expansion Module incorporates two shared RJ-45 connectors, one MDI-X, and one MDI. The MDI-X port performs an internal crossover function that allows easy connection to other devices using standard straight-through cables. The MDI port does not have the internal crossover function.

Cabling Requirements for 100BASE-FX Fast Expansion Module

This expansion module uses two SC-type connectors. Use multimode optical fiber that meets the specifications in TIA/EIA 568A or ISO/IEC 11801. The maximum length of optical fiber cable between devices should not exceed 2000 m (6562 ft) if the link is used in full-duplex mode. If the link is used in half-duplex mode, the length should not exceed 412 m (1352 ft).

Cabling Requirements for the Management Port

The Management Port is a standard DB-9 male connector that provides an EIA/TIA 232 serial interface. You can connect using a null-modem cable to a local workstation or a standard serial cable to a modem for a remote connection using Serial Line Internet protocol (SLIP). Once connected you can manage the Ethernet Workgroup Switch. This is called *out-of-band management*.

Note: You can make a null-modem cable by connecting a null-modem adapter to a standard serial cable.

Physical Characteristics and Requirements

Dimensions

Width	439.4 mm (17.3 in.)
Depth	292 mm (11.5 in.)
Height	66.5 mm (2.62 in.)

Operating Clearances

Front – Adequate space to view VFD

Sides – 50.8 mm (2 in.)

Rear – 127 mm (5 in.)

Weight

4.6 kg (10.14 lb)

Power Requirements

The internal universal power supply can accept ac voltage in the following range: 100–240 V ac, 50-60 Hz

Power Dissipation

50 Watts

Operating Environment

Table 1-2. Operating Environment

Operating Temperature	10°C to 40° C (50° to 104° F)
Storage Temperature	1° C to 60° C (33.8° to 140° F)
Operating Humidity	8% to 80% non-condensing

Chapter 2. Installation

Before installing the Ethernet Workgroup Switch, be sure to read “Safety Information” on page xi and the notices and warranty information in Appendix B, “Notices.”

This chapter provides step-by-step instructions for installing the Ethernet Workgroup Switch. It also explains how to install the optional expansion modules.

Installation Summary

Table 2-1. Ethernet Workgroup Installation Procedures

Step	Procedure	Reference
1	Read the safety information booklet shipped with the Ethernet Workgroup Switch.	SD21-0030
2	Unpack the Ethernet Workgroup Switch	“Unpacking Instructions” on page 2-1
3	Table-Mount the Ethernet Workgroup Switch	“Table-Mounting the Ethernet Workgroup Switch” on page 2-2
4	Rack-Mount the Ethernet Workgroup Switch	“Rack-Mounting the Ethernet Workgroup Switch” on page 2-3
5	Wall-Mount the Ethernet Workgroup Switch	“Wall-Mounting the Ethernet Workgroup Switch” on page 2-4
6	Install an Expansion Module	“Installing Optional Modules” on page 2-6
7	Perform Power-On checkout	“Power-On Checkout” on page 2-7
8	Connect the Cables	“Cabling” on page 2-8
9	Configure the Ethernet Workgroup Switch	“Connecting a Null Modem Cable to the Management Port” on page 2-8

Unpacking Instructions

Step 1. Verify that the items listed here are in the package along with this manual. The package should contain:

- An Ethernet Workgroup Switch
- Two mounting brackets for rack or wall mounting and eight screws
- Wall-mounting Template
- A power cord
- *8275-217/225 Quick Reference Card* (preinstalled in card tray beneath the Ethernet Workgroup Switch)
- Safety Manual
- *8275-217/225 Quick Installation Guide*

Step 2. Visually inspect the unit to ensure that it was not damaged during shipping. If any items are missing or damaged, contact your place of purchase.

Table-Mounting the Ethernet Workgroup Switch

The Ethernet Workgroup Switch can be installed on a flat level surface. To install the Ethernet Workgroup Switch on a flat level surface, refer to Figure 2-1 which provides the clearance information for all sides of the Ethernet Workgroup Switch.

Front — Adequate room to view control panel display
Side — 2 in. (50.8 mm)
Rear — 5 in. (127 mm)

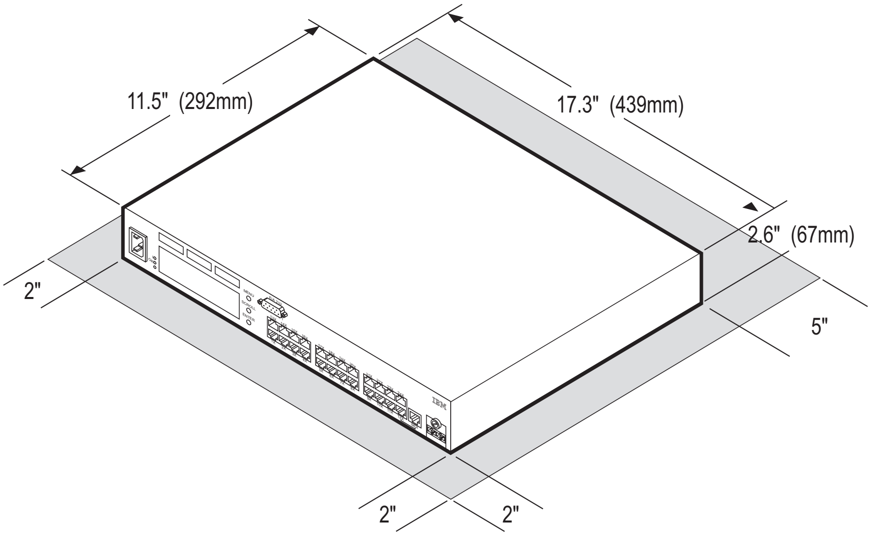


Figure 2-1. Tabletop-Mounting the Ethernet Workgroup Switch

Rack-Mounting the Ethernet Workgroup Switch

The Ethernet Workgroup Switch can also be installed in a standard 19-inch rack. To install the Ethernet Workgroup Switch in a rack, refer to Figure 2-2 and perform the following steps.

Step 1. Install the two mounting brackets to the sides of the Ethernet Workgroup Switch using the brackets and screws provided. Be sure that the tabs face toward the front of the unit.

Step 2. Insert the switch into a 19-inch rack.

Note: The rack-mounting screws are *not* provided. Ensure the ventilation holes are not obstructed.

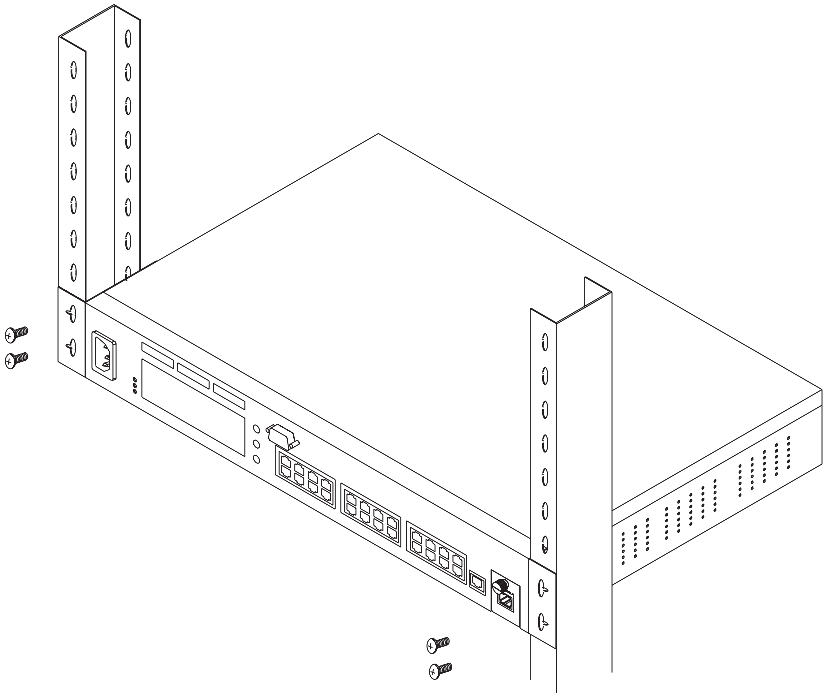


Figure 2-2. Rack-Mounting the Ethernet Workgroup Switch

Wall-Mounting the Ethernet Workgroup Switch

The Ethernet Workgroup Switch can be mounted vertically to either a plywood or drywall surface. See Figure 2-3.

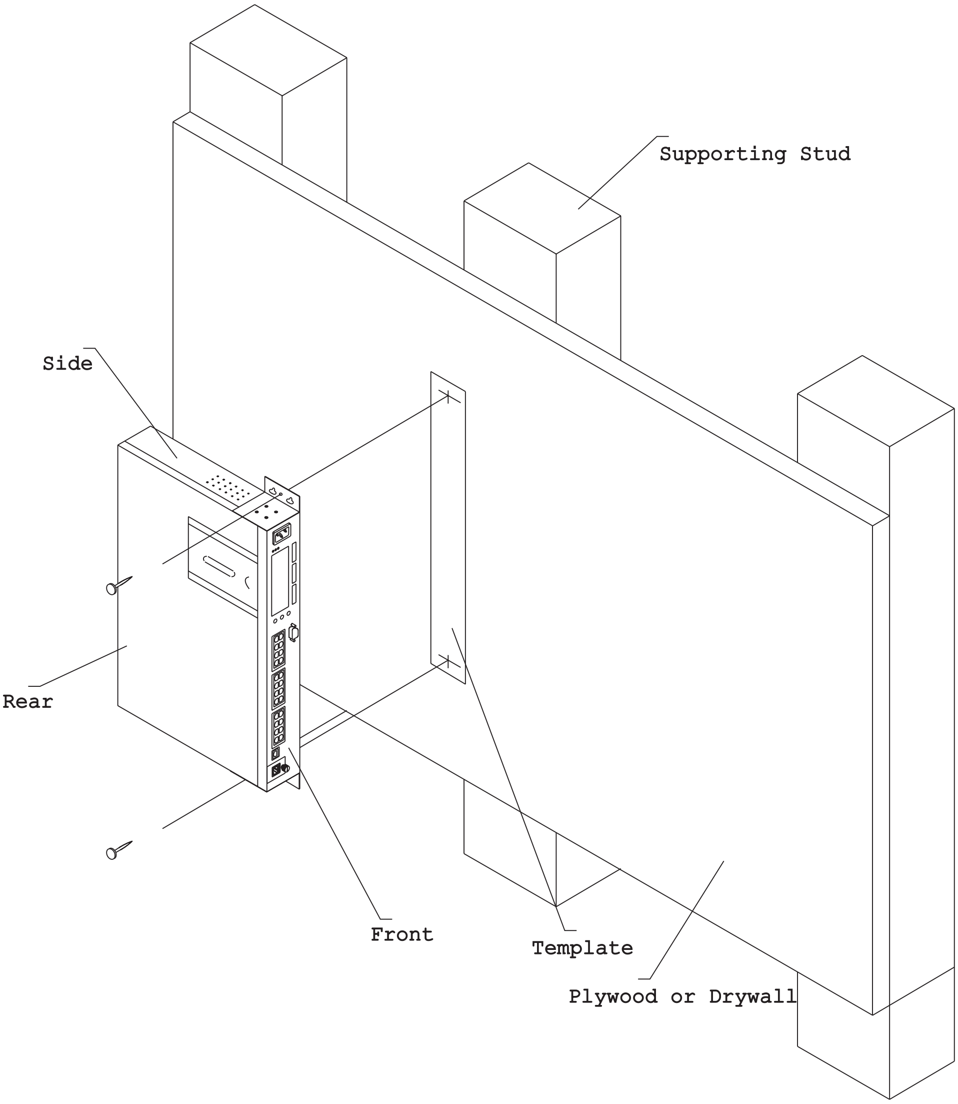


Figure 2-3. Wall-Mounting the Ethernet Workgroup Switch

Note: Before wall mounting the Ethernet Workgroup Switch, ensure you are following all applicable local building and electric codes.

Materials Needed:

Drill with a 1/8 inch (3.2 mm) drill bit
2 — #10 pan-head mounting screws, in the following lengths, and associated screwdriver

- **Screw length for plywood surface mounting** — 3/4 inch (20 mm)
- **Screw length for drywall surface mounting** — 3/4 inch (20 mm) plus thickness of the drywall

Mounting Requirements

When mounting the Ethernet Workgroup Switch, ensure that you have enough room for adequate viewing, ventilation, and access to an ac power outlet. The method of mounting must be able to support the combined weight of the Ethernet Workgroup Switch (10.14 lb / 4.6 kg) plus the suspended weight of all the cables to be attached to the Ethernet Workgroup Switch.

Clearance

Front — Adequate room to view control panel display
Side — 2 in. (50.8 mm)
Rear — 5 in. (127 mm)

Plywood Surface — A minimum plywood thickness — 5/8 inch (16 mm) is recommended.

Drywall Surface — Drywall over either wood or steel studs is acceptable.

Mounting Procedure

1. Install the two wall-mounting brackets to the sides of the Ethernet Workgroup Switch with the screws provided. Be sure that the tabs on the brackets are facing towards the top of the unit.

2. Use the provided template (PN 25L4906) to locate and mark the wall mounting screw positions.

3. Pre-drill the mounting holes.

4. Install the two mounting screws in the pre-drilled holes. Tighten each screw until the head is approximately 1/8 inch (3 mm) from the wall.

5. Using the two center holes in the mounting brackets, slide the brackets down securely into place over the screw heads, and then tighten each screw.

Installing Optional Modules

Two optional modules are available for the Ethernet Workgroup Switch—10/100BASE-TX (PN 30L7631) and 100BASE-FX (PN 30L7630), which are installed on the back panel of the switch.

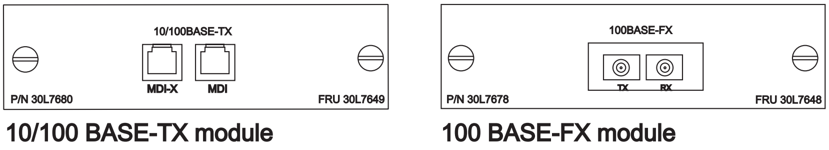


Figure 2-4. The 10/100BASE-TX and 100BASE-FX Optional Modules

To install these modules, perform the following steps:

Note: Expansion modules are ***not*** hot-swappable. You must remove power from the 8275 before installing or replacing an optional module.

Step 1. Turn off the power to the 8275 by disconnecting the power cable from the ac outlet.

Step 2. Remove the installed expansion module, or blank cover, by turning the two knobs on the back counterclockwise as shown in Figure 2-5 on page 2-6.

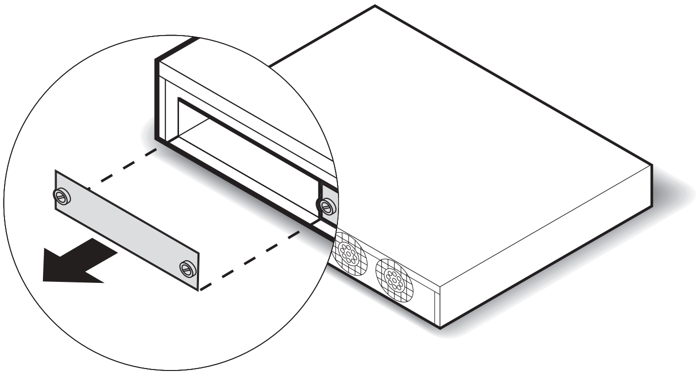


Figure 2-5. Removing the Blank Expansion Module Panel

Step 3. Insert the new expansion module (either type), ensuring that the edges slide through the guides as shown in Figure 2-6 on page 2-7.

Step 4. Turn the two knobs on the new expansion module clockwise until they are securely attached to the 8275.

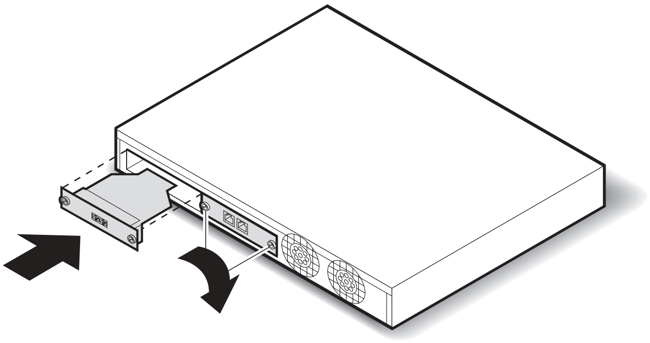


Figure 2-6. Installing an Expansion Module

Step 5. Connect the appropriate communication cable to the new expansion port.

Step 6. Reconnect the ac power cable to the wall outlet.

For information about attaching cables to the newly installed expansion module, see “Cabling” on page 2-8.

Power-On Checkout

Connect the ac power cable from the front panel to the power source. This powers on the Ethernet Workgroup Switch.

When the Ethernet Workgroup Switch is powered-on, it runs a power-on self-test (POST). The tests included are:

- PROM integration checksum test
- System DRAM access test
- Flash memory integration checksum test
- EEPROM read/write test
- NIC port access test
- Switch controller, packet buffer and filtering database test
- Front panel display test

A display area on the control panel called the *message zone* indicates the particular test being run. If all the tests pass, a final result `SELF TEST OK` is displayed in the message zone. If a test detects an error during the POST, an error message is displayed. For information on error messages, see Chapter 6, “Troubleshooting and Service.”

After the POST completes, the control panel defaults to UTILIZATION status.

Cabling

Cable Tips

- Avoid stretching or bending cables.
- Avoid routing cables near potential sources of electromagnetic interference, such as motorized devices or fluorescent lights.
- Route cables away from aisles and walkways to avoid creating trip hazards. Use floor cable covers to secure cables if such routes cannot be avoided.

Attaching Cables to Ports

1. Refer to your network documentation to determine each cable’s port or expansion slot assignment.
2. Using appropriate connectors, connect the cables to the ports or expansion slots.
3. Label each end of the cables so that it is easy to identify the device at the other end of the cable. At the end of the cable nearest the switch, place a label containing a unique identifier for the cable, the location and MAC address of the device at the other end of the cable, and the number of the port to which the device is attached.
4. If required, at the attached device’s end of each cable, connect a cable from the device to any faceplate or other intermediate connection point, as appropriate.
5. At the end of the cable nearest the attached device, place a label containing a unique identifier for the cable, the location, and MAC address of the Ethernet Workgroup Switch at the other end of the cable, and the number of port to which the device is attached.

Connecting a Null Modem Cable to the Management Port

You can connect the management port directly to a local workstation by using a null-modem cable, or you can use a serial cable and a modem to connect to a remote workstation.

Using a Local Workstation

To access the Ethernet Workgroup Switch locally, perform the following steps.

1. Connect one end of a null-modem cable to the Ethernet Workgroup Switch management port labeled EIA 232.
2. Connect the other end of the cable to the communications port on your workstation.

Using a Remote Workstation

To access the Ethernet Workgroup Switch remotely, perform the following steps.

1. Connect one end of a serial cable (direct connection) to the Ethernet Workgroup Switch management port labeled EIA 232.

2. Connect the other end of the cable to your modem.

For information on setting up a session through the management port, see “Setting Up a Management Session” on page 4-1.

Chapter 3. Control Panel Management

The control panel is an effective management tool for monitoring and configuring the Ethernet Workgroup Switch. It displays the following types of information:

- Port Utilization
- Port Statistics
- Port Configuration
- Unit Configuration

Control Panel

The control panel, shown in Figure 3-1, has the following features:

- Vacuum Fluorescent Display (VFD) – Displays port and switch information in an easy-to-read format.
- Control Keys (Menu, Scroll, and Enter) – Allow you to select the port or switch information you want to display.
- Status and Activity Indicators – Display general switch status and activity.

Figure 3-1 shows the Ethernet Workgroup Switch control panel.

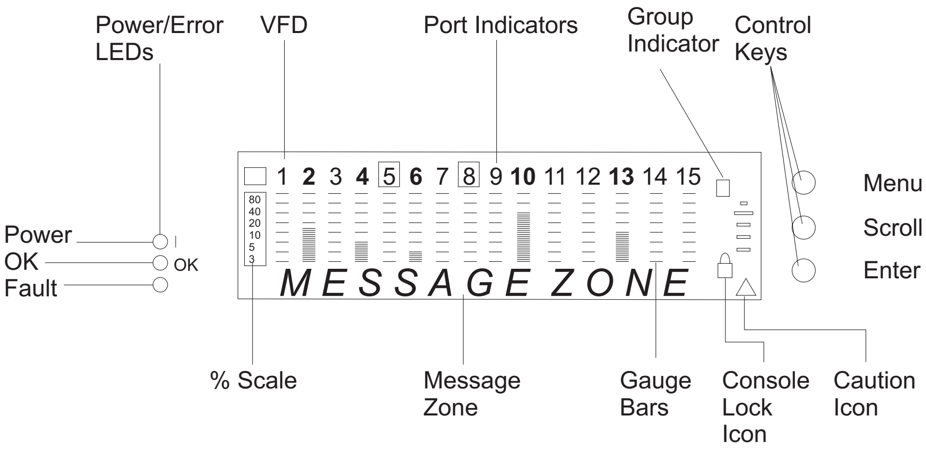


Figure 3-1. The Control Panel

VFD Display

The VFD displays the following port and system information:

% The relative percentage of utilization or collision. Each port has its own % scale.

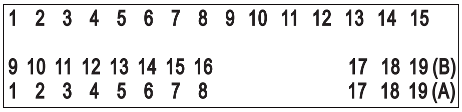
Port Indicators Identify the number of the port, and with their brightness, indicate status information (see Table 3-1 on page 3-2).

Group ID's (A-B)

Identify the group of ports

- For Model 217 :

With Group ID showing ***A***, port numbers *1 to 8* represent ports 1 to 8 and port numbers *13 to 15* represent ports 17 to 19. With Group ID showing ***B***, port numbers *1 to 8* represent ports 9 to 16 and port numbers *13 to 15* still represent ports 17 to 19.

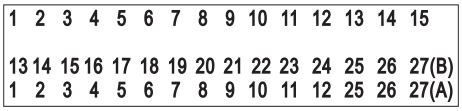


```
1  2  3  4  5  6  7  8  9  10  11  12  13  14  15

9 10 11 12 13 14 15 16                 17  18  19(B)
1  2  3  4  5  6  7  8                 17  18  19(A)
```

Figure 3-2. All ports view for Model 217

- For Model 225 :

With Group ID showing ***A***, port numbers *1 to 12* represent ports 1 to 12 and port numbers *13 to 15* represent ports 25 to 27. With Group ID showing ***B***, port numbers *1 to 12* represent ports 13 to 24 and port numbers *13 to 15* still represent ports 25 to 27.



```
1  2  3  4  5  6  7  8  9  10  11  12  13  14  15

13 14 15 16 17 18 19 20 21 22  23  24  25  26  27(B)
1  2  3  4  5  6  7  8  9  10  11  12  25  26  27(A)
```

Figure 3-3. All ports view for Model 225

Port Indicator Frame (□)

Identifies which ports are disabled or partitioned. (see Table 3-1)

Table 3-1. Port Information

Port Indicators	Frame	Indicates
Normal	Off	Port is available but link is down.
Bright	Off	Port is available and link is up.
Blinking	Off	Link is up and transmitting or receiving data.
Bright	On	The port is disabled by the administrator, or the Operation Status=No, or a network loop is detected.
Bright	Blinking	The port is auto-partitioned due to a broadcast storm alarm.
Off	Off	The expansion port is not installed (ports 18 and 19 only on Model 217/port 26 and 27 only on Model 225).

Message Zone Displays test messages, menu items, and status information.

Gauge Bars Display port-related information such as utilization, collisions, or configuration.

SNMP Indicates that the switch is SNMP-manageable.

WWW Indicates that the web management feature is enabled.

Lock Icon Indicates that the control panel configuration is locked.

Caution Icon Indicates a switch malfunction or a broadcast storm was detected.

OOB Indicates out-of-band is enabled.

Control Keys

The control keys are used to navigate through and make selections from the various menus.

Table 3-2 lists the function of each key.

Table 3-2. Control Keys

Key	Action
Menu	Return to the previous level
Scroll	Choose another topic within the same level
Enter	Go to the next level or view status

Power and Error Indicators

The Ethernet Workgroup Switch has three LEDs that display switch power and error status. Refer to Figure 3-1 on page 3-1 for the location of the LEDs.

Table 3-3 lists the LEDs and their meanings.

Table 3-3. Status LEDs and Their Meanings

LED	Position	State	Meaning
| (Power) (green)	Top	On	The Ethernet Workgroup Switch power supply current is good.
		Off	The Ethernet Workgroup Switch power supply current is bad or the power cord is not connected.
OK (green)	Middle	On	The Ethernet Workgroup Switch is working correctly.
		Off	The Ethernet Workgroup Switch is not working correctly.
		Blinking	Diagnostics are in progress.

Table 3-3. Status LEDs and Their Meanings

LED	Position	State	Meaning
Unlabeled (Fault) (amber)	Bottom	On	A power-on failure has occurred.
		Off	The Ethernet Workgroup Switch is working correctly.
		Blinking	Diagnostics are in progress.

Menu Structure

Figure 3-4 shows the control panel's menu structure.

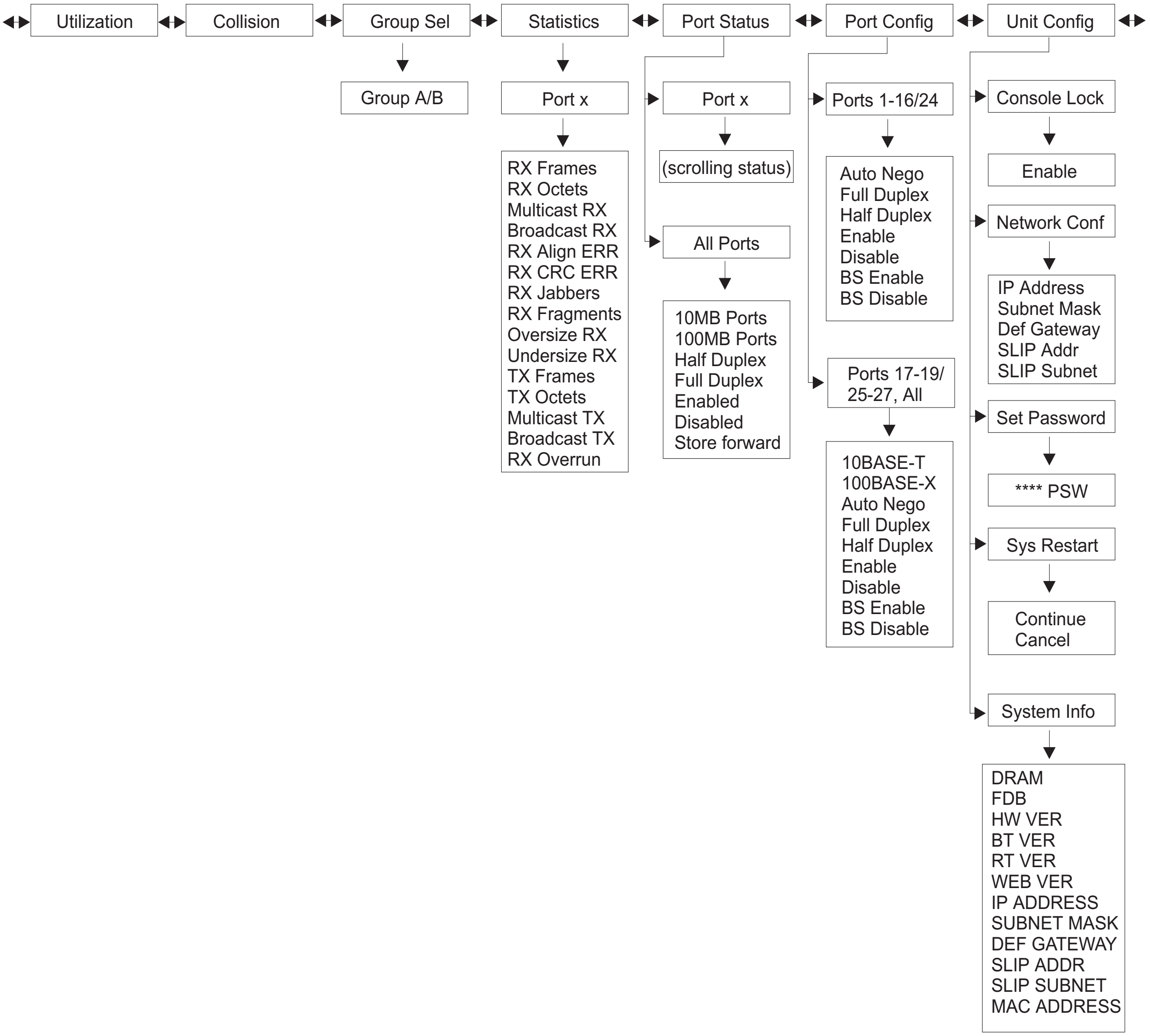


Figure 3-4. Main Structure

Control Panel Inactivity

If the control keys are not used for a period of 15 minutes, the port and switch configuration automatically locks. The message zone switches to displaying UTILIZATION unless COLLISIONS were being displayed. You must unlock the control panel to access the port configuration and unit configuration menus. The default password is 0000.

To unlock the control panel, scroll to **UNIT CONFIG** and press **ENTER**. Scroll to the first digit of the password and press **ENTER**. Scroll to the second digit of the password and press **ENTER**. Repeat until all digits are entered. The control panel is now unlocked.

To lock the control panel at any time, scroll to **CONSOLE LOCK** and press **ENTER**. When **ENABLE** is displayed, press **ENTER**. The lock icon appears and the console panel remains locked until the password is entered.

After an hour of inactivity, the VFD turns off. Pressing any control key reactivates the VFD.

Monitoring Network Utilization

The UTILIZATION menu displays the bandwidth used on each linked port. When the network traffic is greater than 40%, the gauge bars turn amber indicating heavy traffic. This additional traffic uses more system resources, reduces performance, and increases collisions. The Ethernet Workgroup Switch defaults to showing the UTILIZATION menu.

The utilization level corresponds to the speed and the duplex mode at which the port has been set. For example, for a port set at 10 Mbps, half-duplex, 100% utilization indicates 10 Mbps. If the same port was full-duplex, 100% utilization indicates 20 Mbps.

Table 3-4 lists 100% utilization for Ethernet Workgroup Switch ports.

Table 3-4. Bandwidth

Bandwidth	100% Utilization
10 Mbps, half duplex	10 Mbps
10 Mbps, full duplex	20 Mbps
100 Mbps, half duplex	100 Mbps
100 Mbps, full duplex	200 Mbps

Monitoring Collision Level

The COLLISION menu displays the % of collisions on each linked port. The gauge bars indicate the percentage of collision, which is calculated as:

```
Collision Ratio (%) = (Number of packets collided / Number of packets
transmitted) * 100
```

Note: When COLLISION is displayed, the control panel does not revert to

UTILIZATION even if the control panel has been inactive for more than 15 minutes.

Monitoring Detailed Port Statistics

The STATISTICS menu shows various statistic counters for each port. To display a port's statistics, select **STATISTICS**, scroll and select the port number. You can then scroll through the various statistics. Each counter displays the accumulated value since the last time the Ethernet Workgroup Switch was powered on or restarted.

You can display the following statistics:

RX FRAMES The total number of frames received on the switch port. It includes unicast, broadcast, and multicast packets.

RX OCTETS The total number of octets of data received on the switch port.

MULTICAST-RX The total number of good packets received that were directed to a multicast address. Broadcast packets are not included.

BROADCAST-RX The total number of broadcast packets received that were directed to a broadcast address. Multicast packets are not included.

RX-ALIGN ERR The total number of packets received that had a length between 64 and 1518 octets (excluding framing bits, but including FCS octets), that have a bad FCS with a non-integral number of octets.

RX-CRC ERR The total number of packets received that had a length between 64 and 1518 octets (excluding framing bits, but including FCS octets), that have a bad FCS with an integral number of octets.

RX-JABBERS The total number of packets that were received that were longer than 1518 octets and had an FCS error or alignment error.

RX-FRAGMENTS The total number of packets that were received that were less than 64 octets and had an FCS error or alignment error.

OVERSIZE RX The total number of packets that were received that were longer than 1518 octets (including FCS octets but excluding framing bits) and were otherwise well formed. If Long Frame Handling is enabled, only packets longer than 1535 octets are counted.

UNDERSIZE-RX The total number of packets that were received that were less than 64 octets (including FCS octets but excluding framing bits) and were otherwise well formed.

TX FRAMES The total number of packets (including bad packets) that were transmitted successfully.

TX OCTETS The total number of octets (including bad packets) that were transmitted successfully.

MULTICAST-TX The total number of good packets transmitted that were directed to a multicast address. Broadcast packets are not included.

BROADCAST-TX The total number of broadcast packets transmitted that were directed to a broadcast address. Multicast packets are not included.

RX OVERRUN The total number of packets lost due to lack of switch resources during packet reception.

Monitoring Port Status

The PORT STATUS menu shows the current operating mode of an individual port or all ports. The Ethernet Workgroup Switch allows a great deal of flexibility in the monitoring of various ports. For example, ports 1 to 16 on Model 217 and ports 1 to 24 on Model 225 can operate in half- or full- duplex. Ports 17 to 19 on Model 217 and ports 25 to 27 on Model 225 can operate in half- or full-duplex at 10 Mbps or 100 Mbps with the TX module and at 100 Mbps with the FX module.

To check the status of all ports, select **PORT STATUS** and then scroll and select **ALL PORTS**. You can then scroll through the various port statuses. The highlighted gauge bars show which ports are running at the status displayed in the message zone. For example, if the message zone reads FULL DUPLEX, then a gauge bar would identify each full-duplex port.

To check the status of an individual port, select **PORT STATUS** and then scroll and select the port number. The various statuses for the selected port automatically cycle through the message zone.

Note: The port does not need to be linked to view statuses.

The following is a list of port statuses:

- 10MB PORTS
- 100MB PORTS
- HALF DUPLEX
- FULL DUPLEX
- ENABLED
- DISABLED
- STORE-FWD

Configuring Ports

The PORT CONFIG menu allows you to configure individual ports or configure all ports at the same time. The ports must be configured to match the devices at the other end of the link. Settings such as speed and duplex mode must be identical. Asterisks (*) identify the current settings. All ports default to AUTO NEGO. When the AUTO NEGO mode is set, the highest speed and duplex mode supported by both ends are negotiated. If AUTO NEGO is not selected, the speed setting is not selectable on ports 1 to 16 on Model 217/ports 1 to 24 on Model 225 (they must run at 10 Mbps), but you must set the appropriate duplex mode (full or half).

To configure all ports, select **PORT CONFIG**, select **ALL PORTS**, scroll through the settings to the one you want to configure, and press **Enter** until an asterisk (*) is displayed.

The following is a list of port configuration options (for all ports):

- 10BASE-T (configure only 10BASE-T ports)
- 100BASE-X (configure only 100BASE-TX or FX ports)
- AUTO-NEGO
- FULL DUPLEX
- HALF DUPLEX
- ENABLE
- DISABLE
- BS ENABLE
- BS DISABLE

To configure an individual port, select **PORT CONFIG**, scroll through and select the port number you want to configure, scroll through the settings to the one you want to configure, and press **Enter** until an asterisk (*) is displayed.

The following is a list of port configuration options (for individual ports):

- AUTO-NEGO
- FULL DUPLEX
- HALF DUPLEX
- ENABLE
- DISABLE
- BS ENABLE
- BS DISABLE

Protecting Against Broadcast Storms

Broadcast storms congest the network with broadcast packets. An Ethernet Workgroup Switch can detect a broadcast storm in less than one second.

When Broadcast Storm Protection is enabled (BS ENABLE), the switch starts monitoring the incoming packets at all the ports to see if any port is creating a broadcast storm. As soon as the broadcast storm is detected, the port creating the storm is partitioned temporarily. The frame around the port indicator blinks in the control panel, the message zone displays BRDCST STORM, and the caution icon blinks. The port is continuously sampled against the broadcast storm threshold level. When the broadcast storm level falls below the broadcast storm threshold level, the port is reconnected.

The default value for broadcast storm protection is set to enable (BS ENABLE). The default value for broadcast storm threshold (Bcast Alarm Level) is MIDDLE.

For more information on broadcast storm detection and thresholds, see “Switch Port Control/Status” on page 4-19.

Unit Configuration

The UNIT CONFIG menu allows you to configure the Ethernet Workgroup Switch.

Table 3-5 lists the Ethernet Workgroup Switch unit configuration options.

Table 3-5. Unit Configuration Settings

CONSOLE LOCK	ENABLE
NETWORK CONF	IP ADDRESS SUBNET MASK DEF GATEWAY SLIP ADDR SLIP SUBNET
SET PASSWORD	* * * * PSW
SYS RESTART	CONTINUE
SYSTEM INFO	(scrolls)

Console Lock

Control panel security is maintained by the console lock. The lock icon is an amber lock symbol on the lower right of the VFD. When the control panel is unlocked, it automatically locks again after 15 minutes of inactivity. You must unlock the control panel to access the port configuration and unit configuration menus. The default password is 0000.

To unlock the control panel, scroll to UNIT CONFIG and press **Enter**. Scroll to the first digit of the password and press **Enter**. Scroll to the second digit of the password and press **Enter**. Repeat until all digits are entered. The control panel is now unlocked.

To lock the control panel at any time, scroll to CONSOLE LOCK and press **Enter**. When ENABLE is displayed, press **Enter**. The lock icon appears and the console remains locked until the password is entered.

Network Configuration

To configure the network configuration of your Ethernet Workgroup Switch, scroll to UNIT CONFIG and press **Enter**. Scroll to NETWORK CONF and press **Enter**. You then can scroll and select an item described in Table 3-6 on page 3-10.

Note: To configure the addresses, you must scroll and press enter for ***each*** digit until all 12 digits are entered.

Table 3-6. Network Configuration

IP Address	The dotted decimal IP address assigned to the Ethernet Workgroup Switch. The default address is 0.0.0.0.
Subnet Mask	The dotted decimal subnet mask assigned to the Ethernet Workgroup Switch. The default subnet mask is 0.0.0.0.
Default Gateway	The dotted decimal IP address of the default router assigned to the Ethernet Workgroup Switch. The default address is 0.0.0.0.
SLIP Addr	The dotted decimal IP address of the modem assigned to the Ethernet Workgroup Switch. The default address is 0.0.0.0.
SLIP Subnet	The dotted decimal subnet mask assigned to the Ethernet Workgroup Switch. The default subnet mask is 0.0.0.0.

Setting the Password

To change the control panel password, scroll to UNIT CONFIG and press **Enter**. Scroll to SET PASSWORD and press **Enter**. When the first asterisk (*) blinks, scroll to the first new digit and press **Enter**. Repeat until all four digits are entered. If you enter a password of all asterisks (****), the control panel lock is disabled.

Attention: Be sure to record your new password. If you forget the password, you must access the Ethernet Workgroup Switch through a management session using the management port or Telnet to reconfigure another control panel password. For more information, see “User Authentication” on page 4-41.

System Restart

To restart the Ethernet Workgroup Switch, scroll to UNIT CONFIG and press **Enter**. Scroll to SYS RESTART and press **Enter**. Scroll to CONTINUE and press **Enter**. This begins a warm restart. If you have entered SYS RESTART and you want to cancel the restart, scroll to CANCEL and press **Enter**, or press **Menu** to return to UNIT CONFIG.

System Information

The following system information is displayed:

- Size of DRAM
- Size of FDB (Filtering Data Base)
- HW version
- BT version
- RT version
- WEB version
- IP address
- Subnet Mask
- Default Gateway
- SLIP address
- SLIP Subnet

- MAC address

To display the system information, scroll to UNIT CONFIG and press **Enter**. Scroll to SYS INFO and press **Enter**. The system information is displayed in a continuous cycle until it is interrupted by pressing any control key.

Chapter 4. Using the Management Interface

The Ethernet Workgroup Switch incorporates a powerful management interface that can be used to manage switch ports using a terminal emulation program that supports VT100 emulation (referred to as *out of band*), or using Telnet over an IP connection (referred to as *in band*).

Note: Telnet is a component of most TCP/IP applications. You need to install TCP/IP before you can use this interface.

Setting Up a Management Session

You can set up a management session by connecting a direct, null modem cable between the EIA 232 management port on the Ethernet Workgroup Switch and the communication port of your PC or terminal.

To connect a local terminal to the Ethernet Workgroup Switch, perform the following steps:

Step 1. Install a terminal emulation application such as Windows Hyperterminal on your PC.

Step 2. Configure the terminal emulation application as follows:

Baud rate	19200
Parity	None
Data bits	8
Stop bits	1
Flow Control	Off

Step 3. If you are using Microsoft Windows terminal emulation, disable the “Use Function, Arrow, and Ctrl Keys for Windows” option in the Terminal Preferences menu under Settings.

Step 4. Connect the EIA 232 management port on the Ethernet Workgroup Switch to your PC or DTE device using a null-modem cable or straight-through cable and null-modem adapter. The Ethernet Workgroup Switch has a 9-pin, male connector. For more information, see “Connecting a Null Modem Cable to the Management Port” on page 2-8.

Step 5. Press **Enter** 2 or 3 times and the login panel to the management interface appears.

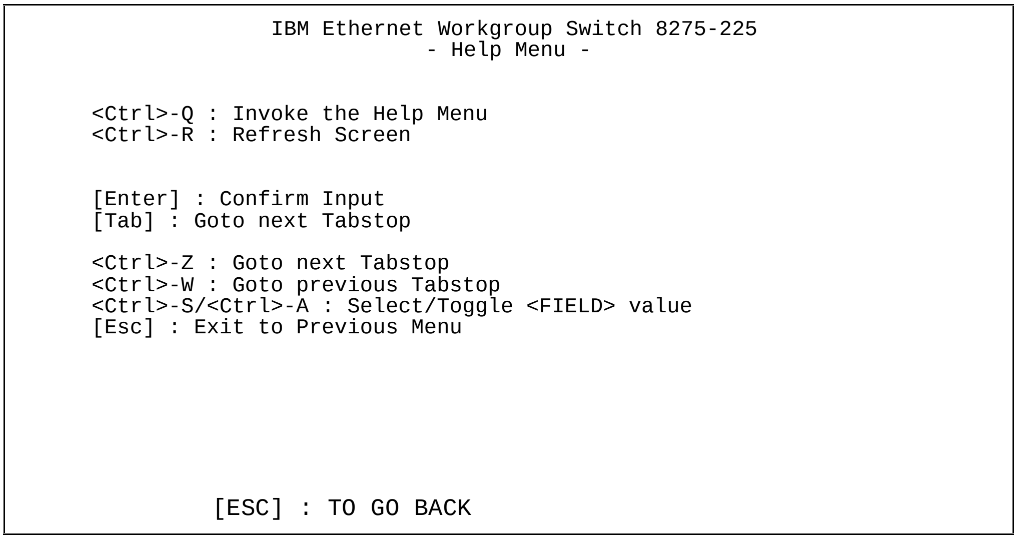
Setting up a Telnet Session

You can use any Telnet application that emulates VT100 to establish a Telnet session with the Ethernet Workgroup Switch over a TCP/IP network. Only one Telnet session can be active at a time. Before you can start a Telnet session, you must configure IP parameters for the Ethernet Workgroup Switch. This is done by using the Network Configuration Menu on the control panel or locally through the management port. To open a Telnet session, you must specify the IP address assigned to the Ethernet Workgroup Switch. For information on how to specify an IP address in your Telnet application, refer to your Telnet application documentation. When the connection is established, the management interface login panel is displayed, as shown in Figure 4-2 on page 4-3.

Note: Your Telnet connection must be over the management VLAN.

Navigating the Management Session

Selecting Help on any panel presents the Help Menu shown in Figure 4-1



```
                    IBM Ethernet Workgroup Switch 8275-225
                                - Help Menu -


      <Ctrl>-Q : Invoke the Help Menu
      <Ctrl>-R : Refresh Screen


      [Enter] : Confirm Input
      [Tab] : Goto next Tabstop

      <Ctrl>-Z : Goto next Tabstop
      <Ctrl>-W : Goto previous Tabstop
      <Ctrl>-S/<Ctrl>-A : Select/Toggle <FIELD> value
      [Esc] : Exit to Previous Menu






               [ESC] : TO GO BACK
```

Figure 4-1. Help Menu

The Help menu lists the additional keystroke functions.

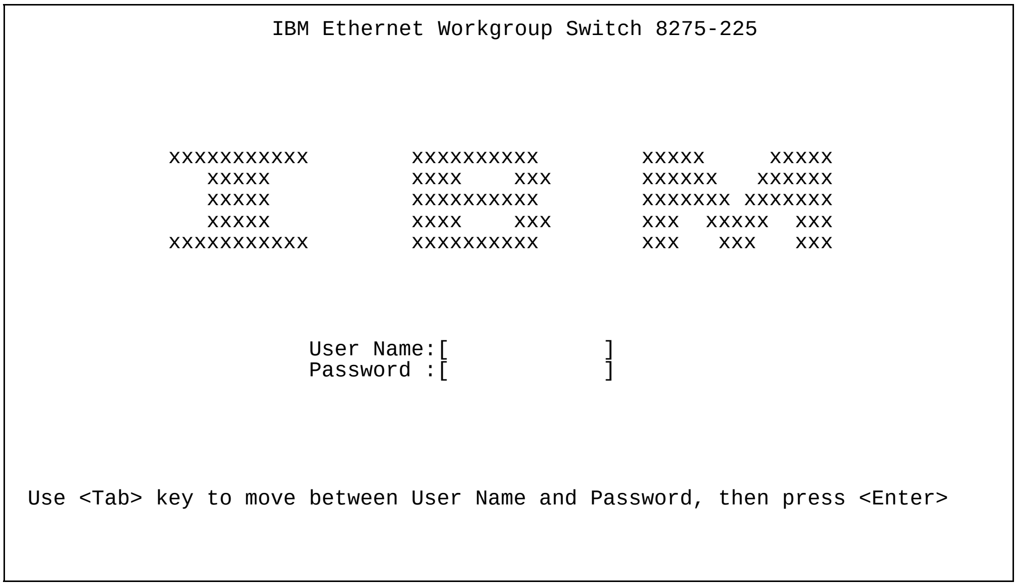
Panel Command Usage: The commands available on each panel are displayed at the bottom of the panel. Use the Tab key and Up/Down arrow keys to toggle through available commands. Use the Left and Right arrow keys to toggle through selections (indicated by “< >“) within a command.

If a field on a panel is enclosed by brackets, [*field*], then you must type in the value for that field. If a field on a panel is enclosed by less-than and greater-than signs, <*field*>, then you can toggle through a list of values to be used for that field.

Beginning a Management Session

The login panel, as shown in Figure 4-2 , appears when you establish a connection between your terminal and the Ethernet Workgroup Switch.

Note: If the login panel does not appear, press **Enter** two or three times.



```
                   IBM Ethernet Workgroup Switch 8275-225




           xxxxxxxxxxx        xxxxxxxxxx        xxxxx     xxxxx
              xxxxx           xxxx    xxx       xxxxxx   xxxxxx
              xxxxx           xxxxxxxxxx        xxxxxxx xxxxxxx
              xxxxx           xxxx    xxx       xxx  xxxxx  xxx
           xxxxxxxxxxx        xxxxxxxxxx        xxx   xxx   xxx



                      User Name:[           ]
                      Password :[           ]




Use <Tab> key to move between User Name and Password, then press <Enter>
```

Figure 4-2. Login Panel

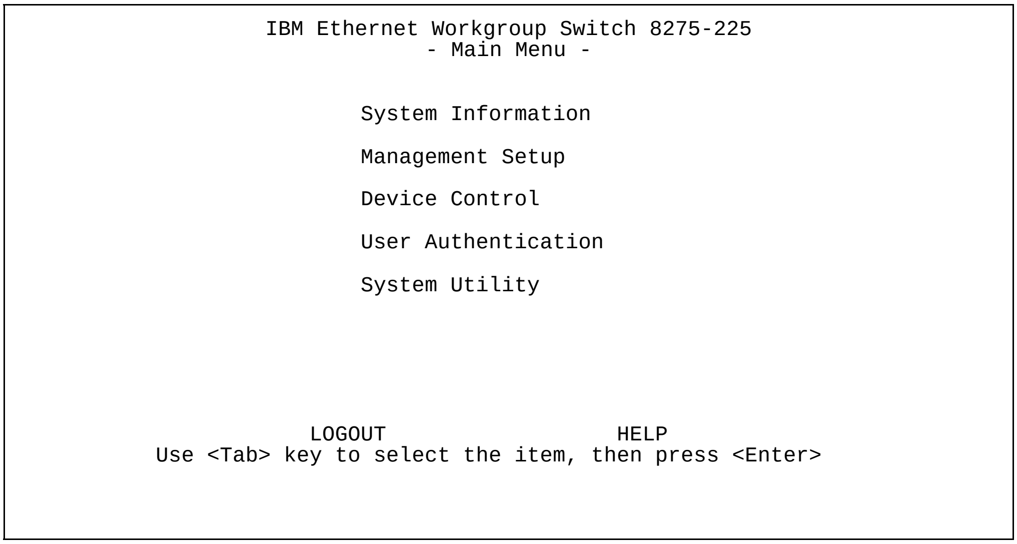
To begin a console session, perform the following steps:

1. Type your *user name*, if one has been configured. User names and passwords are ***not*** case sensitive. The Ethernet Workgroup Switch comes with two default user names. One default is “admin” and requires no password. The other default is “guest” and has a password of “guest”. Press **Enter**.

2. Type in the password, if one has been configured. There is no default password for a user name. Press **Enter** to advance to the Main Menu.

Main Menu

On the Main Menu, shown in Figure 4-3 , you can select an item by highlighting with the **Tab** key and then pressing **Enter**.



```
                    IBM Ethernet Workgroup Switch 8275-225
                                - Main Menu -

                           System Information

                           Management Setup

                           Device Control

                           User Authentication

                           System Utility




                        LOGOUT                  HELP
            Use <Tab> key to select the item, then press <Enter>
```

Figure 4-3. Main Menu

System Information Allows you to view general system information as well as specifying location and contact information.

Management Setup Allows you to view and specify management configurations.

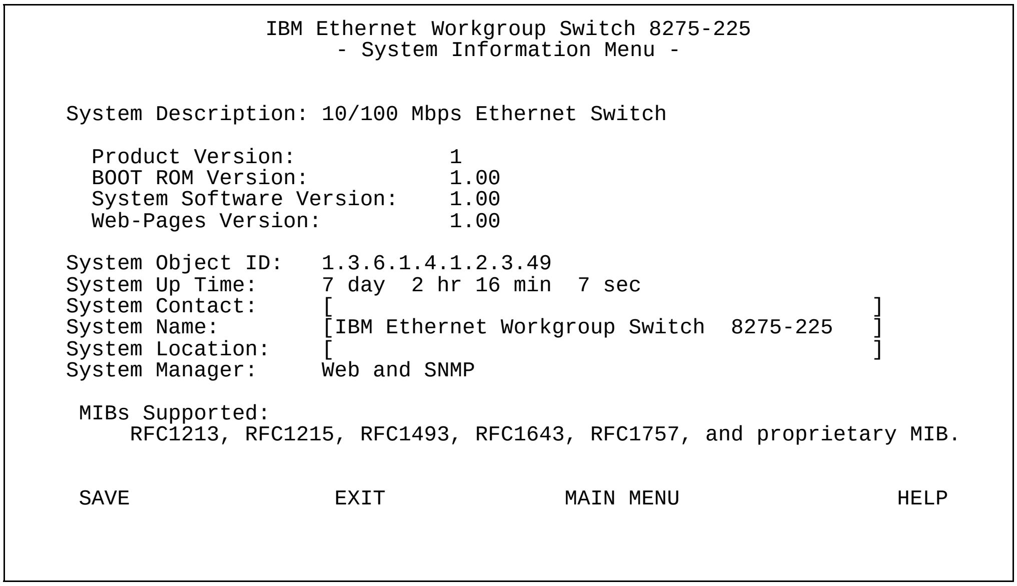
Device Control Allows you to configure switch ports, permanent addresses, VLANs, Spanning Tree Protocol, and Trunk groups.

User Authentication Allows you to configure user names and passwords.

System Utility Allows you to configure software downloads, restart options, Telnet session timeout intervals, configuration file uploads, and ping to other hosts.

System Information

Selecting this option displays the System Information panel shown in Figure 4-4 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                         - System Information Menu -


    System Description: 10/100 Mbps Ethernet Switch

      Product Version:            1
      BOOT ROM Version:           1.00
      System Software Version:    1.00
      Web-Pages Version:          1.00

    System Object ID:   1.3.6.1.4.1.2.3.49
    System Up Time:     7 day  2 hr 16 min  7 sec
    System Contact:     [                                           ]
    System Name:        [IBM Ethernet Workgroup Switch  8275-225   ]
    System Location:    [                                           ]
    System Manager:     Web and SNMP

     MIBs Supported:
         RFC1213, RFC1215, RFC1493, RFC1643, RFC1757, and proprietary MIB.


     SAVE                EXIT              MAIN MENU                 HELP
```

Figure 4-4.   System Information Menu

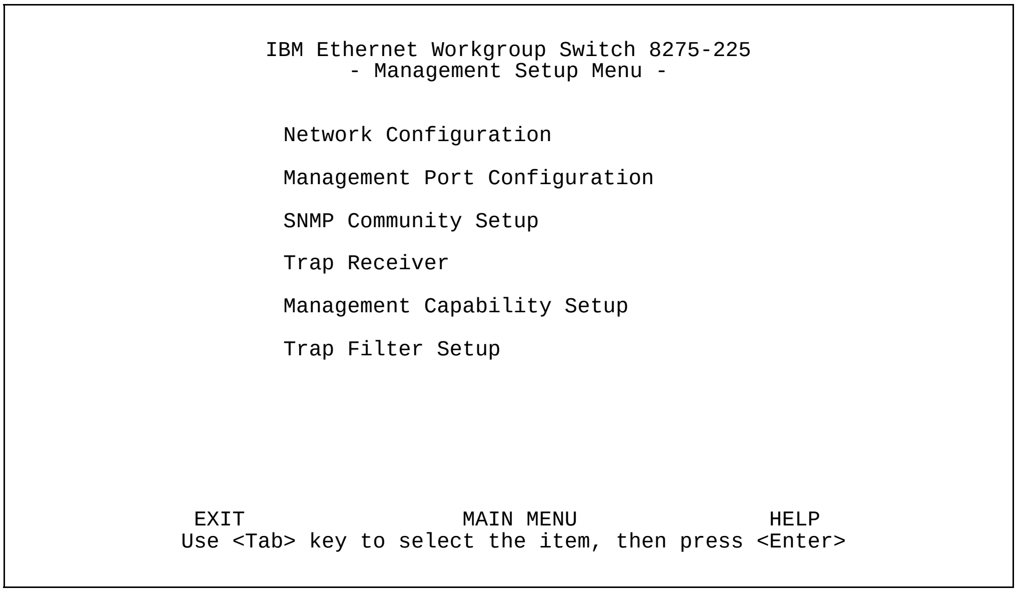
The System Information Menu provides information related to the version of the system software installed on the Ethernet Workgroup Switch.

You can specify up to 48 alphanumeric characters each for the System Name, Contact, and Location to provide useful information to all users concerning the Ethernet Workgroup Switch. The information on this panel should be kept current in case assistance is required.

Note: You must select **Save** to save any changes you have made.

Management Setup

Selecting this option displays the Management Setup Menu shown in Figure 4-5 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                          - Management Setup Menu -

                     Network Configuration

                     Management Port Configuration

                     SNMP Community Setup

                     Trap Receiver

                     Management Capability Setup

                     Trap Filter Setup




              EXIT                 MAIN MENU                HELP
             Use <Tab> key to select the item, then press <Enter>
```

Figure 4-5.   Management Setup Menu

Network Configuration Sets IP address, subnet mask, default gateway address, and SLIP address.

Management Port Configuration Views and configures management port configuration.

SNMP Community Setup Configures community names and access.

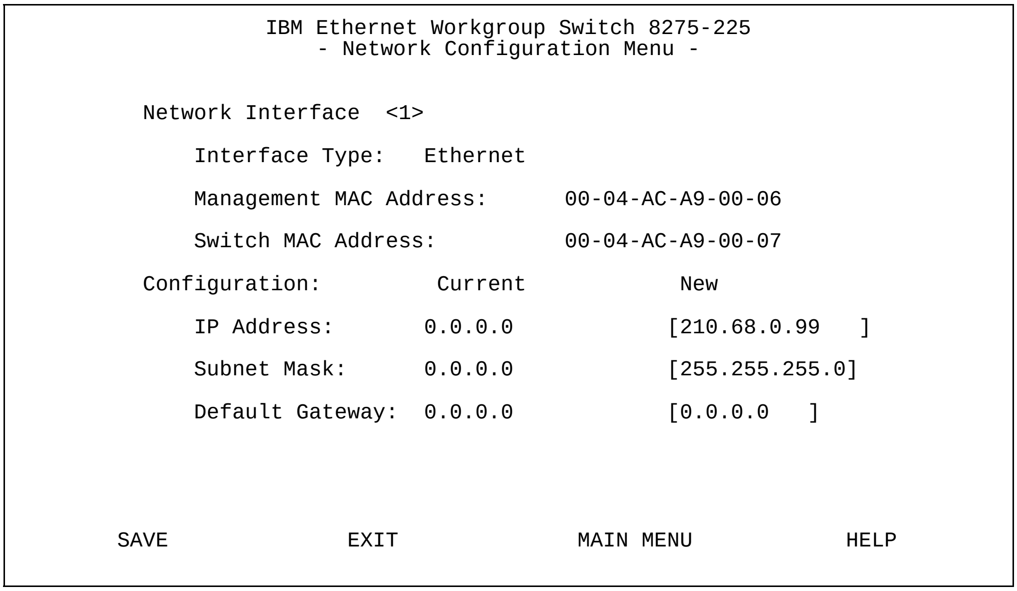
Trap Receiver Sets up community trap addresses.

Management Capability Setup Enables or disables Web access and out-of-band management control.

Trap Filter Setup Enables or disables trap filters.

Network Configuration

Selecting this option displays the Network Configuration Menu shown in Figure 4-6 and Figure 4-7 on page 4-8. Network Interface 1 lets you to set up an Ethernet connection to monitor and configure the Ethernet Workgroup Switch using an Ethernet port.



```
                    IBM Ethernet Workgroup Switch 8275-225
                        - Network Configuration Menu -


          Network Interface  <1>

              Interface Type:   Ethernet

              Management MAC Address:      00-04-AC-A9-00-06

              Switch MAC Address:          00-04-AC-A9-00-07

          Configuration:         Current            New

              IP Address:       0.0.0.0            [210.68.0.99   ]

              Subnet Mask:      0.0.0.0            [255.255.255.0]

              Default Gateway:  0.0.0.0            [0.0.0.0    ]



        SAVE              EXIT              MAIN MENU           HELP
```

Figure 4-6.   Network Configuration Menu - Ethernet Connection

IP Address The dotted decimal address assigned to the Ethernet Workgroup Switch

Subnet Mask The dotted decimal subnet mask assigned to the Ethernet Workgroup Switch

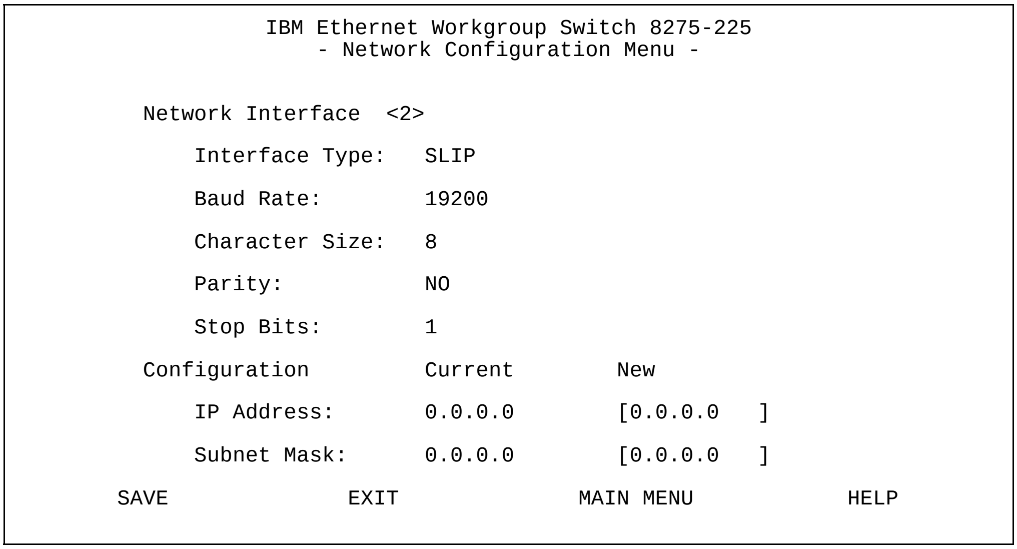
Default Gateway The dotted decimal IP address of the default router assigned to the Ethernet Workgroup Switch

The Ethernet Workgroup Switch must be restarted before the IP address, subnet mask, and default gateway can take effect. To ensure the new information is correct, a “ping” should be done from another device connected to the Ethernet Workgroup Switch.

Notes:

1. The switch does not respond to ping packets that are greater than 1484 bytes.
2. The management MAC address is used for BootP.
3. The Switch MAC address (STP MAC address) is used for STP and GVRP.

Network Interface 2 lets you to set up a SLIP connection to monitor and configure the Ethernet Workgroup Switch remotely using a modem.



```
                    IBM Ethernet Workgroup Switch 8275-225
                        - Network Configuration Menu -

          Network Interface  <2>

              Interface Type:   SLIP

              Baud Rate:        19200

              Character Size:   8

              Parity:           NO

              Stop Bits:        1

          Configuration         Current        New

              IP Address:       0.0.0.0        [0.0.0.0   ]

              Subnet Mask:      0.0.0.0        [0.0.0.0   ]

        SAVE             EXIT             MAIN MENU           HELP
```

Figure 4-7.   Network Configuration Menu - SLIP Connection

The baud rate, character size, parity, and stop bits are for information only and are not configurable on this menu.

Baud Rate The current baud rate of the management port. This baud rate can be changed on the Management Port Configuration Menu. (See Figure 4-9 on page 4-10.)

Character Size 8-bit character size.

Parity None.

Stop Bits One stop bit.

IP Address The dotted decimal address assigned to the SLIP interface of the Ethernet Workgroup Switch.

Subnet Mask The dotted decimal subnet mask assigned to the Ethernet Workgroup Switch.

Note: The new configuration becomes the current configuration after a system restart.

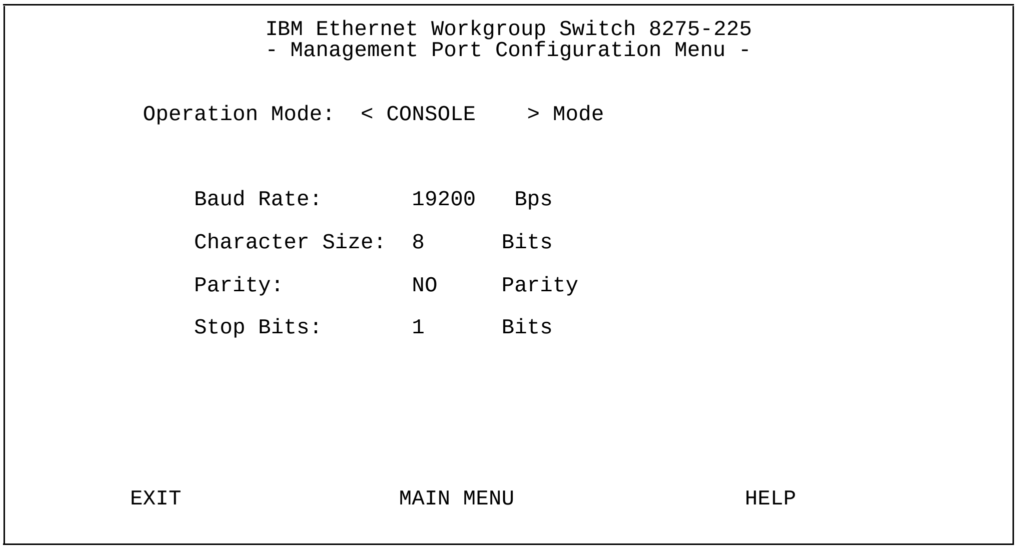
Management Port Configuration

Selecting this option displays the Management Port Configuration Menu shown in Figure 4-8 and Figure 4-9 on page 4-10.

You can select either console mode or out-of-band mode.

Console Mode

Selecting console mode displays the settings used for a local connection to the management port.



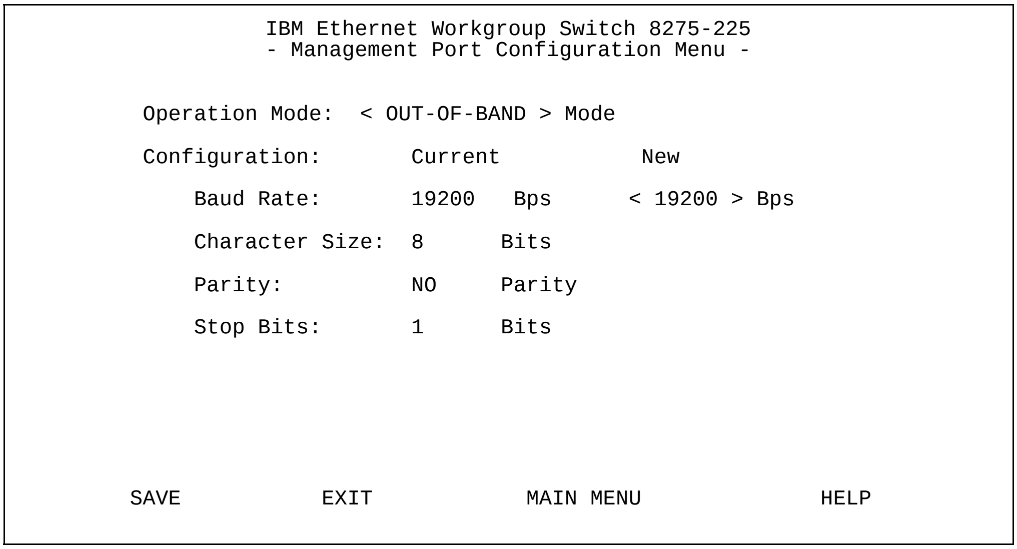
```
                    IBM Ethernet Workgroup Switch 8275-225
                    - Management Port Configuration Menu -

          Operation Mode:  < CONSOLE    > Mode


              Baud Rate:        19200   Bps

              Character Size:   8      Bits

              Parity:           NO     Parity

              Stop Bits:        1      Bits




         EXIT                 MAIN MENU                  HELP
```

Figure 4-8. Management Port Configuration Menu - Console Mode

Note: For console mode, the information displayed on the Management Port Configuration Menu is for information only and is not configurable.

Out-of-Band Mode

Selecting Out-of-Band mode lets you specify the baud rate that to be used when connecting to the management port through a modem.



```
                    IBM Ethernet Workgroup Switch 8275-225
                    - Management Port Configuration Menu -


          Operation Mode:  < OUT-OF-BAND > Mode

          Configuration:       Current           New

              Baud Rate:       19200   Bps      < 19200 > Bps

              Character Size:  8      Bits

              Parity:          NO     Parity

              Stop Bits:       1      Bits




         SAVE           EXIT            MAIN MENU              HELP
```

Figure 4-9. Management Port Configuration Menu - Out-of-Band

Baud Rate The baud rate of the management port. This baud rate can set to one of the following speeds:

- 19200 (This is the default value for both console mode and OOB)
- 9600
- 4800
- 2400

Character Size 8-bit character size.

Stop Bits One stop bit.

Select **Save** to retain the new configuration. The new configuration takes effect if out-of-band is enabled.

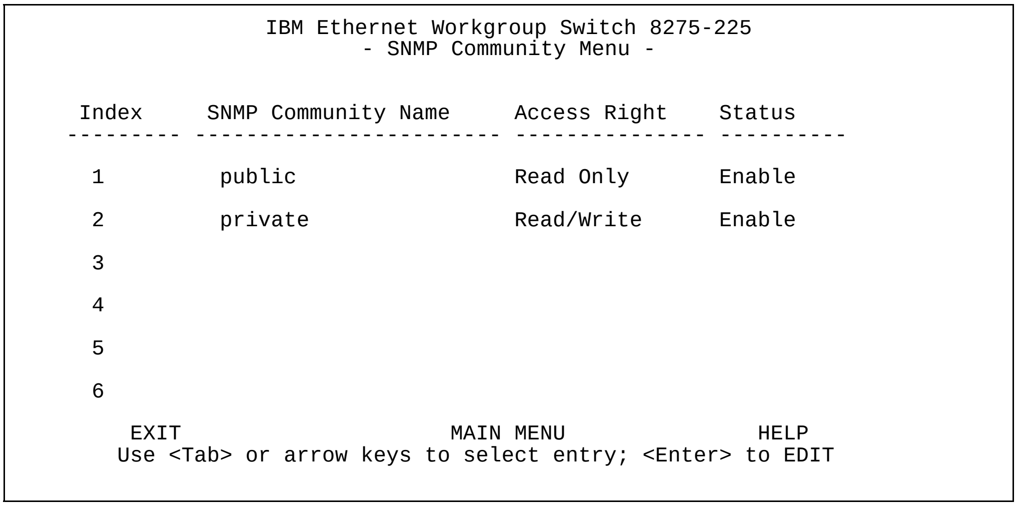
Notes: When SLIP is enabled, the management port can be used for Out-of-Band SLIP connections only. You cannot connect to a console session using VT100 terminal emulation. If the SLIP connection is malfunctioning, you can disable the connection by either of the following ways:

4. Telnet into the Ethernet Workgroup Switch, disable Out-of-Band management using the Management Capability Setup Menu (see Figure 4-12 on page 4-14), and restart the switch.
5. Disconnect your modem and serial cable from the management port. Connect a null modem cable and establish a VT100 emulation session and re-power (cold start) the switch. When `10SEC TO OOB` is displayed on the switch's control panel, press ENTER on the local console. This connects you to the console session

login menu which enables you to disable Out-of-Band Management using the Management Capability Setup Menu (see Figure 4-12 on page 4-14) and restart the switch.

SNMP Community Setup

Selecting this option displays the SNMP Community Menu shown in Figure 4-10 .



```
                IBM Ethernet Workgroup Switch 8275-225
                       - SNMP Community Menu -


 Index     SNMP Community Name     Access Right    Status
--------- ------------------------ --------------- ----------

  1         public                 Read Only       Enable

  2         private                Read/Write      Enable

  3

  4

  5

  6

     EXIT                     MAIN MENU              HELP
    Use <Tab> or arrow keys to select entry; <Enter> to EDIT
```

Figure 4-10. SNMP Community Menu

This menu lets you assign up to six SNMP communities.

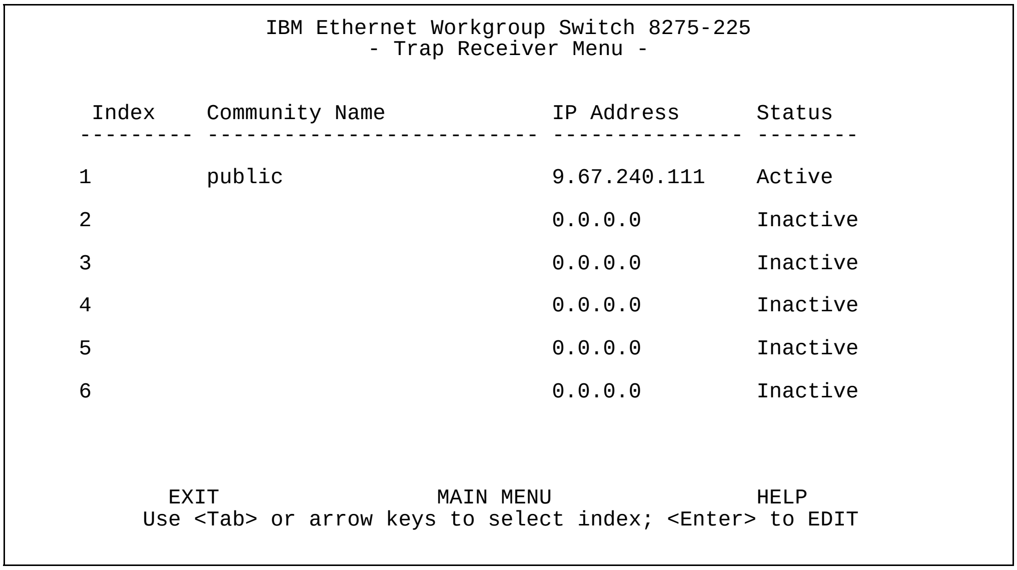
Table 4-1. SNMP Community Setup

Input Field	**Values**
SNMP Community Name	Name that identifies each SNMP community. Maximum number of characters is 16. Alphanumeric symbols such as @, #, %, $, leading blanks are not allowed and trailing blanks are neglected.
Access Right	Read Only or Read/Write
Status	Enable or Disable

Note: Community Names are case sensitive.

Trap Receiver

Selecting this option displays the Trap Receiver Menu shown in Figure 4-11 .



```
               IBM Ethernet Workgroup Switch 8275-225
                       - Trap Receiver Menu -


 Index    Community Name             IP Address      Status
--------- -------------------------- --------------- --------

1         public                     9.67.240.111    Active

2                                    0.0.0.0         Inactive

3                                    0.0.0.0         Inactive

4                                    0.0.0.0         Inactive

5                                    0.0.0.0         Inactive

6                                    0.0.0.0         Inactive



       EXIT                 MAIN MENU                HELP
     Use <Tab> or arrow keys to select index; <Enter> to EDIT
```

Figure 4-11. Trap Receiver Menu

Traps are messages sent across a network to an SNMP Network Manager. These messages alert the manager of changes in the Ethernet Workgroup Switch. You can set up to six trap receivers.

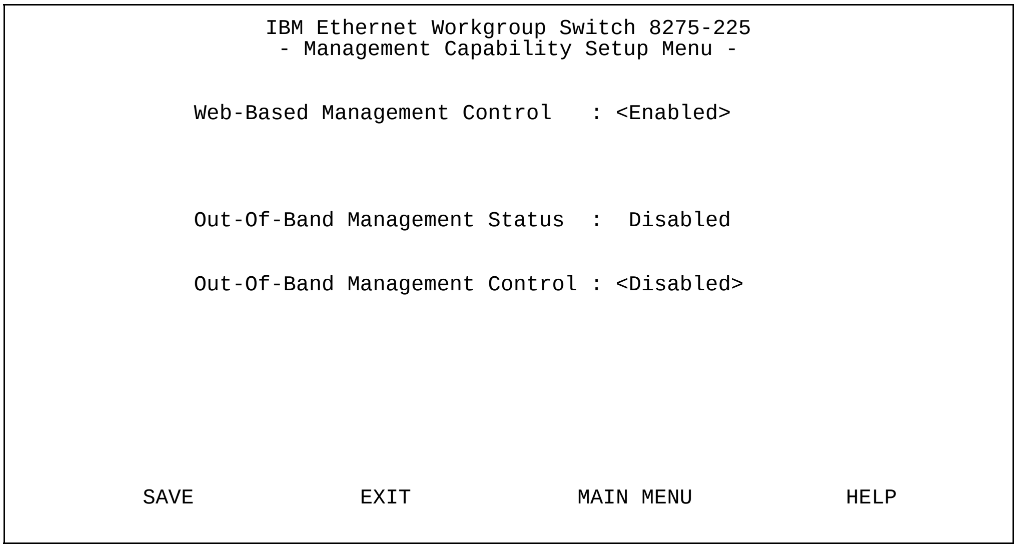
Community Name The SNMP community string of the remote network manager (up to 16 characters).

IP Address The IP Address of the remote network manager station to which traps should be sent.

Status A trap receiver's status can be either active or inactive. Trap receivers with active status will receive all traps sent by the switch.

Management Capability Setup

Selecting this option displays the Management Capability Setup Menu shown in Figure 4-12 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                     - Management Capability Setup Menu -

              Web-Based Management Control   : <Enabled>



              Out-Of-Band Management Status  :  Disabled

              Out-Of-Band Management Control : <Disabled>






          SAVE             EXIT             MAIN MENU           HELP
```

Figure 4-12. Management Capability Setup Menu

This menu lets you enable or disable access to the Ethernet Workgroup Switch through a web browser and out-of-band management capability through the Local Console/Remote Telent, or the SNMP Manager.

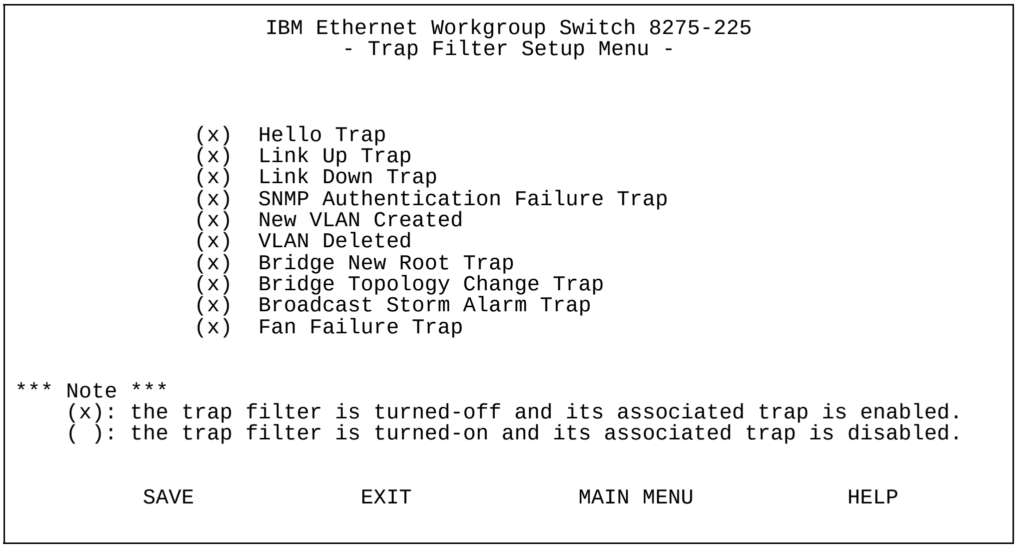
Web-Based Management Control Enables or disables Web-based management. The new configuration takes effect after selecting **Save**.

Out-Of-Band Management Status Displays the current status.

Out-Of-Band Management Control Enables or disables out-of-band management (SLIP). The screen must be saved and the Ethernet Workgroup Switch must be restarted before the new setting becomes effective.

Trap Filter Setup

Selecting this option displays the Trap Filter Setup Menu shown in Figure 4-13 .



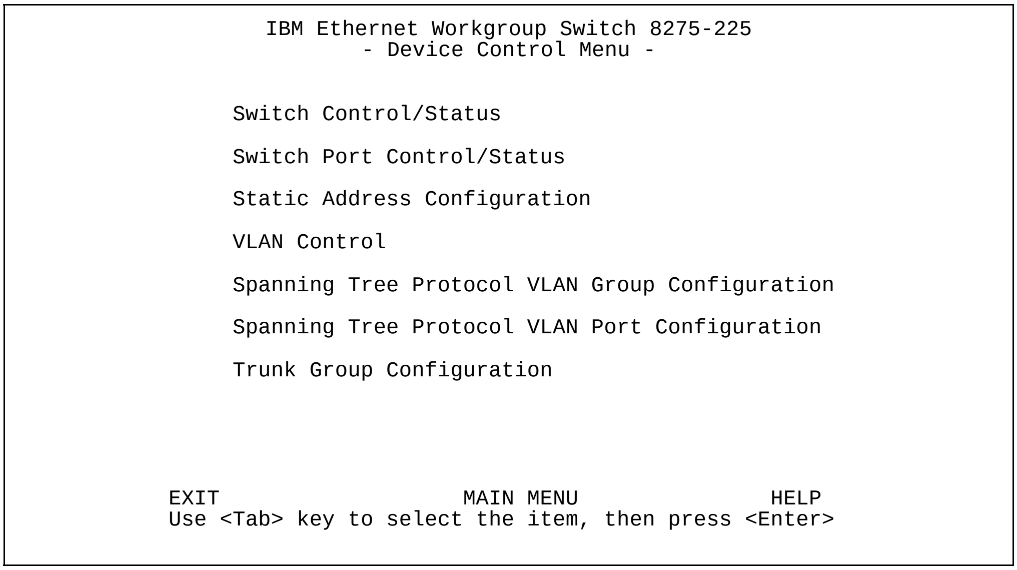
```
                    IBM Ethernet Workgroup Switch 8275-225
                          - Trap Filter Setup Menu -



              (x)  Hello Trap
              (x)  Link Up Trap
              (x)  Link Down Trap
              (x)  SNMP Authentication Failure Trap
              (x)  New VLAN Created
              (x)  VLAN Deleted
              (x)  Bridge New Root Trap
              (x)  Bridge Topology Change Trap
              (x)  Broadcast Storm Alarm Trap
              (x)  Fan Failure Trap


*** Note ***
    (x): the trap filter is turned-off and its associated trap is enabled.
    ( ): the trap filter is turned-on and its associated trap is disabled.


          SAVE             EXIT             MAIN MENU            HELP
```

Figure 4-13. Trap Filter Setup Menu

This menu lets you enable or disable trap filters for those traps defined by RFC1215 and RFC1516. Deselecting a trap filter enables the filter and no traps of that type are sent. The default setting enables all traps.

Device Control

Selecting this option displays the Device Control Menu shown in Figure 4-14 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                           - Device Control Menu -

                  Switch Control/Status

                  Switch Port Control/Status

                  Static Address Configuration

                  VLAN Control

                  Spanning Tree Protocol VLAN Group Configuration

                  Spanning Tree Protocol VLAN Port Configuration

                  Trunk Group Configuration



             EXIT                   MAIN MENU              HELP
             Use <Tab> key to select the item, then press <Enter>
```

Figure 4-14. Device Control Menu

This menu lets you view and configure the Ethernet Workgroup Switch ports and virtual LANs (VLANs).

Switch Control/ Status Enables or disables port monitor function and also selects the Management VLAN.

Switch Port Control/ Status Names and configures ports 1 to 19 on Model 217 and ports 1 to 27 on Model 225.

Static Address Configuration Permanently assigns a MAC address to a switch port.

VLAN Control Configures virtual LANs and GVRP associated parameters.

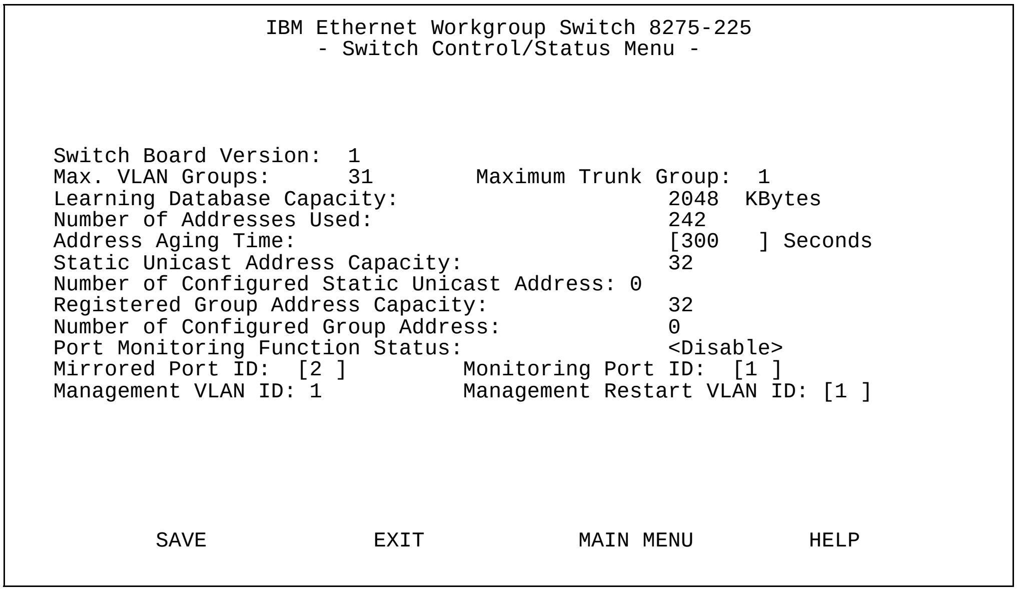
STP Group Configuration Configures the STP parameters for the switch.

STP Port Configuration Configures the individual STP ports parameters for the switch.

Trunk Group Configuration Names and configures the Trunk group.

Switch Control/Status

Selecting this option displays the Switch Control/Status menu shown in Figure 4-15 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                        - Switch Control/Status Menu -



   Switch Board Version:  1
   Max. VLAN Groups:      31        Maximum Trunk Group:  1
   Learning Database Capacity:                     2048  KBytes
   Number of Addresses Used:                       242
   Address Aging Time:                             [300   ] Seconds
   Static Unicast Address Capacity:                32
   Number of Configured Static Unicast Address: 0
   Registered Group Address Capacity:              32
   Number of Configured Group Address:             0
   Port Monitoring Function Status:                <Disable>
   Mirrored Port ID:  [2 ]         Monitoring Port ID:  [1 ]
   Management VLAN ID: 1           Management Restart VLAN ID: [1 ]




           SAVE             EXIT            MAIN MENU         HELP
```

Figure 4-15. Switch Control/Status Menu

This menu displays general information about the switch.

Learning Database Capacity
Displays the maximum number of MAC addresses that can be learned by the system.

Number of Addresses Used
Displays the maximum number of currently learned MAC addresses.

Address Aging Time
Allows you to set the time of aging out the learned address. (ranging from 1 to 65535 seconds)

Static Unicast Address Capacity
Displays the maximum number of permanent unicast MAC addresses allowed.

Number of Configured Static Unicast Addresses
The number of permanent unicast MAC addresses that have been configured.

Port Monitoring Function Status
Allows you to enable or disable the port monitoring function. If enabled, packets received by or sent from the port specified by Mirrored Port ID will be copied to the port that is specified by the Monitoring Port ID.

Mirrored Port ID Allows you to specify the port to be monitored.

Monitoring Port ID This is the port ID to which monitored MAC address frames are sent, and the port to which you should attach your network analyzer to enable you to capture the monitored frames. The default is Port 1.

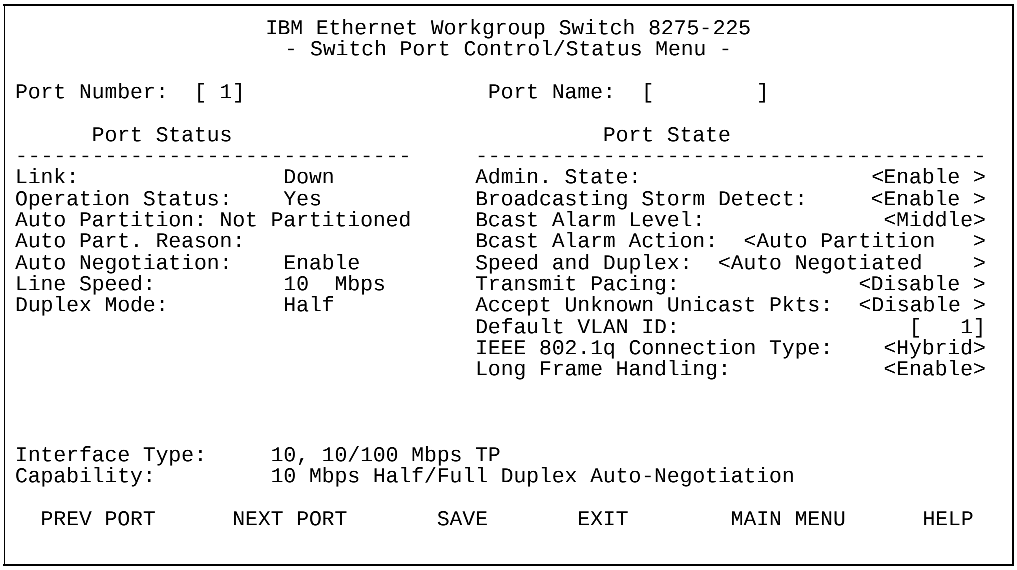
Management Restart VLAN ID Allows you to manually assign the VLAN ID which the system Network Management Unit is joined with after the next system restart.

Notes:

1. The monitoring port cannot be a Trunk Group member.
2. Select **Save** before you exit this menu to save any changes you have made.
3. These are reserved MAC addresses used by the switch which are part of the learned address database.

Switch Port Control/Status

Selecting this option displays the Switch Port Control/Status Menu shown in Figure 4-16 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                       - Switch Port Control/Status Menu -

Port Number:  [ 1]                   Port Name:  [        ]

      Port Status                             Port State
-------------------------------     ----------------------------------------
Link:                Down           Admin. State:                  <Enable >
Operation Status:    Yes            Broadcasting Storm Detect:     <Enable >
Auto Partition: Not Partitioned     Bcast Alarm Level:              <Middle>
Auto Part. Reason:                  Bcast Alarm Action:  <Auto Partition   >
Auto Negotiation:    Enable         Speed and Duplex:  <Auto Negotiated    >
Line Speed:          10  Mbps       Transmit Pacing:              <Disable >
Duplex Mode:         Half           Accept Unknown Unicast Pkts:  <Disable >
                                    Default VLAN ID:                  [   1]
                                    IEEE 802.1q Connection Type:    <Hybrid>
                                    Long Frame Handling:            <Enable>



Interface Type:     10, 10/100 Mbps TP
Capability:         10 Mbps Half/Full Duplex Auto-Negotiation

  PREV PORT      NEXT PORT       SAVE       EXIT        MAIN MENU      HELP
```

Figure 4-16. Switch Port Control/Status Menu

This menu lets you define the operation of individual switched ports.

Port Number Specifies the port number (Ports 1 to19 for Model 217 and ports 1 to 27 for Model 225) to be displayed.

Port Name Specifies the name of the switch port. You can specify up to sixteen characters for a port name.

Admin State Allows you to enable or disable a switch port. If you disable a port, the frame indicator around the port number on the control panel is lit and the port is partitioned.

Broadcasting Storm Detect Allows you to enable or disable the ability to detect broadcast storms. Enable is the default.

Bcast Alarm Level Allows you to set the relative threshold before a broadcast storm alarm is generated. You can specify High (30%), Middle (20%), or Low (10%). The percentage is calculated as:

```
%=(broadcast packets/total packets)*utilization.
```

Middle is the default.

Bcast Alarm Action Allows you to specify the action to be taken in the event of a broadcast storm alarm. You can specify:

- Auto Partition–partitions the port. The port is sampled continuously until the broadcast storm has subsided below the alarm level. The port is then reenabled. Auto Partition is the default.
- Trap Auto Partition–sends a trap message to the trap receiver and partitions the port until the broadcast storm subsides and the port is reenabled.
- Send Trap–only sends a trap message to the trap receiver. The switch port is not partitioned.
- No Action–no action is taken when an alarm level is reached.

Speed and Duplex

Allows you to specify the speed and mode of the switched port. You can specify Auto-Negotiation, 10 Mbps Full Duplex, 10 Mbps Half Duplex, 100 Mbps Full Duplex, or 100 Mbps Half Duplex. The selections are appropriate for the switch port and the device linking to the port. Auto-Negotiation is the default.

Transmit Pacing

Allows the switch to sense high network traffic and insert an extra amount of delay between transmission attempts. This reduces collision rates, reduces the number of retransmissions, reduces CPU utilization, and reduces network traffic.

Accept Unknown Unicast Pkts

If this option is enabled, a frame which has a unicast destination address not contained within the address lookup table is forwarded to all ports in the VLAN.

Default VLAN ID

Allows you to specify the default VLAN ID (ranging from 1 to 4094) which is defined as PVID in the IEEE 802.1q Standard (reference taken from IEEE P802.1Q/D10, March 20, 1998, page 45). A current limitation is set on the PVID, such that it cannot be set to a non-existing VLAN. To ensure that the port can always be set to the PVID, it has to be joined in the Registration Fixed mode. The default VLAN ID is 1.

IEEE 802.1q Connection Type

Allows you to specify the connection type based on IEEE 802.1q. You can specify:

- Access Link–a LAN segment used for multiplexing one or more VLAN-unaware device into a port of a VLAN bridge.
- Hybrid Link–when VLAN-unaware end-stations are added to a trunk link, the resultant link is commonly known as "Hybrid Link".

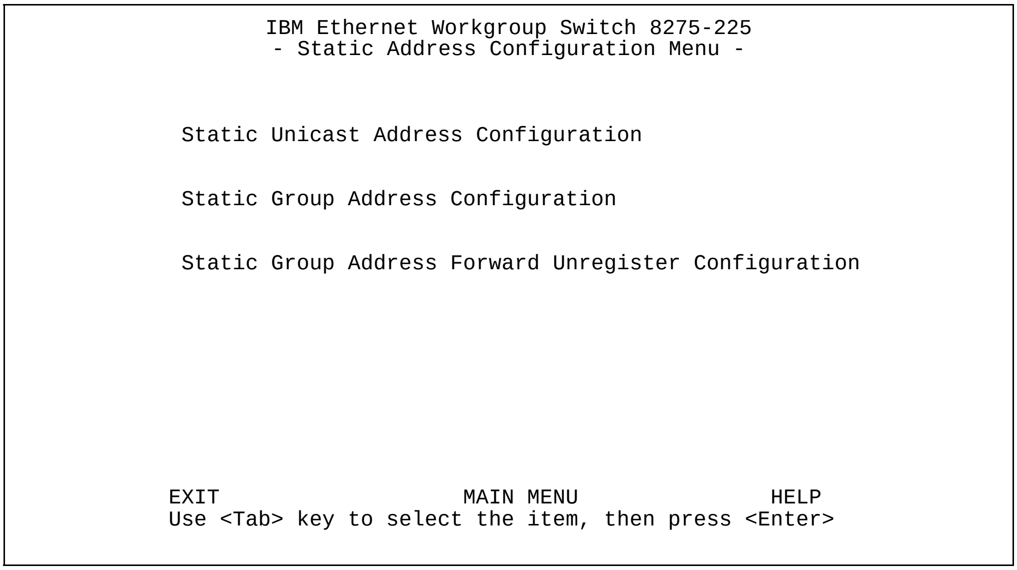
For more information for IEEE 802.1q see Appendix A.

Long Frame Handling

Allows frames of up to 1531 bytes to pass through the switch without error if no VLAN header is inserted, or 1535 if a VLAN header is inserted. If Long Frame Handling is disabled, the maximum received frame length is 1518 bytes. If a VLAN header is inserted into a 1518 bytes frame within the MAC, the frame will be stored as 1522 bytes within the switch.

Static Address Configuration

Selecting this option displays the Static Address Configuration Menu shown in Figure 4-17 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                    - Static Address Configuration Menu -


              Static Unicast Address Configuration


              Static Group Address Configuration


              Static Group Address Forward Unregister Configuration








             EXIT                   MAIN MENU              HELP
             Use <Tab> key to select the item, then press <Enter>
```

Figure 4-17. Static Address Configuration Menu

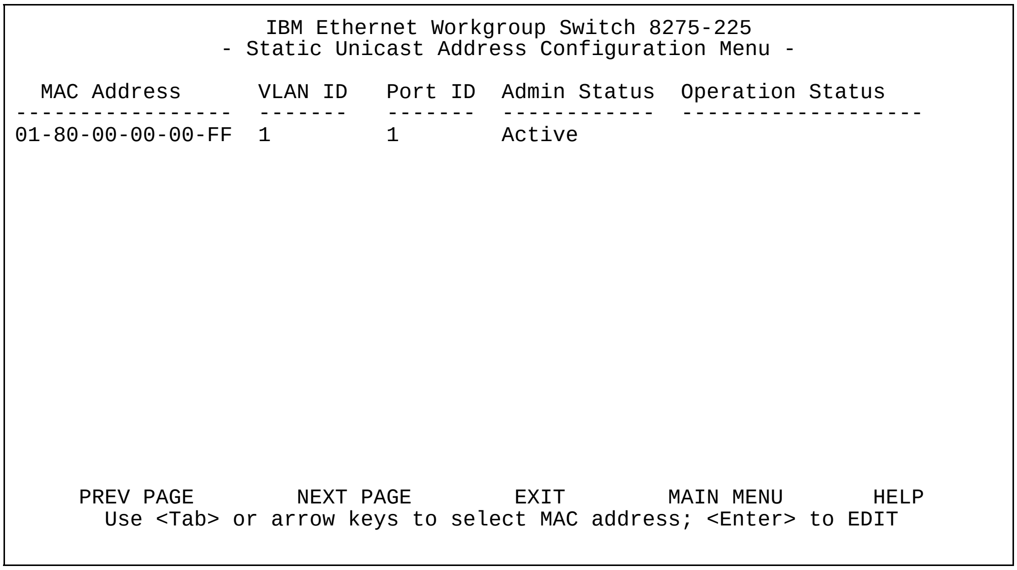
Static Unicast Address Configuration Allows you to define static MAC addresses to each port.

Static Group Address Configuration Allows you to define Group address for each set of ports.

Static Group Address Forward Unregister Configuration Allows you to specify the ports to which packets with unregistered static group address will be forwarded.

Static Unicast Address Configuration

Selecting this option displays the Static Unicast Address Configuration Menu shown in Figure 4-18 .



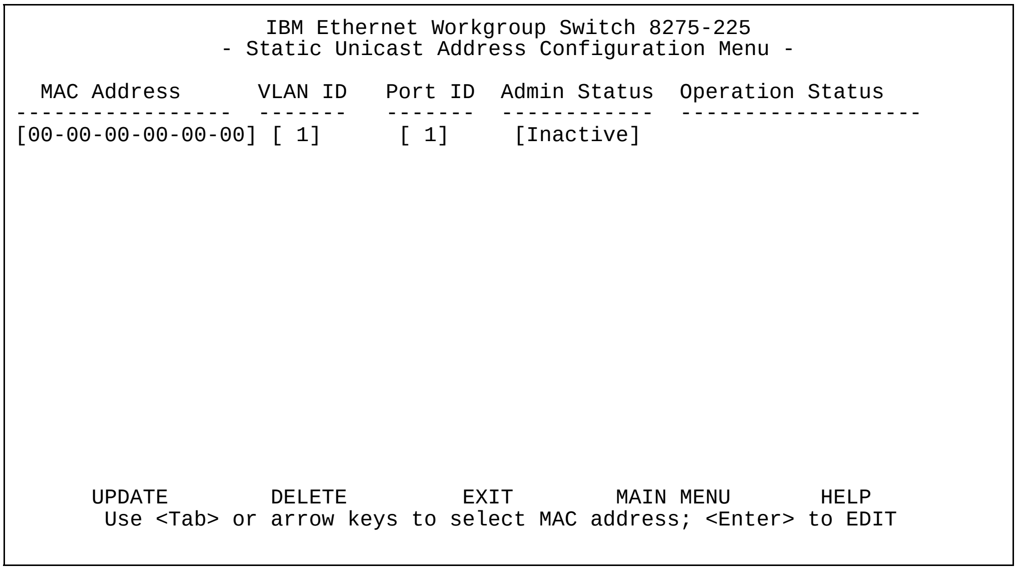
```
                    IBM Ethernet Workgroup Switch 8275-225
                - Static Unicast Address Configuration Menu -

  MAC Address      VLAN ID   Port ID  Admin Status  Operation Status
-----------------  -------   -------  ------------  -------------------
01-80-00-00-00-FF  1         1        Active

















     PREV PAGE        NEXT PAGE        EXIT        MAIN MENU       HELP
       Use <Tab> or arrow keys to select MAC address; <Enter> to EDIT
```

Figure 4-18. Static Unicast Address Configuration Menu - Primary

Note: All MAC addresses must be specified in canonical format (LSB).

This menu lets you define up to 32 static MAC addresses. If a Static Unicast address is assigned to a switch port and the port’s status is ***active***, then that MAC address can be connected only through that assigned switch port. If the device is connected to a port other than the assigned port, the packets are not sent.

To add, delete or edit a static MAC address, use the Tab key to select a blank or existing MAC address and press **ENTER**. The second level of Static Unicast Address Configuration Menu will be displayed as shown in Figure 4-19 on page 4-24.



```
                    IBM Ethernet Workgroup Switch 8275-225
                 - Static Unicast Address Configuration Menu -

  MAC Address      VLAN ID   Port ID  Admin Status  Operation Status
-----------------  -------   -------  ------------  -------------------
[00-00-00-00-00-00] [ 1]      [ 1]     [Inactive]
















      UPDATE        DELETE         EXIT        MAIN MENU       HELP
       Use <Tab> or arrow keys to select MAC address; <Enter> to EDIT
```

Figure 4-19. Static Unicast Address Configuration Menu - Secondary

To add a static MAC address:

1. Use the Tab key to move to a blank or existing MAC address.

2. Press **Enter** to add a MAC address.

3. Define the MAC address, VLAN ID, Port ID, and Admin Status.

4. Select **Update**.

5. Select **EXIT**.

6. Repeat Steps 1 through 5 for each MAC address.

   Note: There are 3 pages of MAC addresses. The next page will be activated when the current page is filled. Use the Next Page command to enter the second page.

To edit a static MAC address:

1. Use the Tab key to an existing MAC address.

2. Press **Enter** to edit.

3. Edit the VLAN ID, Port ID, and Admin Status.

4. Select **Update**.

5. Select **EXIT**.

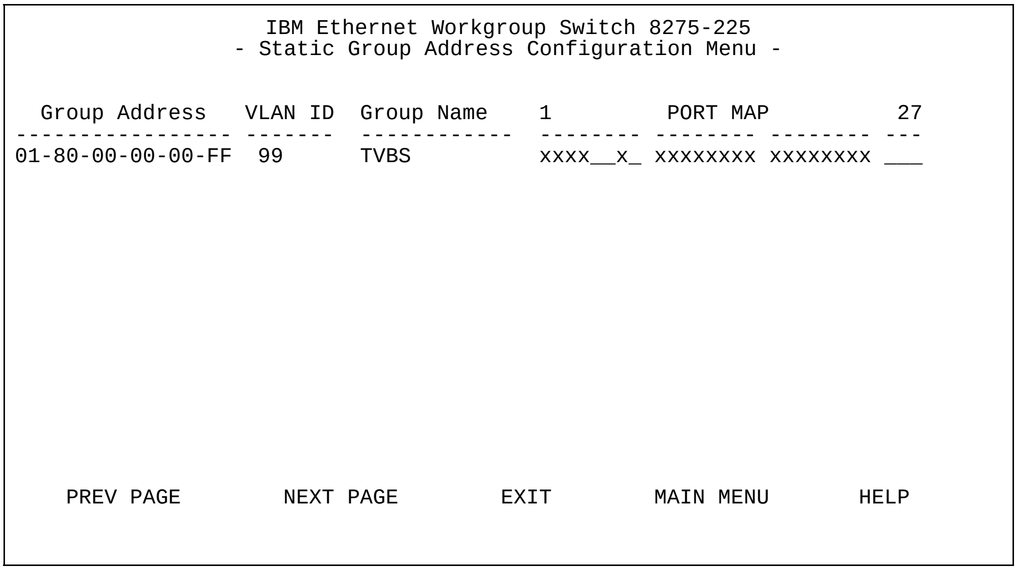
6. Repeat Steps 1 through 5 for each MAC address.

To delete a MAC address:

1. Use the **TAB** key to highlight an existing MAC address.
2. Press **Enter** to edit.
3. Press **Delete** and the MAC address is deleted.
4. Select **EXIT**.

Static Group Address Configuration

Selecting this option displays the Static Group Address Configuration Menu shown in Figure 4-20 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                 - Static Group Address Configuration Menu -


  Group Address   VLAN ID  Group Name    1         PORT MAP          27
----------------- -------  ------------  -------- -------- -------- ---
01-80-00-00-00-FF  99      TVBS          xxxx__x_ xxxxxxxx xxxxxxxx ___










    PREV PAGE        NEXT PAGE        EXIT        MAIN MENU       HELP
```

Figure 4-20. Static Group Address Configuration Menu

This menu lets you define a set of unique pairs of Static Group address and VLAN ID and assigns the associated ports to each pair. The Static Group address is used to tell the system how to handle the multicast/broadcast packets. The menu allows you to define a maximum of 32 Group addresses. The same Group addresses with two different VLAN IDs must be entered separately and are treated as different entities.

Group Address A MAC address entry that specifies a group address.

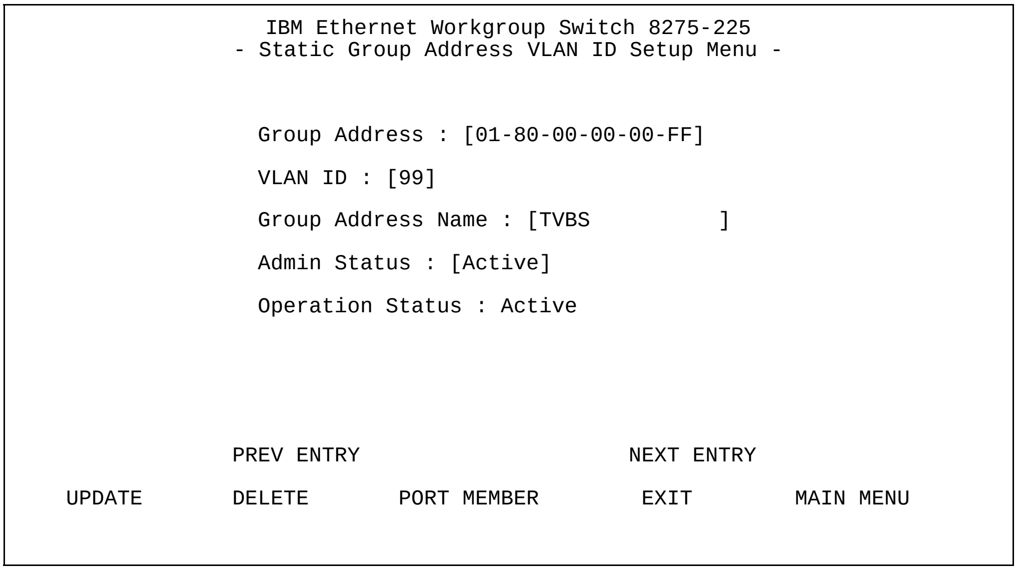
VLAN ID VLAN ID associated to the Group Address, ranging from 1 to 4094.

Group Name A name for each Group Address and VLAN ID pair.

PORT MAP Allows you to assign ports to each Group Address.

To add, delete or edit a static group address, use the Tab key to select a blank or existing MAC address and press **ENTER**. The second level of Static Group Address Configuration Menu will be displayed as shown in Figure 4-21 on page 4-27.

Note: The next page will be activated when the current page is filled. Use the **NEXT PAGE** command to enter the second page.



```
                    IBM Ethernet Workgroup Switch 8275-225
                 - Static Group Address VLAN ID Setup Menu -


                   Group Address : [01-80-00-00-00-FF]

                   VLAN ID : [99]

                   Group Address Name : [TVBS          ]

                   Admin Status : [Active]

                   Operation Status : Active




                 PREV ENTRY                    NEXT ENTRY

    UPDATE       DELETE       PORT MEMBER       EXIT        MAIN MENU
```

Figure 4-21. Static Group Address VLAN ID Setup Menu

To add/change a static group address:

1. Use the Tab key to select a blank or existing group address.

2. Press **Enter** to edit.

3. Define the Group Address, VLAN ID, and Group Name.

4. Select **Update**.

5. Select **PORT MEMBER** and define the Port Map.

6. Select **EXIT**.

7. Repeat Steps 1 through 4 for each group address.

To delete a group address:

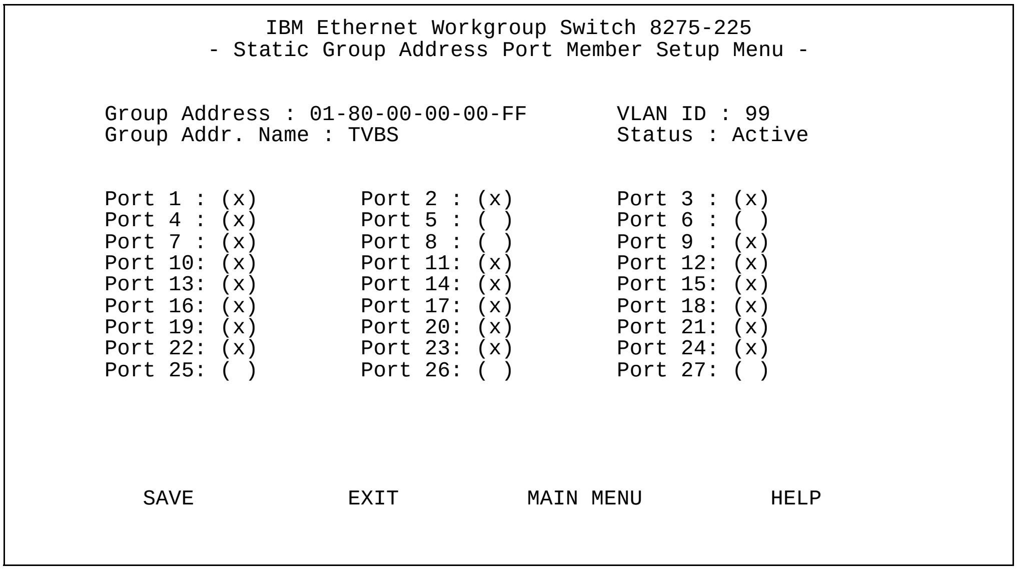
1. Use the **TAB** key to select an existing group address.

2. Press **Enter** to edit.

3. Press **Delete** to delete the group address.

4. Select **EXIT**.

To assign the port map to a group address, select PORT MEMBER. The Static Group Address Port Member Setup Menu is displayed as shown in Figure 4-22 on page 4-28.



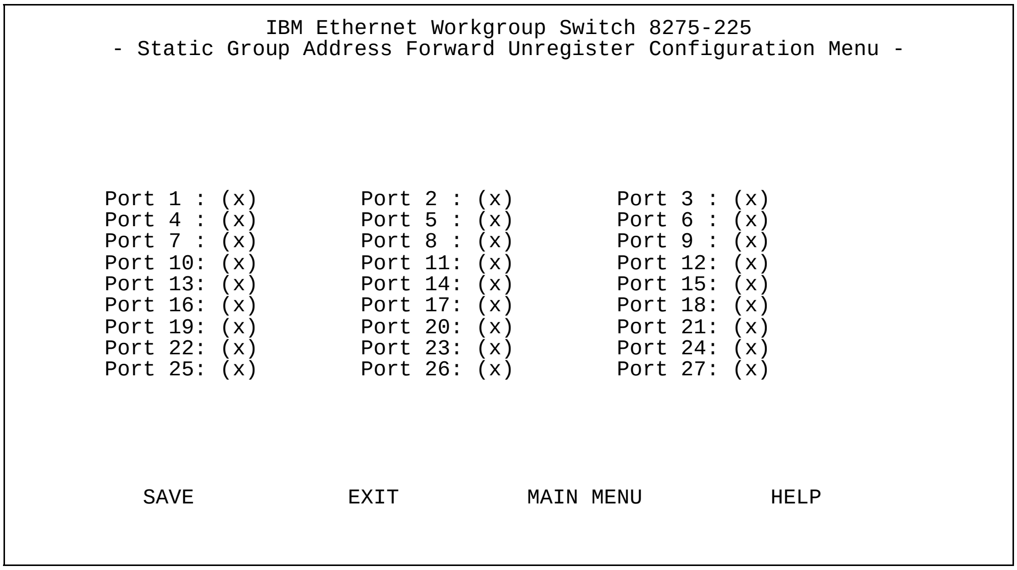
```
                 IBM Ethernet Workgroup Switch 8275-225
             - Static Group Address Port Member Setup Menu -


       Group Address : 01-80-00-00-00-FF       VLAN ID : 99
       Group Addr. Name : TVBS                 Status : Active


       Port 1 : (x)        Port 2 : (x)        Port 3 : (x)
       Port 4 : (x)        Port 5 : ( )        Port 6 : ( )
       Port 7 : (x)        Port 8 : ( )        Port 9 : (x)
       Port 10: (x)        Port 11: (x)        Port 12: (x)
       Port 13: (x)        Port 14: (x)        Port 15: (x)
       Port 16: (x)        Port 17: (x)        Port 18: (x)
       Port 19: (x)        Port 20: (x)        Port 21: (x)
       Port 22: (x)        Port 23: (x)        Port 24: (x)
       Port 25: ( )        Port 26: ( )        Port 27: ( )




          SAVE            EXIT          MAIN MENU         HELP
```

Figure 4-22. Static Group Address Port Member Setup Menu

A port is assigned to this group address when it is selected. The default value for each port is selected. Select **Save** to save the data.

Static Group Address Forward Unregister Configuration

Selecting this option displays the Static Group Address Forward Unregister Configuration Menu shown in Figure 4-23 .



```
                     IBM Ethernet Workgroup Switch 8275-225
        - Static Group Address Forward Unregister Configuration Menu -





       Port 1 : (x)        Port 2 : (x)        Port 3 : (x)
       Port 4 : (x)        Port 5 : (x)        Port 6 : (x)
       Port 7 : (x)        Port 8 : (x)        Port 9 : (x)
       Port 10: (x)        Port 11: (x)        Port 12: (x)
       Port 13: (x)        Port 14: (x)        Port 15: (x)
       Port 16: (x)        Port 17: (x)        Port 18: (x)
       Port 19: (x)        Port 20: (x)        Port 21: (x)
       Port 22: (x)        Port 23: (x)        Port 24: (x)
       Port 25: (x)        Port 26: (x)        Port 27: (x)




          SAVE            EXIT          MAIN MENU          HELP
```

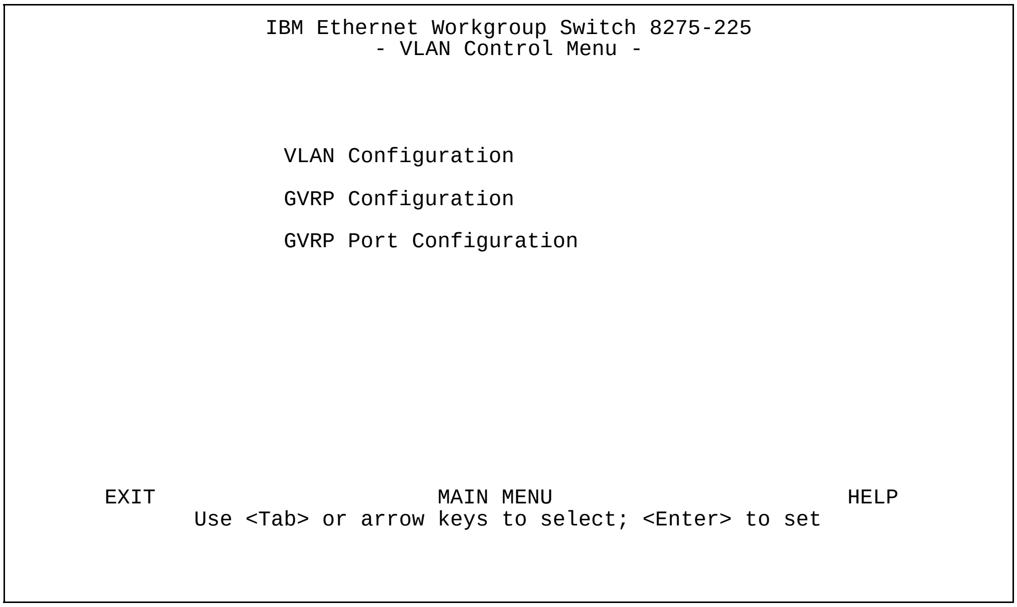
Figure 4-23. Static Group Address Forward Unregister Configuration Menu

This menu lets you specify the ports to which a packet is forwarded when the group address specified was not defined and registered in the system.

The packets will be forwarded to the port which is selected. The default value for each port is selected. Select **Save** to save the configuration.

VLAN Control

Selecting this option displays the VLAN Control Menu shown in Figure 4-24 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                            - VLAN Control Menu -



                      VLAN Configuration

                      GVRP Configuration

                      GVRP Port Configuration









        EXIT                      MAIN MENU                       HELP
               Use <Tab> or arrow keys to select; <Enter> to set
```

Figure 4-24. VLAN Control Menu

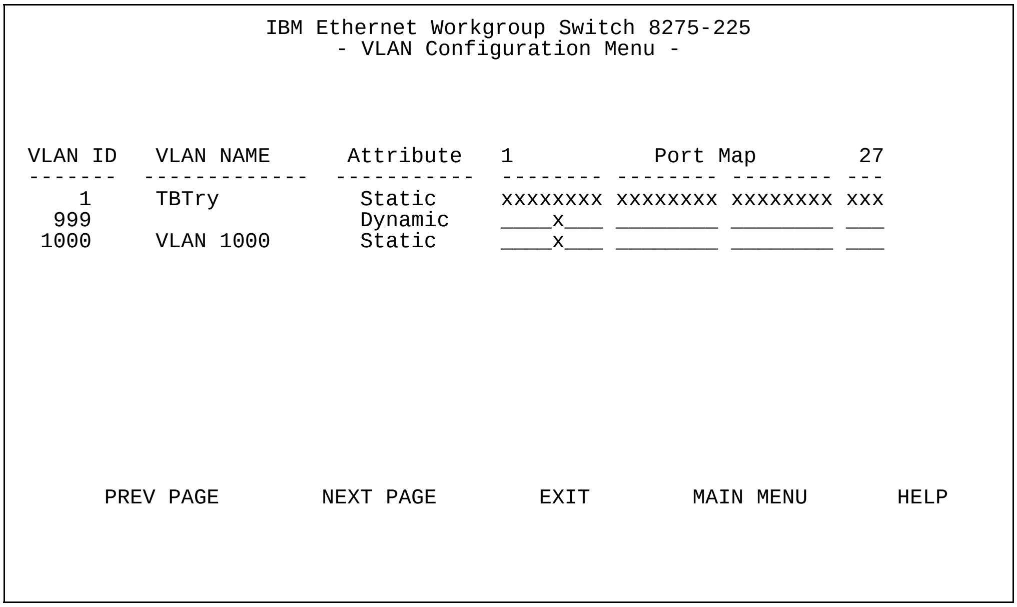
VLAN Configuration Allows you to configure VLANs. This menu shows all the VLAN information including the Static VLAN assigned by the administrator and those dynamically created by GVRP.

GVRP Configuration Allows you to enable/disable the function of GVRP for the switch and to configure the parameters of GVRP.

GVRP Port Configuration Allows you to enable/disable GVRP function for each port.

VLAN Configuration

Selecting this option displays the VLAN Configuration Menu shown in Figure 4-25 .



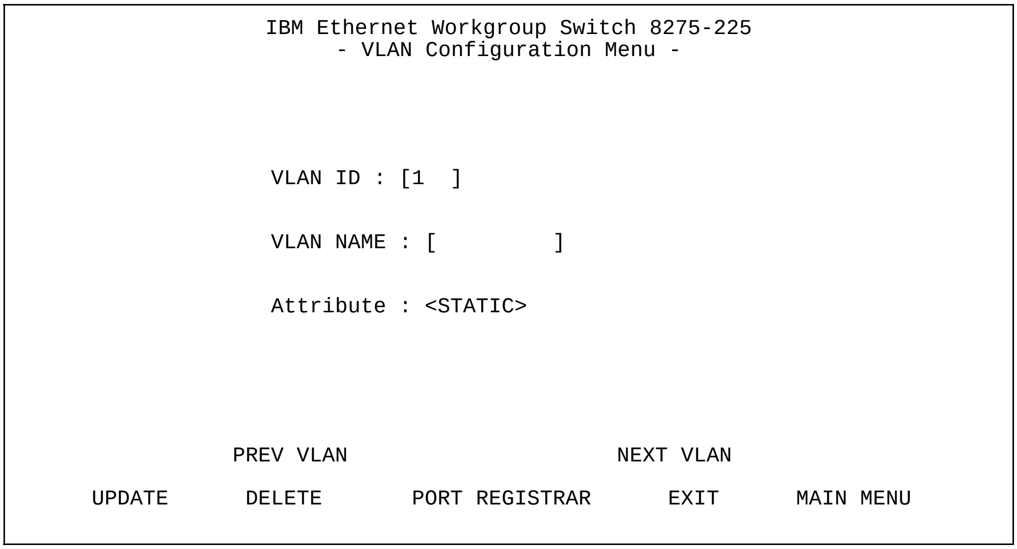
```
                  IBM Ethernet Workgroup Switch 8275-225
                        - VLAN Configuration Menu -



VLAN ID   VLAN NAME      Attribute   1           Port Map        27
-------  -------------  -----------  -------- -------- -------- ---
    1     TBTry           Static     xxxxxxxx xxxxxxxx xxxxxxxx xxx
  999                     Dynamic    ____x___ ________ ________ ___
 1000     VLAN 1000       Static     ____x___ ________ ________ ___









      PREV PAGE        NEXT PAGE        EXIT        MAIN MENU       HELP
```

Figure 4-25. VLAN Configuration Menu - Primary

This menu lets you configure up to 31 VLANs (ranging from 1 to 4094) on the Ethernet Workgroup Switch. VLAN devices can communicate only with other devices on the same VLAN. When a VLAN is created by the user, its attribute will be "Static". If it is created by GVRP, it becomes "Dynamic". (see “Static vs. Dynamic VLANs” on page A-7 in Appendix A, “Introduction to Virtual LANs (VLANs) and Spanning Tree Protocol (STP)”)

To configure a VLAN, use the Tab key to select a blank or existing VLAN ID and press **ENTER**. The second level of VLAN Configuration Menu will be displayed as shown in Figure 4-26 on page 4-32.

Note: The next page will be activated when the current page is filled. Use the **NEXT PAGE** command to enter the second page.



```
                    IBM Ethernet Workgroup Switch 8275-225
                         - VLAN Configuration Menu -



                    VLAN ID : [1  ]

                    VLAN NAME : [         ]

                    Attribute : <STATIC>




                 PREV VLAN                     NEXT VLAN

      UPDATE      DELETE       PORT REGISTRAR      EXIT      MAIN MENU
```

Figure 4-26. VLAN Configuration Menu - Secondary

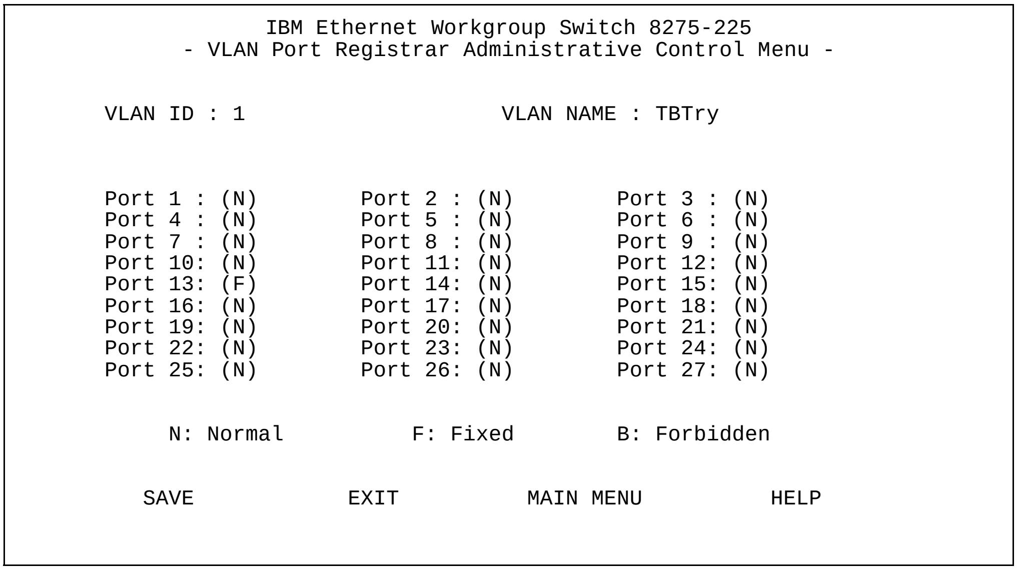
To add or change VLAN:

1. Use the Tab key to select a VLAN as shown in Figure 4-25 on page 4-31.
2. Press **Enter** to edit.
3. Define the VLAN ID and a name.
4. Select **Update**.
5. Select **PORT REGISTRAR** and define the port's attributes.
6. Select **EXIT**.
7. Repeat Steps 1 through 5 for each VLAN.

To delete a VLAN:

1. Use the Tab key to select a VLAN as shown in Figure 4-25 on page 4-31.
2. Press **Enter** to edit.
3. Press **Delete** to delete the VLAN.
4. Select **EXIT**.

To configure the ports of the VLAN, select PORT REGISTRAR. The VLAN Port Registrar Administrative Control Menu is displayed as shown in Figure 4-27 on page 4-33.



```
                 IBM Ethernet Workgroup Switch 8275-225
            - VLAN Port Registrar Administrative Control Menu -


     VLAN ID : 1                   VLAN NAME : TBTry



     Port 1 : (N)        Port 2 : (N)        Port 3 : (N)
     Port 4 : (N)        Port 5 : (N)        Port 6 : (N)
     Port 7 : (N)        Port 8 : (N)        Port 9 : (N)
     Port 10: (N)        Port 11: (N)        Port 12: (N)
     Port 13: (F)        Port 14: (N)        Port 15: (N)
     Port 16: (N)        Port 17: (N)        Port 18: (N)
     Port 19: (N)        Port 20: (N)        Port 21: (N)
     Port 22: (N)        Port 23: (N)        Port 24: (N)
     Port 25: (N)        Port 26: (N)        Port 27: (N)

          N: Normal          F: Fixed        B: Forbidden


        SAVE            EXIT          MAIN MENU          HELP
```

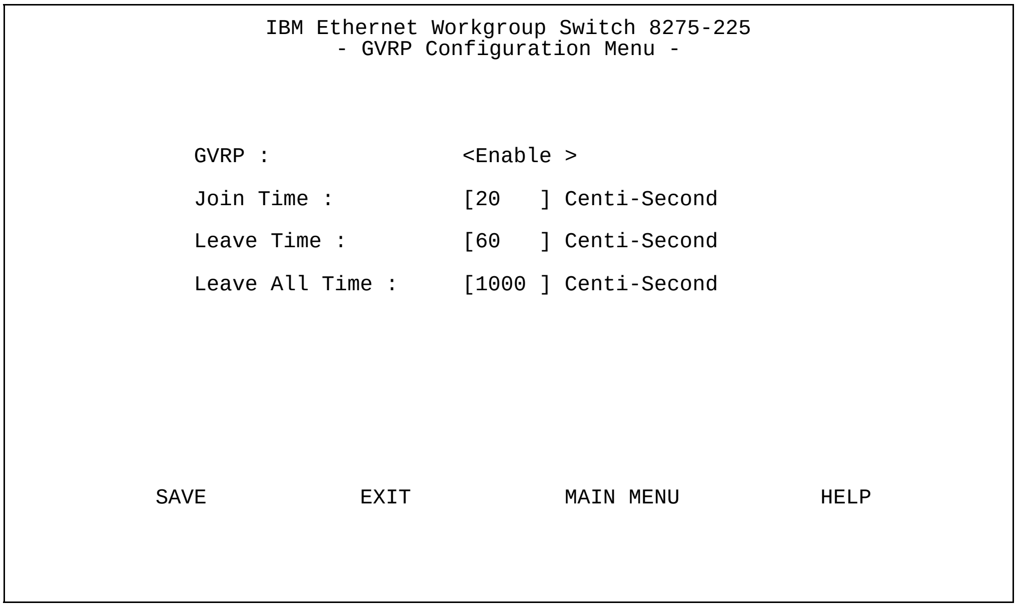
Figure 4-27. VLAN Port Registrar Administrative Control Menu

A port is configured to this VLAN when it is selected with the following pre-defined codes. Select **Save** to save the configuration.

- Fixed: The port belongs to the specified VLAN.
- Normal: The port belongs to the specified VLAN only if it is registered via GVRP.
- Forbidden: The port is never allowed to join this VLAN even when a GVRP registration request occurs.

GVRP Configuration

Selecting this option displays the GVRP Configuration Menu shown in Figure 4-28 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                         - GVRP Configuration Menu -



              GVRP :              <Enable >

              Join Time :         [20   ] Centi-Second

              Leave Time :        [60   ] Centi-Second

              Leave All Time :    [1000 ] Centi-Second






           SAVE            EXIT            MAIN MENU           HELP
```

Figure 4-28. GVRP Configuration Menu

This menu lets you enable or disable GVRP. A Dynamic VLAN entry will automatically be aged out after a period of time when no port member is registered to that VLAN.

GVRP Allows the GVRP protocol to be enabled or disabled for the entire switch.

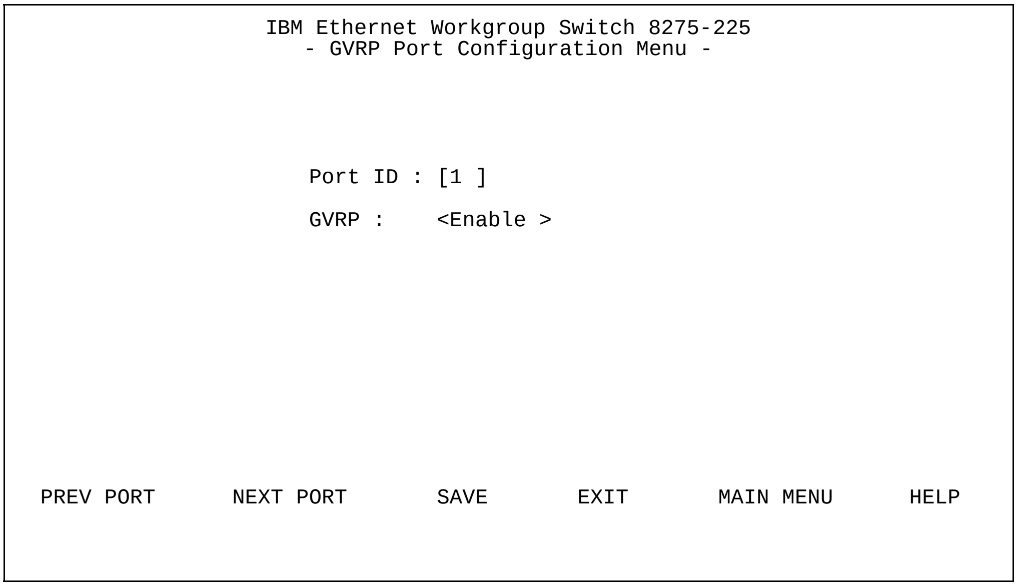
Join Time The join time is the time within which a registered port has to register after the Dynamic VLAN received an unregistering signal. Its value is 10-200 centi-seconds with a default value of 20.

Leave Time The leave time is the time that the dynamic VLAN, after receiving an unregistering signal, will wait before actually being aged out. Its value is 30-600 centi-seconds with a default value of 60.

Leave All Time The Leave All Time is the interval that the dynamic VLAN will broadcast aging out signal. Its value is 200-6000 centi-seconds with a default value of 1000.

GVRP Port Configuration

Selecting this option displays the Group VLAN Registration Protocol (GVRP) Port Configuration Menu shown in Figure 4-29 .



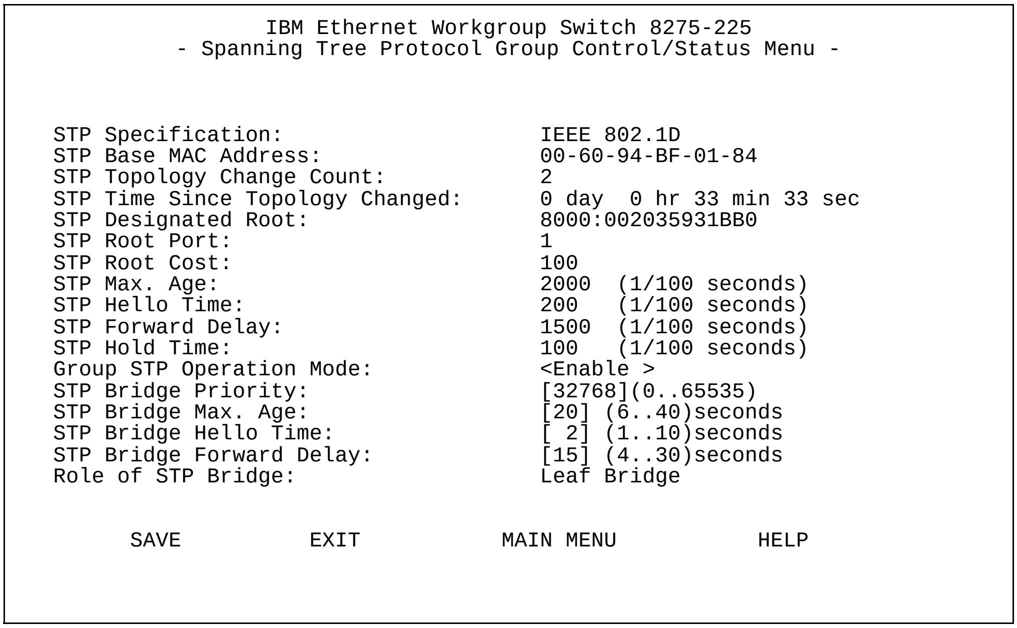
```
                    IBM Ethernet Workgroup Switch 8275-225
                       - GVRP Port Configuration Menu -



                       Port ID : [1 ]

                       GVRP :    <Enable >







  PREV PORT      NEXT PORT       SAVE       EXIT       MAIN MENU      HELP
```

Figure 4-29. GVRP Port Configuration Menu

This menu lets you enable or disable the GVRP function for each port. Fill in the Port ID field and select **Enable/Disable** of the GVRP to enable or disable the GVRP function of that port. Then move the cursor to **SAVE** and press **Enter**. To configure the next port or previous port, move to **NEXT PORT** or **PREV PORT** and press **Enter**. You can decide which ports have the GVRP function. The default value is Enable and you may want to disable it to prevent the port sending GVRP traps periodically.

Spanning Tree Protocol Group Configuration

Selecting this option displays the Spanning Tree Protocol Group Control/Status Menu shown in Figure 4-30 .



```
                    IBM Ethernet Workgroup Switch 8275-225
             - Spanning Tree Protocol Group Control/Status Menu -



   STP Specification:                    IEEE 802.1D
   STP Base MAC Address:                 00-60-94-BF-01-84
   STP Topology Change Count:            2
   STP Time Since Topology Changed:      0 day  0 hr 33 min 33 sec
   STP Designated Root:                  8000:002035931BB0
   STP Root Port:                        1
   STP Root Cost:                        100
   STP Max. Age:                         2000  (1/100 seconds)
   STP Hello Time:                       200   (1/100 seconds)
   STP Forward Delay:                    1500  (1/100 seconds)
   STP Hold Time:                        100   (1/100 seconds)
   Group STP Operation Mode:             <Enable >
   STP Bridge Priority:                  [32768](0..65535)
   STP Bridge Max. Age:                  [20] (6..40)seconds
   STP Bridge Hello Time:                [ 2] (1..10)seconds
   STP Bridge Forward Delay:             [15] (4..30)seconds
   Role of STP Bridge:                   Leaf Bridge


         SAVE          EXIT           MAIN MENU           HELP
```

Figure 4-30. Spanning Tree Protocol Group Control/Status Menu

This menu allows you to configure and manage the STP system on the Ethernet Workgroup Switch. The Ethernet Workgroup Switch has a single STP system and one MAC address is assigned to the switch.

Table 4-2. Spanning Tree Protocol Group Port Configuration

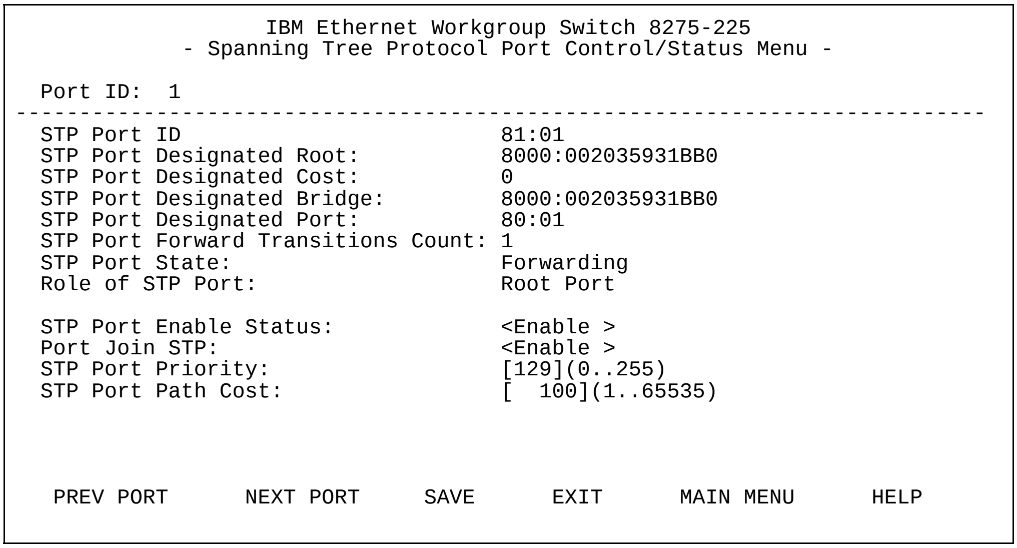
STP Topology Change Count	Shows the number of network topology changes as a group that have occurred.
STP Time Since Topology Change	Shows the time since the last topology change was detected (read only).
STP Designated Root	Shows the bridge identifier of the designated root bridge (read only).
STP Root Port	Shows the root port of the switch (read only).
STP Root Cost	Shows the path cost from the switch to the root bridge (read only).
STP Hold Time	Shows the shortest time interval allowed between the transmission of BPDUs (read only).
Group STP Operation Mode	Allows you to enable or disable the STP for the switch.
STP Bridge Priority	Allows you to specify the priority of the switch. By changing the priority of the switch, you can make it more or less likely to become the root bridge. The lower the number, the more likely the bridge will become the root bridge. The range is 0–65535. The default is 32768.

Table 4-2. Spanning Tree Protocol Group Port Configuration

STP Bridge Max. Age	Allows you to specify the time in seconds that the switch waits before trying to reconfigure the network when it is the root bridge. If the switch has not received a BPDU within the time specified in this field, it tries to reconfigure the STP topology. The range is 6–40 seconds. The default is 20 seconds.
STP Bridge Hello Time	Allows you to specify the time delay in seconds between the transmission of BPDUs from the switch when it is the root bridge. The range is 1–10 seconds. The default is 2 seconds.
STP Bridge Forward Delay	Allows you to specify the time in seconds that the ports on the switch spend in the learning and listening and learning states when the switch is in the root bridge. The range is 4–30 seconds. The default setting is 15 seconds.

Spanning Tree Protocol Port Configuration

Selecting this option displays the Spanning Tree Protocol Port Control/Status Menu shown in Figure 4-31 .



```
                     IBM Ethernet Workgroup Switch 8275-225
               - Spanning Tree Protocol Port Control/Status Menu -

  Port ID:  1
----------------------------------------------------------------------------
  STP Port ID                         81:01
  STP Port Designated Root:           8000:002035931BB0
  STP Port Designated Cost:           0
  STP Port Designated Bridge:         8000:002035931BB0
  STP Port Designated Port:           80:01
  STP Port Forward Transitions Count: 1
  STP Port State:                     Forwarding
  Role of STP Port:                   Root Port

  STP Port Enable Status:             <Enable >
  Port Join STP:                      <Enable >
  STP Port Priority:                  [129](0..255)
  STP Port Path Cost:                 [  100](1..65535)



   PREV PORT      NEXT PORT     SAVE      EXIT      MAIN MENU      HELP
```

Figure 4-31.   Spanning Tree Protocol Port Control/Status Menu

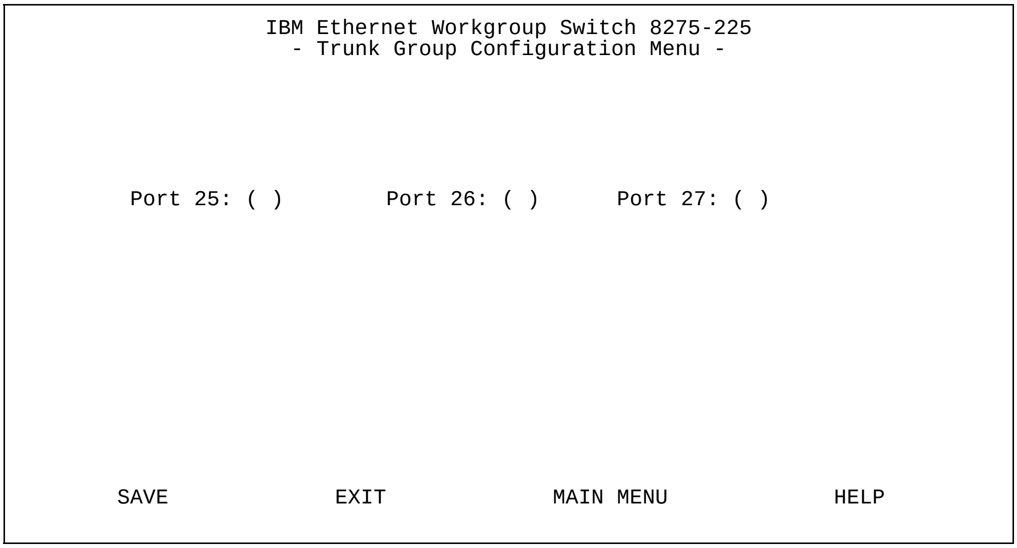
This menu allows you to configure and manage the STP parameters of each port on the Ethernet Workgroup Switch. Port ID 20 is used to configure and manage the STP parameters of the Trunk Group for Model 217 and Port ID 28 is used for Model 225.

Table 4-3. Spanning Tree Protocol VLAN Port Configuration

Port ID	Scroll to the next port ID by selecting NEXT PORT
STP Port ID	Shows the ID of the designated bridge port for the current port’s VLAN (read only).
STP Port Designated Root	Shows the bridge identifier of the root bridge (read only).
STP Port Designated Cost	Shows the path cost from the root bridge to the designated bridge port for the current port’s VLAN (read only).
STP Port Designated Bridge	Shows the bridge identifier of the designated bridge for the current port’s VLAN (read only).
STP Port Designated Port	Shows the ID of the designated bridge port for the current port’s VLAN (read only).
STP Port Forward Transitions Count	Shows the number of times that the current port has changed from the learning state to the forwarding state (read only).
STP Port Enable Status	Allows you to enable or disable the port. This function does the same as the "Admin State" function as shown in “Switch Port Control/Status” on page 4-19
Status Port Join STP	Allows you to enable or disable the port as part of a VLAN group.
STP Port Priority	Allows you to specify the priority of the port. By changing the priority of the port, you can make it more or less likely to become the root port. The lower the number, the more likely it is that the port will be the root port. The range is 0–255. The default is 129.
STP Port Path Cost	Allows you to specify the path cost of the port. The default port costs are: 100 for 10-Mbps ports (ports 1 to 16 on Model 217 and ports 1 to 24 on Model 225) 10 for 10/100-Mbps ports (ports 17 to 19 on Model 217 and ports 25 to 27 on Model 225) 8 for Trunk group (port 20 on Model 217 and port 28 on Model 225)

Trunk Group Configuration

Selecting this option displays the Trunk Group Configuration Menu shown in Figure 4-32 .



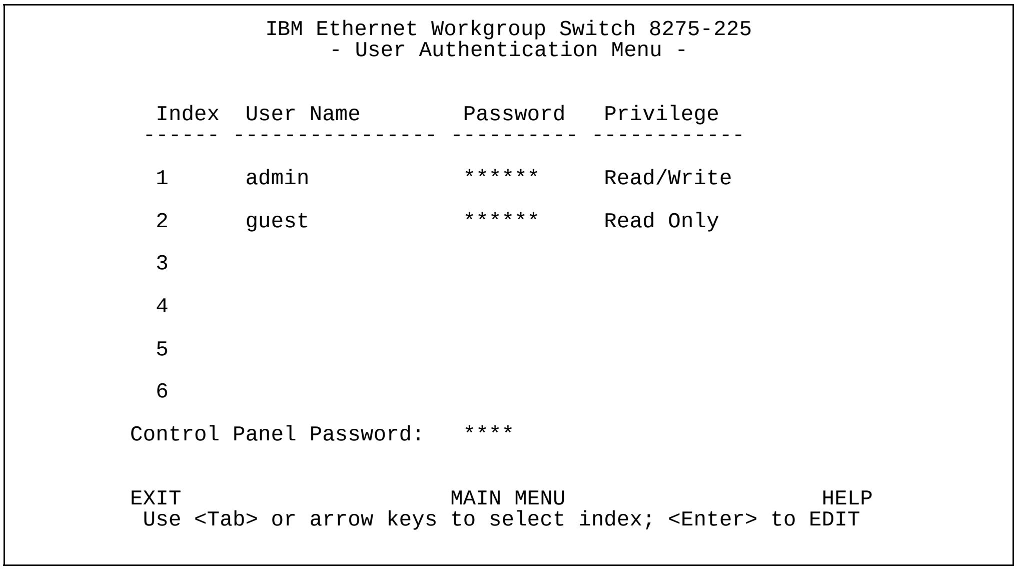
```
                    IBM Ethernet Workgroup Switch 8275-225
                     - Trunk Group Configuration Menu -




          Port 25: ( )        Port 26: ( )      Port 27: ( )









         SAVE             EXIT             MAIN MENU            HELP
```

Figure 4-32.   Trunk Group Configuration Menu

This menu allows you to configure and manage the Trunk Group on the Ethernet Workgroup Switch. The switch provides a Port Trunking algorithm to allow two or three 100 Mbps ports to be connected in parallel between switches to increase the bandwidth between devices. The Trunk group has an STP port instance for it which is specified as port 20 on Model 217 or port 28 on Model 225. It is possible to trunk between Model 217 and Model 225 only. It is only possible to trunk ports 17, 18, 19 on Model 217 and ports 25, 26 and 27 on Model 225.

User Authentication

Selecting this option displays the User Authentication Menu shown in Figure 4-33 .



```
                   IBM Ethernet Workgroup Switch 8275-225
                        - User Authentication Menu -


          Index  User Name        Password   Privilege
         ------ ---------------- ---------- ------------

          1      admin            ******     Read/Write

          2      guest            ******     Read Only

          3

          4

          5

          6

        Control Panel Password:   ****


        EXIT                     MAIN MENU                    HELP
         Use <Tab> or arrow keys to select index; <Enter> to EDIT
```

Figure 4-33. User Authentication Menu

This menu lets you define up to six different users. The passwords are the same for both the management session and the web. You can also change the password for the control panel.

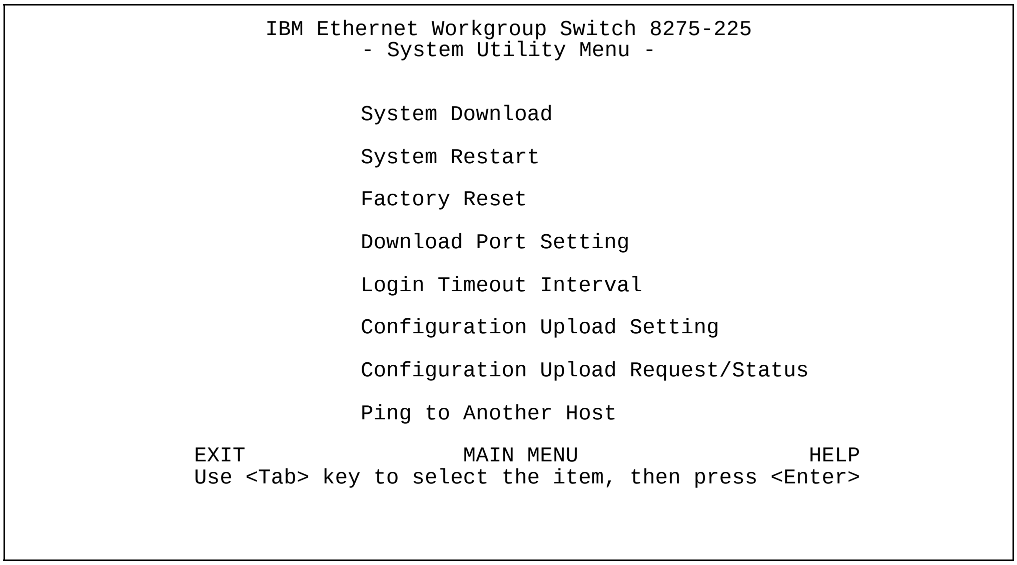
Note: User Names and Passwords are not case sensitive. To define a user, perform the following steps:

1. Select an Index number and press **Enter**.
2. Enter a user name of up to 12 alphanumeric characters.
3. Enter a password of up to 6 alphanumeric characters.
4. Re-enter the password for confirmation.
5. Specify Read Only or Read/Write privilege, and press **Enter**.
6. Select **ADD**.
7. Select **EXIT**.

Note: The control panel password can be only four digits (0–9). It can be changed by highlighting the "Control Panel Password" field, press **Enter**, enter a new password, and confirm it.

System Utility

Selecting this option displays the System Utility Menu shown in Figure 4-34 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                           - System Utility Menu -

                           System Download

                           System Restart

                           Factory Reset

                           Download Port Setting

                           Login Timeout Interval

                           Configuration Upload Setting

                           Configuration Upload Request/Status

                           Ping to Another Host

              EXIT                 MAIN MENU                 HELP
              Use <Tab> key to select the item, then press <Enter>
```

Figure 4-34. System Utility Menu

This menu lets you download microcode, restart the switch, reset the switch to the factory defaults, specify which port will receive the downloaded microcode, and specify the inactivity time for Telnet and console logouts.

System Download Allows you to configure the type of download.

System Restart Allows you to restart the switch.

Factory Reset Allows you to reset to factory configuration

Download Port Setting Allows you to specify the port that will receive the software download.

Login Timeout Interval Allows you to specify the inactivity time for Telnet logouts.

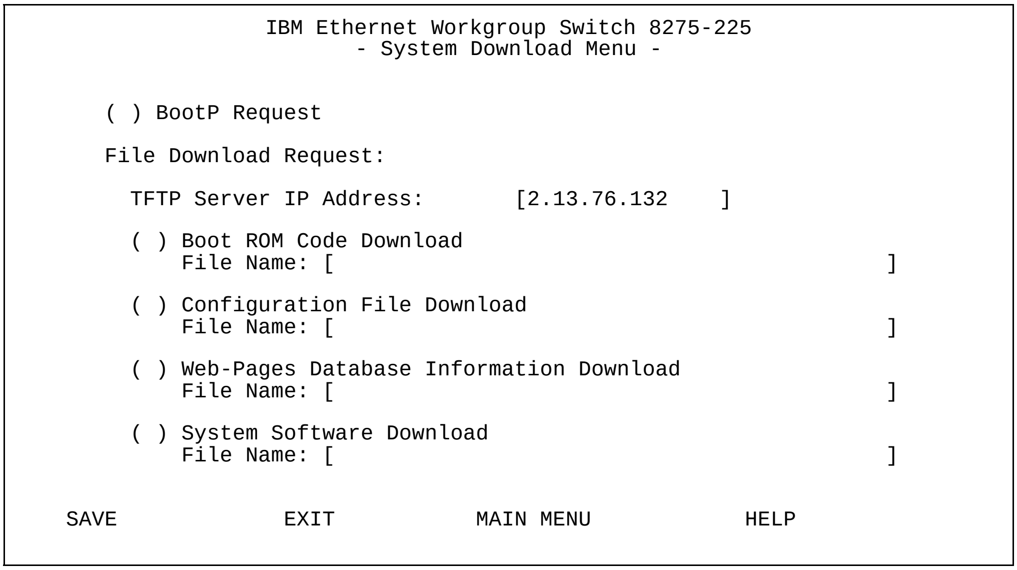
Configuration Upload Setting Allows you to set the IP address of the TFTP server and the file name to be uploaded.

Configuration Upload Request/ Status Allows you to request a configuration upload.

Ping to Another Host Allows you to ping to another host.

System Download

Selecting this option displays the System Download Menu shown in Figure 4-35 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                           - System Download Menu -


       ( ) BootP Request

       File Download Request:

         TFTP Server IP Address:       [2.13.76.132    ]

         ( ) Boot ROM Code Download
             File Name: [                                            ]

         ( ) Configuration File Download
             File Name: [                                            ]

         ( ) Web-Pages Database Information Download
             File Name: [                                            ]

         ( ) System Software Download
             File Name: [                                            ]


    SAVE             EXIT           MAIN MENU            HELP
```

Figure 4-35.   System Download Menu

This menu lets you perform a BootP request and a TFTP code download. To request an IP address, subnet mask, and a default gateway address from your BootP server perform the following steps:

1. Select **BootP Request**

2. Perform a cold restart on the system. For information on restarting your system, see “System Restart” on page 4-45.

You should perform a code download only to update existing software or if existing code has become corrupted. Before performing a system download, make sure that you know the IP address of your TFTP server and the location of the files on the server.

Use the following naming convention:

- Boot ROM Code download - 8275B*xxx*.BT
- Configuration File Download - refer to the name previously chosen on the Configuration Upload Menu (see "Configuration Upload Setting Menu" on page 4-49)
- Web Pages Database Information Download - 8275B*xxx*.WEB
- System Software Download - 8275B*xxx*.RT

where, *xxx* is the version number.

To perform a TFTP code download, do the following steps:

1. Enter the IP address of the TFTP server.

2. Select the downloads that you want to perform.

3. Enter the path and filename for each of the downloads you have selected (for example, C:\microcode\8275B101.BT).

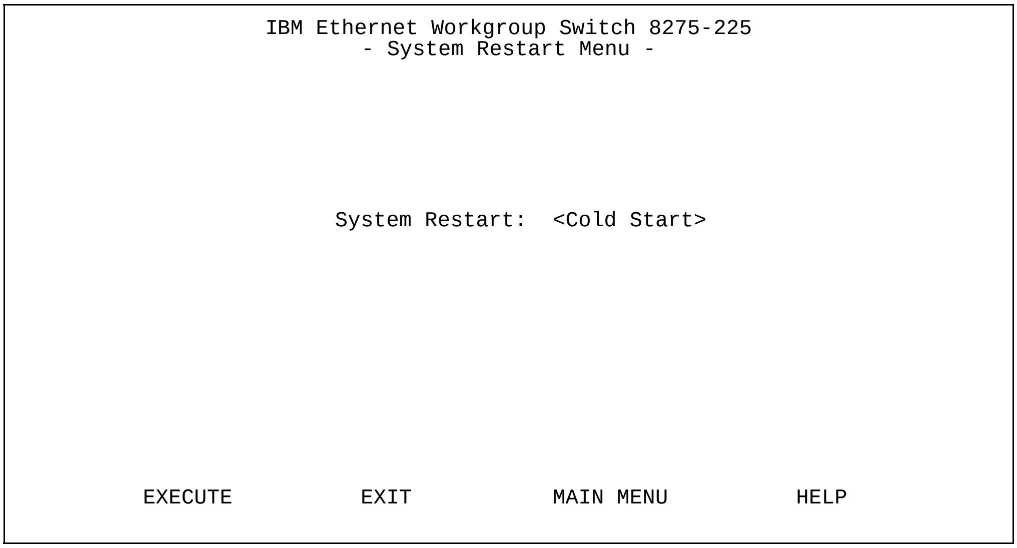
4. Save the configuration.

5. Set the download port (see “Download Port Setting” on page 4-47).

6. Restart the system (see “System Restart” on page 4-45).

System Restart

Selecting this option displays the System Restart Menu shown in Figure 4-36 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                           - System Restart Menu -



                     System Restart:  <Cold Start>







          EXECUTE          EXIT          MAIN MENU          HELP
```

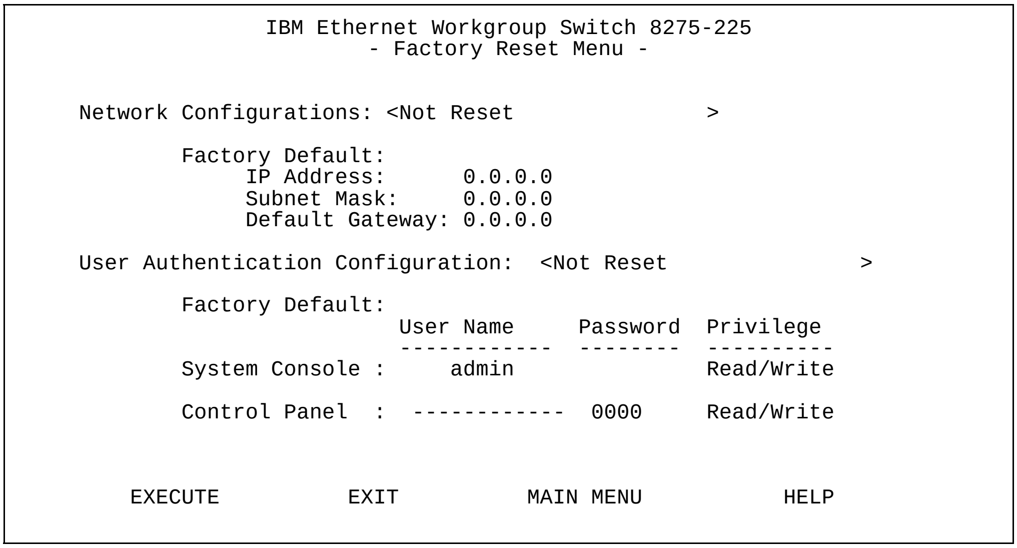
Figure 4-36. System Restart Menu

This menu lets you perform a *cold* or *warm* restart.

You can restart the system at any time without losing configuration settings, unless you do a factory reset. For most restarts, a warm restart is sufficient. A cold restart will run both the BOOT ROM code and the run time code whereas a warm restart will run only the run time code. A cold restart is needed when you perform a BootP request or code download.

Factory Reset

Selecting this option displays the Factory Reset Menu shown in Figure 4-37 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                            - Factory Reset Menu -


     Network Configurations: <Not Reset               >

             Factory Default:
                  IP Address:      0.0.0.0
                  Subnet Mask:     0.0.0.0
                  Default Gateway: 0.0.0.0

     User Authentication Configuration:  <Not Reset               >

             Factory Default:
                              User Name     Password  Privilege
                              ------------  --------  ----------
             System Console :     admin               Read/Write

             Control Panel  :  ------------  0000     Read/Write


         EXECUTE          EXIT          MAIN MENU          HELP
```

Figure 4-37. Factory Reset Menu

This menu lets you return all switch settings to the original default settings. When you execute a factory reset all of your custom settings are overwritten.

To perform a factory reset, do the following steps:

1. Select how you want your network configuration processed during a factory reset:

   – *Not Reset*—Your current network configuration is saved.

   – *Reset from BootP*—You request a new network configuration from your BootP server.

   – *Reset to Factory default*—Your current network configuration is reset to factory defaults.

2. Select how you want to have your user authentication configuration processed during a factory reset:

   – *Not Reset*—Your current user authentication configuration is saved.

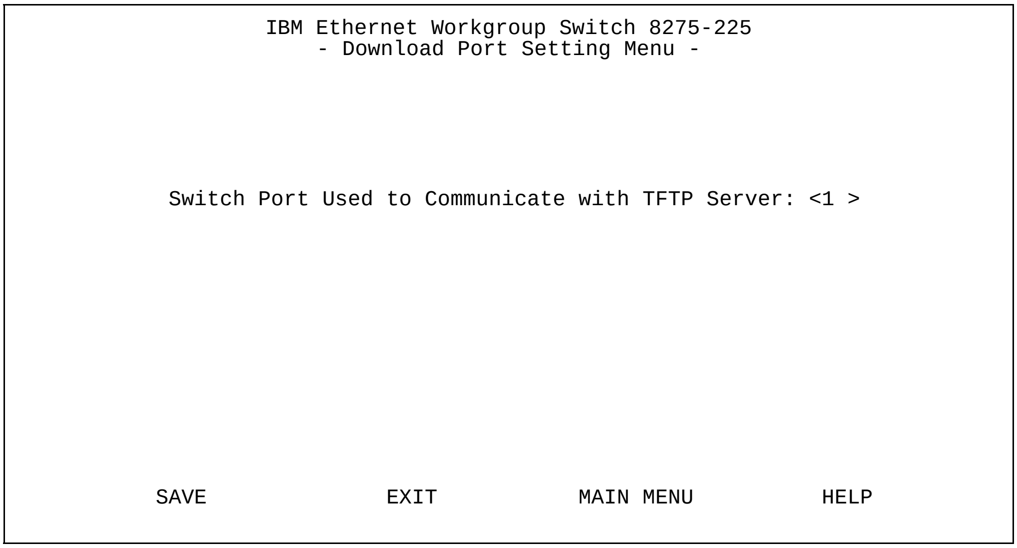
   – *Reset to Factory default*—Your current user authentication configuration returns to factory defaults.

3. Select **Execute** and press **Enter**.

   The switch performs a cold restart and returns your custom configuration to factory default values.

Download Port Setting

Selecting this option displays the Download Port Setting Menu shown in Figure 4-38 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                        - Download Port Setting Menu -



            Switch Port Used to Communicate with TFTP Server: <1 >









           SAVE              EXIT            MAIN MENU          HELP
```

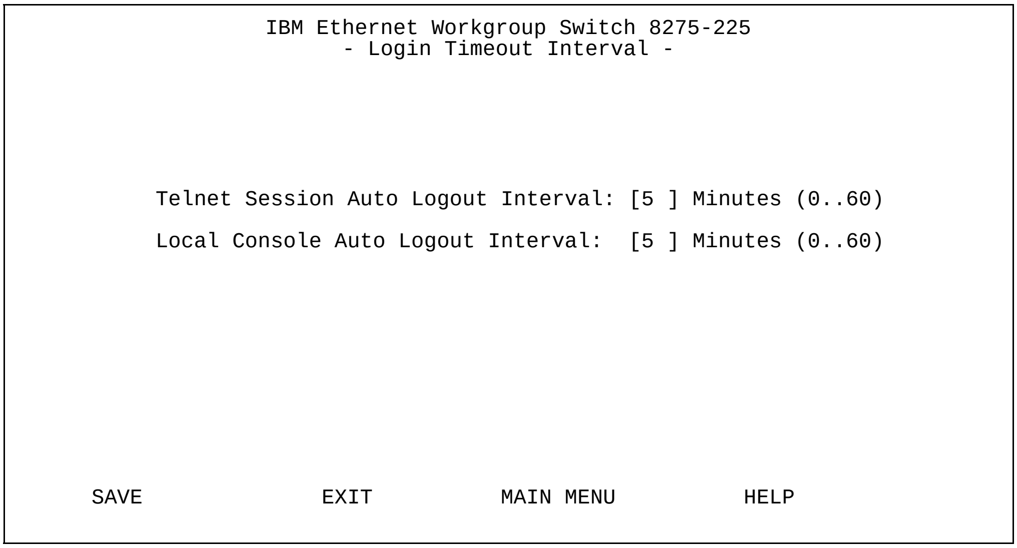
Figure 4-38. Download Port Setting Menu

This menu lets you specify which port will receive downloaded system software. The download port must be set before you can perform a download. The download port is the switch port that is connected to your TFTP server.

Port Trunking is not functional during a code load. However, a single port of an existing Trunk Group can be assigned as a Download Port.

Login Timeout Interval

Selecting this option displays the Login Timeout Interval menu shown in Figure 4-39 .



```
                   IBM Ethernet Workgroup Switch 8275-225
                         - Login Timeout Interval -




           Telnet Session Auto Logout Interval: [5 ] Minutes (0..60)

           Local Console Auto Logout Interval:  [5 ] Minutes (0..60)








      SAVE              EXIT          MAIN MENU          HELP
```

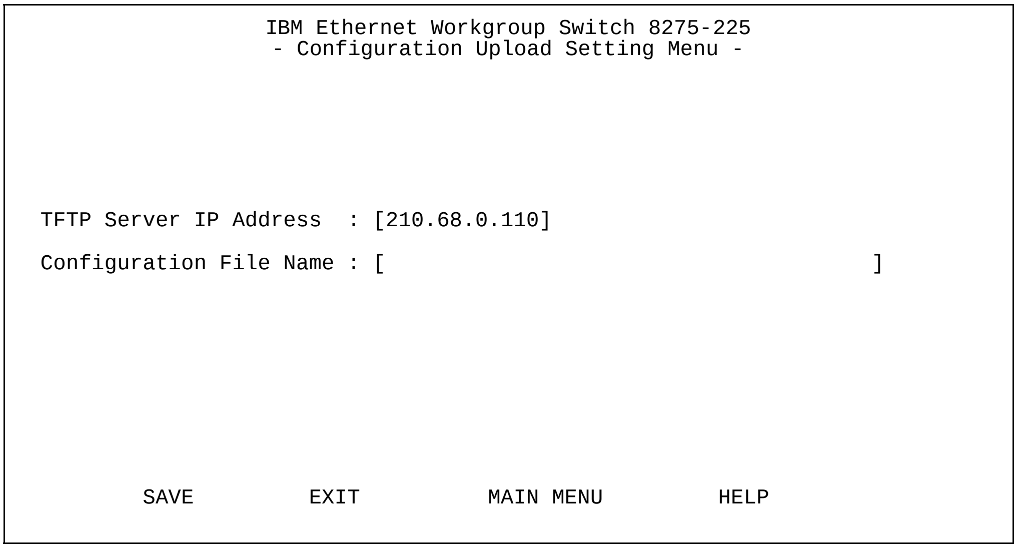
Figure 4-39. Login Timeout Interval Menu

This menu lets your select the time after which an established Telnet session or Local Console is automatically logged out if inactive. The range is 0 to 60 minutes. The default is 5 minutes. If you specify zero, the session remains logged in regardless of how long it is inactive.

Note: Any configuration changes will be lost if not saved before the console logs off.

Configuration Upload Setting

Selecting this option displays the Configuration Upload Setting Menu shown in Figure 4-40 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                     - Configuration Upload Setting Menu -




  TFTP Server IP Address  : [210.68.0.110]

  Configuration File Name : [                                      ]






          SAVE         EXIT          MAIN MENU         HELP
```

Figure 4-40. Configuration Upload Setting Menu

This menu lets you upload the switch configuration data to the remote server in binary format. You can upload your configuration files and save them as a backup in case you want to restore your system settings.

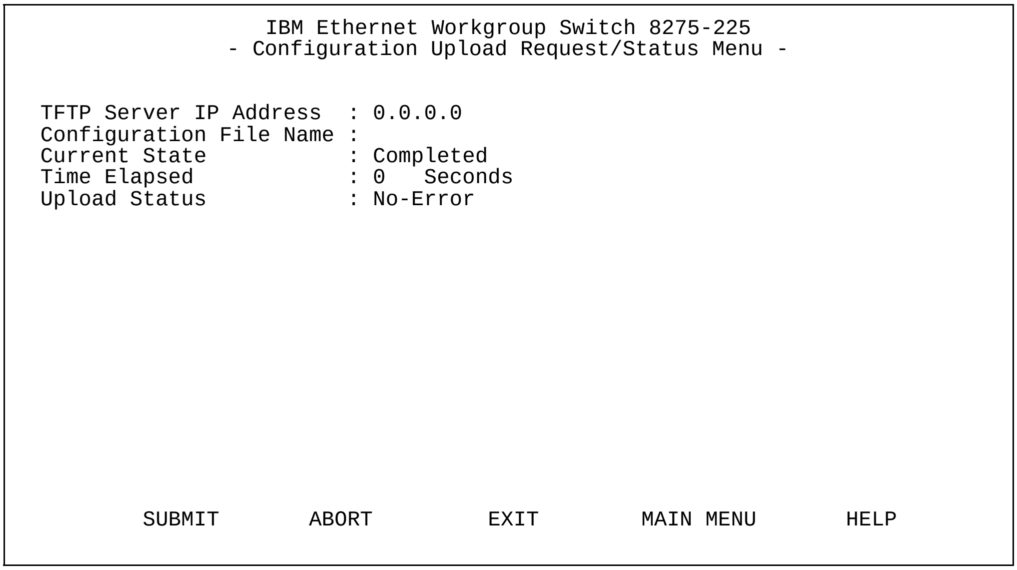
Enter the TFTP server IP address and the configuration name (for example *filename*.CFG) and path information. Select **Save** to save your configuration settings, and then request an upload by using the Configuration Upload Request/Status Menu. See "Configuration Upload Request/Status" on page 4-50.

TFTP Server IP Address The IP address of the server on which the configuration files are to be stored.

Configuration File Name The name of the configuration file and the full path of the saving location on the server.

Configuration Upload Request/Status

Selecting this option displays the Configuration Upload Request/Status Menu shown in Figure 4-41 .



```
                 IBM Ethernet Workgroup Switch 8275-225
              - Configuration Upload Request/Status Menu -


  TFTP Server IP Address  : 0.0.0.0
  Configuration File Name :
  Current State           : Completed
  Time Elapsed            : 0   Seconds
  Upload Status           : No-Error
```

Figure 4-41. Configuration Upload Request/Status Menu

This menu lets you view the current upload setting and submit an upload request. To change the upload settings, see “Configuration Upload Setting” on page 4-49.

Select **SUBMIT** to request a configuration upload. You may cancel the upload request by selecting **ABORT**.

TFTP Server IP Address The IP address of the server to which the configuration files are to be loaded.

Configuration File Name The name of the configuration file and the full path of the saving location on the server.

Current State Current status of the upload. When the upload is finished, the field says `Completed`.

Time Elapsed The elapsed time since the beginning of the upload.

Upload Status The following types of error status can be displayed:

No-Error The upload completed successfully.

No-Such-File The path specified in the Configuration File Name is Write Protected.

Disk-Full The disk specified in the Configuration File Name is full.

Timeout The TFTP upload timeout (20 seconds) has expired.

Other-Error Other errors that are defined by the system.

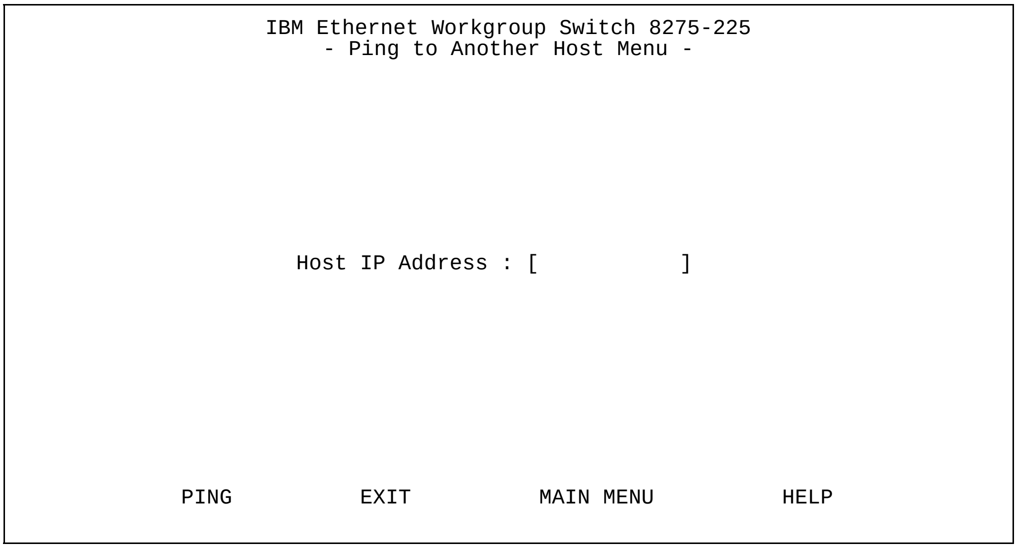
A progress bar is displayed on the menu.

After you have uploaded your configuration files, you can download them as required. For information on downloading your configuration files, see “System Download” on page 4-43.

Note: The TFTP Server IP Address and Configuration File Name may differ from that on the Configuration Upload Setting Menu if an upload is already in progress.

Ping to Another Host

Selecting this option displays the Ping to Another Host Menu shown in Figure 4-42 .



```
                    IBM Ethernet Workgroup Switch 8275-225
                        - Ping to Another Host Menu -









                       Host IP Address : [            ]









              PING          EXIT          MAIN MENU          HELP
```

Figure 4-42. Ping to Another Host Menu

This menu lets you ping another host machine. The administrator simply fills in the IP address of the machine and issues a "ping" command.

Chapter 5. Using Web Management

Using Web Browser Management

You can use your web browser to configure the Ethernet Workgroup Switch. Enter the IP address or host name in your web browser's address field. You are prompted for a user name and password.

Notes:

1. The Ethernet Workgroup Switch comes with two default user names. One default is "`admin`" and requires no password. The other default is "`guest`" and has a password of `guest`. (User names and passwords are not case sensitive.)
2. Your web management connection must be over the management VLAN.

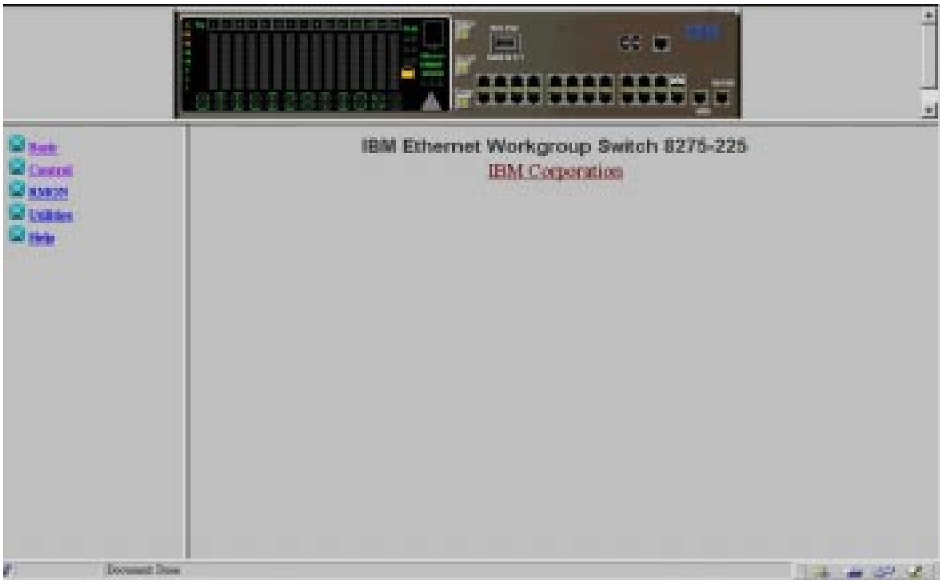
Basic Functions

Select **Basic** to view the following list of basic functions:

- Home Page–returns you to the Ethernet Workgroup Switch home page.
- System Information–provides version information and contacts.
- Management Capability Setup–allows you to view and enable the OOB management capability.
- Networking for Ethernet–allows you to view the current Ethernet MAC address, its IP address, subnet mask and default gateway, as well as allows you to set new IP address, subnet mask, and default gateway address.
- Networking for SLIP–allows you to view the current OOB IP address, subnet mask, baud rate, character size, parity and stop bit; also allows you to set a new IP address and subnet mask.
- Management Port for Console–views the directly connected management port configuration.
- Management Port for OOB–views OOB management port configuration, as well as allows the user to set a new baud rate.

Home Page

Selecting this option returns you to the IBM Ethernet Workgroup Switch 8275-217/225 home page shown in Figure 5-1. This panel also contains a link to the IBM home page (www.ibm.com).



IBM Ethernet Workgroup Switch 8275-225

IBM Corporation

Figure 5-1. The IBM Ethernet Workgroup Switch 8275-217/225 Home Page

Trap Frame Panel

The Trap Frame panel is displayed when the web browser connects to the Ethernet Workgroup Switch.

This panel receives all traps from the switch except for coldstart, Hello, and RMON traps. The maximum number of traps displayed depends on system resources and capacity.

Table 5-1. Trap Frame Information

Display	Lets you manage how you want to display traps: • Pause - Stops displaying any new traps. • Continue - Resumes displaying new traps. • Clear - Clears the traps displayed on the Trap Frame panel.
Buffer	Lets you control the traps in the buffer: • Delete - Deletes all the traps in the buffer. • Dump - Dumps all the traps in the buffer to the Trap Frame panel.

Switch Graphic

A graphic picture of the Ethernet Workgroup Switch displayed in the top section of the each of the web pages is a Java applet that allows you to operate the Ethernet Workgroup Switch. The control panel keys work the same as if you were at the switch itself. Use your left mouse button to “press” the keys. For information on the menu structure you can access, see “Menu Structure” on page 3-4.

Note: You need to enter the control panel password to access port and unit configuration menus.

If you click with the right mouse button on any port, a menu is presented. You can use your left mouse button to make the following port selections:

Table 5-2. Port Information

INFO	Displays the Switch Port Control/Status panel for the selected port (see Figure 5-10 on page 5-14).
Statistics	Displays the RMON Information Statistics Group panel for the selected port (see Figure 5-26 on page 5-35).
Control	Lets you enable or disable ports: • ADMIN Enable - enables the selected port • ADMIN Disable - disables the selected port

The status of the individual ports is shown in the switch picture. Figure 5-2 shows how port status is graphically displayed for each port.

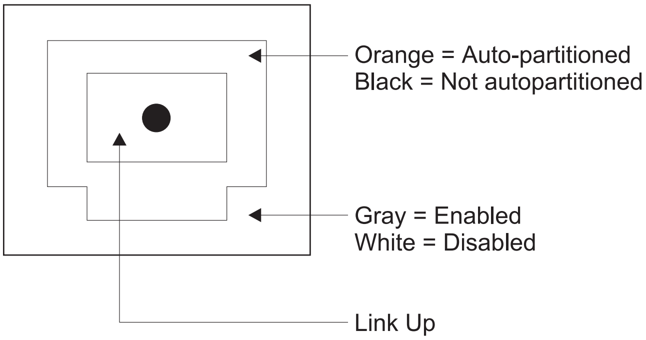


Figure 5-2. Switch Port Status Legend

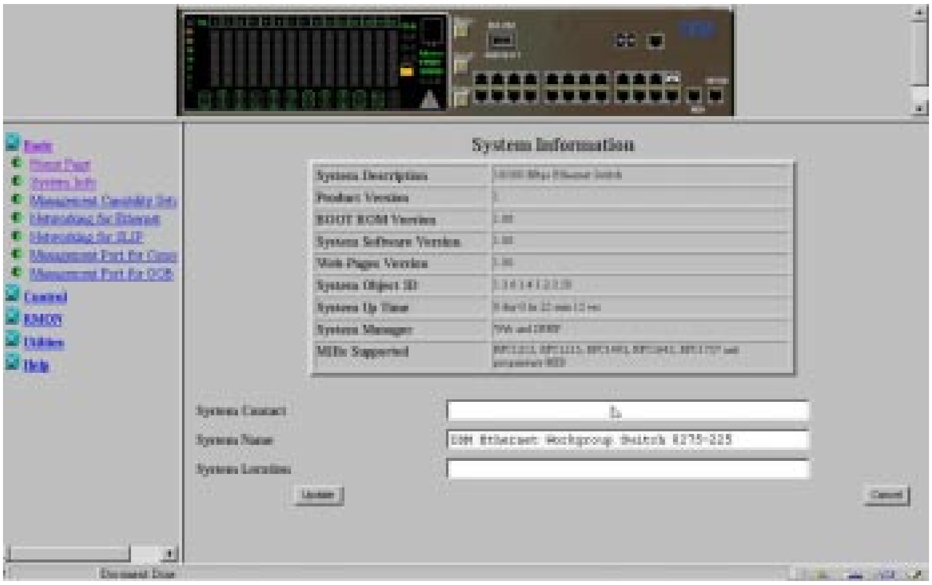
If you click with the right mouse button on the unit itself, a menu is presented. You can use your left mouse button to make the following unit selections:

Table 5-3. Unit Information

INFO	Displays the Switch Control/Status panel for the unit. (see Figure 5-9 on page 5-12).
Trap	Displays the Trap Frame panel.

System Information

Selecting the System Info option displays the System Information panel shown in Figure 5-3.



System Information

System Description	10/100 Mbps Ethernet Switch
Product Version	1
BOOT ROM Version	1.00
System Software Version	1.00
Web Pages Version	1.00
System Object ID	[illegible]
System Up Time	[illegible]
System Manager	Web and SNMP
MIBs Supported	RFC1213, RFC1215, RFC1493, RFC1643, RFC1757 and proprietary MIB

System Contact

System Name: IBM Ethernet Workgroup Switch 8275-225

System Location

Figure 5-3. System Information Panel

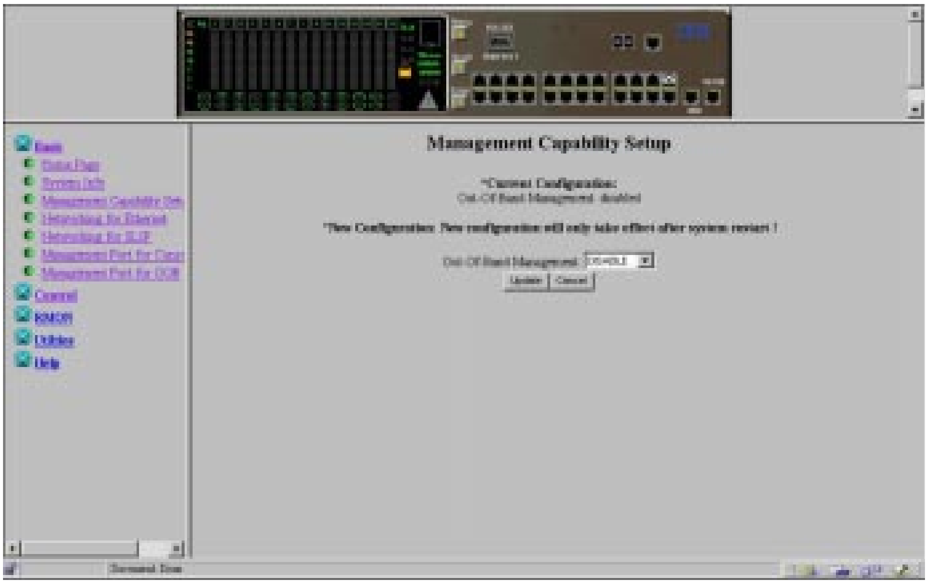
This panel provides information related to the version of the system software installed on the Ethernet Workgroup Switch.

You can specify up to 48 alphanumeric characters each for the System Name, Contact, and Location to provide useful information to all users concerning the Ethernet Workgroup Switch. The information on this panel should be kept current in case assistance is required.

Note: You must select **Update** to save any changes you have made.

Management Capability Setup

Selecting this option displays the Management Capability Setup panel shown in Figure 5-4.



Management Capability Setup

*Current Configuration:
Out-Of Band Management: disabled

*New Configuration: New configuration will only take effect after system restart !

Out-Of Band Management: DISABLE

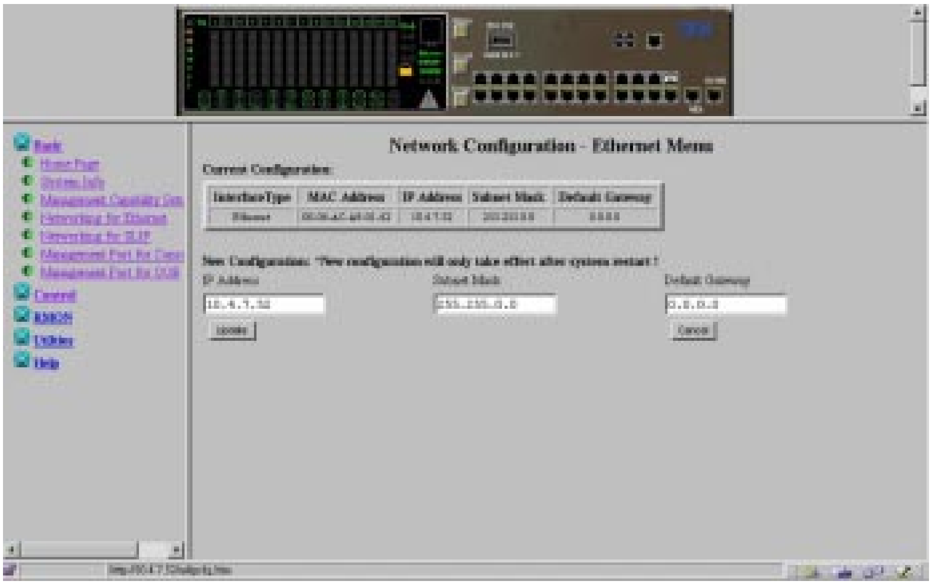
Figure 5-4. Management Capability Setup Panel

Out-Of-Band Management Enables or Disables the Out-Of-Band (OOB) management capability.

Note: You must select **Update** to save any changes you have made.

Networking For Ethernet

Selecting this option displays the Network Configuration - Ethernet Menu shown in Figure 5-5.



Network Configuration - Ethernet Menu

Current Configuration:

InterfaceType	MAC Address	IP Address	Subnet Mask	Default Gateway
Ethernet	[illegible]	10.4.7.32	255.255.0.0	0.0.0.0

New Configuration: *New configuration will only take effect after system restart !

IP Address: 10.4.7.32

Subnet Mask: 255.255.0.0

Default Gateway: 0.0.0.0

Figure 5-5. Network Configuration - Ethernet Menu

Current Configuration The IP configuration that is currently running on the Ethernet Workgroup Switch.

IP Address The dotted decimal IP address assigned to the Ethernet Workgroup Switch.

Subnet Mask The dotted decimal subnet mask assigned to the Ethernet Workgroup Switch.

Default Gateway The dotted decimal IP address of the default router assigned to the Ethernet Workgroup Switch.

New Configuration Used to update IP configuration. Enter the IP address, subnet mask, and default gateway fields you want to change and select **Update**. The restart configuration then reflects your changes.

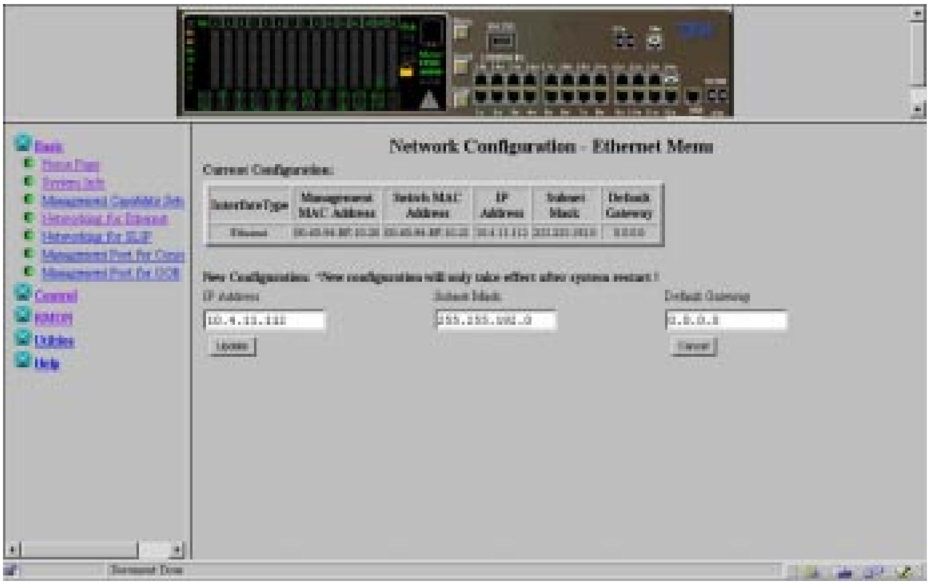
The Ethernet Workgroup Switch must be restarted before the IP address, subnet mask, and default gateway can take effect. To ensure the new information is correct, a “ping” should be done from another device connected to the Ethernet Workgroup Switch.

Notes:

1. The Ethernet Workgroup Switch must be restarted for the changes to take effect . For information on restarting the Ethernet Workgroup Switch, see " Utilities" on page 5-39.
2. The management MAC address is used for BootP.
3. The Switch MAC address (STP MAC address) is used for STP and GVRP.

Networking For SLIP

Selecting this option displays the Network Configuration - SLIP Menu panel shown in Figure 5-6.



Network Configuration - Ethernet Menu

Current Configuration:

InterfaceType	Management MAC Address	Switch MAC Address	IP Address	Subnet Mask	Default Gateway
Ethernet	[illegible]	[illegible]	[illegible]	[illegible]	0.0.0.0

New Configuration: *New configuration will only take effect after system restart !

IP Address: 10.4.11.112

Subnet Mask: 255.255.192.0

Default Gateway: 0.0.0.0

Figure 5-6. Network Configuration - SLIP Menu

Current Configuration The configuration that is currently assigned to the SLIP interface of the Ethernet Workgroup Switch.

IP Address The dotted decimal IP address assigned to the Ethernet Workgroup Switch.

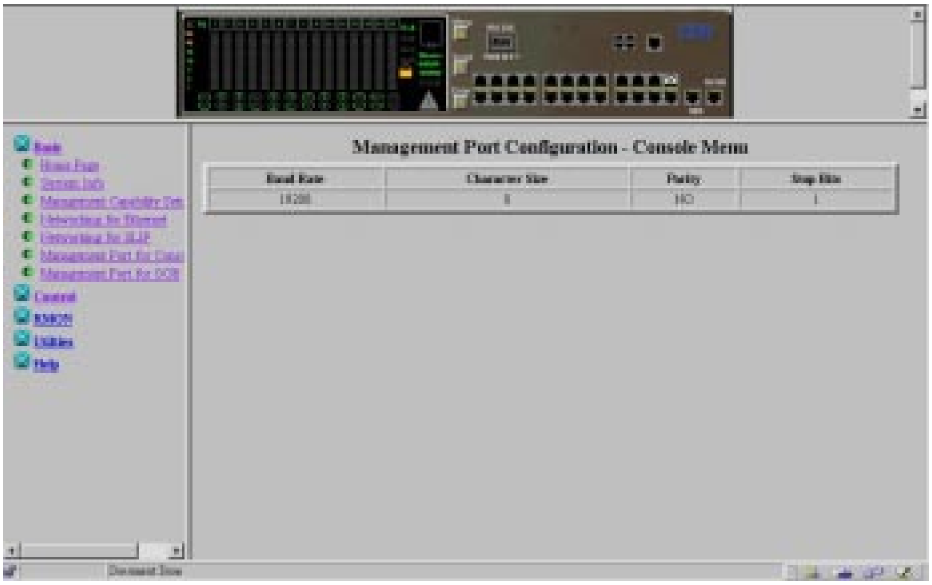
Subnet Mask The dotted decimal subnet mask assigned to the Ethernet Workgroup Switch.

New Configuration The IP configuration that will become the new current configuration when the switch is restarted.

Note: The Ethernet Workgroup Switch must be restarted for the changes to take effect. For information on restarting the Ethernet Workgroup Switch, see “Utilities” on page 5-39.

Management Port for Console

Selecting **Management Port for Console** displays the Management Port Configuration — Console Menu shown in Figure 5-7.



Management Port Configuration - Console Menu

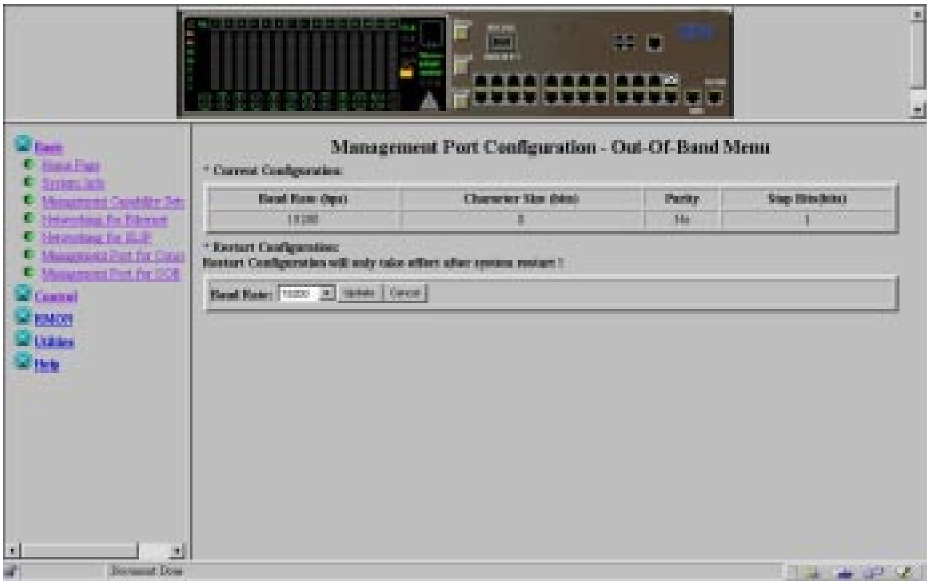
Baud Rate	Character Size	Parity	Stop Bits
19200	8	NO	1

Figure 5-7. Management Port Configuration — Console Menu

Note: The information displayed on the Management Port Configuration — Console Menu is for information only and is not configurable.

Management Port for Out-Of-Band

Selecting **Management Port for OOB** displays the Management Port Configuration – Out-Of-Band Menu shown in Figure 5-8.



Management Port Configuration - Out-Of-Band Menu

* Current Configuration:

Baud Rate (bps)	Character Size (bits)	Parity	Stop Bits(bits)
19200	8	No	1

* Restart Configuration:

Restart Configuration will only take effect after system restart !

Baud Rate: 19200

Figure 5-8. Management Port for OOB Information

Note: The only information you can change on the Management Port Configuration – Out-of-Band Menu is the baud rate. The change takes effect after the system is restarted.

Use the pull-down menu to select one of the following baud rates:

- 19200 (This is the default value for both console mode and OOB)
- 9600
- 4800
- 2400

Control

This function lets you view and configure the Ethernet Workgroup Switch ports, virtual LANs (VLANs), and trunk groups.

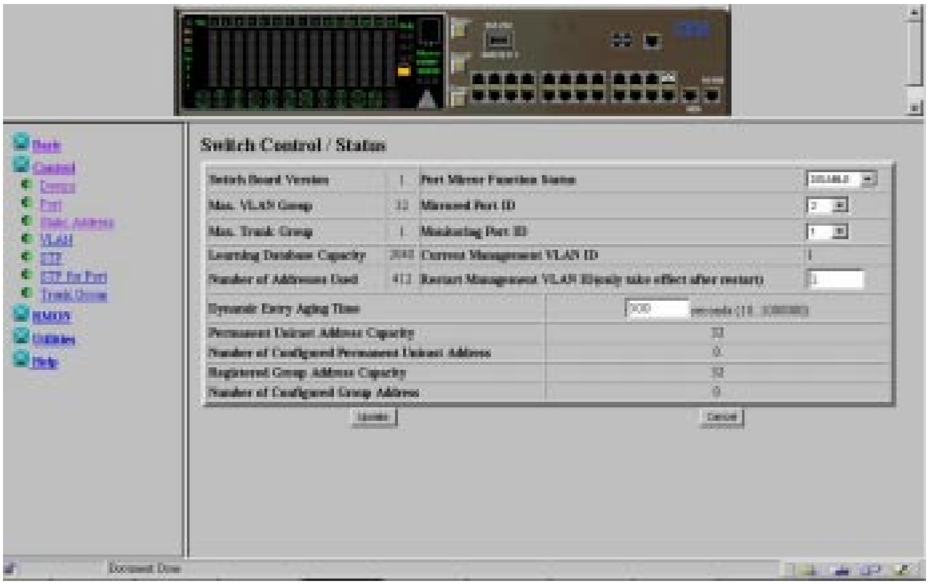
Select **Control** to view the following list of control functions:

- Device—Enables the monitoring port.
- Port—Names and configures ports 1 to 19 on Model 217 and 1 to 27 on Model 225.
- Static Address—Permanently assigns a MAC address to a switch port.
- VLAN—Configures virtual LANs and GVRP associated parameters.
- STP—Configures the STP parameters for the switch.
- STP for Port—Configures the individual STP ports parameters for the switch.
- Trunk Group—Names and configures the Trunk group.

Device

Selecting this option displays the Switch Control/Status panel shown in Figure 5-9.

The Switch Control/Status panel displays general information about the switch.



Switch Control / Status

Switch Board Version	1	Port Mirror Function Status	DISABLE
Max. VLAN Group	32	Mirrored Port ID	2
Max. Trunk Group	1	Monitoring Port ID	1
Learning Database Capacity	2048	Current Management VLAN ID	1
Number of Addresses Used	412	Restart Management VLAN ID(only take effect after restart)	1

Dynamic Entry Aging Time	300 seconds (10..1000000)
Permanent Unicast Address Capacity	32
Number of Configured Permanent Unicast Address	0
Registered Group Address Capacity	32
Number of Configured Group Address	0

Figure 5-9. Switch Control/Status

Learning Database Capacity Displays the maximum number of MAC addresses that can be learned by the system.

Number of Addresses Used Displays the maximum number of currently learned MAC addresses.

Address Aging Time Allows you to set the time of aging out the learned address. (ranging from 1 to 65535 seconds)

Static Unicast Address Capacity Displays the maximum number of permanent unicast MAC addresses allowed.

Number of Configured Static Unicast Addresses The number of permanent unicast MAC addresses that have been configured.

Port Monitoring Function Status Allows you to enable or disable the port monitoring function. If enabled, packets received by or sent from the port specified by Mirrored Port ID will be copied to the port that is specified by the Monitoring Port ID.

Mirrored Port ID Allows you to specify the port to be monitored.

Monitoring Port ID This is the port ID to which monitored MAC address frames are sent, and the port to which you should attach your network analyzer to enable you to capture the monitored frames. The default is Port 1.

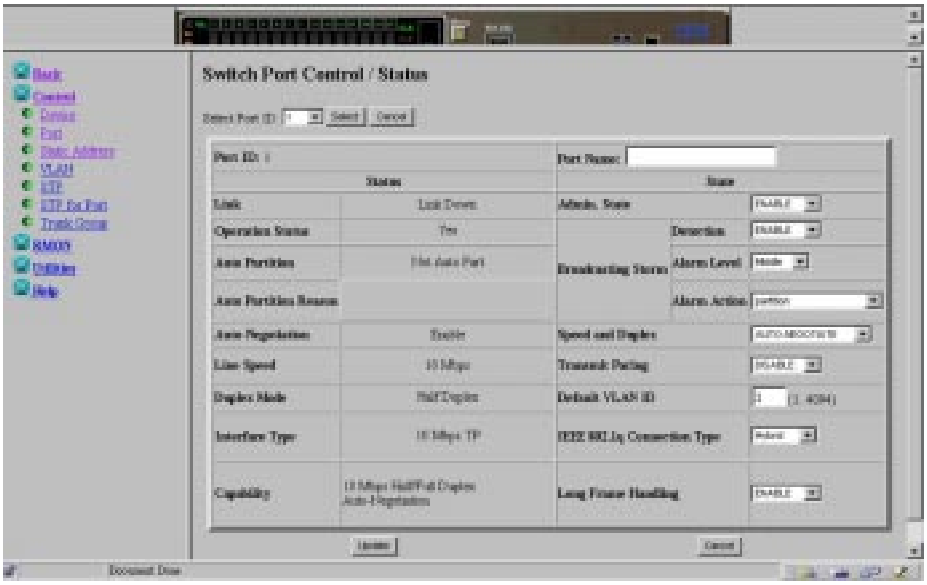
Management Restart VLAN ID Allows you to manually assign the VLAN ID which the system Network Management Unit is joined with after the next system restart.

Notes:

1. The monitoring port cannot be a Trunk Group member.
2. Select **Save** before you exit this menu to save any changes you have made.
3. These are reserved MAC addresses used by the switch which are part of the learned address database.

Port

Selecting this option displays the Switch Port Control/Status panel shown in Figure 5-10.



Switch Port Control / Status

Select Port ID: 1

Port ID: 1		Port Name:		
Status		State		
Link	Link Down	Admin. State		ENABLE
Operation Status	Yes	Broadcasting Storm	Detection	ENABLE
Auto Partition	Not Auto Part		Alarm Level	Middle
Auto Partition Reason			Alarm Action	partition
Auto Negotiation	Enable	Speed and Duplex		AUTO-NEGOTIATE
Line Speed	10 Mbps	Transmit Pacing		DISABLE
Duplex Mode	Half Duplex	Default VLAN ID		1 (1..4094)
Interface Type	10 Mbps TP	IEEE 802.1q Connection Type		Hybrid
Capability	10 Mbps Half/Full Duplex Auto-Negotiation	Long Frame Handling		ENABLE

Figure 5-10. Switch Port Control/Status

This panel shows the Ethernet Workgroup Switch’s port status and port state. To configure a port, select the Port ID Number and then select **Query**.

The following status information is presented:

Port Name Allows you to specify the name of the switch port. You can specify up to 16 characters for a port name.

Broadcasting Storm Detection Allows you to enable broadcast storm detection. Enable is the default.

Broadcasting Storm Alarm Level Allows you to set the relative threshold before a broadcast storm alarm is generated. You can specify High (30%), Middle (20%), or Low (10%). The percentage is calculated as:

%=(broadcast packets/total packets)*utilization.

Middle is the default.

Broadcasting Storm Alarm Action Allows you to specify the action to be taken in the event of a broadcast storm alarm. You can specify:

- Auto Partition–partitions the port. The port is sampled continuously until the broadcast storm has subsided below the alarm level. The port is then reenabled. Auto Partition is the default.
- Trap Auto Partition–sends a trap message to the trap receiver and partitions the port until the broadcast storm subsides and the port is reenabled.
- Send Trap–only sends a trap message to the trap receiver. The switch is not partitioned.
- No Action–no action is taken when an alarm level is reached.

Speed and Duplex

Allows you to specify the speed and mode of the switched port. You can specify Auto-Negotiation, 10 Mbps Full Duplex, 10 Mbps Half Duplex, 100 Mbps Full Duplex, or 100 Mbps Half Duplex. The selections are appropriate for the switch port and the device linking to the port. Autonegotiation is the default.

Transmit Pacing

Allows the switch to sense high network traffic and insert an extra amount of delay between transmission attempts. This reduces collision rates, reduces the number of retransmissions, reduces CPU utilization, and reduces network traffic.

Default VLAN ID

Allows you to specify the default VLAN ID (ranging from 1 to 4094) which is defined as PVID in the IEEE 802.1q Standard (reference taken from IEEE P802.1Q/D10, March 20, 1998, page 45). A current limitation is set on the PVID, such that it cannot be set to a non-existing VLAN. To ensure that the port can always be set to the PVID, it has to be joined in the Registration Fixed mode. The default VLAN ID is 1.

IEEE 802.1q Connection Type

Allows you to specify the connection type based on IEEE 802.1q. You can specify:

- Access Link–a LAN segment used for multiplexing one or more VLAN-unaware device into a port of a VLAN bridge.
- Hybrid Link–when VLAN-unaware end-stations are added to a trunk link, the resultant link is commonly known as Hybrid Link.

For more information for IEEE 802.1q see Appendix A.

Long Frame Handling

Allows frames of up to 1531 bytes to pass through the switch without error if no VLAN header is inserted, or 1535 if a VLAN header is inserted. If Long Frame Handling is disabled, the maximum received frame length is 1518 bytes. If a VLAN header is inserted into a 1518 bytes frame within the MAC, the frame will be stored as 1522 bytes within the switch.

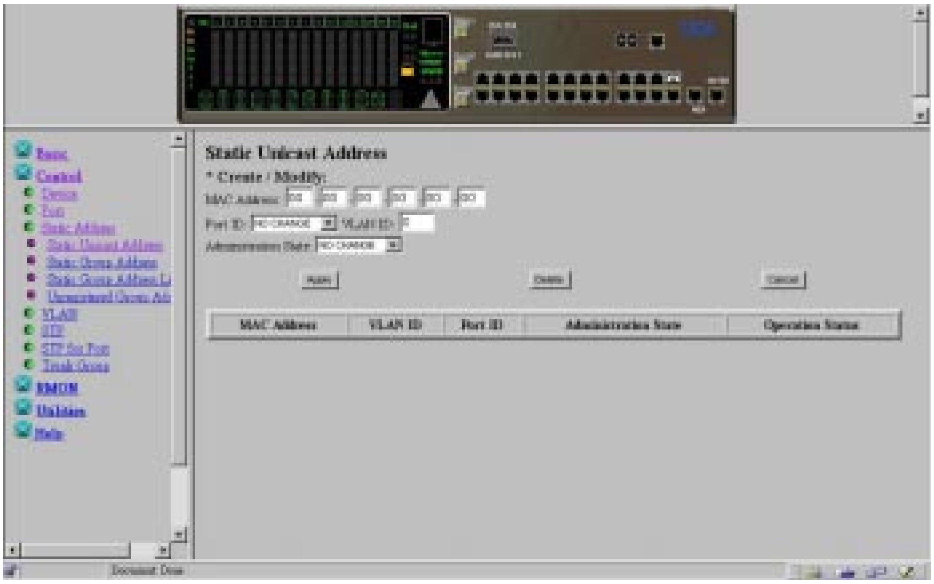
Notes:

1. Port Speed and Duplex defaults to Auto-Negotiation. You should only need to change this setting if the connected device doesn't support auto-negotiation. In order for auto-negotiate to work consistently, both the switch port and the device should be set to auto-negotiation.
2. You must select **Update** to save any changes you have made.

Static Address

Static Unicast Address

Selecting this option displays the Static Unicast Addresses panel shown in Figure 5-11.



Static Unicast Address

* Create / Modify:

MAC Address: 00 : 00 : 00 : 00 : 00 : 00

Port ID: NO CHANGE VLAN ID: 1

Administration State: NO CHANGE

MAC Address	VLAN ID	Port ID	Administration State	Operation Status

Figure 5-11. Static Unicast Address

This panel lets you define up to 32 permanent MAC addresses. If a permanent address is assigned to a switch port and the port's status is *active*, then that MAC address can only be connected through that assigned switch port. If the device is connected to a port other than the assigned port, then a violation occurs and the packets are not sent.

To assign a Static Unicast MAC address to a port, perform the following steps:

1. Enter the MAC address and select the port ID and the VLAN ID.

2. Set the Administration State to enabled.

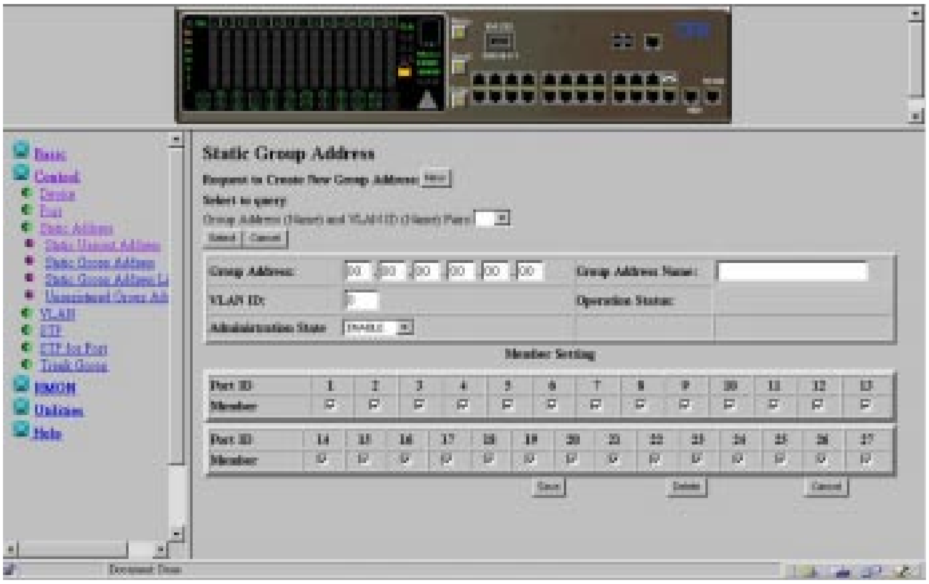
3. Select **Apply**.

4. Repeat step 1 through 3 for each MAC address.

A list of permanent addresses appears at the bottom of the panel.

Static Group Address

Selecting this option displays the Static Group Addresses panel shown in Figure 5-12.



Static Group Address

Request to Create New Group Address: New

Select to query:

Group Address (Hexa) and VLAN ID (Hexa) Pairs:

Select Cancel

Group Address:	00 . 00 . 00 . 00 . 00 . 00	Group Address Name:	
VLAN ID:	0	Operation Status:	
Administration State	ENABLE		

Member Setting

Port ID	1	2	3	4	5	6	7	8	9	10	11	12	13
Member	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Port ID	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Member	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Save Delete Cancel

Figure 5-12. Static Group Address

This menu lets you define a set of unique pairs of Static Group address and VLAN ID, and assign the associated ports to each pair.

Group Address A MAC address entry that specifies a group address.

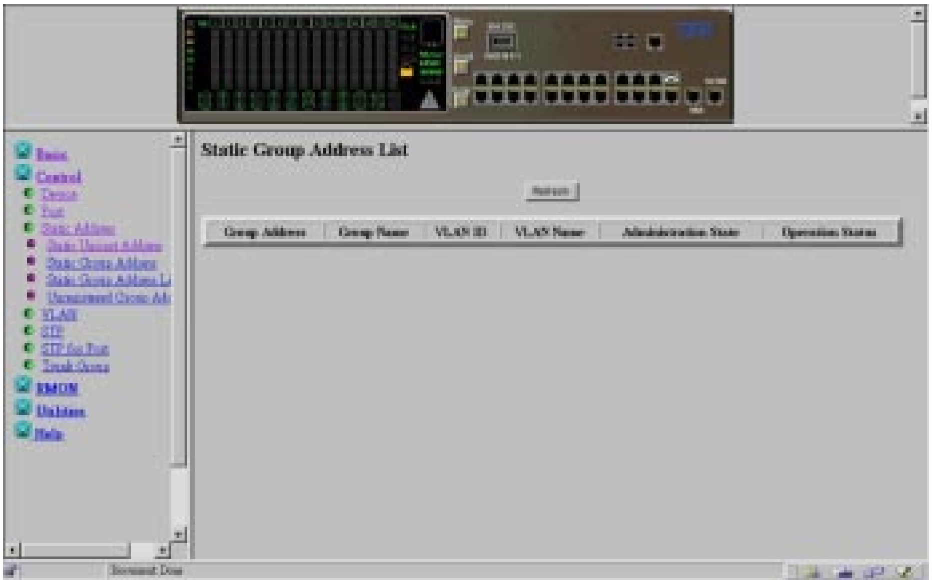
| **VLAN ID** VLAN ID associated to the Group Address, ranging from 1 to 4094.

| **Group Name** A name for each Group Address and VLAN ID pair.

| **Member Setting** Allows you to assign ports for each Group Address.

Group Address List

Selecting this option displays the Group Address List panel shown in Figure 5-13.



Static Group Address List

Group Address	Group Name	VLAN ID	VLAN Name	Administration State	Operation Status

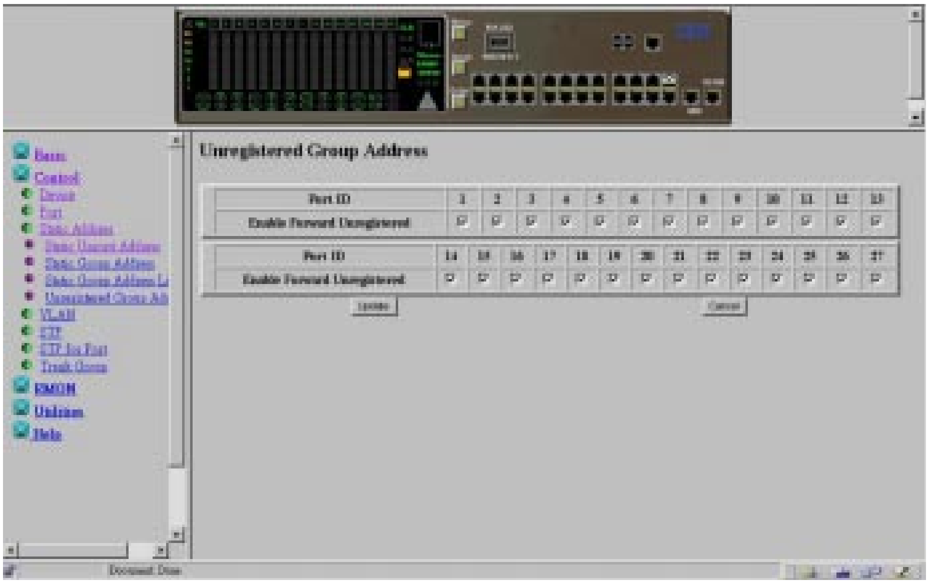
Figure 5-13. Group Address Listing

The Group Address List include Group Address, Group Name, VLAN ID, VLAN Name, Administration State, and Operation Status that can be registered by the user.

The menu above appears the list of entries originally created in the Static Group Address. For information on how entries can be created, please refer to the section on “Static Group Address” on page 5-18.

Unregistered Group Address

Selecting this option displays the Unregistered Group Address panel shown in Figure 5-14.



Unregistered Group Address

Port ID	1	2	3	4	5	6	7	8	9	10	11	12	13
Enable Forward Unregistered	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Port ID	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Enable Forward Unregistered	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Figure 5-14. Unregistered Group Address

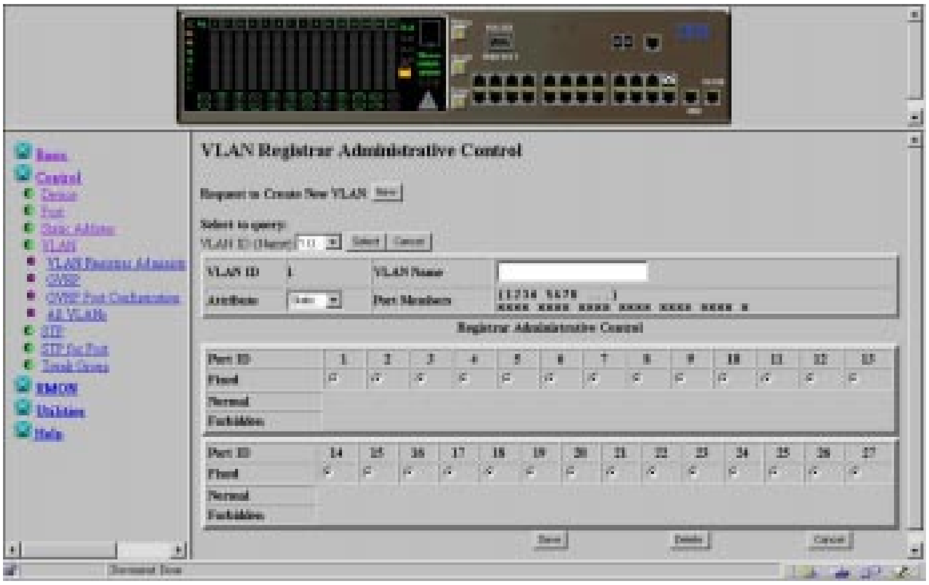
This menu lets you specify the ports to which a packet is forwarded when the group address specified was not defined and registered in the system.

The packets will be forwarded to the port which is selected. The default value for each port is selected. Select **Update** to save the configuration.

VLAN Control

VLAN Registrar Administrative Control

Selecting this option displays the VLAN Registrar Administrative Control panel shown in Figure 5-15.



VLAN Registrar Administrative Control

Request to Create New VLAN

Select to query:
VLAN ID (Name) 1(1)

VLAN ID	1	VLAN Name	
Attribute	Static	Port Members	11234 5678 1 xxxx xxxx xxxx xxxx xxxx xxxx x

Registrar Administrative Control

Port ID	1	2	3	4	5	6	7	8	9	10	11	12	13
Fixed	●	●	●	●	●	●	●	●	●	●	●	●	●
Normal													
Forbidden													

Port ID	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Fixed	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Normal														
Forbidden														

Figure 5-15. VLAN Registrar Administrative Control

This menu lets you configure up to 31 VLANs (ranging from 1 to 4094) on the Ethernet Workgroup Switch. VLAN devices can communicate only with other devices on the same VLAN. When a VLAN is created by the user, its attribute will be "Static". If it is created by GVRP, it becomes "Dynamic". (see “Static vs. Dynamic VLANs” on page A-7 in Appendix A, “Introduction to Virtual LANs (VLANs) and Spanning Tree Protocol (STP)”)

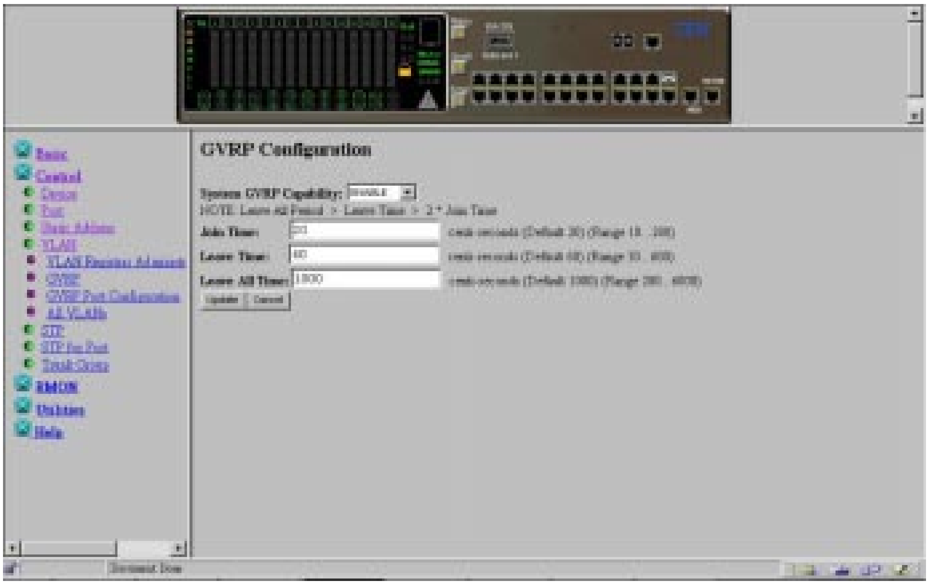
To configure a VLAN, select a blank or existing VLAN ID and **Select**.

- Fixed: The port belongs to the specified VLAN.
- Normal: The port belongs to the specified VLAN only if it is registered with GVRP.
- Forbidden: The port is never allowed to join this VLAN even when a GVRP registration request occurs.

Note: You must select **SAVE** to save any changes.

GVRP Configuration

Selecting this option displays the GVRP Configuration panel shown in Figure 5-16.



GVRP Configuration

System GVRP Capability: DISABLE

NOTE: Leave All Period > Leave Time > 2 * Join Time

Join Time: 20 centi-seconds (Default 20) (Range 10 .. 200)

Leave Time: 60 centi-seconds (Default 60) (Range 30 .. 600)

Leave All Time: 1000 centi-seconds (Default 1000) (Range 200 .. 6000)

Figure 5-16. GVRP Configuration

This panel lets you enable or disable GVRP, a Dynamic VLAN. A Dynamic VLAN entry will automatically be aged out after a period of time when no port member is registered to that VLAN.

System GVRP Capability Allows the GVRP protocol to be enabled or disabled for the entire switch.

Join Time The join time is the time within which a registered port have to reregister after the Dynamic VLAN received an unregistering signal. Its value is 10-200 centi-seconds with default value of 20.

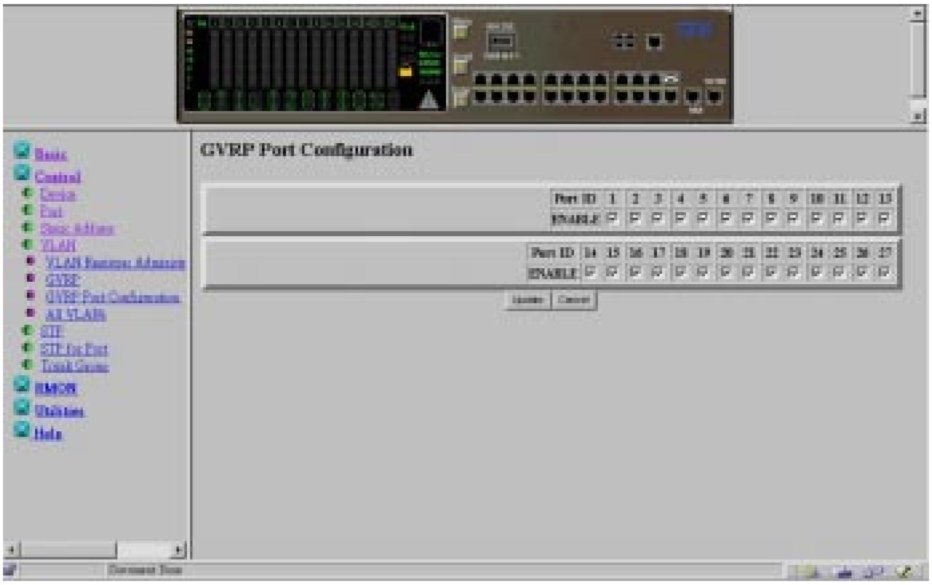
Leave Time The leave time is the time that the dynamic VLAN, after receiving an unregistering signal, will wait before actually being aged out. Its value is 30-600 centi-seconds with default value of 60.

Leave All Time The leave all time is the interval that the dynamic VLAN will broadcast an aging out signal. Its value is 200-6000 centi-seconds with default value of 1000 .

Select **Update** to save your changes.

GVRP Port Configuration

Selecting this option displays the GVRP Port Configuration panel shown in Figure 5-17.



GVRP Port Configuration

Port ID	1	2	3	4	5	6	7	8	9	10	11	12	13
ENABLE	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

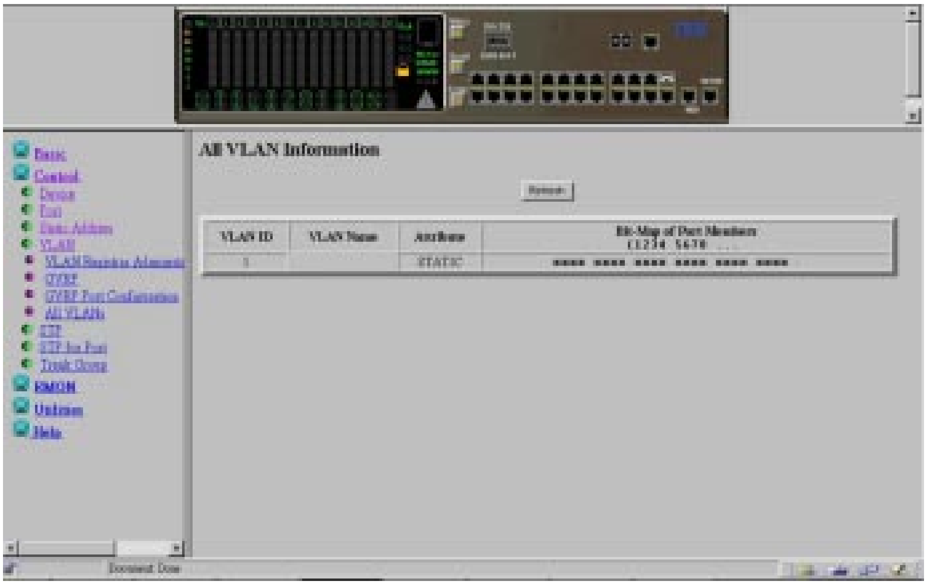
Port ID	14	15	16	17	18	19	20	21	22	23	24	25	26	27
ENABLE	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Figure 5-17. GVRP Port Configuration

This panel lets you enable or disable the GVRP function for each port. Select the box under Port ID and select "Update" of GVRP.

All VLANs

Selecting this option displays the All VLANs panel shown in Figure 5-18.



All VLAN Information

Refresh

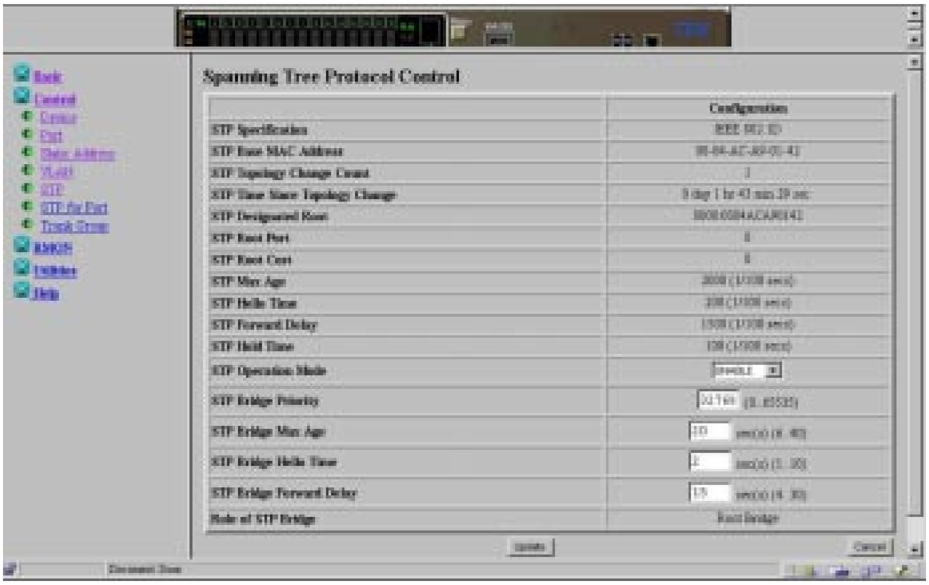
VLAN ID	VLAN Name	Attribute	Bit-Map of Port Members (1234 5678 ...
1		STATIC	■■■■ ■■■■ ■■■■ ■■■■ ■■■■ ■■■■

Figure 5-18. All VLANs Information

This panel displays all the VLAN attributes created and is read only.

Spanning Tree Protocol Control

Selecting this option displays the Spanning Tree Protocol Control panel shown in Figure 5-19.



Spanning Tree Protocol Control

	Configuration
STP Specification	IEEE 802.1D
STP Base MAC Address	00-04-AC-A0-01-42
STP Topology Change Count	3
STP Time Since Topology Change	3 day 1 hr 43 min 29 sec
STP Designated Root	8000.0004ACA00142
STP Root Port	0
STP Root Cost	0
STP Max Age	2000 (1/100 secs)
STP Hello Time	200 (1/100 secs)
STP Forward Delay	1500 (1/100 secs)
STP Hold Time	100 (1/100 secs)
STP Operation Mode	Disable
STP Bridge Priority	32768 (0..65535)
STP Bridge Max Age	20 sec(s) (6..40)
STP Bridge Hello Time	2 sec(s) (1..10)
STP Bridge Forward Delay	15 sec(s) (4..30)
Role of STP Bridge	Root Bridge

Figure 5-19. Spanning Tree Protocol Control

This panel allows you to configure and manage the STP system on the Ethernet Workgroup Switch.

Table 5-4 on page 5-26 lists the fields on the Spanning Tree Protocol Control for Group panel.

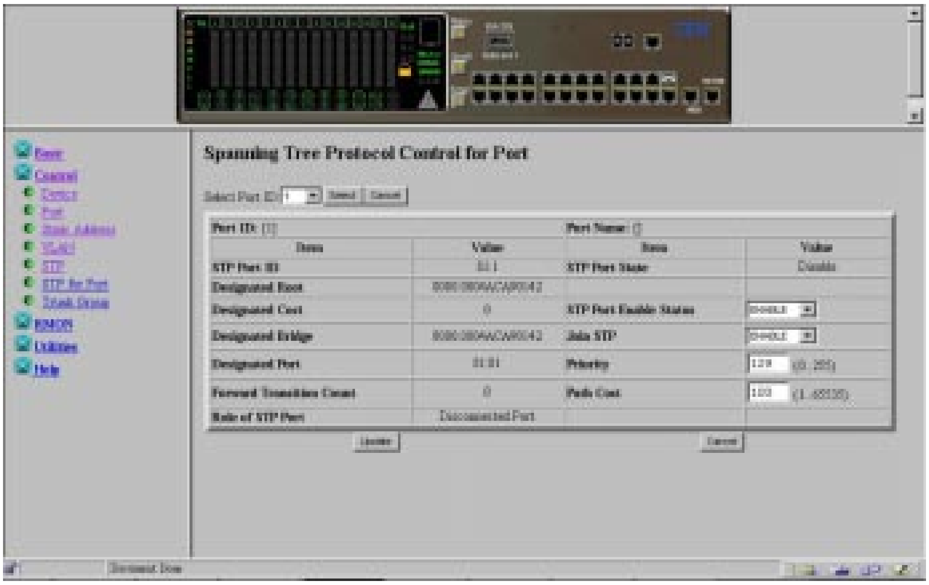
Table 5-4. Spanning Tree Protocol Control

STP Topology Change Count	Shows the number of network topology changes as a group that have occurred.
STP Time Since Topology Change	Shows the time since the last topology change was detected (read only).
STP Designated Root	Shows the bridge identifier of the designated root bridge (read only).
STP Root Port	Shows the root port of the switch (read only).
STP Root Cost	Shows the path cost from the switch to the root bridge (read only).
STP Hold Time	Shows the shortest time interval allowed between the transmission of BPDUs (read only).
Group STP Operation Mode	Allows you to enable or disable the STP for the switch.
STP Bridge Priority	Allows you to specify the priority of the switch. By changing the priority of the switch, you can make it more or less likely to become the root bridge. The lower the number, the more likely the bridge will become the root bridge. The range is 0–65535. The default is 32768.
STP Bridge Max. Age	Allows you to specify the time in seconds that the switch waits before trying to reconfigure the network when it is the root bridge. If the switch has not received a BPDU within the time specified in this field, it tries to reconfigure the STP topology. The range is 6–40 seconds. The default is 20 seconds.
STP Bridge Hello Time	Allows you to specify the time delay in seconds between the transmission of BPDUs from the switch when it is the root bridge. The range is 1–10 seconds. The default is 2 seconds.
STP Bridge Forward Delay	Allows you to specify the time in seconds that the ports on the switch spend in the learning and listening and learning states when the switch is in the root bridge. The range is 4–30 seconds. The default setting is 15 seconds.

Note: You must select **Update** to save any changes.

Spanning Tree Protocol Control for Port

Selecting this option displays the Spanning Tree Protocol for Port panel shown in Figure 5-20.



Spanning Tree Protocol Control for Port

Select Port ID: 1

Port ID: [1]　Port Name: []

Item	Value	Item	Value
STP Port ID	80:01	STP Port State	Disable
Designated Root	8000:0800AACA0042		
Designated Cost	0	STP Port Enable Status	DISABLE
Designated Bridge	8000:0800AACA0042	Join STP	DISABLE
Designated Port	80:01	Priority	128 (0..255)
Forward Transition Count	0	Path Cost	100 (1..65535)
Role of STP Port	Disconnected Port		

Figure 5-20. Spanning Tree Protocol Control for Port

This panel allows you to configure and manage the STP parameters of each port on the Ethernet Workgroup Switch. Port ID 20 is used to configure and manage the STP parameters of the Trunk group for Model 217 and Port ID 28 is used for Model 225.

You can query a different switch port by selecting the Port ID and selecting **Query**.

Table 5-5 on page 5-28 lists the fields on the Spanning Tree Protocol Control for VLAN Ports panel.

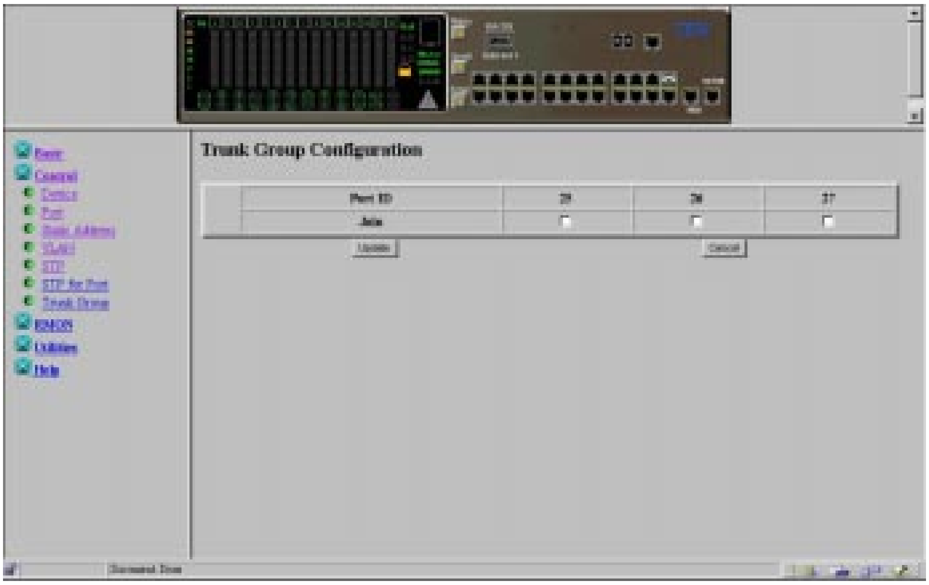
Table 5-5. Spanning Tree Protocol Control for VLAN Port

Port ID	The port number, currently queried.
Port Name	The name of the port, currently queried.
Designated Root	Shows the bridge identifier of the root bridge (read only).
Designated Cost	Shows the path cost from the root bridge to the designated bridge port for the current port's VLAN (read only).
Designated Bridge	Shows the bridge identifier of the designated bridge for the current port's VLAN (read only).
Forward Transition Count	Shows the number of times that the current port has changed from the learning state to the forwarding state (read only).
STP Port State	Listening Forward.
STP Port Enable Status	Allows you to enable or disable the port.
Join STP	Allows you to enable or disable the port as part of a VLAN group.
Priority	Allows you to specify the priority of the port. By changing the priority of the port, you can make it more or less likely to become the root port. The lower the number, the more likely it is that the port will be the root port. The range is 0–255. The default is 129.
Path Cost	Allows you to specify the path cost of the port. The default port costs are 10 for 100BASE-X 100 for 10BASE-T 8 for Virtual Trunk Port 20 on Model 217 and 28 on Model 225

Note: You must select **Update** to save any changes.

Trunk Group

Selecting this option displays the Trunk Group Configuration panel shown in Figure 5-21.



Trunk Group Configuration

	Port ID	25	26	27
	Join	□	□	□

Figure 5-21. Trunk Group Configuration

This menu allows you to configure and manage the Trunk Group on the Ethernet Workgroup Switch. The switch provides a Port Trunking algorithm to allow two or three 100 Mbps ports to be connected in parallel between switches to increase the bandwidth between devices. The Trunk group has an STP port instance for it which is specified as port 20 on Model 217 or port 28 on Model 225. It is possible to trunk between Model 217 and Model 225 only. It is only possible to trunk ports 17, 18, 19 on Model 217 and ports 25, 26 and 27 on Model 225.

Note: You must select **Update** to save changes.

RMON

Remote Monitoring MIB (RMON) allows you to monitor LANs remotely. RMON allows you to remain at one workstation and collect information on all switch ports.

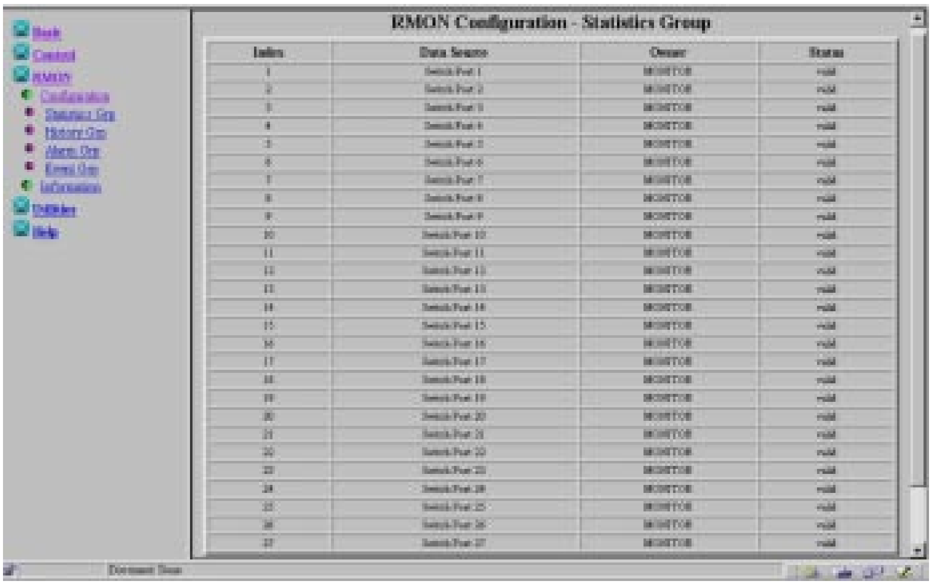
Configuration

Selecting this option allows you to select from the following types of RMON configuration information:

- Statistics
- History
- Alarm
- Event

RMON Configuration - Statistics Group

Selecting **Statistics Grp** displays the RMON Configuration - Statistics Group panel shown in Figure 5-22.



RMON Configuration - Statistics Group

Index	Data Source	Owner	Status
1	Switch Port 1	MONITOR	valid
2	Switch Port 2	MONITOR	valid
3	Switch Port 3	MONITOR	valid
4	Switch Port 4	MONITOR	valid
5	Switch Port 5	MONITOR	valid
6	Switch Port 6	MONITOR	valid
7	Switch Port 7	MONITOR	valid
8	Switch Port 8	MONITOR	valid
9	Switch Port 9	MONITOR	valid
10	Switch Port 10	MONITOR	valid
11	Switch Port 11	MONITOR	valid
12	Switch Port 12	MONITOR	valid
13	Switch Port 13	MONITOR	valid
14	Switch Port 14	MONITOR	valid
15	Switch Port 15	MONITOR	valid
16	Switch Port 16	MONITOR	valid
17	Switch Port 17	MONITOR	valid
18	Switch Port 18	MONITOR	valid
19	Switch Port 19	MONITOR	valid
20	Switch Port 20	MONITOR	valid
21	Switch Port 21	MONITOR	valid
22	Switch Port 22	MONITOR	valid
23	Switch Port 23	MONITOR	valid
24	Switch Port 24	MONITOR	valid
25	Switch Port 25	MONITOR	valid
26	Switch Port 26	MONITOR	valid
27	Switch Port 27	MONITOR	valid

Figure 5-22. RMON Configuration - Statistics Group

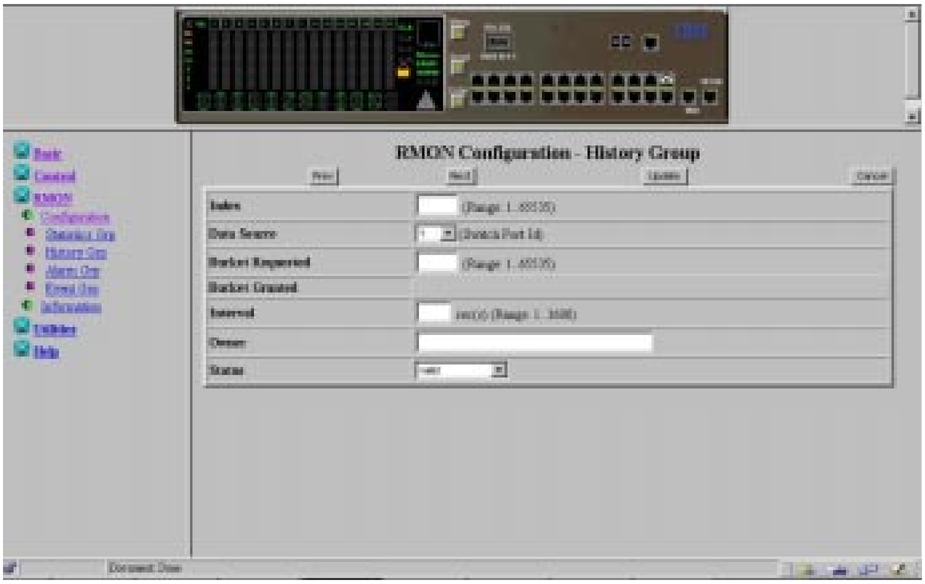
This panel provides an overview of the current switch port activity.

Table 5-6. RMON Configuration - Statistics Group

Index	Displays the switch port indexes from ports 1 to 19 on Model 217 and ports 1 to 27 on Model 225.
Data Source	Displays the data source as the switch ports 1 to 19 on Model 217 and ports 1 to 27 on Model 225.
Owner	Displays the owner of the statistics. The owner is always the monitor.
Status	Displays the current status of each port—Valid.

RMON Configuration - History Group

Selecting **History Grp** displays the RMON Configuration - History Group panel shown in Figure 5-23.



RMON Configuration - History Group

Index	(Range: 1..65535)
Data Source	1 (Switch Port Id)
Bucket Requested	(Range: 1..65535)
Bucket Granted	
Interval	sec(s) (Range: 1..3600)
Owner	
Status	valid

Figure 5-23. RMON Configuration - History Group

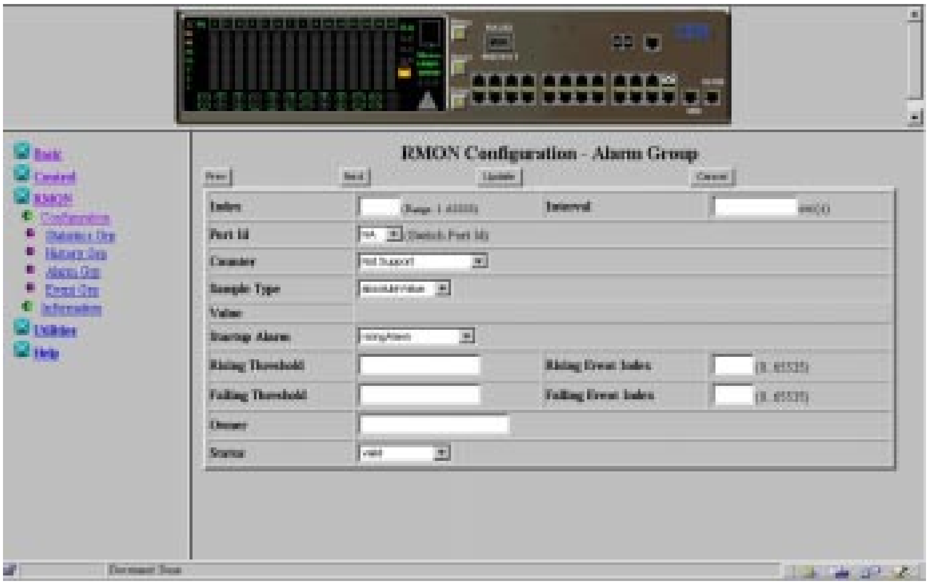
This panel provides a means of correlating the data gathered by the statistics group over time. It records statistical samples according to the user-specified time interval and duration and stores them for later retrieval.

Table 5-7. RMON Configuration - History Group

Index	Number chosen to identify the entry. The range is 1 to 65535.
Data Source	Port ID for which data will be gathered (ports 1 to 19 for Model 217 and ports 1 to 27 for Model 225).
Bucket Requested	Number of sample buckets you want to collect and store. The range is 1– 65535. The default is 50.
Bucket Granted	Number of sample buckets what will be collected and stored. The number granted is affected by the number of buckets requested and by available resources. Bucket Granted will change as resources fluctuate.
Interval	Time in seconds over which the data is sampled for each bucket. The range is 1 to 3600 seconds (1 hour). The default is 1800 seconds.
Owner	Text field to identify the owner.
Status	• Valid - An entry is fully configured and consistent. • underCreation—Entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made underCreation to be modified. • Invalid—Entry is cleared.

RMON Configuration - Alarm Group

Selecting **Alarm Grp** displays the RMON Configuration - Alarm Group panel shown in Figure 5-24.



RMON Configuration - Alarm Group

Index	(Range: 1..65535)	Interval	sec(s)
Port Id	NA (Switch Port Id)		
Counter	Not Support		
Sample Type	AbsoluteValue		
Value			
Startup Alarm	RisingAlarm		
Rising Threshold		Rising Event Index	(0..65535)
Falling Threshold		Falling Event Index	(0..65535)
Owner			
Status	Valid		

Figure 5-24. RMON Configuration - Alarm Group

This panel tracks extraordinary events or activities. It permits you to set the RMON alarms to specific thresholds. When the traffic volume exceeds or drops below those thresholds, an event is activated. A *rising* threshold is used to monitor the value of a counter when it rises above a particular level. A *falling* threshold is used to monitor the value of a counter when it falls below a particular level. Thresholds can be set against either an absolute value or a *delta* (change in) value. Alarms can generate an action response through the Events Group.

Table 5-8. RMON Configuration - Alarm Group

Index	Number chosen to identify the entry. The range is 1 to 65535.
Interval	Time in seconds over which the data is sampled for each bucket. The range is 1 to 3600 seconds (1 hour). The default is 1800 seconds.
Port ID	Switch Port number for ports 1 to 19 on Model 217 and ports 1 to 27 on Model 225.
Counter	Choose an event to track. If Not Support is chosen, the counter field defaults to the octets counter.
Sample Type-Absolute Value	Value stored is compared directly to the threshold level.
Sample Type-Delta Value	The value of the selected variable at the last sample is subtracted from the current value, and the difference is compared with the threshold value.
Value	Value of the statistic during the last sampling period.

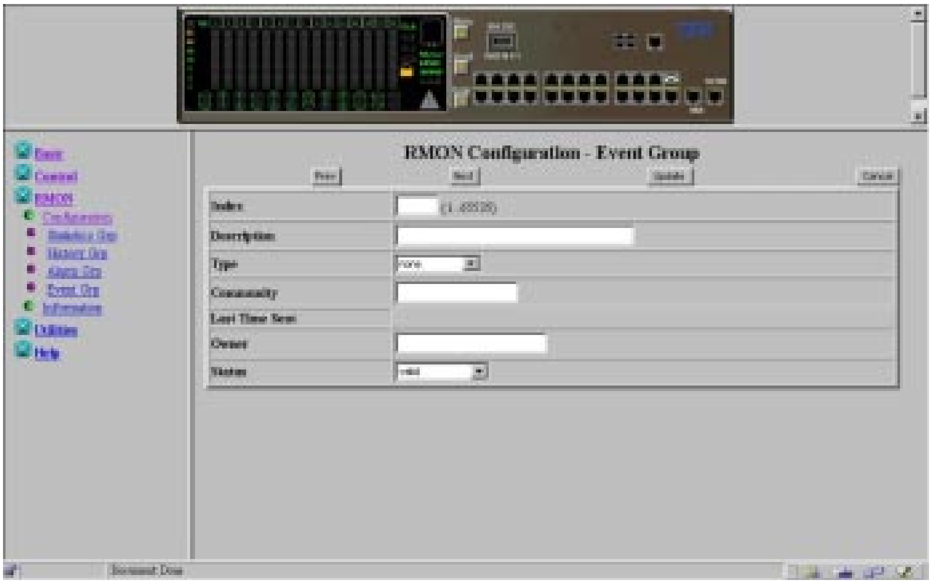
Table 5-8. RMON Configuration - Alarm Group

Startup Alarm	Of rising and falling thresholds, the one that must be crossed first for an event to be generated. • risingAlarm - Event is generated when the rising threshold is crossed first. • fallingAlarm - Event is generated when the falling threshold is crossed first. • risingOrfallingAlarm - Event is generated when either the rising or falling threshold is crossed first.
Rising Threshold	Threshold for the sampled statistic. When the current sampled value is ***greater than or equal to*** this threshold, ***and*** the value of this sample at the last sampling interval was ***less than*** the threshold, then a single event is generated. After a rising event is generated, another rising event is not generated until the sampled value falls below this threshold and reaches the falling threshold.
Rising Event Index	Index of the event entry that is used when the rising threshold is crossed. It must coincide with the Event Group Index. If you choose 0, no event is generated when this threshold is met.
Falling Threshold	Threshold for the sampled statistic. When the current sampled value is ***less than or equal to*** this threshold, ***and*** the value of this sample at the last sampling interval was ***greater than*** the threshold, then a single event is generated. After a falling event is generated, another falling event is not generated until the sampled value rises above this threshold and reaches the rising threshold.
Falling Event Index	Index of the event entry that is used when the falling threshold is crossed. It must coincide with the Event Group Index. The range is 0 to 65535. If you choose 0, no event is generated when this threshold is met.
Owner	Text field to identify the owner.
Status	• Valid - An entry is fully configured and consistent. • underCreation—An entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made underCreation to be modified. • Invalid—Entry is cleared.

Note: Select **Update** to save changes.

RMON Configuration - Event Group

Selecting **Event Grp** displays the RMON Configuration - Event Group panel shown in Figure 5-25.



RMON Configuration - Event Group

Index	(1..65535)
Description	
Type	none
Community	
Last Time Sent	
Owner	
Status	valid

Figure 5-25. RMON Configuration - Event Group

This panel creates entries in an event log and sends SNMP traps to the management workstation.

Table 5-9. RMON Configuration - Event Group

Index	A number that identifies an entry in the event table.
Description	A comment that describes this event.
Type - none	No action taken.
Type - log	An entry is made in the log table for each event.
Type - snmp-trap	An SNMP trap is sent to one or more management stations.
Type - log-and-trap	An entry is made in the log table and an SNMP trap is sent to one or more management stations.
Community	An octet string that specifies the SNMP community to which an SNMP trap is to be sent.
Last Time Sent	The value of System Up Time at the time this event entry last generated an event.
Owner	Text field to identify the owner.
Status	• Valid - An entry is fully configured and consistent. • underCreation—An entry is in the process of being created and might be incomplete. If an entry is valid, the entry should be made underCreation to be modified. • Invalid—Entry is cleared.

Note: Select **Update** to save changes.

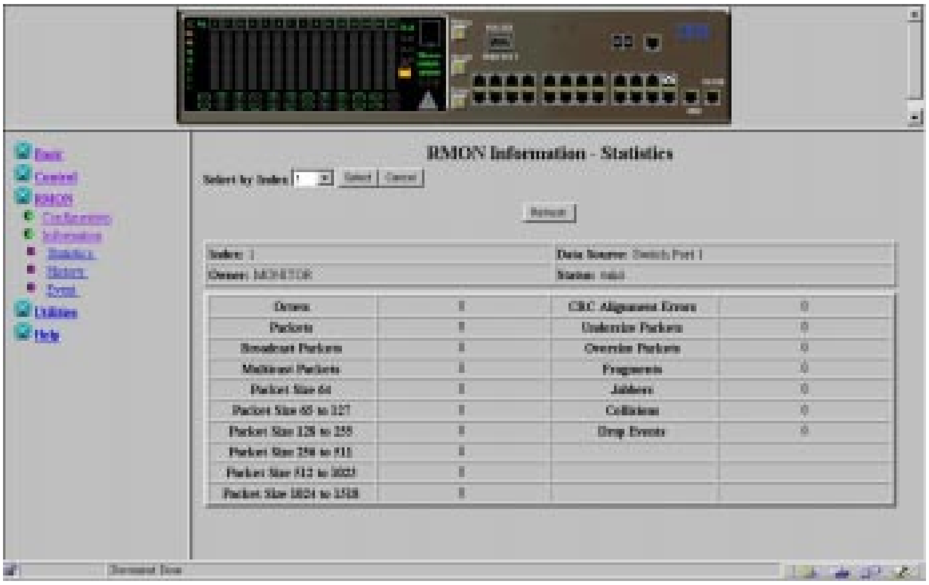
Information

Selecting this option allows you to select from the following types of RMON informational topics:

- Statistics
- History
- Event

RMON Information - Statistics

Selecting **Statistics** displays the RMON Information - Statistics Event Group panel shown in Figure 5-26.



RMON Information - Statistics

Select by Index: 1

Index: 1 | Data Source: Switch Port 1
Owner: MONITOR | Status: valid

Octets	0	CRC Alignment Errors	0
Packets	0	Undersize Packets	0
Broadcast Packets	0	Oversize Packets	0
Multicast Packets	0	Fragments	0
Packet Size 64	0	Jabbers	0
Packet Size 65 to 127	0	Collisions	0
Packet Size 128 to 255	0	Drop Events	0
Packet Size 256 to 511	0		
Packet Size 512 to 1023	0		
Packet Size 1024 to 1518	0		

Figure 5-26. RMON Information - Statistics

This panel provides traffic and error statistics counters. To view other ports, select either **Prev** or **Next** or enter a port ID in the Query by Index field and select **Update**. See Table 5-10 on page 5-35 for the type of statistic counters that are recorded.

Table 5-10. RMON Information - Statistics

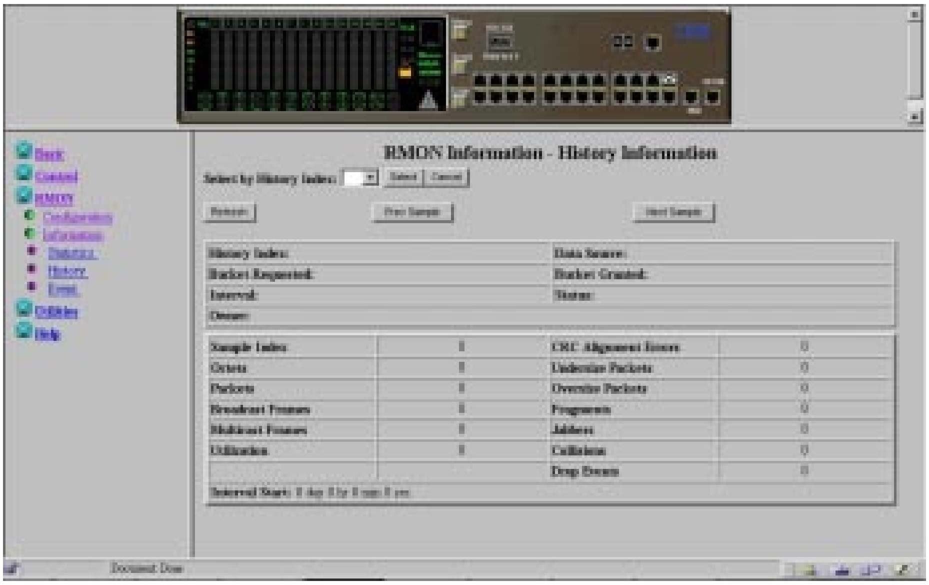
Octets	A whole number representing the total readable octets received by the port.
CRC Alignment Errors	The total CRC or alignment error frames within the proper size (64 to 1518 octets) received by the port.
Packets	Total number of packets received by the port, including bad packets, broadcast packets and multicast packets.
Undersize Packets	The number of small (less than 64 octets long) packets received.
Broadcast Packets	The total number of packets transmitted that were directed to the broadcast address.

Table 5-10. RMON Information - Statistics

Oversize Packets	The number of large (greater than 1518 octets long) packets received. If the Long Frame mode is selected, only those packets longer than 1535 octets are counted.
Multicast Packets	The number of packets received that were directed to the Multicast Address.
Fragments	The total number of packets that were received that were longer than 1518 octets and had an FCS or alignment error.
Packet Size 64	The number of packets received that were 64 octets.
Jabbers	The total number of packets that were received that were less than 64 octets and had an FCS or alignment error.
Packet Size 65 to 127	The number of packets received that were from 65 to 127 octets.
Collisions	The number of collisions.
Packet Size 128 to 255	The number of packets received that were from 128 to 255 octets.
Drop Events	The number of events in which packets were dropped by the monitor because of lack of resources.
Packet Size 256 to 511	The number of packets received that were from 256 to 511 octets.
Packet Size 512 to 1023	The number of packets received that were from 512 to 1023 octets.
Packet Size1024 to 1518	The number of packets received that were from 1024 to 1518 octets.

RMON Information - History Information

Selecting **History** displays the RMON Information - History Information panel shown in Figure 5-27.



RMON Information - History Information

Select by History Index:

History Index:		Data Source:	
Bucket Requested:		Bucket Granted:	
Interval:		Status:	
Owner:			

Sample Index	0	CRC Alignment Errors	0
Octets	0	Undersize Packets	0
Packets	0	Oversize Packets	0
Broadcast Frames	0	Fragments	0
Multicast Frames	0	Jabbers	0
Utilization	0	Collisions	0
		Drop Events	0

Interval Start: 0 day 0 hr 0 min 0 sec

Figure 5-27. RMON Information - History Information

The History Group provides a means of correlating the data gathered by the Statistical Group over time. Each interval saved is called a *bucket*. The number of buckets requested represents the number of times you want to collect and store the samples. The probe responds with the number of buckets granted depending on the request and the resources available.

Table 5-11. RMON Information - History

Prev Sample	Selects the previous sample.
Next Sample	Selects the next sample.

You can also enter a specific history index and **Select**.

For definitions of the Information History fields, see the field definitions in “RMON Information - Statistics” on page 5-35.

RMON Information - Event Group

Selecting **Event** displays the RMON Information - Event Group panel shown in Figure 5-28.

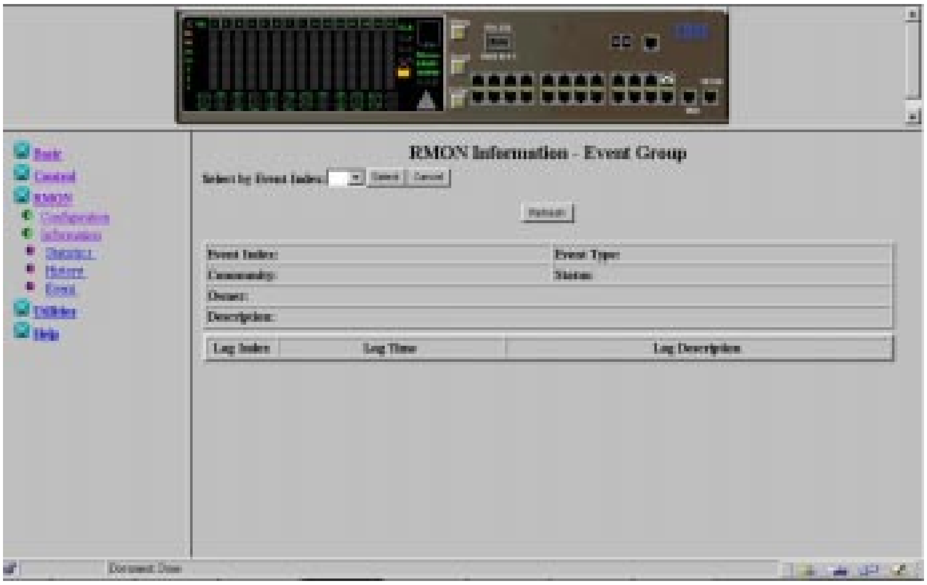


Figure 5-28. RMON Information - Event Group

The Event Group requires implementation the Alarm Group. The Alarm Group periodically takes statistical samples and compares them with thresholds that have been configured. The event table stores configuration entries that define an index, polling period, and alarm threshold values.

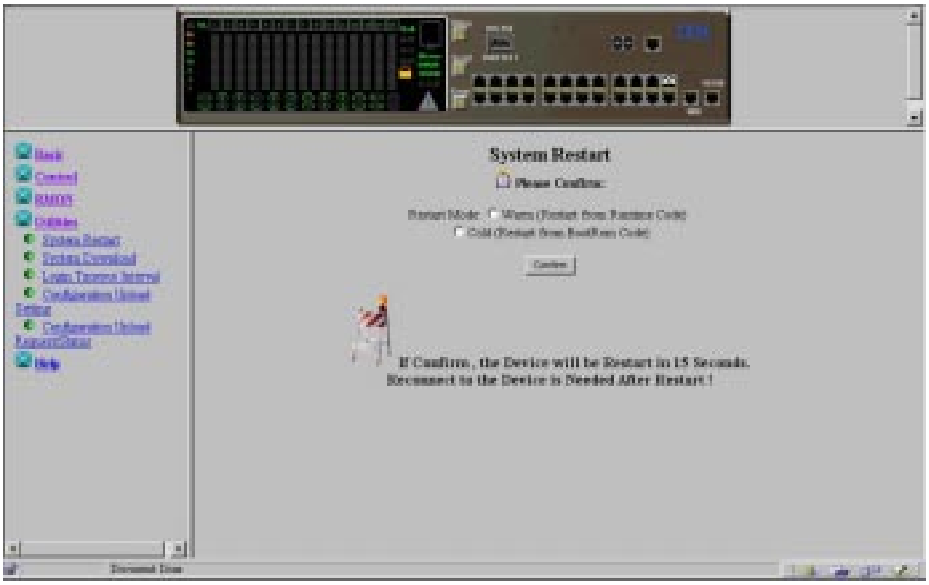
To Query an Event Group, enter the group index in the Event Index field and **Select**.

For definitions of the Information Event fields, see the field definitions in “RMON Configuration - Event Group” on page 5-34.

Utilities

System Restart

Selecting this option displays the System Reset panel shown in Figure 5-29.



System Restart

Please Confirm:

Restart Mode: ○ Warm (Restart from Runtime Code)
○ Cold (Restart from BootRom Code)

If Confirm , the Device will be Restart in 15 Seconds.
Reconnect to the Device is Needed After Restart !

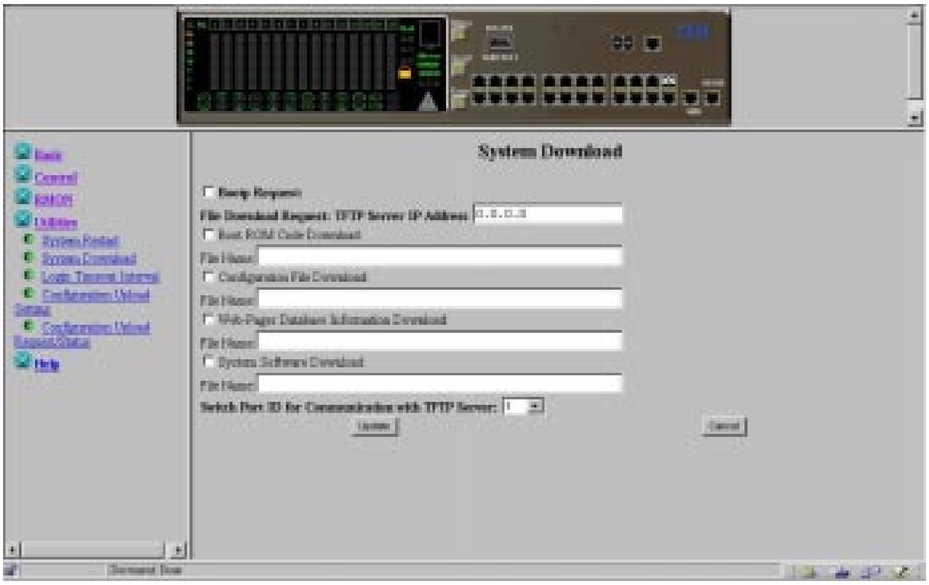
Figure 5-29. System Restart

This panel lets you perform a *cold* or *warm* restart.

You can restart the system at any time without losing configuration settings, except if you do a factory reset. For most restarts, a warm restart is sufficient. A cold restart will run both the BOOT ROM code and the run time code whereas a warm restart will run only the run time code. A cold restart is needed when you perform a BootP request or code download.

System Download

Selecting this option displays the System Download panel shown in Figure 5-30.



System Download

☐ Bootp Request

File Download Request: TFTP Server IP Address: 0.0.0.0

☐ Boot ROM Code Download

File Name:

☐ Configuration File Download

File Name:

☐ Web-Pages Database Information Download

File Name:

☐ System Software Download

File Name:

Switch Port ID for Communication with TFTP Server: 1

Update   Cancel

Figure 5-30. System Download

This panel lets you perform a BootP request and a TFTP code download. To request an IP address, subnet mask, and a default gateway address from your BootP server perform the following steps:

1. Select **BootP Request**

   Note: Not all DHCP servers support basic BootP services.

2. Define the **TFTP Server IP Address**.

3. Select which system files to be downloaded.

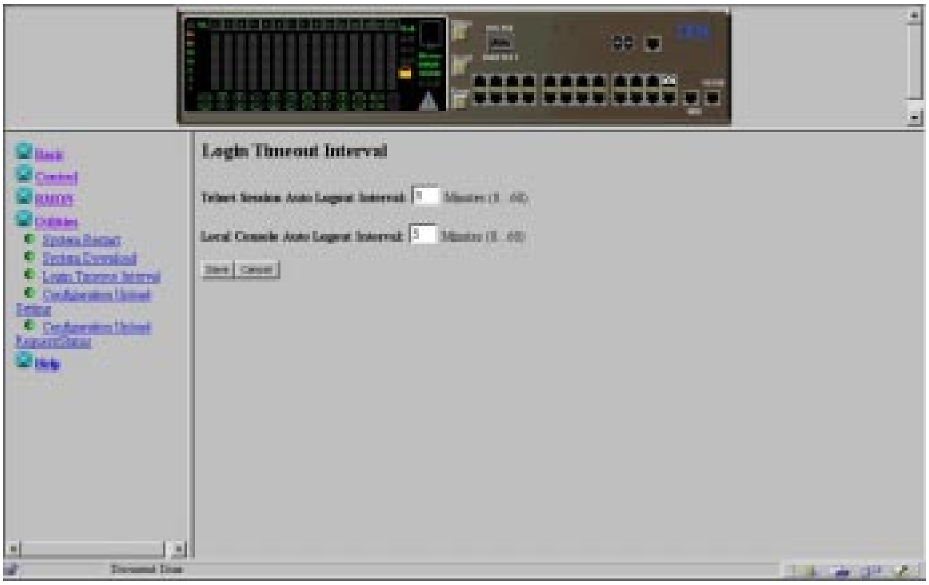
4. Select a **Switch Port ID** for communication with the TFTP Server.

5. Perform a cold restart on the system, see “System Restart” on page 5-39.

Note: Port trunking is not functional during a code load. However, a single port of an existing Trunk Group can be assigned as a switch port ID.

Login Timeout Interval

Selecting this option displays the Login Timeout Interval panel shown in Figure 5-31.



Login Timeout Interval

Telnet Session Auto Logout Interval: 5 Minutes (0 .. 60)

Local Console Auto Logout Interval: 5 Minutes (0 .. 60)

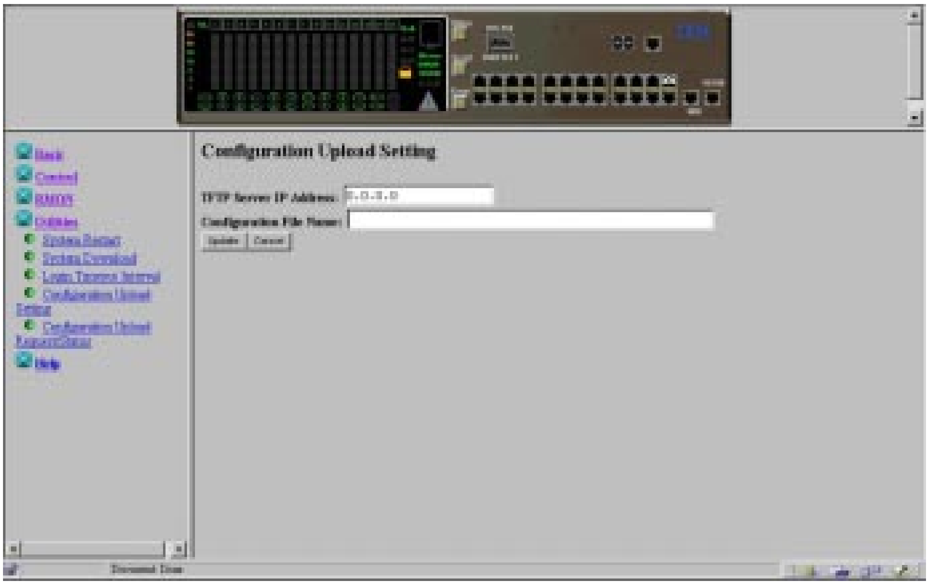
Figure 5-31. Login Timeout Interval

This panel lets your select the time after which an established Telnet session or Local Console is automatically logged out if inactive. The range is 0 to 60 minutes. The default is 5 minutes. If you specify zero, the session remains logged in regardless of how long it is inactive.

Note: Select **SAVE** to save your changes.

Configuration Upload Setting

Selecting this option displays the Configuration Upload Setting panel shown in Figure 5-32.



Configuration Upload Setting

TFTP Server IP Address: 0.0.0.0

Configuration File Name:

Figure 5-32. Configuration Upload Setting

This menu lets you upload the switch configuration data to the remote server in binary format. You can upload your configuration files and save them as a backup in case you want to restore your system settings.

Enter the TFTP server IP address and the configuration name (for example *filename*.CFG) and path information. Select **Save** to save your configuration settings, and then request an upload by using the Configuration Upload Request/Status Menu. See “Configuration Upload Request/Status” on page 5-43.

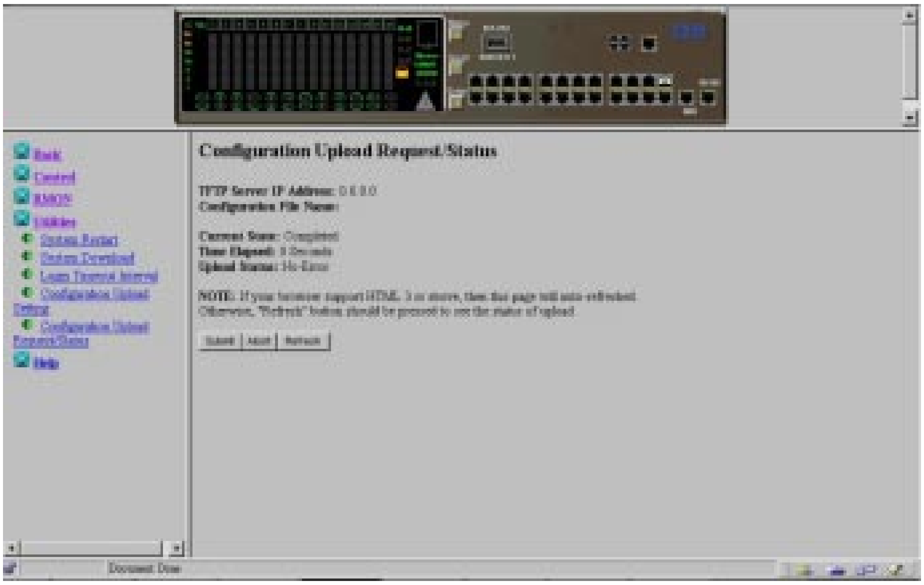
TFTP Server IP Address The IP address of the server on which the configuration files are to be stored.

Configuration File Name The name of the configuration file and the full path of the saving location on the server.

Note: Select **Update** before you exit this menu to save any changes you have made.

Configuration Upload Request/Status

Selecting this option displays the Configuration Upload Request/Status panel shown in Figure 5-33.



Configuration Upload Request/Status

TFTP Server IP Address: 0.0.0.0
Configuration File Name:

Current State: Completed
Time Elapsed: 8 Seconds
Upload Status: No-Error

NOTE: If your browser support HTML 3 or above, then this page will auto-refreshed. Otherwise, "Refresh" button should be pressed to see the status of upload.

Figure 5-33. Configuration Upload Request/Status

This menu lets you perform the configuration file upload and shows the status of uploading activity. Execute **SUBMIT** to start the TFTP upload operation.

TFTP Server IP Address The IP address of the server to which the configuration files are to be loaded.

Configuration File Name The name of the configuration file and the full path of the saving location on the server.

Current State Current status of the upload. When the upload is finished, the field says `Completed`.

Time Elapsed The elapsed time since the beginning of the upload.

Upload Status The following types of error status can be displayed:

No-Error The upload completed successfully.

No-Such-File The path specified in the Configuration File Name is Write Protected.

Disk-Full The disk specified in the Configuration File Name is full.

Timeout The TFTP upload timeout (20 seconds) has expired.

Other-Error Other errors that are defined by the system.

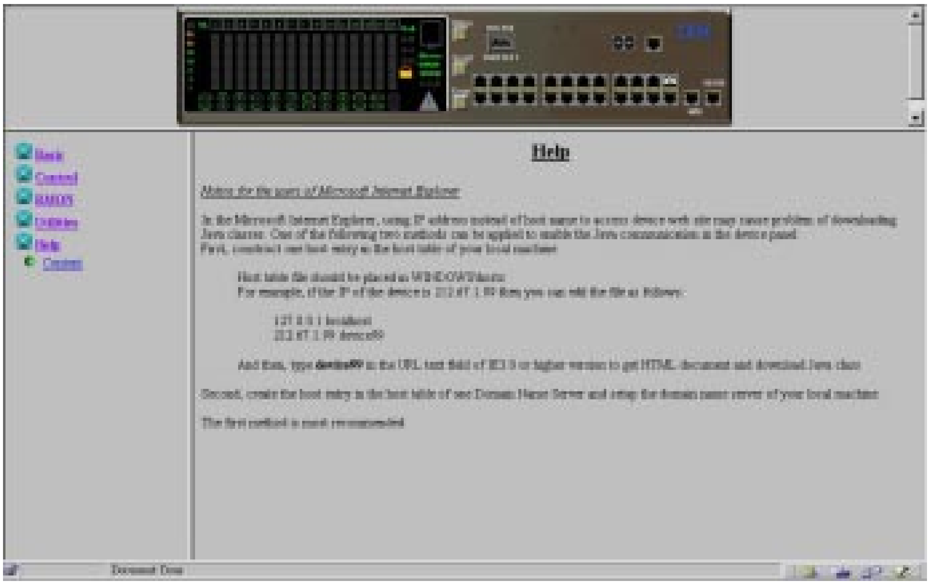
A progress bar is displayed on the menu.

After you have uploaded your configuration files, you can download them as required. For information on downloading your configuration files, see “System Download” on page 5-40.

The TFTP Server IP Address and Configuration File Name may differ from that on the Configuration Upload Setting Menu if an upload is already in progress.

Help

Selecting this option displays the Help panel shown in Figure 5-34.



Help

Notes for the users of Microsoft Internet Explorer

In the Microsoft Internet Explorer, using IP address instead of host name to access device web site may cause problem of downloading Java classes. One of the following two methods can be applied to enable the Java communication in the device panel.
First, construct one host entry in the host table of your local machine.

Host table file should be placed in WINDOWS\hosts
For example, if the IP of the device is 212.67.1.99 then you can edit the file as follows:

```
127.0.0.1 localhost
212.67.1.99 device99
```

And then, type **device99** in the URL text field of IE3.0 or higher version to get HTML document and download Java class

Second, create the host entry in the host table of one Domain Name Server and setup the domain name server of your local machine.

The first method is most recommended.

Figure 5-34. Help Panel

The Help panel provides information for Microsoft Internet Explorer users.

Chapter 6. Troubleshooting and Service

This chapter contains procedures that help you troubleshoot problems with an Ethernet Workgroup Switch and its connections to other devices.

Be sure to read “Safety Information” on page xi before proceeding.

Diagnosing Problems

The following sections contain lists of symptoms and actions to assist in problem resolution prior to contacting IBM Support.

Power-On Self-Test Failures

When the Ethernet Workgroup Switch is powered on or if a cold restart is initiated, it performs a power-on self-test (POST). If you are connected to the EIA 232 port and have your VT100-compatible terminal running, the following scrolling text appears on your monitor depending on whether the test fails or completes successfully:

```
BOOT ROM Integrity Test     ........ OK
BOOT ROM Integrity Test     ........ FAILED
      Expected checksum = 0x12345678
      Error checksum    = 0xFFFFFFFF
DRAM Test (04096 Kbytes)    ........ OK
DRAM Test (00000 Kbytes)    ........ FAILED
      Failed location = 0x80000000
      Test pattern    = 0x80001234
      Error pattern   = 0xFFFFFFFF
Secondary BOOT LOADER Detect    .. OK
Secondary BOOT LOADER Detect    .. NOT FOUND
```

if (Secondary BOOT LOADER Detect = NOT FOUND)

```
Extracting botrom code     .. OK
Extracting bootrom code    .. FAILED
```

if (Secondary BOOT LOADER Detect = OK)

```
Extracting second bootrom code    OK
Extracting second bootrom code     FAILED
NMU -- Switch Communication Channel Test   ........ OK
NMU -- Switch Communication Channel Test   ........ FAILED
Flash Memory (2048 Kbytes) Installed   ........ OK
Flash Memory Device Type    ........ UNKNOWN
Run Time Image Integrity Test    ........ OK
Run Time Image Integrity Test    ........ FAILED
-- Please reload run time image
Web-Pages Integrity Test     ........ OK
Web-Pages Integrity Test     ........ FAILED
-- Please reload Web-Pages
EEPROM Read/Write Test    .. OK
EEPROM Read/Write Test    .. FAILED
NIC Controller Access Test    ........ OK
NIC Controller Access Test    ........ FAILED
MAC Address = 00 60 94 bf 12 34
```

```
Switch Controller Access Test     ........ OK
Switch Controller Access Test     ........ FAILED
```

If any of the POST fails, disconnect and reconnect the power to retry the POST.

RunTime Integrity Test Failures: If the runtime integrity test fails, you might have a problem that could be corrected by reloading the system software. For information on reloading your system software, see “Boot ROM Console.”.

Web Pages Integrity Test Failures: If the Web pages integrity test fails, you might have a problem that could be corrected by reloading the Web Pages Database information. For information on reloading your Web Pages Database information, see “Boot ROM Console.”

If any other test fails, contact IBM Support.

Boot ROM Console

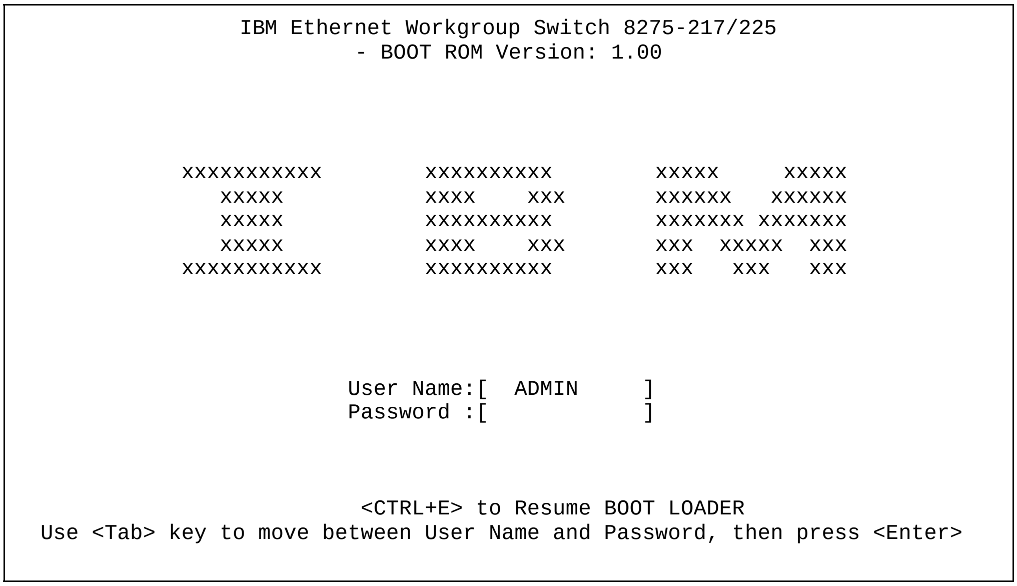
Connect your VT100-compatible terminal emulator to the EIA 232 management port to see the POST’s text messages. When the POST completes, the following message is displayed:

```
>>> Please select abort command to enter console menu
```

Notes:

1. If you do not select the abort command within 12 seconds, the Ethernet Workgroup Switch is automatically reset.
2. The boot ROM menu is a subset of the functions available on the main menu of the management interface described in Chapter 4, “Using the Management Interface.”

Selecting the abort command displays the boot ROM login panel shown in Figure 6-1.

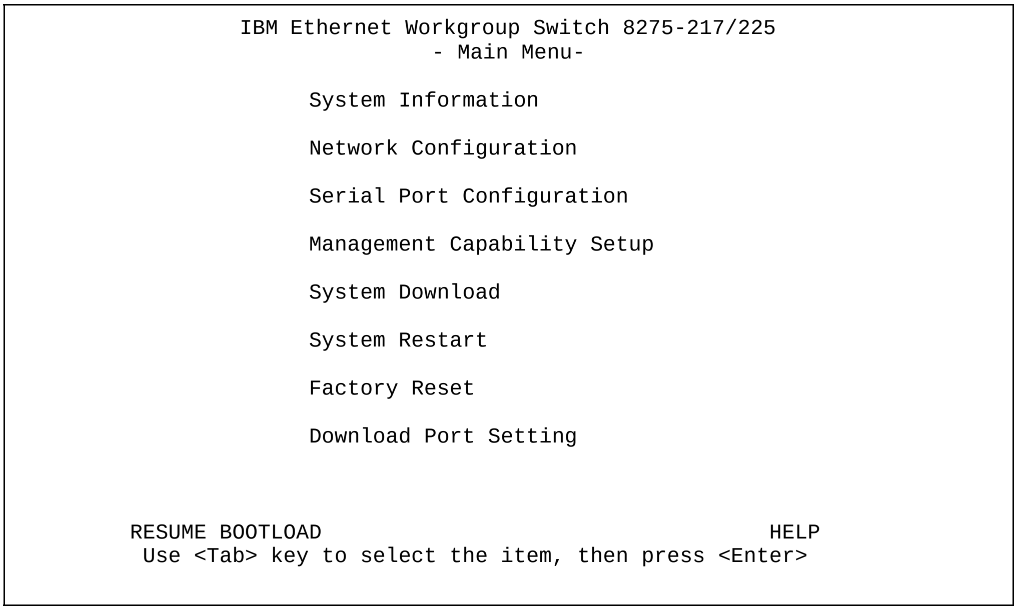


```
                IBM Ethernet Workgroup Switch 8275-217/225
                         - BOOT ROM Version: 1.00




           xxxxxxxxxxx        xxxxxxxxxx        xxxxx     xxxxx
              xxxxx           xxxx    xxx       xxxxxx   xxxxxx
              xxxxx           xxxxxxxxxx        xxxxxxx xxxxxxx
              xxxxx           xxxx    xxx       xxx  xxxxx  xxx
           xxxxxxxxxxx        xxxxxxxxxx        xxx   xxx   xxx




                        User Name:[  ADMIN     ]
                        Password :[            ]



                         <CTRL+E> to Resume BOOT LOADER
Use <Tab> key to move between User Name and Password, then press <Enter>
```

Figure 6-1.   Boot ROM Login Panel

You can log in using a previously defined user name and password, or you can use one of the two default user names. One default user name, ADMIN, requires no password. The other default user name, GUEST, has a password of GUEST. (Note that the user IDs and passwords are not case sensitive.)

After you have logged in, the boot ROM console main menu, shown in Figure 6-2, is presented.



```
                  IBM Ethernet Workgroup Switch 8275-217/225
                                - Main Menu-

                        System Information

                        Network Configuration

                        Serial Port Configuration

                        Management Capability Setup

                        System Download

                        System Restart

                        Factory Reset

                        Download Port Setting



          RESUME BOOTLOAD                                   HELP
           Use <Tab> key to select the item, then press <Enter>
```

Figure 6-2. Boot ROM Main Menu

You can select **System Download** to reload the code on your Ethernet Workgroup Switch. See “System Download” on page 4-43 more information on downloading code. To exit the main menu, select **RESUME BOOTLOAD** to continue booting the Ethernet Workgroup Switch.

LEDs

Symptom	Action
Power LED does not light.	• Check the power cable to ensure that it is firmly connected to both the Ethernet Workgroup Switch and the power outlet. • Ensure that there is power at the power outlet.
OK LED is Off or fault LED is On	The Ethernet Workgroup Switch is malfunctioning. Re-power or cold restart the switch. If the Ethernet Workgroup Switch still fails, contact IBM Support.

Control Panel

Symptom	Action
Caution Icon Indicator On	• Check the control panel message zone for errors or failures such as a broadcast storm or a cooling fan failure. • If you have an SNMP manager, check your trap log for messages. • Re-power or cold restart the switch to see if the POST identifies a failure. • Reset the indicator by pressing one of the control keys. If the message reappears, contact IBM Support.
Port indicator frame on	• The port has been disabled by the administrator. • The operating status of this port is set to "No". • STP has found a network loop and has partitioned the port.
Port number frame blinking	The port has been partitioned due to a broadcast storm. The message zone displays BRDCST STORM and the caution icon is lit. Locate the source of the broadcast storm and correct.
Port number indicator on, port number frame off, port is available, but link is still down.	• All connections are secure. • .The devices at both ends of the cable are powered-on. • The cable is good. • The correct type of cable (either crossover or straight through) is used. If connected device is MDI-X only, ensure that you are using either a straight through cable with an MDI port or a crossover cable and an MDI-X port.

EIA 232 Port

Symptom	Action
Menu panels incorrectly displayed.	Check that the terminal emulator is correctly configured: 19200 bps, 8 data bits, 1 stop bit, no parity, no flow control, and VT100 emulation.
Login menu does not display.	• Check that the terminal emulator is correctly configured: 19200 bps, 8 data bits, 1 stop bit, no parity, no flow control, and VT100 emulation. • Perform the command line "wake up" procedure by pressing **Enter** two or three times or press **Ctrl+R** to refresh the panel. • Verify that you are using a null-modem cable or a serial cable with a null-modem adapter.

Telnet Session

Symptom	Action
Telnet workstation cannot access the Ethernet Workgroup Switch.	• Check that the Ethernet Workgroup Switch’s IP address, subnet mask, and default gateway are correctly configured. • Ensure that you entered the IP address or host name of the Ethernet Workgroup Switch correctly when invoking the Telnet facility. • If you have configured VLANs, check that the Telnet connection is to a port in the management VLAN.

Traffic Flow

Symptom	Action
Traffic does not flow over a linked port.	• If the MAC address is assigned to a port in the Static Unicast Address Configuration Menu and connected to the correct port.

Password

Symptom	Action
Lost Control Panel Password.	Use the management interface (either by a Telnet session or by using the EIA 232 port) and reset the control panel password using the User Authentication Menu, see “User Authentication” on page 4-41.

Symptom	Action
Lost Login Panel Password (Web or Management Interface)	• Contact network administrator for a new password. • Contact another user with READ/WRITE access and have that user assign you a new password by using the User Authentication Menu. **Note:** If no user has READ/WRITE access, contact IBM support.

Performance

If a large volume of traffic lowers performance and increases the number of collisions, you can optimize Ethernet Workgroup Switch performance by:

- Setting the switch to detect broadcast storms and take action when a certain level of broadcast storms is detected (for example, allowing automatic partitioning of the port). (See “Switch Port Control/Status” on page 4-19)
- Setting up virtual LANs to group ports together into logical workgroups. (See “VLAN Configuration” on page 4-31 and “VLAN Control” on page 5-21).

Web Browser

Note: Web browsers must support Java 1.0 and Multiframe HTML. The Ethernet Workgroup Switch has been tested using Netscape Navigator Version 3.04, Netscape Communicator Version 4.03 and 4.04, and Microsoft Internet Explorer 3.02 and 4.0 in both Microsoft Windows 95 and Microsoft Windows NT 4.0.

Symptom	Action
Web browser cannot access the switch.	• Check that the Ethernet Workgroup Switch’s IP address, subnet mask, and default gateway are correctly configured. • Ensure that you enter the IP address of the switch correctly on your web browser. • If you are using Microsoft Internet Explorer, see “Help for Using Internet Explorer”.
The Java applet graphic of the switch does not appear.	Clear the memory cache and the disk cache of your Web browser. For example, in Netscape 4.03: • Select **Edit/Preferences/Advanced/Cache** • Then select **Clear Memory Cache** and **Clear Disk Cache**.

Help for Using Internet Explorer

In the Microsoft Internet Explorer, using an IP address instead of a host name can cause problems related to Java classes. You can use either of the following methods to enable the Java communication in the switch panel.

Method One:

1. Construct a host entry in the host table of your local machine.

   - Place the host table file in WINDOWS\hosts. For example, if the IP address of the switch is 212.67.1.99 and you choose a unique host name, "device99", then you can edit the file as follows:
     - 127.0.0.1 localhost
     - 212.67.1.99 device99

2. Type **device99** in the URL text field of IE 3.0 or IE 4.0 to get the HTML document and download the Java class.

Method Two: Create the host entry in the host table of one Domain Name Server and set up the domain name server of your local machine.

Note: Method One is the recommended method.

Obtaining Software

You can obtain the latest level of code, MIBs, tips, and publications about the Ethernet Workgroup Switch through the Internet.

- WWW Site

  1. Access the IBM Networking Technical Support:

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

  2 Select **8275** from the Product Number menu.

     You can access product announcements, publications, technical tips, and code downloads. You can also subscribe to receive e-mail notifications of code updates, tips, and FAQs for the Ethernet Workgroup Switch.

  3 Locate and download the file 8275B*xxx*.EXE. This file includes Boot ROM, Web Pages Database information, system software code, and readme file.

     Note: In this file name, *xxx* is the version number.

Obtaining Service

If you need assistance in troubleshooting or if you need service for your Ethernet Workgroup Switch, call IBM at **1-800-772-2227** in the United States and **1-800-426-7378 (1-800-IBM-SERV)** in Canada. See “Warranty” on page B-7 for information concerning service for the product.

Appendix A. Introduction to Virtual LANs (VLANs) and Spanning Tree Protocol (STP)

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 on 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.

How VLANs Provide Extra Security

Devices within each VLAN can communicate only with devices in the same VLAN. If a device in VLAN 1 needs to communicate with devices in VLAN 2, the traffic must cross a router.

Figure A-1 shows a network configured with three VLANs — one for each of the departments that access the network.

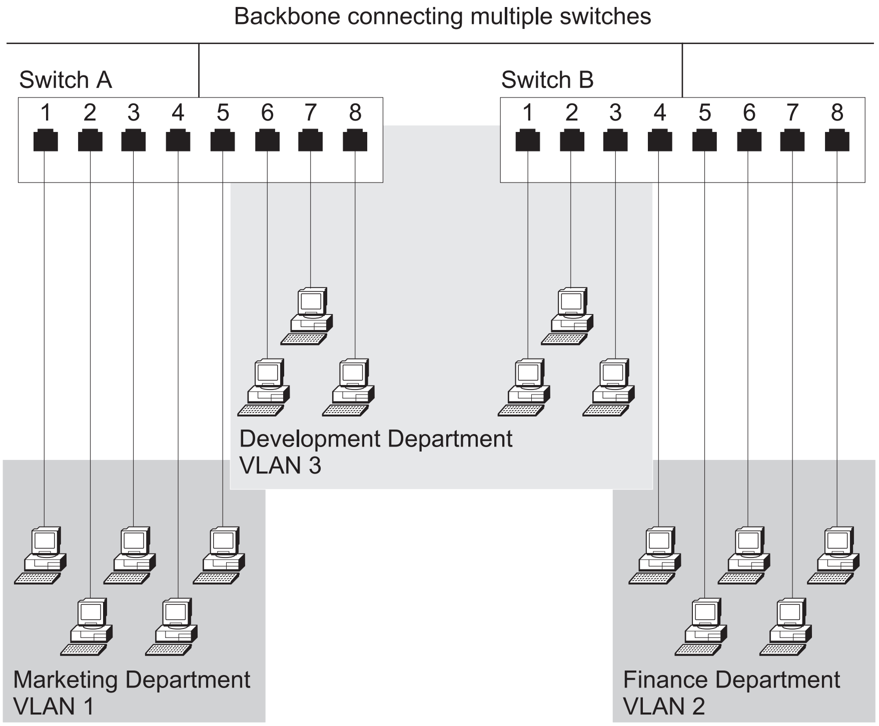


Figure A-1. An Example of VLANs

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 multi-vendor network. This provides the services of traditional port based VLANs, but also allow true interoperability with other devices that support the 802.1q standard. In addition, the switch supports GVRP, a protocol that will automate the registration of VLANs across networks that support this protocol.

The switch will support a maximum of 31 user configured VLANs, and a port may belong to multiple VLANs. This is useful if you wish to segment your network by functional area, and need some users to access multiple functional areas.

Overview of IEEE 820.1q VLAN Support

The switch supports IEEE 802.1q standards based VLANs. The 802.1q standard provides port based VLANs as well as propagation of VLAN membership across compliant devices (GVRP). This VLAN information is passed among devices by the addition of a 4 byte VLAN tag onto each frame. This tag contains information concerning what VLAN 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. 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 will be discussed below, followed by some configuration examples.

Default VLAN ID (PVID)

The Default VLAN ID, or PVID, specifies a default VLAN for all untagged devices attached to the port. Only one Default VLAN is supported per port. This setting is used to determine what VLAN that untagged frames belong to as they enter the switch. In addition, it serves to determine if the frame should have the tag removed before sending it out of the switch. The specific use of this value will be discussed in the sections below.

Port Connection Types

There are two port connection types on the switch, *Access* and *Hybrid*. Frames may enter and exit the switch on either type of port.

An *Access* port is intended to connect to a network with untagged devices only. When a frame arrives at an access port, it becomes a member of the VLAN that is set by the Default VLAN ID (or PVID). As the frame enters the switch, it is tagged with a VLAN Tag with a value equal to the PVID of the port. This frame is then sent to other ports in the switch that belong to this VLAN.

When a frame leaves an Access port, the tag on the frame compared against the Default VLAN ID (PVID) for the port. If the PVID does not match the tag of the frame, the frame is dropped and not sent out of the switch. Otherwise the tag is removed and the frame is sent onto the network untagged.

It is important to note that while Access ports are intended to be connected to a network that contains untagged frames only, the switch will not prohibit tagged frames from being received on this port type. If a tagged frame is received on an Access port, a new tag will be inserted on the frame with the VLAN ID equal to the PVID of the port. This new tag is inserted in front of the existing tag, and the new tag will be used to guide the frame to the destination port(s) in the switch. If a frame with multiple tags exits the switch through an Access port, only the last tag added (tag at the front of the frame) is removed.

Hybrid ports can receive and send tagged or untagged frames. If an untagged frame is received at a Hybrid port, it follows the same rules as an untagged frame received at an Access port. The untagged frame will have a tag inserted with a value equal to the PVID of the port and the frame will be switched to the set of ports that belong to this VLAN.

If a tagged frame arrives at the port, a new tag is not inserted onto the frame. This frame is only received by the switch is the port belongs to a VLAN that matches the VLAN tag of the incoming frame. If the port is not a member of the frame's VLAN, the frame is dropped.

As a frame exits a Hybrid port, a check is performed to determine if the frame's tag matches the PVID of the port. If the frame's tag matches the PVID, the tag is stripped from the frame and the frame is sent untagged. Otherwise, the frame is sent onto the network tagged.

By understanding the flow of frames in and out of the two port types, it can be determined how to interconnect the 8275 to other devices in the network. To summarize the flow of frames, and if the frames are tagged the following diagrams are provided.

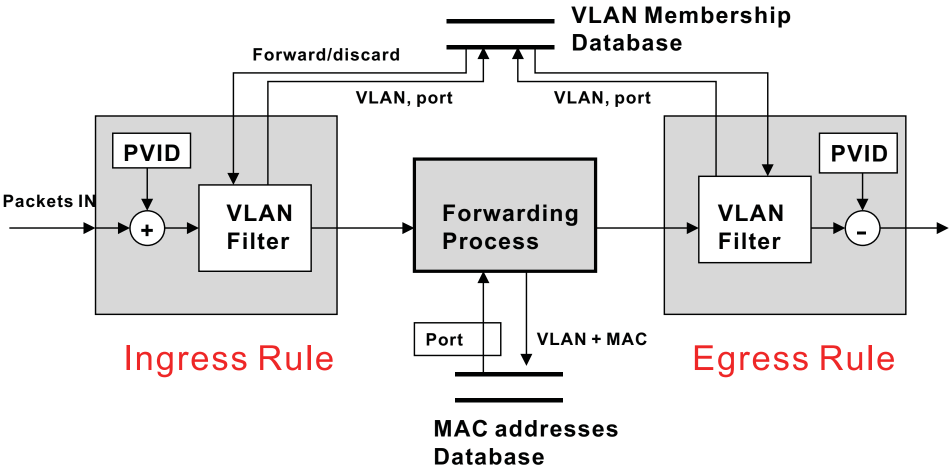


Figure A-2. Overall Flow of Packets Through the Switch

The diagram in Figure A-2 shows the overall flow of packets through the switch. Decisions on how to process the frames as they move through the switch are based on the port settings, VLAN configurations, and the learned address table of the switch. As frames are received at a port, the Ingress Rule is applied to determine how the frame is handled. This Ingress Rule can be seen in *Figure A-3*

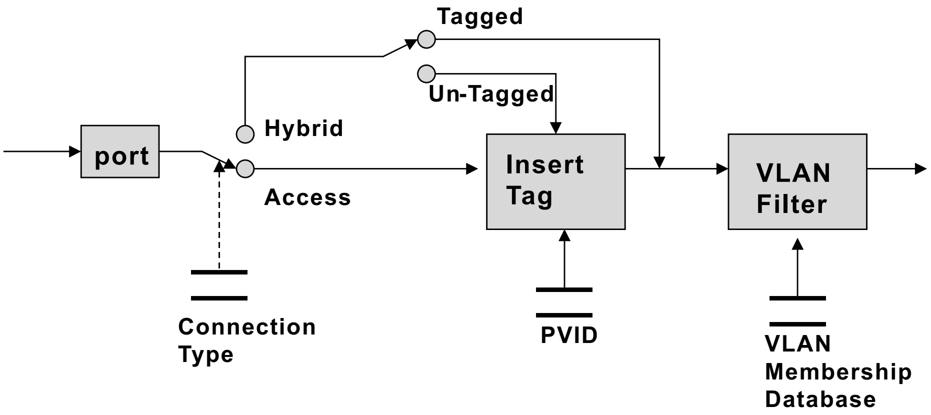


Figure A-3. Switch Ingress Rule

As the frame arrives at the port, it is handled differently depending if the port is an access or hybrid port. If the port is an access port, a tag is inserted onto the frame with the VLAN ID equal to the PVID of the port. This tag is then compared to determine if the port belongs to the VLAN (in order for a PVID to be set on a port, the port must belong to the VLAN). The frame is then sent on to the forwarding process that determines what ports to send the frame to for transmit.

If the port is configured as a hybrid port, the frame is checked to see if it is tagged. If the frame is not tagged, it is handled as if the port were an access port. Otherwise, the tag of the frame is checked to determine if the port belongs to the VLAN. If the port does not belong to the VLAN that the frame is assigned to, the frame is dropped.

The forwarding process determines what ports the incoming frame is to be sent to. If the destination address of the frame is unknown, the frame will be sent to all ports that below to the VLAN of the frame. If the destination address of the frame is know, then the frame is sent directly to the outbound port where the destination device exist.

As the frame arrives at the port(s) to be transmitted, the egress rule is applied to determine how to handle the frame. This rule is shown in *Figure A-4 on page A-6*

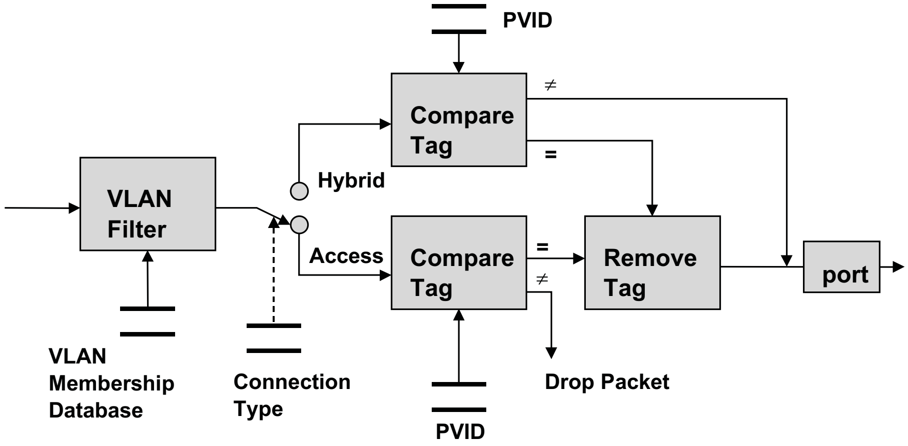


Figure A-4. Switch Egress Rule

The VLAN filter shown in Figure A-4 above will determine if the frame arrives at the given port to be transmitted. Since the frame may be going out onto a network that does not support tagged devices, a check must be made to determine if the tag must be removed from the frame. If the port is an Access port, a check is first made to see if the tag on the frame matches the port's PVID. If the frame's tag does not match the PVID, the frame is dropped. This frame is dropped because an access link can belong to only one VLAN as it consist of untagged devices. If the VLAN tag matches the PVID, then the tag is removed and set onto the network.

If the port is set to hybrid, a comparison is also made of the frame's tag to the port's PVID. If the frame's tag matches the port's PVID, then the tag is removed and the frame is sent onto the network. Once again, the PVID is essentially the "untagged" VLAN and thus any frames that belong to this VLAN must be untagged.

If the frame's tag does not match the port's PVID, then the frame is sent with the tag intact.

Automatic VLAN Registration (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 GVRP that is defined as a part of the IEEE 802.1q standard. GVRP registration messages are sent across the network and received by GVRP enabled devices (switches, adapters, etc). 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, the network administrator would not have to manually reconfigure the switch ports to add the new switch port to the VLAN(s) that the user belongs to. GVRP messages are sent across the network as BPDUs and a new BPDU type has been defined for these messages. Older network analyzers will detect these GVRP registration messages as "Invalid BPDU Types." The switch allows the administrator to disable this function on a switch basis or on an individual port basis.

Static vs. Dynamic VLANs

There are two VLAN types, *Static* and *Dynamic* that are associated the 8275. Static VLANs are manually configured on the administrator on the switch. Dynamic VLANs are created on the switch as a result of GVRP registration messages. Likewise, a Dynamic VLAN can be automatically removed from the switch if it is no longer being used by other devices in the network. An administrator can modify the port settings of a Dynamic VLAN. Once this is done, the VLAN becomes a static VLAN, and will remain configured on the switch until removed by the administrator.

In order to support devices that do not participate in GVRP registration to inter-operate with the switch, the administrator has the ability to configure if a port participates in GVRP registration. For each VLAN that is registered on the switch, the administrator may set the port mode in relation to GVRP registration. There are three port modes, *Fixed*, *Normal*, and *Forbidden*.

When a Port is placed into the fixed mode, the port is always a member of the specified VLAN. This is similar to Port based VLANs from previous products. The primary exception is that VLAN membership of fixed ports will propagate across the network. Ports must be placed in fixed mode if they are connected to devices that do not support GVRP. This must be done for each VLAN that exists on the segment connected to the port.

A port that is in normal mode does not currently belong to the given VLAN. However, the port may join the VLAN if a GVRP registration message is received. Ports may be left in Normal 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 forbidden is prevented from being a part of the specified VLAN. This would be used if an administrator wishes that certain ports never join a VLAN by means of GVRP registration messages. If the administrator wishes that a given port never receive or propagate GVRP registration messages, the administrator may disable GVRP on a specific port or set of ports.

Relationship of Default VLAN ID (PVID) to VLAN Port Mode

In order for a Port's Default VLAN ID (PVID) to be set to a specific VLAN, the port must first be fixed to that VLAN. The reason for this is that by setting the Default VLAN for a port, the administrator is assigning all untagged frames received at this port to this VLAN. In order to change the Default VLAN ID on the switch, the administrator must first define the VLAN and Fix the desired port to the VLAN. At this point, the Default VLAN ID may be changed to the new value.

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

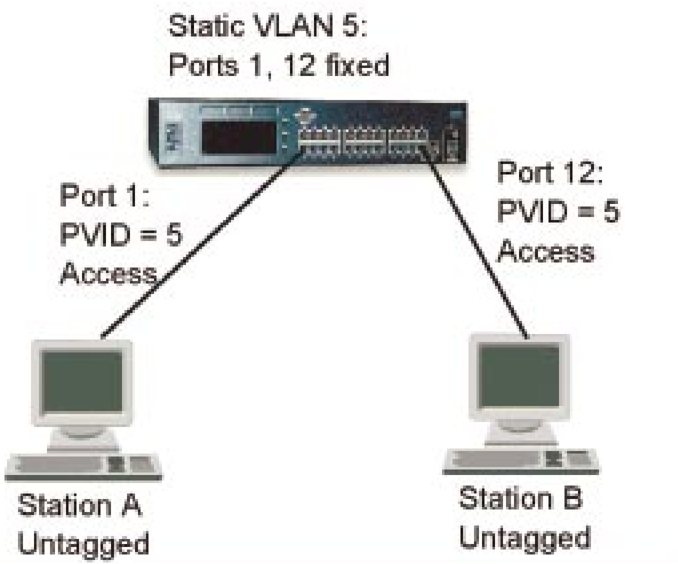


Figure A-5. Untagged Device to Untagged Device Configuration

This configuration consists to 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 Default VLAN ID (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 port's PVID, a static VLAN must first be created and these ports Fixed to this VLAN.

After this configuration is complete, the frames from Station A will arrive a Port 1 untagged, and then be tagged internally to the switch with the PVID (VLAN 5). These frames will be sent to the port 12 that is a member of the same VLAN, and since the PVID of this port is set to the same value, the tag will be removed and the frame sent to Device B untagged.

Since these devices are untagged, it is recommended that the ports be configured as Access ports. However, careful examination of the Ingress and Egress Rules will show that the ports can be set to either Access or Hybrid. The default configuration of the switch is for all ports to be set to Hybrid.

802.1q Compliant Device (Tagging and GVRP) to 802.1q Compliant Device (Tagging and GVRP)

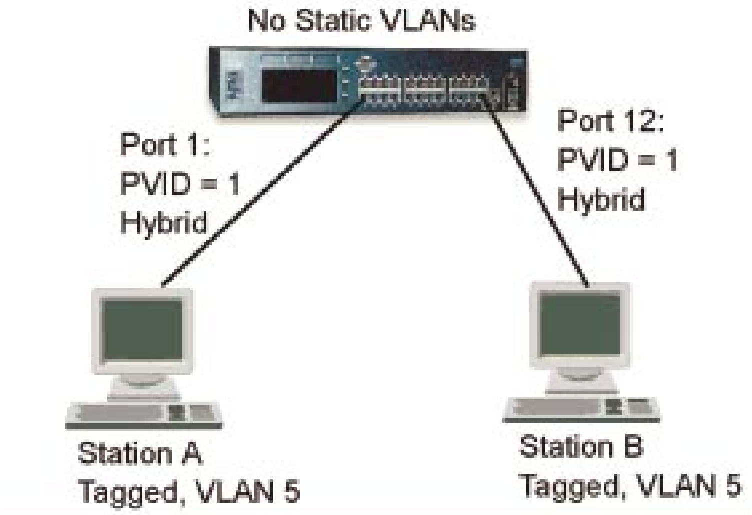


Figure A-6. 802.1q Compliant Device (Tagging and GVRP) to 802.1q Compliant Device (Tagging and GVRP) Configuration

In this configuration, both devices support tagging and GVRP. Therefore, no configuration other than the Factory Defaults needs to be done on the switch. The default configuration for the 8275 is for all ports to be in Hybrid mode, PVID set to 1 and GVRP enabled.

When Station A attempts to communicate with Station B, VLAN 5 that Station A is a member of will be automatically registered at Port 1 via GVRP. Likewise, Station B will automatically register its membership with VLAN 5 on Port 12. Note, that this VLAN will be Dynamic since the administrator has not explicitly configured the VLAN on the switch. Frames will arrive at Port 1 from Device A, tagged for VLAN 5. These frames will be sent to Port 12, and since Port 12's PVID is set to 1, the frame will keep its tag and be sent on to Station B.

In this configuration, it is important that the ports be configured as Hybrid so that they will correctly accept and pass tagged frames. In addition, it is important that the devices belong to a VLAN that is not the Default VLAN. If the devices were members of the Default VLAN, then the frames would be correctly received, however, on transmit from the switch, the tags would be stripped and they would be sent without a tag onto the network. Depending on the implementation of the "downstream" device, or other devices in the network, communication may be prevented.

Untagged Device to 802.1q Compliant Device (Tagging and GVRP)

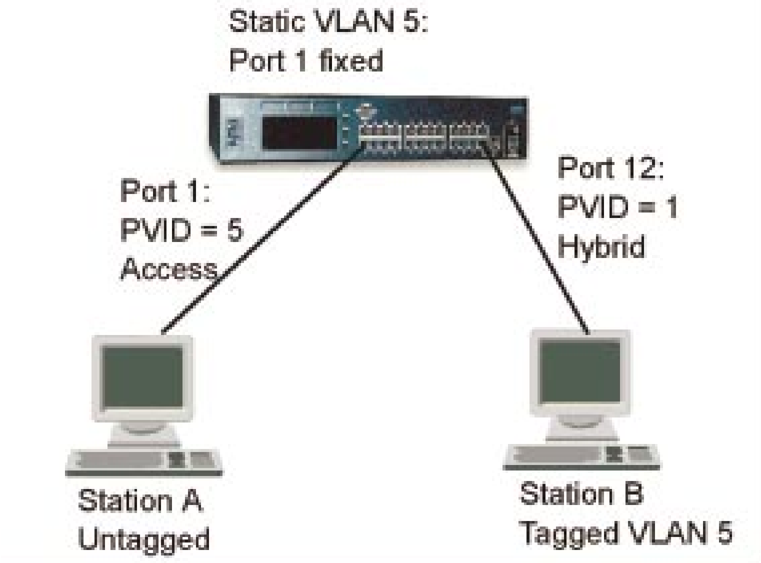


Figure A-7. Untagged Device to 802.1q Compliant Device (Tagging and GVRP) Configuration

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 configuration needed for this example is to assign the PVID for port 1 to the VLAN that is being used. This requires the administrator to first statically create VLAN 5 on the switch and fix port 1 to this VLAN.

The Station B is also assigned to VLAN 5, and since it supports both tagging and GVRP it will automatically register its membership to VLAN 5. The PVID for this port should not be the same value as the VLAN that Station A and B are members of.

Frames from Station A will arrive at Port 1 and be tagged with a VLAN ID equal to the PVID of Port 1 (VLAN 5). The frames will then be switched to Port 12, where they will be sent out of the switch with the tag still attached since the PVID of port 12 is different than the tag value of the outbound frames. On the return path, frames tagged with the 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 since the PVID of port 1 matches the VLAN of the frame, the tag will be stripped and the frame sent untagged to Station A.

Note that in this case, Port 1 does not have to be an Access port, however, if all devices on this link are untagged, it would be best to set the port to Access to ensure that the frames are correctly handled.

Untagged Device to 802.1q Compliant Device (Tagging Only)

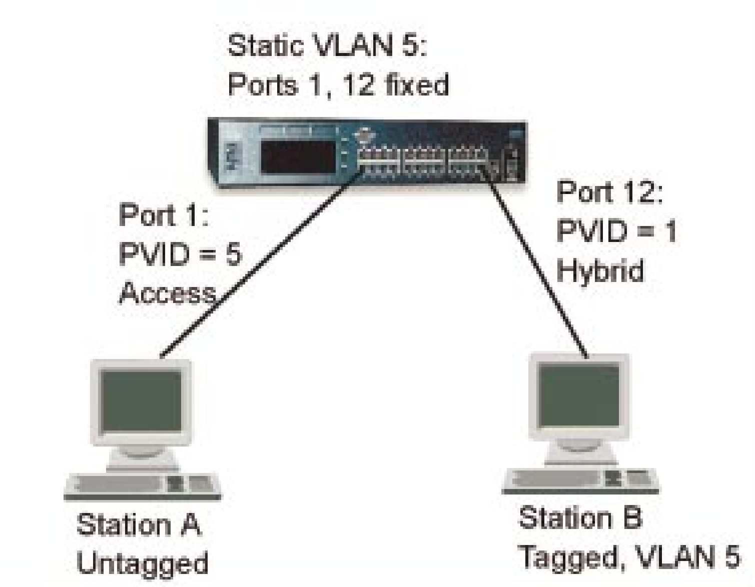


Figure A-8. Untagged Device to 802.1q Compliant Device (Tagging Only) Configuration

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 administrator must configure the VLAN membership for the port 12. Port 12, must be fixed into VLAN 5. If this is not done, Station B's frames will be dropped as they are received at the switch since 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.

Multiple VLANs, Tagged and Untagged Stations

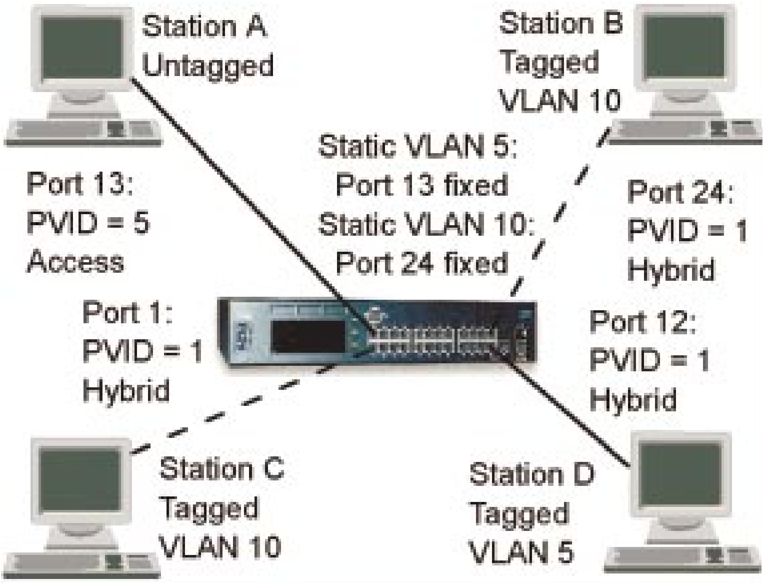


Figure A-9. Multiple VLANs, Tagged and Untagged Stations Configuration

This example combines aspects of the previous examples into a configuration where multiple VLANs are being used. In this scenario, Station A is untagged and belongs to VLAN 5. Since this is an untagged device, port 13 must be configured to have its PVID set to the VLAN that the station is a member of (VLAN 5). In addition, VLAN 5 must be statically created on the switch and have port 13 fixed into this VLAN.

Station D is to communicate with Station A and also belongs to VLAN 5. This station has an adapter that supports both tagging and GVRP. Since the adapter belongs to VLAN 5, no configuration needs to be done to the switch. GVRP will register the port on the switch as a member of VLAN 5. Once this occurs, Station A and D can communicate.

Station B has an adapter that supports tagging but not GVRP. This adapter is a member of VLAN 10. Since the adapter does not support GVRP, the switch will not automatically register the port to this VLAN. Therefore, the administrator must create VLAN 1o and fix port 24 to this VLAN.

Station C belongs to VLAN 10 and supports both tagging and GVRP. Like Station D, no configuration is required for this station. GVRP will register port 1 as a part of VLAN 10 and at this point Station B and C will be able to communicate.

Since Station A and D belong to a different VLAN than station B and C, their communication is independent of each other and secure.

Connecting VLANs to a Router

If the devices in a VLAN need to talk to devices in a different VLAN, each VLAN requires a connection to a router. Communications between VLANs can take place only if they are all connected to the router. A VLAN not connected to a router is an isolated VLAN. You need one port for each VLAN connected to the router.

Using Non-routable Protocols

If you are running non-routable protocols on your network (for example, DEC LAT, or NetBIOS), devices within one VLAN are not able to communicate with devices in a different VLAN.

Using Unique MAC Addresses

If you connect a server with multiple network adapters to the switch, you should configure each network adapter with a unique MAC address.

Spanning Tree Protocol

Using the Spanning Tree Protocol (STP) function makes your network more fault-tolerant. The following sections explain more about STP and the STP features supported by the switch.

What is STP?

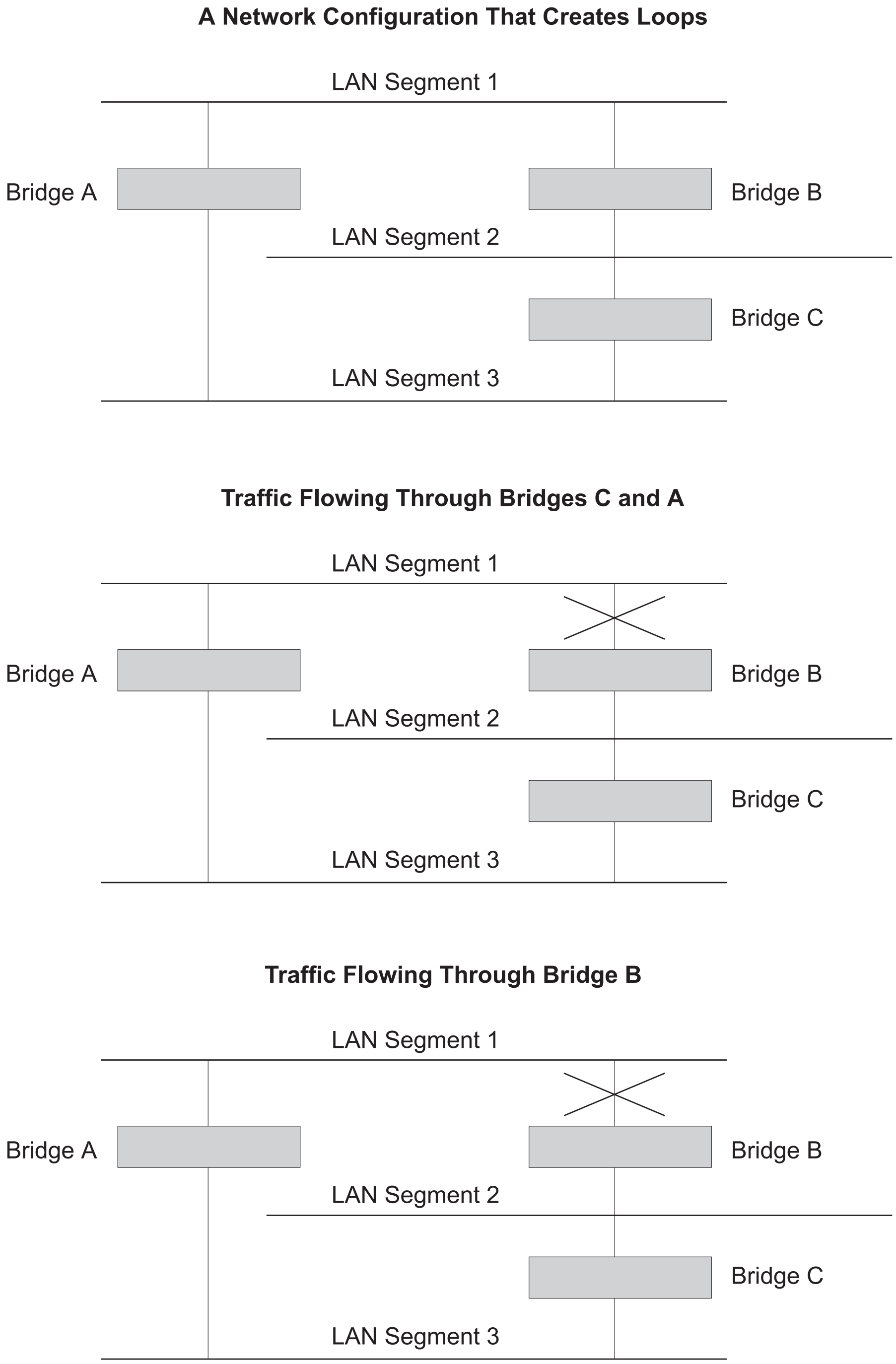
Note: STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP more effectively, the Ethernet Workgroup Switch will be shown as a bridge.

STP is a bridge-based system for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic and ensure that:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main paths fail.

For example, Figure A-10 on page A-15 shows a network containing three LAN segments separated by three bridges. With this configuration, each segment can communicate with the others using two paths. This configuration creates loops that cause the network to overload; however, STP allows you to have this configuration because it detects duplicate paths and immediately prevents, or:hp1.blocks:ehp1., one of them from forwarding traffic.

Figure A-10 on page A-15 shows the result of enabling STP on the bridges in the configuration.


A Network Configuration That Creates Loops

Traffic Flowing Through Bridges C and A

Traffic Flowing Through Bridge B

Figure A-10.Using STP to Control Traffic Flow

The STP system has decided that traffic from LAN segment 2 to LAN segment 1 can flow only through Bridges C and A.

If the link through Bridge C fails, as shown in Figure A-10, the STP system reconfigures the network so that traffic from segment 2 flows through Bridge B.

How STP Works

Initially, the STP system has the following requirements before it can configure the network:

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.

- One bridge to start as a master or root bridge, a central point from which the network is configured.

The root bridge is selected on the basis of its having the lowest bridge identifier value. This is a combination of the unique MAC address of the bridge and a priority component defined for the bridge.

The root bridge generates BPDUs on all ports at a regular interval known as the *hello time*. All other bridges in the network have a root port. This is the port nearest to the root bridge, and it is used for receiving the BPDUs initiated by the root bridge.

STP Stabilization

Once the network has stabilized, two rules apply to the network:

1. Each network segment has one designated bridge port. All traffic destined to pass in the direction of or through the root bridge flows through this port. The designated bridge port is the port that has the lowest root path cost for the segment. The root path cost consists of the path cost of the root port of the bridge, plus the path costs across all the root ports back to the root bridge.

2. After all the bridges on the network have determined the configuration of their ports, each bridge forwards traffic only between the root port and the ports that are the designated bridge ports for each network segment. All other ports are *blocked*, which means that they are prevented from forwarding traffic.

STP Reconfiguration

In the event of a network failure, such as a segment going down, the STP system reconfigures the network to cater for the changes. If the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

Figure A-11 on page A-17 illustrates part of a network.

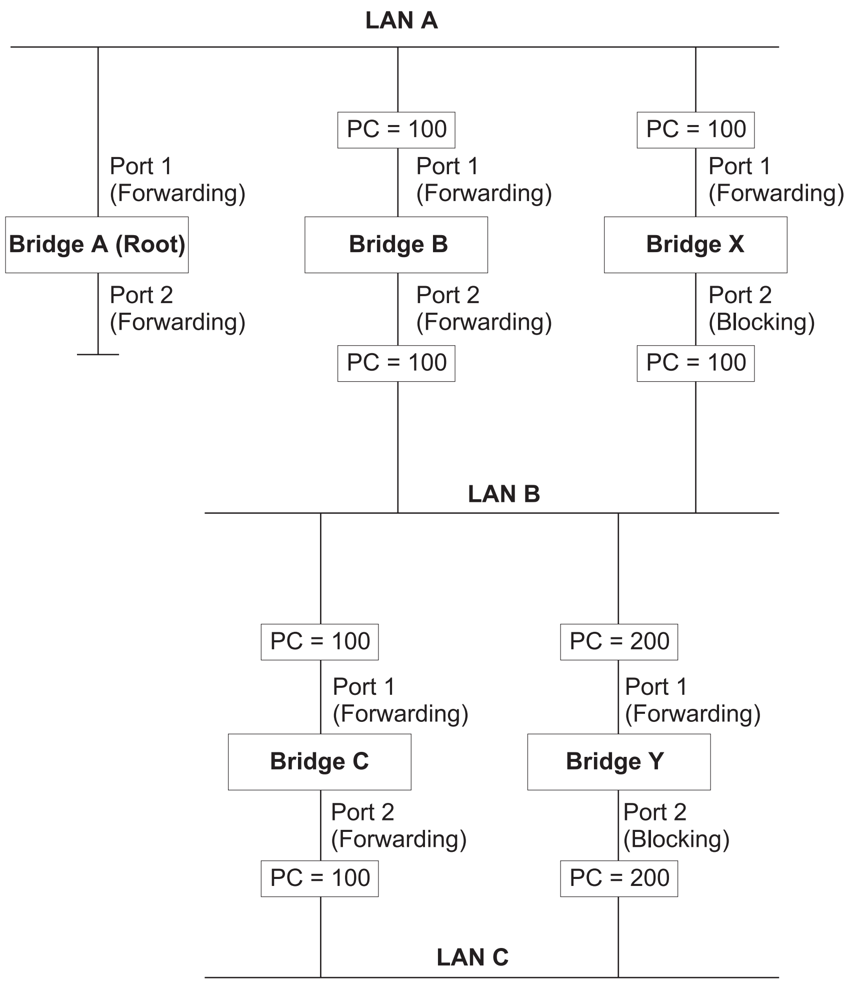


Figure A-11.Part of a Network

All bridges have a path cost value assigned to each port, identified by PC=*xxx* (where *xxx* is the value).

Bridge A is selected by STP as the root bridge, because it has the lowest bridge identifier. The designated bridge port for LAN A is port 1 on Bridge A. Each of the other four bridges has a root port (the port closest to the root bridge). Bridge X and Bridge B can offer the same path cost to LAN B. In this case Bridge B's port is chosen as the designated bridge port, because it has the lowest root path cost (the route through Bridge C and B costs 200, the route through Bridge Y and B would cost 300). You can set the path cost of a bridge port to influence the configuration of a network with a duplicate path.

Once the network topology is stable, all the bridges listen for special "Hello" BPDUs transmitted from the root bridge at regular intervals. If the STP Max Age time of a bridge expires before receiving a Hello BPDU, the bridge assumes that the root bridge, or a link between itself and the root bridge, has gone down. The bridge then initiates a reconfiguration of the network topology.

You can adjust timers to determine how quickly a network reconfigures and therefore how rapidly it recovers from a path failure.

Appendix B. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service in this publication is not intended to state or imply that only IBM’s product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM’s intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by IBM, are the user’s responsibility.

IBM may have patents or pending patent applications covering 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 the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood NY 10594 USA.

Notice to Users of Online Versions of This Book

For online versions of this book, you are authorized to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine-readable documentation.

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 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 conformite aux normes d’Industrie Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Norm (EN) Statement

This product is in conformity with the protection requirements of EC 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 for 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.

European Norm (EN) Statement for Shielded Cables

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 B Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Zulassungsbescheinigung Laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richlinie 89/336)950.

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 B.

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."

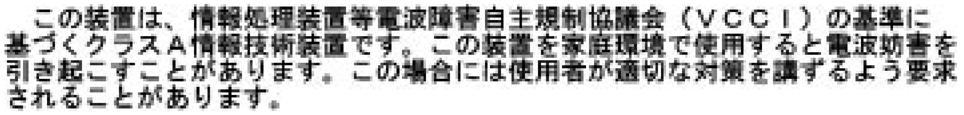
Anmerkung:

Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den IBM Handbüchern angegeben, zu installieren und zu betreiben.

Properly shielded and grounded cables and connectors must be used in order to reduce the potential for causing interference to radio and TV communications and to other electrical or electronic equipment. Such cables and connectors are available from IBM authorised dealers. IBM cannot accept responsibility for any interference caused by using other than recommended cables and connectors.

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 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.

LED Statement

Class 1 LED Statement

Class 1 LED Product

LED Klasse 1

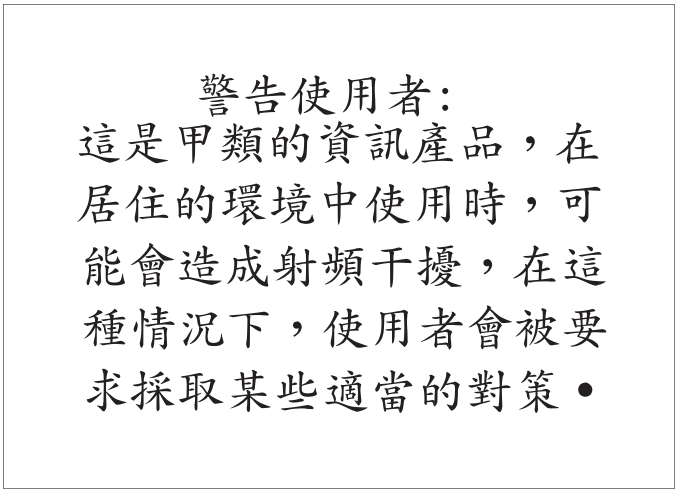
LED Klass 1

Luokan 1 Ledlaite

Appraeil À LED de Classe 1

To IEC 825-1:1993

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•

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX
IBM
Nways

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

Other company, product and service names may be trademarks or service marks of other companies.

Warranty

International Business Machines Corporation *Armonk, NY 10504*

Statement of Limited Warranty

The warranties provided by IBM in this Statement of Limited Warranty apply only to Machines you originally purchase for your use, and not for resale, from IBM or an IBM authorized reseller. The term “Machine” means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. Machines are subject to these terms only if purchased in the United States or Puerto Rico, or Canada, and located in the country of purchase. If you have any questions, contact IBM or your reseller.

Machine	Ethernet Workgroup Switch (8275) Model 217 and 225
Warranty Period*	One Year

**Elements and accessories are warranted for three months. Contact your place of purchase for warranty service information.*

Production Status

Each Machine is manufactured from new parts, or new and serviceable used parts (which perform like new parts). In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine’s production status, IBM’s warranty terms apply.

The IBM Warranty

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM’s Official Published Specifications. IBM calculates the expiration of the warranty period from the Machine’s Date of Installation. The date on your receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period, IBM or your reseller will provide warranty service under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine. IBM or your reseller will specify the type of service.

For a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Some of these transactions (called “Net-Priced” transactions) may include additional parts and associated replacement parts that are provided on an exchange basis. All removed parts become the property of IBM and must be returned to IBM.

Replacement parts assume the remaining warranty of the parts they replace.

If a Machine does not function as warranted during the warranty period, IBM in its sole discretion will repair, replace it (with a Machine that is at least functionally equivalent), or refund the purchase price. To obtain coverage under the warranty you may be required to present proof of purchase.

This warranty is non-transferable by the end-user customer.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States call **1-800-772-2227**. In Canada, call **1-800-IBM-SERV (1-800-426-7378)**. You may be required to present proof of purchase.

Depending on the Machine, the service may be 1) a “Repair” service at your location (called “On-site”) or at one of IBM’s or a reseller’s service locations (called “Carry-in”) or 2) an “Exchange” service, either On-site or Carry-in.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced.

It is your responsibility to:

1 obtain authorization from the owner (for example, your lessor) to have IBM or your reseller service a Machine that you do not own;

2 where applicable, before service is provided —

a follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,

b secure all programs, data, and funds contained in a Machine,

c inform IBM or your reseller of changes in a Machine’s location, and

d for a Machine with exchange service, remove all features, parts, options, alterations, and attachments not under warranty service. Also, the Machine must be free of any legal obligations or restrictions that prevent its exchange; and

3 be responsible for loss of, or damage to, a Machine in transit when you are responsible for the transportation charges.

Extent of Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

Misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible may void the warranties.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HOWEVER, SOME LAWS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES. IF THESE LAWS APPLY, THEN ALL EXPRESS AND IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

In Canada, warranties include both warranties and conditions.

Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.

Limitation of Liability

Circumstances may arise where, because of a default on IBM' part (including fundamental breach) or other liability (including negligence and misrepresentation), you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages, IBM is liable only for:

1. bodily injury (including death), and damage to real property and tangible personal property; and

2. the amount of any other actual loss or damage, up to the greater of $100,000 or the charge for the Machine that is the subject of the claim.

Under no circumstances is IBM liable for any of the following:

1. third-party claims against you for losses or damages (other than those under the first item listed above);

2. loss of, or damage to, your records or data; or

3. economic consequential damages (including lost profits or savings) or incidental damages, even if IBM is informed of their possibility.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

This warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

Index

Tell Us What You Think?

IBM Ethernet Workgroup Switch 8275-217/225
Installation and Planning Guide
Part Number 30L7656

We hope you find this publication useful, readable, and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form. If you are in the U.S.A., you can mail this form postage free or fax it to us at 1-800-253-3520. Elsewhere, your local IBM branch office or representative will forward your comments or you may mail them directly to us.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	□	□

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	□	□
Complete	□	□
Easy to find	□	□
Easy to understand	□	□
Well organized	□	□
Applicable to your task	□	□

Specific Comments or problems

____

____

____

Please tell us how we can improve this book:

____

____

____

Thanks you for your comments. If you would like a reply, provide the necessary information below.

____________________ ____________________

Name Address

____________________ ____________________

Company or Organization

____________________ ____________________

Phone Number

Tell Us What You Think!
30L7656

Cut or Fo
Along Lin

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAILPERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Design & Information Development
Dept. CGF/Bldg. 656
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape Please do not staple Fold and Tape

30L7656

Cut or Folc
Along Line

IBM®

Part Number: 30L7656
Printed in Taiwan