

8271 Nways Ethernet LAN
Switch Model 524



User's Guide

OPTIONS
by IBM



Before using this information and the product it supports, be sure to read the general information under Appendix A, "Safety Information" and Appendix G, "Notices, Trademarks, and Warranties".

First Edition (October 1997)

This edition applies to the IBM 8271 Nways Ethernet LAN Switch Model 524 with agent software version 3.1.

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

If you have any comments on this publication, please address them to:

Department CGF
Design & Information Development
IBM Corporation
PO Box 12195
RESEARCH TRIANGLE PARK NC 27709
U.S.A.

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

© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION
1997. ALL RIGHTS RESERVED.

Note to US Government Users — Documentation released to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corporation.

CONTENTS

ABOUT THIS GUIDE

- Introduction 1
- How to Use This Guide 1
- Conventions 2
- Related Documentation 2

1 GETTING STARTED

- About the 8271 Model 524 Switch 1-1
 - Summary of Features 1-1
 - Port Connections 1-2
 - 10BASE-T Ports 1-2
 - 100BASE-TX Port 1-2
 - Plug-in Module 1-2
 - Transceiver Module 1-2
 - Backbone Port 1-2
 - Switch Operation and Features 1-3
 - How Does the Switch Compare to a Bridge? 1-3
 - Forwarding of Packets 1-3
 - Intelligent Flow Management 1-4
 - Full Duplex 1-4
 - Security 1-5
 - Resilient Links 1-5
 - Virtual LANs 1-5
 - Spanning Tree Protocol 1-6
 - PACE 1-6
- Network Configuration Example 1-7

- Unit Overview — Front 1-8
 - Unit Serial Number 1-9
 - 10BASE-T Ports 1-9
 - 100BASE-TX Port 1-9
 - LEDs 1-9
- Unit Overview — Rear 1-10
 - Power Socket 1-11
 - Redundant Power System Socket 1-11
 - Reset Button 1-11
 - Console Port 1-11
 - Plug-in Module Slot 1-11
 - Transceiver Module Slot 1-11
 - Ethernet Address 1-11
- Unit Defaults 1-12
- Managing the Switch 1-12
- Quick Start For SNMP Users 1-13
 - Entering an IP Address for the Switch 1-13

2 INSTALLATION AND SETUP

- Following Safety Information 2-1
- Positioning the Switch 2-1
- Configuration Rules for Fast Ethernet 2-2
- Configuration Rules with Full Duplex 2-2
- Installing the Switch 2-4
 - Rack Mounting 2-4
 - Stacking the Switch and Other Units 2-4
 - Wall Mounting 2-5

- Powering-Up the Switch 2-6
- Connecting a Redundant Power System (RPS) 2-6
- Connecting Equipment to the Console Port 2-7
 - Connecting a VT100 Terminal 2-7
 - Connecting a VT100 Terminal Emulator 2-7
 - Connecting a Workstation Running SLIP 2-8

3 SETTING UP FOR MANAGEMENT

- Methods of Managing the Switch 3-1
 - Using the VT100 Management Interface 3-1
 - Using Telnet 3-2
- Managing Over The Network 3-2
 - IP Addresses 3-2
 - Obtaining a Registered IP Address 3-3
- Navigating the VT100 Screens 3-4
 - Screen Conventions 3-4
 - Keyboard Shortcuts 3-5
 - Correcting Text Entry 3-5
- Setting Up the Switch for Management 3-6
 - Logging On 3-7
 - After Logging On 3-8
 - Switch Management Setup 3-9
 - Logging Off 3-11
 - Auto Logout 3-11

4 MANAGING THE SWITCH

- Setting Up Users 4-2
- Creating a New User 4-3
- Deleting a User 4-4
- Editing User Details 4-5
- Assigning Local Security 4-6
- Choosing a Switch Management Level 4-7

- Setting Up the Switch Unit 4-9
- Setting Up the Switch Ports 4-12
- Setting Up the Switch Database (SDB) 4-16
 - The Database View 4-17
 - Searching the Switch Database 4-18
 - By MAC Address 4-18
 - By Port 4-18
 - Adding an Entry into the SDB 4-18
 - Deleting an Entry from the SDB 4-18
 - Specifying that an Entry is Permanent 4-18
- Setting Up Resilient Links 4-19
 - Configuring Resilient Links 4-20
 - Creating a Resilient Link Pair 4-21
 - Deleting a Resilient Link Pair 4-21
 - Viewing the Resilient Links Setup 4-22
- Setting Up Traps 4-24
- Setting Up the Console Port 4-25
- Resetting the Switch 4-27
- Initializing the Switch 4-28
- Upgrading Software 4-29

5 ADVANCED MANAGEMENT

- Virtual LANs (VLANs) 5-1
 - What are VLANs? 5-1
 - Benefits of VLANs 5-1
 - How VLANs Ease Change and Movement 5-2
 - How VLANs Control Broadcast Traffic 5-2
 - How VLANs Provide Extra Security 5-2
 - An Example 5-2

- VLANs and the Switch 5-3
 - The Default VLAN and Moving Ports From the Default VLAN 5-3
 - Connecting VLANs to a Router 5-3
 - Connecting Common VLANs Between Switch Units 5-3
 - Using Non-routable Protocols 5-4
 - Using Unique MAC Addresses 5-4
 - Extending VLANs into an ATM Network 5-4
- VLAN Configurations 5-4
 - Example 1 5-4
 - Example 2 5-5
 - Example 3 5-6
- Setting Up VLANs on the Switch 5-7
 - Assigning a Port to a VLAN When Using Port VLAN Mode 5-9
 - Specifying a Backbone Port 5-9
 - Specifying that a Port is a VLT Port 5-9
- Spanning Tree Protocol 5-10
 - What is STP? 5-10
 - How STP Works 5-12
 - STP Initialization 5-12
 - STP Stabilization 5-12
 - STP Reconfiguration 5-12
 - An Example 5-13
 - STP Configurations 5-14
 - Enabling STP on the Switch 5-15
 - Configuring STP on the Switch 5-16
 - Configuring the STP Parameters of VLANs 5-16
 - Configuring the STP Parameters of Ports 5-18
- RMON 5-20
 - What is RMON? 5-20
 - About the RMON Groups 5-21
 - Statistics 5-21

- History 5-21
- Alarms 5-21
- Hosts 5-21
- Hosts Top N 5-21
- Matrix 5-22
- Filter 5-22
- Capture 5-22
- Events 5-22
- Benefits of RMON 5-23
- RMON and the Switch 5-23
- RMON Features of the Switch 5-24
- About Alarm Actions 5-25
- About Default Alarm Settings 5-26
- About the Audit Log 5-26

6 STATUS MONITORING AND STATISTICS

- Summary Statistics 6-2
- Port Statistics 6-3
- Port Traffic Statistics 6-4
- Port Error Analysis 6-6
- Status Monitoring 6-8
- Fault Log 6-9
- Remote Polling 6-10

A SAFETY INFORMATION

- Safety Notices A-1
 - World Trade Safety Information A-1
- Power Cords A-4
- Important Safety Information A-6

B SCREEN ACCESS RIGHTS

C TROUBLESHOOTING

LEDs C-1
Using the VT100 Interface C-2
Using the Switch C-3

D PIN-OUTS

Null Modem Cable D-1
PC-AT Serial Cable D-1
Modem Cable D-2
RJ45 Pin Assignments D-2

E SWITCH TECHNICAL SPECIFICATIONS

F TECHNICAL SUPPORT AND SERVICE

Electronic Support F-1
 WWW F-1
 FTP F-1
 IBM Bulletin Board System F-1
Voice Support F-1

G NOTICES, TRADEMARKS, AND WARRANTIES

Trademarks G-1
Statement of Limited Warranty G-2
 Production Status G-2
 The IBM Warranty for Machines G-2
Warranty Service G-3
 Extent of Warranty G-3
 Limitation of Liability G-4

Electronic Emission Notices G-5

Federal Communications Commission (FCC) Statement
G-5

Canadian Department of Communications (DOC)
Compliance Statement G-5

Avis de conformite aux normes du ministere des
Communications du Canada G-5

European Community (CE) Mark of Conformity Statement
for Unshielded Cable G-5

European Union (EU) Statement for Shielded Cable G-7

Japanese Voluntary Control Council for Interference
(VCCI) Statement Class A for Unshielded Cables G-8

Japanese Voluntary Control Council for Interference
(VCCI) Statement Class B for Shielded Cables G-8

Korean Communications Statement G-8

Information To The User G-8

GLOSSARY

INDEX

ABOUT THIS GUIDE

About This Guide provides an overview of this guide, describes the guide conventions, tells you where to look for specific information, and lists other publications that may be useful.

Introduction



Throughout this guide, the IBM 8271Nways Ethernet Model 524 Switch is referred to as the 8271 Model 524 Switch or Switch.

This guide provides the information you need to install and configure the 8271 Model 524 Switch with version 3.1 agent software.

The guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of Local Area Networks.

If the information in the Release Notes shipped with your product differs from the information in this guide, follow the Release Notes.

How to Use This Guide

This table shows where to find specific information in this guide.

If you are looking for...	Turn to...
An overview of the Switch	Chapter 1
Information about installing the Switch into your network	Chapter 2
Information about the methods you can use to manage the Switch	Chapter 3
Information about managing the Switch	Chapter 4
Information about more advanced management features; for example VLANs, Spanning Tree, and RMON	Chapter 5
Information about monitoring the status of the Switch	Chapter 6
Safety information	Appendix A
Information about the access rights for each VT100 screen	Appendix B
Troubleshooting information	Appendix C
Information about the pin-outs relating to the Switch	Appendix D
Information about the Technical Specifications of the Switch	Appendix E
Information about the Technical Support	Appendix F
Warranty, trademark and other reference information	Appendix G





Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names appear in text in one of two ways: <ul style="list-style-type: none"> ■ Referred to by their labels, such as "the Return key" or "the Escape key" ■ Written with brackets, such as [Return] or [Esc]. <p>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example:</p> <p>Press [Ctrl]+[Alt]+[Del].</p>
Menu commands and buttons	Menu commands or button names appear in italics. Example: <p>From the <i>Help</i> menu, select <i>Contents</i>.</p>
Words in <i>italicized</i> type	Italics emphasize a point or denote new terms at the place where they are defined in the text.
Words in bold-face type	Bold text denotes key features.

Table 2 Notice Icons

Icon	Notice Type	Alerts you to...
	Information note	Important features or instructions
	ATTENTION	Risk of system damage or data loss
	CAUTION	Conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous
	DANGER	Conditions or procedures that can result in death or severe personal injury

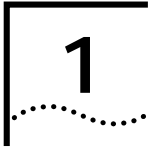
Related Documentation

The 8271 Model 524 Switch document set includes:

- *IBM 8271 Nways Ethernet LAN Switch Model 524 Quick Reference Guide.*
Part Number 02L1326
- *IBM 8271 Nways Ethernet LAN Switch Model 524 Quick Installation Guide.*
Part Number 02L1349
- *IBM 8271 Nways Ethernet LAN Switch Model 524 Release Notes.*
Part Number 02L1327

Other publications you may find useful:

- Documentation accompanying the Plug-in Modules.
- Documentation accompanying the Redundant Power System.



GETTING STARTED

About the 8271 Model 524 Switch

The 8271 Model 524 Switch is designed to dedicate a full 10Mbps of bandwidth to each user. It is simple to install and use, and it ensures sufficient performance for the increasing load on today's networks.

Use the Switch to provide your users with dedicated bandwidth and support for bandwidth demanding applications, such as video-conferencing and other real-time applications that require a very high quality of service.

Summary of Features

The Switch has the following features:

- 24 switched Ethernet 10BASE-T ports
- Fast Ethernet 100BASE-TX port
- Plug-in Module slot (Asynchronous Transfer Mode (ATM) and Fast Ethernet)
- Transceiver Module slot (10Mbps Ethernet)
- Support for desktop switching — one endstation per port, unlimited stations on backbone port
- Four forwarding modes for packets
- Intelligent Flow Management for congestion control
- Full duplex on all fixed Ethernet and Fast Ethernet ports, and Fast Ethernet Plug-in Module ports
- Security
- Resilient Links
- Support for 16 Virtual LANs (VLANs)
- Spanning Tree Protocol (STP) per VLAN
- PACE (Priority Access Control Enabled) for supporting multimedia applications over Ethernet
- Connects to Redundant Power System
- Integrated network management
- 19-inch rack or stand-alone mounting
- IP and IPX management over SNMP
- RMON
- Repeater and Bridge MIB
- Broadcast storm control
- Easy software upgrades
- BOOTP for automatic IP address configuration
- Local management

Port Connections

10BASE-T Ports

The Switch has 24 10BASE-T ports configured as MDIX (cross-over), which provide a full 10Mbps bandwidth to attached endstations. Maximum segment length is 100m (328ft) over grade 3, 4, or 5 twisted pair cable.



As these ports are configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only.

100BASE-TX Port

The Switch has a single Fast Ethernet 100BASE-TX port configured as MDIX (cross-over), which provides a 100Mbps connection to, for example, a local server. Maximum segment length is 100m (328ft) over grade 5 twisted pair cable.



As this port is configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only.

Plug-in Module

A slot at the rear of the unit can take a Plug-in Module, providing an additional high-speed port. This could be used, for example, to provide a Fast Ethernet or Asynchronous Transfer Mode (ATM) backbone connection to the rest of your network.

Transceiver Module

A slot at the rear of the unit allows you to install a suitable 10Mbps Ethernet Transceiver Module. When a Transceiver Module is fitted, port 1 automatically switches to become the Transceiver Module port. The Transceiver Module can provide a 10Mbps link to the rest of your network.

Backbone Port

The Switch allows you to specify any port to be a *backbone port* with the following attributes:

- Addresses received on the port are not stored in the Switch Database (the database which contains the device addresses received by the Switch)
- Frames with unknown addresses received by the Switch are forwarded to the port

A backbone port is typically used to connect the Switch to the backbone of large networks. For information about how to specify a backbone port for a new or initialized Switch, refer to "Setting Up the Switch Unit" on page 4-9.



You can specify one backbone port for each VLAN defined on the Switch. For more information about how to specify a backbone port for a VLAN, refer to "Setting Up VLANs on the Switch" on page 5-7.

Switch Operation and Features

How Does the Switch Compare to a Bridge?

The table below shows how Switch operation compares to that of a conventional IEEE 802.1d bridge.

	IEEE 802.1d Bridge	8271 Model 524 Switch
Address Learning	All ports	All ports except backbone port
Forwarding Mode	Store and forward	Fast Forward, Fragment Free, Store and Forward, or Intelligent
Operation when packet buffers full	Discard packets	Invoke Intelligent Flow Management to suppress transmissions at source
Spanning Tree	Supported	Optional
Action on Unknown Destination Address	Flood all ports	Forward to backbone port
Database size	4000 addresses	Four addresses per port

In all other ways, 8271 Model 524 Switch and bridge operation is identical.

Forwarding of Packets

The table below shows how a packet is processed when it arrives at the Switch.

Packet Source	Destination Address	Action
Any port EXCEPT backbone (Unicast packet)	Unknown	Forward to backbone port only
	Same port as source address	Filter
Any port EXCEPT backbone (Multi/Broadcast packet)	Another port (not backbone)	Forward to specific port only
	Not applicable	Forward to all ports (including backbone) in the same VLAN as source port
Backbone port (Unicast packet)	Unknown	Filter
	Known port (not backbone)	Forward to known port only
Backbone port (Multi/Broadcast packet)	Not applicable	Forward to all ports within specific VLAN

To best suit your networking requirements, the Switch allows you to select one of four frame forwarding modes:

- **Fast Forward** — Frames are forwarded as soon as the destination address is received and verified. The forwarding delay, or latency, for all frames in this mode is just 40 μ s, but with the lack of checking time any error frames received are propagated through the Switch.
- **Fragment Free** — A minimum of 64 bytes of the received frame is buffered prior to the frame being forwarded. This ensures that collision fragments are not propagated through the network. The forwarding delay, or latency, for all frames in this mode is 64 μ s.
- **Store and Forward** — Received packets are buffered in their entirety prior to forwarding. This ensures that only good frames are passed to their destination. The forwarding delay for this mode varies between 64 μ s and 1.2ms, depending on frame length. In Store and Forward mode, latency is measured as the time between receiving the last bit of the frame and transmitting the first bit. For the 8271 Model 524 Switch, this is 8 μ s.
- **Intelligent** — The Switch monitors the amount of error traffic on the network and changes the forwarding mode accordingly. If the Switch detects less than 18 errors a second, it operates in Fast Forward mode. If the Switch detects 18 or more errors a second, it operates in Store and Forward mode until the number of errors a second returns to zero.



For more information about selecting forwarding modes, refer to “Setting Up the Switch Unit” on page 4-9.

Intelligent Flow Management

Intelligent Flow Management (IFM) is a system for controlling congestion on your network. Congestion can be caused by one or more devices sending traffic to an already congested port on the Switch. If a port on the 8271 Model 524 Switch is connected to another switch or endstation, IFM prevents packet loss and inhibits the device from generating more packets until the period of congestion ends.

IFM should be enabled on a port if it is connected to another switch, or an endstation. IFM should be disabled on a port connected to a repeater.



For more information about enabling IFM on a port, refer to “Setting Up the Switch Ports” on page 4-12.

Full Duplex

The Switch provides full duplex support for all its fixed Ethernet and Fast Ethernet ports, and Fast Ethernet Plug-in Module ports. Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link. In addition, full duplex also supports 100BASE-FX cable runs of up to 2km.

Full duplex can be enabled on all the relevant ports, all the Fast Ethernet ports, or on individual ports. Full duplex is not supported by the Transceiver Module.



For more information about enabling full duplex, refer to “Setting Up the Switch Unit” and “Setting Up the Switch Ports” in Chapter 4.

Security

The Switch contains advanced security features which guard against users connecting unauthorized endstations to your network. When security is enabled on a port, it enters single address learning mode. In this mode, the port learns a single Ethernet address; once this is learned, the port is disabled if a different address is seen on the port. Until security is disabled, no other address can be learned.



For more information about enabling security on a port, refer to “Setting Up the Switch Ports” on page 4-12.

Resilient Links

The Resilient Link feature in the Switch enables you to protect critical links and prevent network downtime should those links fail.

Setting up resilience ensures that should a main communication link fail, a standby duplicate link immediately and automatically takes over the task of the main link. Each main and standby link pair is referred to as a resilient link pair.



For more information about resilient links, refer to “Setting Up Traps” on page 4-24.

Virtual LANs

The Switch has a Virtual LAN (VLAN) feature which allows you to build your network segments without being restricted by physical connections. A VLAN is defined as a group of location- and topology-independent devices that communicate as if they are on the same physical LAN. Implementing VLANs on your network has three main advantages:

- It eases the change and movement of devices on IP networks. If an endstation 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.
- It helps to control broadcast traffic. If an endstation in VLAN 1 transmits a broadcast frame, then only VLAN 1 devices receive the frame.
- It provides extra security. Devices in VLAN 1 can only communicate with devices in VLAN 2 using a router.



For more information about VLANs, refer to “Virtual LANs (VLANs)” on page 5-1.

Spanning Tree Protocol

The Switch supports the Spanning Tree Protocol (STP) which 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 traffic paths fail



For more information about STP, refer to “Spanning Tree Protocol” on page 5-10.

PACE

The Switch supports PACE (Priority Access Control Enabled) technology, which allows multimedia traffic to be carried over standard Ethernet and Fast Ethernet LANs. PACE provides two features:

- *Implicit Class of Service* — When multimedia traffic is transmitted, it is given a higher priority than other data and is therefore forwarded ahead of other data when it arrives at the Switch. The Implicit Class of Service feature minimizes latency through the Switch and protects the quality of multimedia traffic.

- *Interactive Access* — When two-way multimedia traffic passes over an Ethernet network, interference can occur because access to the bandwidth is unequally allocated to traffic in one direction. The Interactive Access feature allocates the available bandwidth equally in both directions, therefore increasing the quality of the traffic.



For more information about setting up PACE on the Switch, refer to “Setting Up the Switch Unit” and “Setting Up the Switch Ports” in Chapter 4.

Network Configuration Example

Figure 1-1 shows how the Switch can be placed on your network. In this example, the Switch is used for a group of heavy-traffic users in a large corporate network. Switching is brought to the desktop with a single endstation per port, and a local server is connected using the 100Mbps Fast Ethernet port.

Examples of how the Switch can be used in a VLAN-based network are given in Chapter 5.

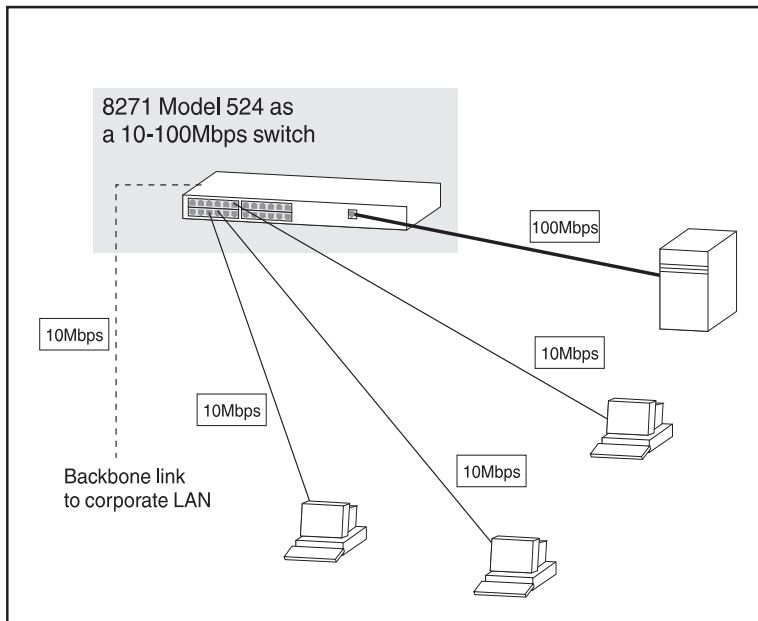


Figure 1-1 Example network configuration for desktop switching

Unit Overview — Front

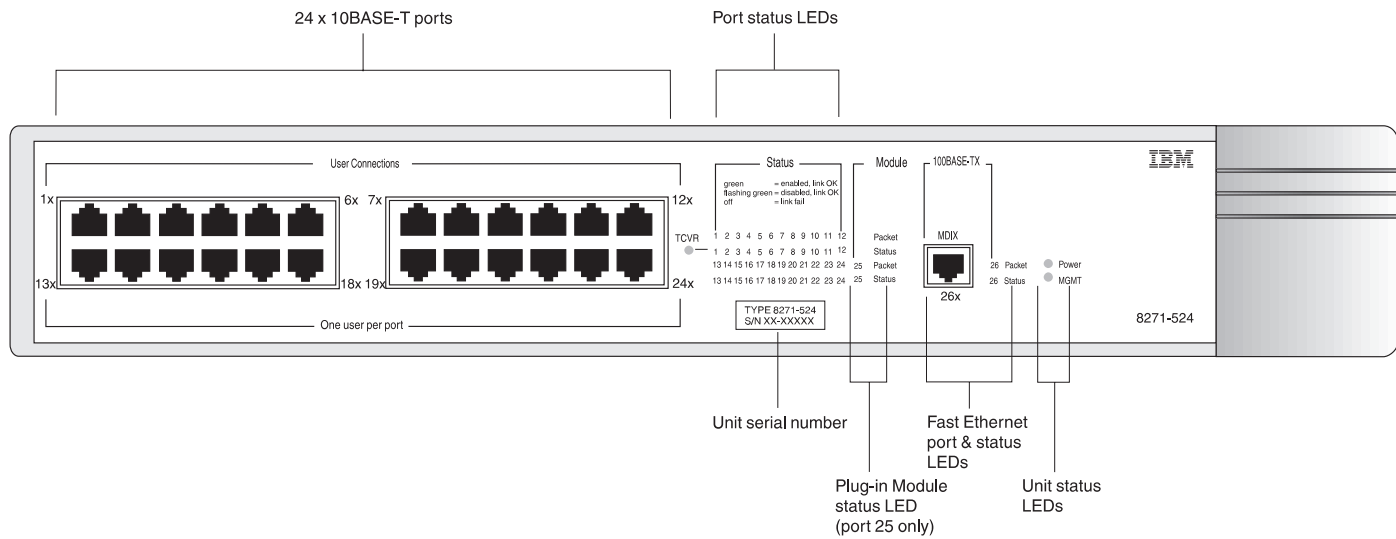


Figure 1-2 8271 Model 524 Switch front view

Unit Serial Number

You may need this serial number for fault reporting purposes.

10BASE-T Ports

The Switch has 24 10BASE-T RJ45 ports configured as MDIX (cross-over), which provide a full 10Mbps bandwidth to attached endstations. The maximum segment length is 100m (328ft) over category 3, 4, or 5 UTP cable.



As these ports are configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only.

100BASE-TX Port

The Switch has a single Fast Ethernet 100BASE-TX RJ45 port configured as MDIX (cross-over), which provides a 100Mbps connection to, for example, a local server. The maximum segment length is 100m (328ft) over category 5 UTP or STP cable.



As this port is configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only.

LEDs

The table below describes the LED behavior on the Switch. For more details about corrective action in the event of a problem, refer to “LEDs” on page C-1.

LED	Color	Indicates
TCVR	Yellow	Port 1 is a Transceiver Module fitted to the rear of the unit.
Port Status LEDs (ports 1–24 and 26)		
Packet	Yellow	Frames are being transmitted/received on the port.
Status	Green	Link is present; port is enabled.
	Green flashing	Link is present; port is disabled.
	Off	Link is not present.
Plug-in Module Status LEDs (port 25)		
Packet	Yellow	Frames are being transmitted/received on the Plug-in Module port.
Status	Green	Link is present; port is enabled.
	Green flashing	Link is present; port is disabled.
	Green flashing (long on, short off)	Refer to the “ <i>IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User's Guide</i> ”.
	Yellow	Plug-in Module has failed its Power On Self Test (if the MGMT LED is flashing yellow), or the agent software of the Plug-in Module is not installed correctly.
	Yellow flashing	Plug-in Module is not recognized.
	Off	Link is not present or Plug-in Module is not installed in the Switch.
Unit Status LEDs		
Power	Green	Switch is powered-up.
MGMT	Green	Switch is operating normally.
	Green flashing	Switch or Plug-in Module is either downloading or initializing (which includes a Power On Self Test).
	Yellow	Switch has failed its Power On Self Test.
	Yellow flashing	Plug-in Module has failed its Power On Self Test.

Unit Overview — Rear

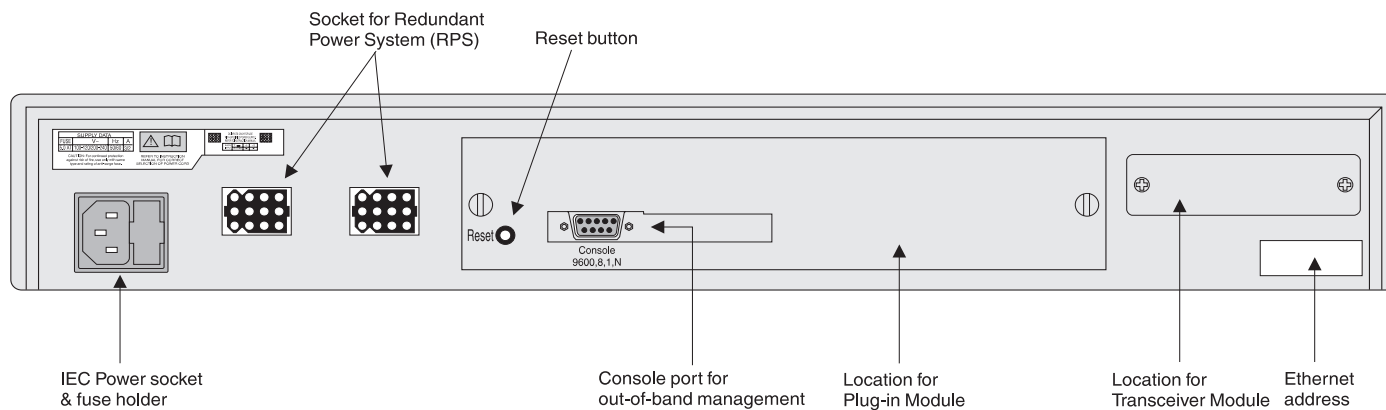


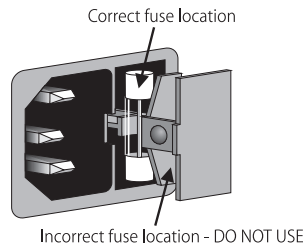
Figure 1-3 8271 Model 524 Switch rear view

Power Socket

The Switch automatically adjusts to the supply voltage. The fuse is suitable for both 110V A.C. and 220–240V A.C. operation.



DANGER: Ensure that the power is disconnected before opening the fuse holder cover. Only 5A Time Delay (anti-surge) fuses of the same type and manufacture as the original should be used.



To change the fuse, release the fuse holder by gently levering a small screwdriver under the fuse holder catch.

Redundant Power System Socket

Use one of these sockets to connect a Redundant Power System (RPS) to the unit. You can use either socket. Refer to “Connecting a Redundant Power System (RPS)” on page 2-6.

Reset Button

Using the reset button simulates a power-off/on cycle. This has the same effect as carrying out a reset via the VT100 interface; refer to “Resetting the Switch” on page 4-27.

Console Port

Connect a terminal to the console port to carry out remote or local out-of-band configuration and management. The console port is set to auto-baud, 8 data bits, no parity, and 1 stop bit.

Plug-in Module Slot

Use this slot to install a Plug-in Module. The Module can be used to provide a high speed link to the rest of your network.



When a Plug-in Module is not installed, ensure the blanking plate is secured in place.

Transceiver Module Slot

Use this slot to connect a Transceiver Module and provide a 10Mbps link to the rest of the network. Port 1 is automatically switched from the front 10BASE-T port to the Transceiver Module port when a Module is installed.



When a Transceiver Module is not installed, ensure the blanking plate is secured in place.

Ethernet Address

This label shows the unique Ethernet (or MAC) address assigned to the unit.

Unit Defaults

The following table shows the factory defaults for the Switch features.

Port Status	Enabled
Forwarding Mode	Fast Forward
Intelligent Flow Management	Enabled
Duplex Mode	Half duplex on all relevant ports
Virtual LANs	All ports use Port VLAN Mode and belong to the Default VLAN (VLAN 1)
PACE	Disabled
Spanning Tree (STP)	Disabled
Power On Self Test (POST)	Normal (Fast Boot)
System Alarm (broadcast bandwidth used)	Enabled <ul style="list-style-type: none"> ■ High threshold: 20% — Notify and Blip ■ Low threshold: 10% — No action
System Alarm (errors per 10,000 packets)	Enabled <ul style="list-style-type: none"> ■ High threshold: 2% — Notify ■ Low threshold: 1% — No action
System Alarm (bandwidth used)	Enabled <ul style="list-style-type: none"> ■ High threshold: 85% — No action ■ Low threshold: 50% — No action
System Alarm (percentage of frames forwarded)	Enabled <ul style="list-style-type: none"> ■ High threshold: 85% — No action ■ Low threshold: 50% — No action

Managing the Switch

The menu-driven interface built into the Switch is known as the VT100 interface. You can access it using a VT100 terminal, or a PC using terminal emulation software. You can connect the terminal directly to the Switch or through a modem. You can also access the VT100 interface remotely using Telnet running over the TCP/IP protocol.

Remote management is also possible using a Network Manager. The management protocol is SNMP (Simple Network Management Protocol) and any SNMP-based management facility can manage the unit if the Management Information Base (MIB) is installed correctly in the management workstation. The Switch supports SNMP over both IP and IPX protocols.

Quick Start For SNMP Users

This section describes how to get started if you want to use an SNMP Network Manager to manage the Switch. It assumes you are already familiar with SNMP management.

- If you are using IP and you have a BOOTP server set up correctly on your network, the IP address for the Switch is detected automatically and you can start managing the Switch without any further configuration.
- If you are using the IPX protocol, the Switch is allocated an IPX address automatically. You can start the SNMP Network Manager and begin managing the Switch.
- If you are using IP without a BOOTP server, you must enter the IP address of the Switch before the SNMP Network Manager can communicate with the device. To do this, refer to “Entering an IP Address for the Switch” below.

If you need more information about IP and IPX, refer to Chapter 3.

Entering an IP Address for the Switch

- 1 Connect a terminal to the console port of the Switch (refer to “Connecting a VT100 Terminal” on page 2-7). The terminal should be configured to 9600 line speed (baud rate), 8 data bits, no parity, and 1 stop bit.
- 2 Press [Return] one or more times until the Main Banner screen appears.

- 3 At the Main Banner screen, press [Return] to display the Logon screen. Logon using the default user name *admin* (no password is required). Select OK.
- 4 The Main Menu is displayed. From this menu, select the MANAGEMENT SETUP option. The Switch Management Setup screen is displayed.
- 5 On the Management Setup screen, fill in the following fields:
 - Device IP Address
 - Device SubNet Mask (if necessary)
 - Default Router (if necessary)

For further information on the Management Setup screen, refer to “Setting Up the Switch for Management” on page 3-6.

- 6 If you need the Switch to send SNMP traps to the Network Manager, you may need to set up the address of the Network Manager in the Trap Table. Refer to “Setting Up Traps” on page 4-24.



Some Network Managers may automatically configure the Switch to send traps to them. Please read the documentation supplied with your network management software.

- 7 When you have finished with the Management Setup screen, select OK.



2

INSTALLATION AND SETUP

Following Safety Information

Before installing or removing any components from the Switch or carrying out any maintenance procedures, you must read the safety information provided in Appendix A of this guide.

Positioning the Switch

The Switch is suitable for use in the office where it can be wall-mounted, mounted in a standard 19-inch equipment rack, or free standing. Alternatively, the unit can be rack-mounted in a wiring closet or equipment room. A wall- or rack-mounting kit, containing two mounting brackets and six screws, is supplied with the Switch.

When deciding where to site the unit, ensure that:

- You are able to meet the configuration rules detailed in the following section.
- The unit is accessible and cables can be connected easily.
- Cabling is away from:
 - Sources of electrical noise such as radios, transmitters and broadband amplifiers.
 - Power lines and fluorescent lighting fixtures.

- Water or moisture cannot enter the case of the unit.
- Air-flow around the unit and through the vents in the side of the case is not restricted. We recommend that you provide a minimum of 25mm (1in.) clearance.
- No objects are placed on top of the unit.
- Units are not stacked more than four high if free-standing.

Configuration Rules for Fast Ethernet

The topology rules for 100Mbps Fast Ethernet are slightly different to those for 10Mbps Ethernet. Figure 2-1 illustrates the key topology rules and provides examples of how they allow for large-scale Fast Ethernet networks.

The key topology rules are:

- Maximum UTP cable length is 100m (328ft) over category 5 cable.
- A 412m (1352ft) fiber run is allowed for connecting switch to switch, or endstation to switch, using half-duplex 100BASE-FX.
- A total network span of 325m (1066ft) is allowed in single-repeater topologies (one hub stack per wiring closet with a fiber run to the collapsed backbone). For example, a 225m (738ft) fiber downlink from a repeater to a router or switch, plus a 100m (328ft) UTP run from a repeater out to the endstations.

Configuration Rules with Full Duplex

The Switch provides full duplex support for all its fixed Ethernet and Fast Ethernet ports, and the Fast Ethernet Plug-in Module ports. Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

With full duplex, the Ethernet topology rules are the same, but the Fast Ethernet rules are:

- Maximum UTP cable length is 100m (328ft) over category 5 cable.
- A 2km (6562ft) fiber run is allowed for connecting switch-to-switch, or endstation-to-switch.

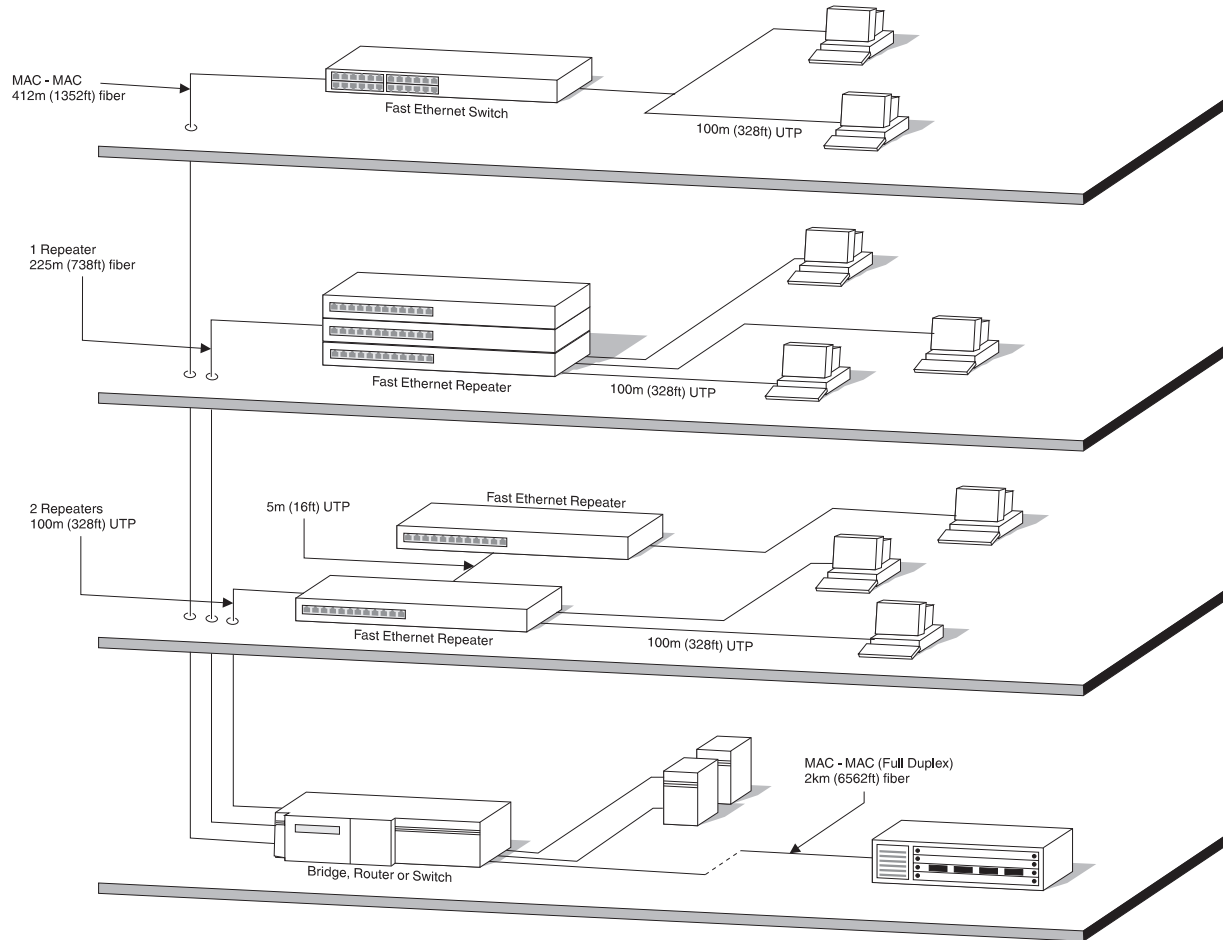


Figure 2-1 Fast Ethernet configuration rules

Installing the Switch

Rack Mounting

The Switch is 1.5U high and will fit in most standard 19-inch racks.



ATTENTION: Disconnect any cables from the unit before continuing. Remove self-adhesive pads from the underside of the unit if they have been previously fitted.

- 1 Place the unit the right way up on a hard flat surface, with the front facing towards you.
- 2 Locate a mounting bracket over the mounting holes on one side of the unit, as shown in Figure 2-2.

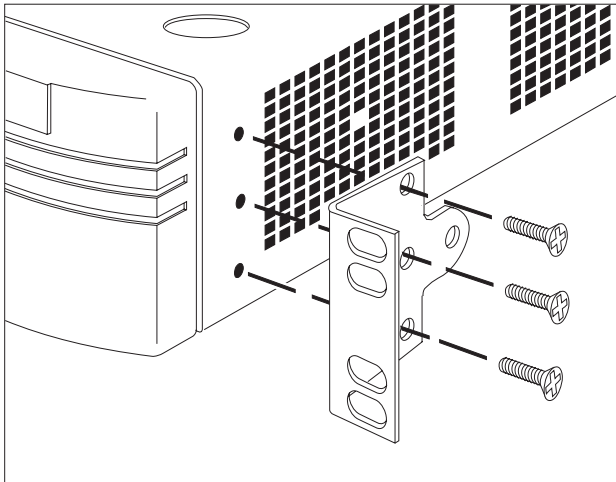


Figure 2-2 Fitting a bracket for rack mounting

- 3 Insert the three screws and fully tighten with a suitable screwdriver.
- 4 Repeat steps 2 and 3 for the other side of the unit.
- 5 Insert the unit into the 19-inch rack and secure with suitable screws (not provided). Ensure that ventilation holes are not obstructed.
- 6 Connect network cabling.

Stacking the Switch and Other Units

If the units are free standing, up to four units can be placed on top of one another. If mixing a variety of units, the smaller units must be positioned at the top.

The Switch is supplied with four self-adhesive rubber pads. Apply the pads to the underside of the unit, sticking a pad in the marked area at each corner of the unit. Place the units on top of each other, ensuring that the pads of the upper unit line up with the recesses of the lower unit.

Wall Mounting

A single Switch can be wall-mounted.



ATTENTION: Disconnect any cables from the unit before continuing. Remove self-adhesive pads from the underside of the unit if they have been previously fitted.

- 1 Place the Switch the right way up on a hard flat surface, with the front facing towards you.
- 2 Locate a mounting bracket over the mounting holes on one side of the unit, as shown in Figure 2-3.
- 3 Insert the two screws and tighten with a suitable screwdriver.
- 4 Repeat for the other side of the unit.
- 5 Ensure that the wall you are going to use is smooth, flat, dry, and sturdy. Attach a piece of plywood, approximately 305mm x 510mm x 12mm (12in. x 20in. x 0.5in.) securely to the wall if necessary, and mount the Switch as follows:
 - a Position the base of the unit against the wall (or plywood) ensuring that the ventilation holes face sideways and the front panel faces upwards. Mark on the wall the position of the screw holes in both wall brackets. Drill the four holes.
 - b Using suitable fixings and screws (not provided), attach the Switch unit securely to the wall or plywood.
 - c Connect network cabling.

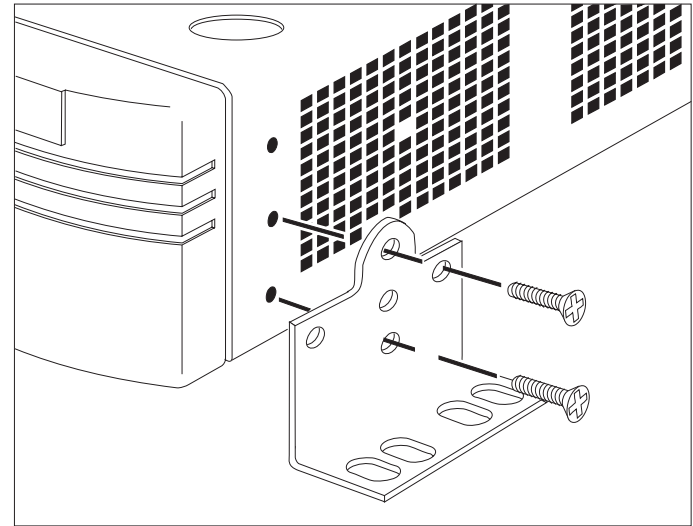


Figure 2-3 Fitting a bracket for wall mounting

Powering-Up the Switch

- 1 Connect the power cord to the IEC socket on the rear of the Switch, and to your mains socket.



The Switch has no ON/OFF switch; the only method of connecting or disconnecting mains power is through the power cord.

- 2 The Switch enters a Power On Self Test (POST). The time taken for the test to complete is dependent on the type of POST configured (refer to “Switch Management Setup” on page 3-9 for details of how to configure the type of POST.) For a new Switch that is being installed for the first time, power-up takes approximately 13 seconds.
- 3 Check the status LEDs to ensure the Switch is operating correctly (refer to “LEDs” on page 1-9).

Connecting a Redundant Power System (RPS)

You can connect a Redundant Power System (RPS) to the Switch.

At +5V, the current requirement for the Switch is 4.8A, including any Transceiver Module that might be fitted, but excluding a Plug-in Module. Check the documentation supplied with your Plug-in Module for power consumption figures.

For most configurations, you need only one RPS output, and this can be connected to either of the two sockets on the rear of the unit.

If the current consumption of the Switch plus any optional Plug-in Module exceeds the capability of the RPS (8.5A), you need a SuperStack II Advanced RPS with one Advanced RPS 100W module.

If the RPS is used incorrectly, its Output Fault LED lights yellow.

You should check the documentation supplied with the RPS or Advanced RPS to see if the outputs can be used in parallel.

Connecting Equipment to the Console Port

The Switch console port settings are set to:

- 8 data bits
- no parity
- 1 stop bit

The terminal connected to the console port on the Switch must be configured with the same settings. This procedure is described in the documentation supplied with the terminal. If you have enabled auto-configuration for the Switch, the terminal's line speed (baud rate) is detected automatically.

Connection to the console port can be direct for local management, or through a modem for remote management. The maximum baud rate the auto-configuration detects is 19,200 baud.

Appropriate cables are available from your local supplier. If you need to make your own cables, pin-outs are detailed in Appendix D.

Connecting a VT100 Terminal

To connect a VT100 terminal directly to the console port on the Switch, you need a standard null modem cable:

- 1 Connect one end of the cable to the console port on the Switch, and the other to the console port on the VT100 terminal.
- 2 Ensure that your terminal is set to:
 - 8 data bits
 - no parity
 - 1 stop bit

If auto-configuration is enabled for the Switch, the terminal's line speed (baud rate) is detected automatically.

Connecting a VT100 Terminal Emulator

- 1 Ensure that the workstation is running a suitable terminal emulation package. There are many available; contact your local supplier for further details.
- 2 If you are using a PC, you need a null modem cable with an appropriate connector. Connect one end of the cable to the workstation, and the other end to the console port on the Switch.
- 3 Ensure that your workstation is set to:
 - 8 data bits
 - no parity
 - 1 stop bit

If auto-configuration is enabled for the Switch, the workstation's line speed (baud rate) is detected automatically.

Connecting a Workstation Running SLIP

You can communicate with the Switch via the console port from a workstation running SLIP (Serial Line Internet Protocol). In this way, you can perform out-of-band management using Telnet or SNMP.

Cables required for this connection depend on the type of workstation you are using. You must configure the workstation to run SLIP. Refer to the documentation supplied with the workstation for more details.

You must configure the console port of the Switch to accept SLIP and set up the SLIP parameters (address and subnet mask). Refer to “Switch Management Setup” on page 3-9.



You may need a 5-wire cable when running SLIP. Two of the wires are required for Flow Control.

3

SETTING UP FOR MANAGEMENT

Methods of Managing the Switch

You can manage the Switch in four ways:

- Using the VT100 interface by connecting a VT100 terminal (or workstation with terminal emulation software) to the Switch console port.
- Using the VT100 interface over a TCP/IP network using a workstation running VT100 terminal emulation and Telnet.
- Using the VT100 interface by connecting a workstation running SLIP to the Switch console port.
- Using an SNMP Network Manager over a network running either the IP or IPX protocol. Each Network Manager provides its own user interface to the management facilities.

Using the VT100 Management Interface

The menu-driven user interface built into the Switch is known as the *VT100* or *Local Management* interface. The VT100 management interface provides a forms-based structure with pre-defined security levels, enabling access to be restricted to particular users. The Switch can support up to four management user sessions concurrently (for example one console port and three Telnet connections).

You can establish VT100 management communication with the Switch through two different interfaces:

- **Via the Console Port** — You can access the local management interface using a VT100 terminal, PC or any terminal emulator using suitable terminal emulation software. The terminal can be connected directly to the Switch, or through a modem. You can also connect a management workstation running SLIP to the console port, which allows you to use out-of-band Telnet. The workstation can be connected directly or remotely, through a modem. This method provides a way of managing the Switch in situations where the LAN is not providing a reliable service, where the Network Manager does not have direct LAN connectivity, or when a Network Manager does not support SNMP.
- **Via a Network Connection** — The local management facility is also accessible via Telnet over a network running the TCP/IP protocol. The management available through Telnet is exactly the same as that of a locally connected terminal. The Telnet application requires a VT100 terminal or PC with VT100 emulation software.

Using Telnet

Any Telnet facility that emulates a VT100 terminal should be able to communicate with the Switch over a TCP/IP network. Up to three active Telnet sessions can access the Switch concurrently. If a connection to a Telnet session is lost inadvertently, the connection is closed by the Switch after 2–3 minutes of inactivity.

Before you can start a Telnet session you must set up the IP parameters described in “Switch Management Setup” on page 3-9.

To open the Telnet session, you must specify the IP address of the device that you want to manage. Check the user manual supplied with the Telnet facility if you are unsure how to do this.

When the connection is established, the main banner of the VT100 management interface is displayed and you can log on.

Managing Over The Network

Any Network Manager running the Simple Network Management Protocol (SNMP) can manage the Switch, provided the MIB (Management Information Base) is installed correctly on the management workstation. Each Network Manager provides its own user interface to the management facilities.

The Switch supports SNMP over both IP and IPX protocols.

IP Addresses

If you are uncertain about IP addresses that may be assigned to your devices, contact your network administrator first.

To operate correctly, each device on your network must have a unique IP address. IP addresses have the format *n.n.n.n* where *n* is a decimal number between 0 and 255. An example IP address is: 191.128.40.120

The IP address can be split into two parts:

- The first part (191.128 in the example) identifies the network on which the device resides.
- The second part (40.120 in the example) identifies the device within the network.

If your network is internal to your organization only, you may use any arbitrary IP address. We suggest you use addresses in the series 191.100.X.Y, where X and Y are numbers between 1 and 254. Use 191.101.X.Y for the SLIP address.

If your network has a connection to the external IP network, you will need to apply for a registered IP address. This system ensures that every IP address used is unique; if you do not have a registered IP address, you may be using an identical address to someone else and your network will not operate correctly.

Obtaining a Registered IP Address

InterNIC Registration Services is the organization responsible for supplying registered IP addresses. The following contact information is correct at the time of publication:

Network Solutions
Attn: InterNIC Registration Service
505, Huntmar Park Drive
Herndon
VA 20170
U.S.A.

Telephone: (1) (703) 742 4777

If you have access to the Internet, you can find further information about InterNIC by entering the following URL into your web browser:

<http://www.internic.net>

Navigating the VT100 Screens

Screen Conventions

To differentiate types of information, the VT100 screens use the following conventions:

Type of information	Shown on screen as...	Description
Choice Field	✦text✦	Text enclosed with markers is a list from which you can select one option only. Press the spacebar to cycle through the options. Press [Down Arrow] or [Return] to move to the next field.
Entry Field	[text]	Text enclosed in square brackets on the screen is a <i>text entry</i> field. An entry field allows you to enter text, numeric data or hexadecimal data from the keyboard. Password fields are hidden, which means that the text you type is not shown on the screen. In some cases an entry field has a default entry. If you wish to replace the default, simply enter a new value for this field; the default entry is erased. Press [Down Arrow] or [Return] to move to the next field.
Button	OK	Text for a button is always shown in uppercase letters. A button carries out an action, for example, OK or CANCEL. To operate a button, move the cursor to the button and press [Return].
List Box	monitor manager security	<p>A list box allows you to select one or more items from a list. There are several keys that allow you to use a list box.</p> <p>[Return] moves the cursor to the next field and actions your selections.</p> <p>The spacebar toggles through the options in a choice field or selects and deselects an entry in the list box. List box selections are highlighted.</p> <p>[Down Arrow] moves item by item down the list box until it reaches the end of the list. At the end of the list it moves the cursor to the next field.</p> <p>[Ctrl] + [U] moves the cursor one page up the list box.</p> <p>[Ctrl] + [D] moves the cursor one page down the list box.</p>

Keyboard Shortcuts

There are several special characters or combinations of characters that allow you to make shortcuts.

[Tab] allows you to move from one field to the next, on any screen, without making any changes.

[Return] moves you to the next field on a form after you have made changes to the data in a field.

[Left Arrow] moves you to the previous field on the screen or the next character in an editable field.

[Right Arrow] moves you to the next field on the screen or the previous character in an editable field.

[Ctrl] + [R] refreshes the screen.

[Ctrl] + [B] moves the cursor to the next button.

[Ctrl] + [P] aborts the current screen and returns you to the previous screen.

[Ctrl] + [N] actions the inputs for the current screen and moves to the next screen.

[Ctrl] + [K] displays a list of the available key strokes.

Correcting Text Entry

Use [Delete] on a VT100 terminal or [Backspace] on a PC. This moves the cursor one space to the left and deletes a character.



If you are using Telnet or a terminal emulation program you may find that some of the Control keys do not operate or that they activate other functions. Check carefully in the manual accompanying your Telnet or terminal emulation software before using the Control keys.

Setting Up the Switch for Management

The following sections describe how to get started if you want to use an SNMP Network Manager to manage the Switch. It assumes you are already familiar with SNMP management. If not, we recommend the following publication:

“The Simple Book” by Marshall T. Rose
ISBN 0-13-812611-9
Published by Prentice Hall

- If you are using IP and you have a BOOTP server set up correctly on your network, the IP address for the Switch is detected automatically and you can start managing the Switch without any further configuration.
- If you are using the IPX protocol, the Switch is allocated an IPX address automatically. You can start the SNMP Network Manager and begin managing the Switch.
- If you are using IP without a BOOTP server, you must enter the IP address of the Switch before the SNMP Network Manager can communicate with the device. To do this, take the following steps:

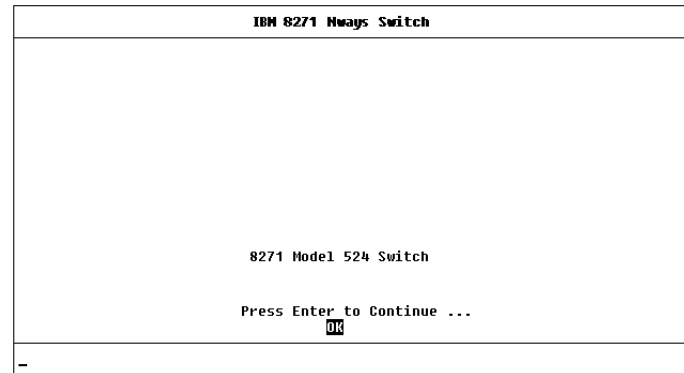


Figure 3-1 Main Banner

- 1 At your terminal, press [Return] two or more times until the Main Banner is displayed (shown in Figure 3-1). The console port detects the line speed (baud rate) from these keystrokes and defaults to:
 - auto-baud
 - 8 data bits
 - no parity
 - 1 stop bitData bits, parity, and stop bit values cannot be changed. If your terminal is already set up with these values, the Main Banner is displayed as soon as power-up is complete.
- 2 At the Main Banner, press [Return] to display the Logon screen.

Logging On

At the Logon screen displayed in Figure 3-2, enter your user name and password (note that they are both case-sensitive):

- If you have been assigned a user name and password, enter those details.
- If you are logging on for the first time (after installation or initialization), use a default user name and password to match your access requirements. The defaults are shown in Table 3-1. If you are setting up the Switch for management, we suggest that you log on first as *admin*.

Table 3-1 Default Users

User Name	Default Password	Access Level
<i>monitor</i>	monitor	<i>monitor</i> — this user can view, but not change all manageable parameters
<i>manager</i>	manager	<i>manager</i> — this user can access and change the operational parameters but not special/security features
<i>security</i>	security	<i>security</i> — this user can access and change all manageable parameters
<i>admin</i>	(no password)	<i>security</i> — this user can access and change all manageable parameters

The screenshot shows a terminal window titled "IBM 8271 Nways Switch Logon". Inside the window, there are two lines of text for input: "User Name: []" and "Password: []". The password field is currently empty. Below these fields, centered, is the text "OK".

Figure 3-2 Logon screen

After Logging On

When you have successfully logged on to the Switch, the Main Menu screen appears as shown in Figure 3-3. From here, you can select the options needed to manage the unit. Refer to the screen map on page 4-1.



If you have installed an ATM OC-3c Module into the Switch, the Main Menu screen contains an ATM CONFIGURATION option. Refer to the "IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User's Guide" for more information.

Access to options depends on the access level you have been assigned. Access rights to the VT100 screens for the Switch are listed in Appendix B.

If you are a user with *security* access level, and are using the management facility for the first time, we suggest that you:

- Assign a new password for your user, using the Edit User screen, as described in "Editing User Details" on page 4-5.
- Log on as each of the other default users, and change their passwords using the Edit User screen.
- Create any new users, in addition to the default ones. To do this, you assign each a user name, password and security level, as described in "Creating a New User" on page 4-3.

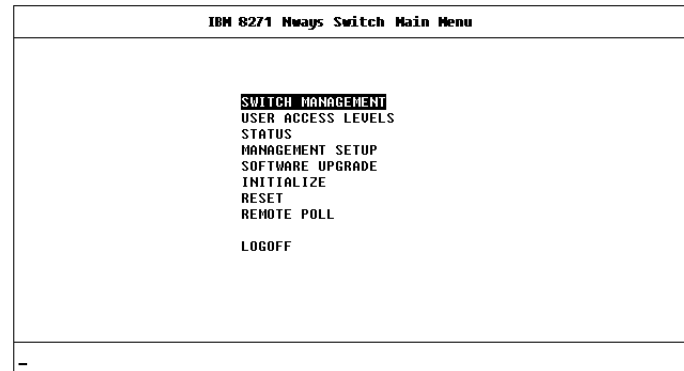


Figure 3-3 Main Menu screen

Switch Management Setup

The Management Setup screen allows you to configure IP, IPX, and SLIP parameters for the Switch. This screen also allows you to display screens for setting up the console port and traps.

To access the Setup screen, from the Main Menu screen, select the MANAGEMENT SETUP option. The Setup screen is displayed, as shown in Figure 3-4.



If you change some of the following parameters, the Switch must be reset for the change to take effect. Reset the Switch by selecting OK and pressing the Reset button on the rear of the unit. Refer to “Reset Button” on page 1-11.

The screen shows the following:

MAC Address This read-only field shows the MAC address of the Switch unit, which is required for management.

Power On Self Test Type *Normal / Extended* This field allows you to determine the type of self-test that the Switch carries out when it is powered-up. If the field is set to *Normal*, the Switch performs a Fast Boot — a basic confidence check lasting approximately 13 seconds. When the Switch performs a Fast Boot, it carries out the following tests:

- Checksum test of boot and system areas of Flash memory
- System memory tests
- MAC address verification test
- System timer test

IBM 8271 Always Switch Management Setup			
MAC Address:	08004E0B99A5		
Power On Self Test Type:	◆Normal ◆		
Device IP Address:	[191.1.1.50]	SLIP Address:	[192.101.1.1]
Device SubNet Mask:	[255.255.255.0]	SLIP SubNet Mask:	[255.255.255.0]
Default Router:	[191.1.1.20]		
BOOTP Select:	◆Enabled ◆		
IPX Network	Node	Status	Data Link Protocol
[00356501]	: 08004e0b99a5	◆Enabled ◆	Ethernet_002.3
[00356502]	: 08004e0b99a5	◆Enabled ◆	Ethernet_002.2
[00356503]	: 08004e0b99a5	◆Enabled ◆	Ethernet_II
[00000000]	: 08004e0b99a5	◆Enabled ◆	Ethernet_SNAP
OK SETUP TRAPS CONSOLE PORT CANCEL			

Figure 3-4 Management Setup screen

- CAM (Contents Addressable Memory) tests
- Console port tests
- Internal packet forwarding tests
- ASIC (Application Specific Integrated Circuit) tests
- ASIC memory tests
- Switch–Plug-in Module interface test
- Plug-in Module packet forwarding tests
- Plug-in Module ASIC tests
- Plug-in Module ASIC memory tests

If the field is set to *Extended*, the Switch performs an Extended test which may take up to 70 seconds to complete. When the Switch performs an Extended test, it carries out more extensive system memory tests and ASIC memory tests in addition to the Fast Boot tests. The default setting for the field is *Normal*.

If you suspect that there is a problem with the Switch that has not been detected by the Normal tests, set this field to Extended and reset the Switch (refer to “Resetting the Switch” on page 4-27).



If you set the Switch to perform an Extended test, the Switch must be isolated from the rest of your network when it is powered-up. The Switch fails an Extended test if it receives any network traffic during the test.

Device IP Address If you are using IP, a unique IP address must be specified in this field. If you do not know the IP address of the Switch, consult your network administrator. You must reset the Switch after changing this parameter.

Device SubNet Mask If you are using IP, enter a suitable network mask. For a Class B IP address, 255.255.0.0 is suitable. For more information, consult your network administrator. You must reset the Switch after changing this parameter.

Default Router If a default router exists on your network, enter the IP address of the router. You must reset the Switch after changing this parameter.

BOOTP Select *Enabled / Disabled* If BOOTP is enabled and you have a BOOTP server on your network, an IP address is automatically mapped to the Switch when it is first powered-up. In addition to mapping an IP address, BOOTP can also assign the subnet mask and default router. Using a BOOTP server avoids having to configure devices individually.

SLIP Address If you are using SLIP, enter an address that has a network part different to the network address of the Switch. For more information, consult your network administrator. You must reset the Switch after changing this parameter.

SLIP SubNet Mask Enter a suitable subnet mask. For a Class B address, 255.255.0.0 is suitable. For more information, consult your network administrator. You must reset the Switch after changing this parameter.

There are four entries under the following four fields; one for each data link layer protocol that can be used by IPX:

IPX Network This read-only field shows the address of the network for this protocol. This address is learned automatically from the local IPX router or NetWare File Server, and you do not need to change it.

Node This read-only field shows the node address of the Switch which is learned automatically.

Status *Enabled / Disabled* If this field is set to Enabled, you have access to the medium-access protocol. Set this field to Disabled if you wish to prevent access for security reasons.

Data Link Protocol This read-only field shows the name of the IPX data link layer protocol.

SETUP TRAPS Select this button to display the setup screen for trap parameters. Trap setup is described in “Setting Up Traps” on page 4-24.

CONSOLE PORT Select this button to display the setup screen for console port parameters. Console port setup is described in “Setting Up the Console Port” on page 4-25.

Logging Off

If you have finished using the VT100 management interface, select the LOGOFF option from the bottom of the Main Menu screen. If you accessed the VT100 management interface using a Telnet session or modem connection, the connection is closed automatically.

Auto Logout

There is a built-in security timeout on the VT100 interface. If you do not press any keys for three minutes, the management facility warns you that the inactivity timer is about to expire. If you do not press a key within 10 seconds, the timer expires and the screen is locked; any displayed statistics continue to be updated. When you next press any key, the display changes to the Auto Logout screen.

The Auto Logout screen (shown in Figure 3-5) requests you to enter your password again. If the password is correctly entered, the screen that was active when the timer expired is displayed. If you make a mistake entering your password, you are returned to the Logon screen.

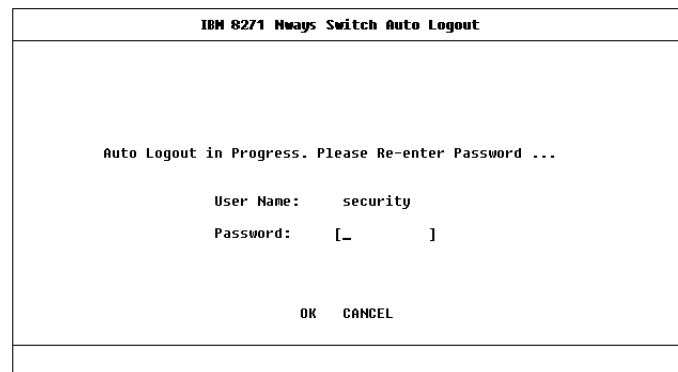


Figure 3-5 Auto Logout screen



4

MANAGING THE SWITCH

Chapters 4, 5 and 6 describe all management facilities for the Switch. While following steps in these chapters, you may find the screen map below useful.



If an ATM OC-3C Module is installed in the Switch, extra screens are available. Refer to the "IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User's Guide" for more information.

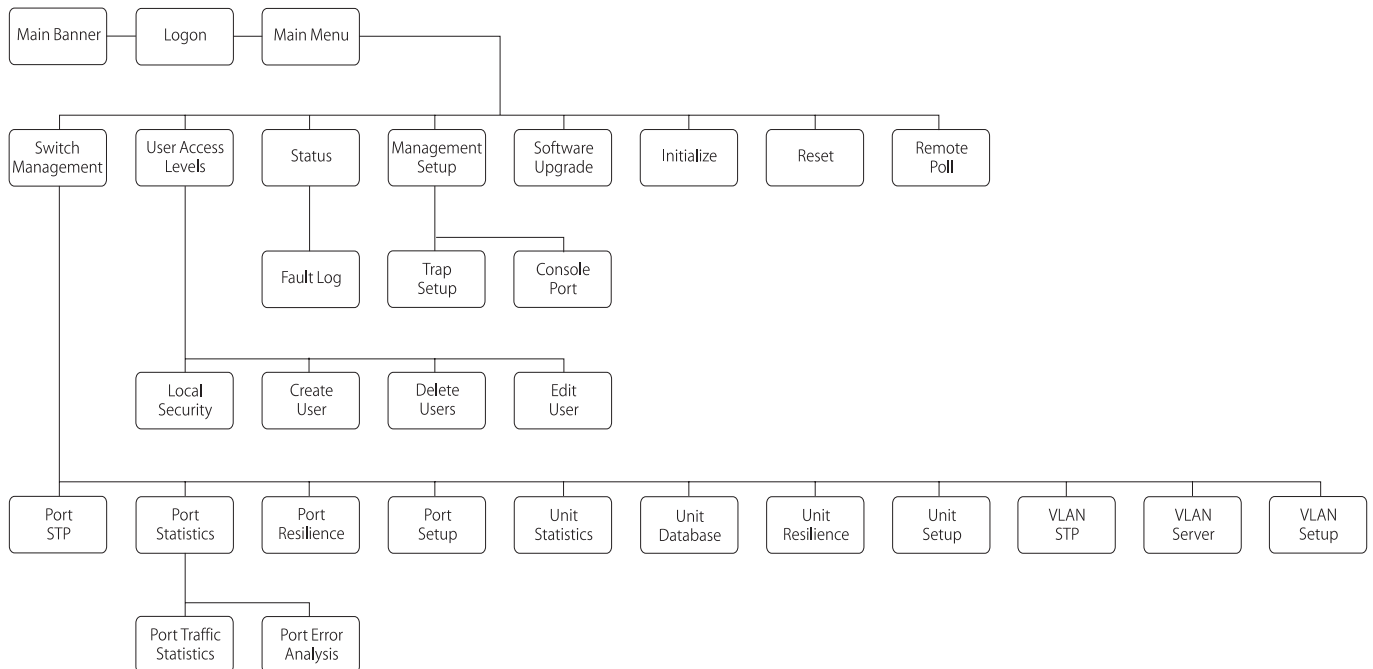


Figure 4-1 Screen map

Setting Up Users

From the Main Menu, select USER ACCESS LEVELS. The User Access Levels screen appears as shown in Figure 4-2.

From this screen you can access:

- **LOCAL SECURITY screen** — This allows you to set up access levels for users on the Switch.
- **CREATE USER screen** — This allows you to create up to ten users in addition to the default users set up on the Switch.
- **DELETE USERS screen** — This allows you to delete users from the Switch. The default users cannot be deleted.
- **EDIT USER screen** — This allows you to change your own password and community string. You cannot change details for other users.

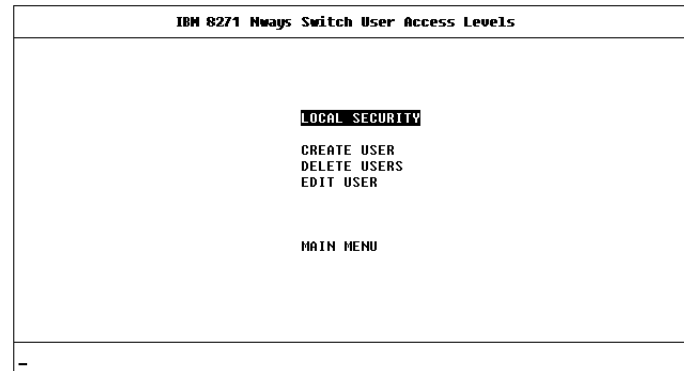


Figure 4-2 User Access Levels screen

Creating a New User

These steps assume the User Access Levels screen is displayed.

- 1 Select the CREATE USER option. The Create User screen is displayed, as shown in Figure 4-3.
- 2 Fill in the fields and assign an access level for the new user.
- 3 When the form is complete, select OK.

The Create User screen shows the following fields:

User Name Type in the name of this new user. The name can consist of up to 10 characters and is case-sensitive.

Password Type in the password for this new user. The password can consist of up to 10 characters and is case-sensitive. For security reasons, the password is not displayed on screen.

Access Level Assign an access level for this new user, as follows:

- *monitor* — access to view, but not change, a subset of the manageable parameters of the Switch
- *secure monitor* — as *monitor*
- *manager* — access to all the manageable parameters of the Switch, except security features
- *specialist* — as *manager*
- *security* — access to all manageable parameters of the Switch

Figure 4-3 Create User screen

Community String By default, a community string identical to the user name is generated. You can change this to any text string of 32 characters or less. The community string is only needed for SNMP access. If you are using a remote SNMP Network Manager, the community string specified in the Network Manager's database must be the same as that for the device.



If you enter a community string that is greater than 32 characters, it is truncated to 32 characters.

Deleting a User

These steps assume the User Access Levels screen is displayed.

- 1 Select the DELETE USERS option. The Delete Users screen is displayed, as shown in Figure 4-4.
- 2 Use the spacebar to highlight the user that you want to delete. Note that you cannot delete default users or the current user (that is, yourself).
- 3 Select DELETE USERS.

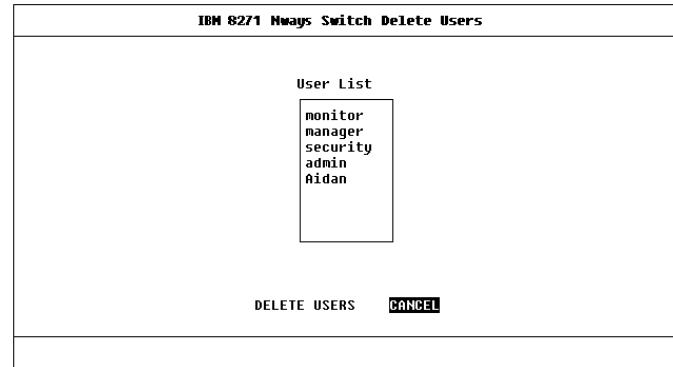


Figure 4-4 Delete Users screen

Editing User Details

These steps assume the User Access Levels screen is displayed.

- 1 Select the EDIT USER option. The Edit User screen is displayed, as shown in Figure 4-5.
- 2 Fill in the fields as required.
- 3 When you have completed the changes, select OK.

The Edit User screen shows the following fields:

User Name This read-only field shows the name of the user. This field cannot be changed; if you need to change the user name, you must delete this user and create a new one.

Old Password To change the user's password, you need to enter the current password in this field.

New Password This field allows you to enter a new password for the user.

Confirm Password Re-enter the new password into this field.

Community String This field allows you to enter a community string for the user.



If you forget your password while logged out of the Switch VT100 interface, contact your local technical support representative who will advise on your next course of action.

```
IBM 8271 Always Switch Edit User

User Name:      security
Old Password:   [      ]
New Password:   [      ]
Confirm Password: [      ]
Community String: [security ]

                                OK  CANCEL
```

Figure 4-5 Edit User screen

Assigning Local Security

The Local Security screen shows a matrix of options for access method (Console Port, Remote Telnet, Community-SNMP) and access level. (Monitor, Secure Monitor, Manager, Specialist, Security)

These steps assume the User Access Levels screen is displayed.

- 1 Select the LOCAL SECURITY option. The Local Security screen is displayed, as shown in Figure 4-6.
- 2 Fill in the fields as required.
- 3 When you have filled in the form, select OK.

Access options are:

Console Port *Enabled / Disabled* To prevent access to the management facilities via the console port, disable access to the facility for each access level. Console port access for *Security* is enabled and cannot be changed. This prevents accidental disabling of all access levels from management.

Remote Telnet *Enabled / Disabled* Telnet is an insecure protocol. You may want to disable all access to the management facilities via Telnet if there is important or sensitive data on your network.

Community-SNMP *Enabled / Disabled* The Switch can be managed via SNMP using a remote Network Manager. Community-SNMP does have some simple security features, but it is an insecure protocol. You may want to disable all access to the management facilities if there is important or sensitive data on your network.

IBM 8271 Hways Switch Local Security					
	Monitor	Secure Monitor	Manager	Specialist	Security
Console Port	◆Enabled◆	◆Enabled◆	◆Enabled◆	◆Enabled◆	Enabled
Remote Telnet	◆Enabled◆	◆Enabled◆	◆Enabled◆	◆Enabled◆	◆Enabled◆
Community-SNMP	◆Enabled◆	◆Enabled◆	◆Enabled◆	◆Enabled◆	◆Enabled◆
OK CANCEL					

Figure 4-6 Local Security screen

Choosing a Switch Management Level

The Switch Management screen lets you:

- Choose between managing a port, the unit, or a VLAN
- Display screens for setting up the Switch
- Display a screen for managing the Switch Database
- Display screens for managing resilient links
- Display screens for managing STP
- Display screens showing statistics

From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed, as shown in Figure 4-7.

Management Level *Port / Unit / VLAN* If you choose *Port*, the screen is appears similar to Figure 4-7, and all options at the foot of the screen relate to an individual port. If you choose *Unit*, the screen appears similar to Figure 4-8, and all options relate to the Switch unit. If you choose *VLAN*, the screen appears similar to Figure 4-9, and all options relate to VLANs.

Port ID *1 / 2 / 3 ... 24 / 25 / 26* If you choose to manage the Switch at port level, enter the particular port number into this field before selecting the next screen. Ports 1–24 are the 10BASE-T ports, port 25 is the Plug-in Module port at the rear of the unit, and port 26 is the 100BASE-TX port.

Figure 4-7 Switch Management screen for Port level

Figure 4-8 Switch Management screen for Unit level

STP Use this button to display screens for managing Spanning Tree Protocol (STP) information for the level of management you have chosen (port or VLAN). Refer to “Spanning Tree Protocol” on page 5-10.



STP is not supported over Asynchronous Transfer Mode (ATM). If you specify that you want to manage the Plug-in Module port and the Switch has an ATM OC-3c Module installed, the STP button is not displayed.

SERVER This button displays a screen (the VLAN Server screen) that is not applicable for this device.

STATS Use this button to display statistics screens for the level of management you have chosen (port or unit). Refer to Chapter 6.

SDB Use this button to display the Unit Database View screen, which is used to manage the Switch Database. Refer to “The Database View” on page 4-17.

RESILIENCE Use this button to display resilient link management screens for the level of management you have chosen (port or unit). Refer to “Setting Up Resilient Links” on page 4-19.



You cannot set up resilient links if the Switch uses Spanning Tree (STP). Consequently, the RESILIENCE button is not displayed if STP is enabled.

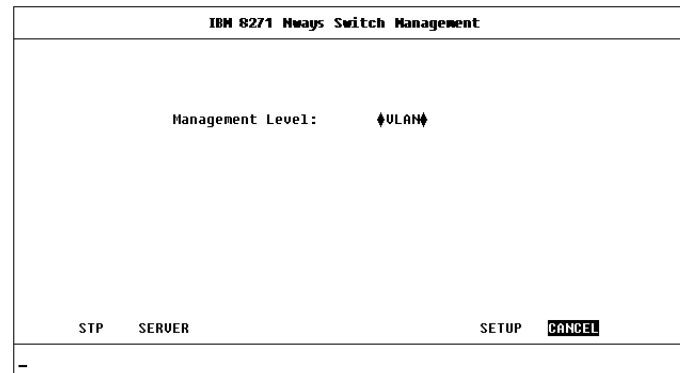


Figure 4-9 Switch Management screen for VLAN level

SETUP Use this button to display setup screens for the level of management you have chosen (port, unit or VLAN). For information about the Port Setup and Unit Setup screens, refer to “Setting Up the Switch Ports” and “Setting Up the Switch Unit” in this chapter. For information about the VLAN Setup screen, refer to “Setting Up VLANs on the Switch” on page 5-7.

Setting Up the Switch Unit

With the Switch Management screen displayed, choose the management level *Unit*, then select the SETUP button.

The Unit Setup screen is displayed, as shown in Figure 4-10. The screen shows the following:

Unit Name This read-only field shows the type of device.

sysName This field takes its name from the MIB II System Group object. You can edit the first 30 characters of this field to make the name more meaningful. This name is displayed on the Main Banner when you first access the VT100 screens, and is also accessible to an SNMP Network Manager.

Forwarding Mode *Fast Forward / Fragment Free / Store and Forward / Intelligent* This field allows you to set the forwarding mode for the Switch:

- *Fast Forward* — Frames are forwarded as soon as the destination address is received and verified. The forwarding delay, or latency, for all frames in this mode is just 40 μ s but with the lack of checking time, error frames are propagated onto the network.
- *Fragment Free* — A minimum of 512 bits of the received frame is buffered prior to the frame being forwarded. This ensures that collision fragments are not propagated through the network. The forwarding delay, or latency, for all frames in this mode is 64 μ s.

IBM 8271 Mways Switch Unit Setup	
Unit Name:	Desktop Switch
sysName (Max 30 chars):	[Desktop Switch]
Forwarding Mode:	♦Fast Forward ♦
Intelligent Forwarding:	N/A
PAGE:	♦Disable♦
ULAN Configuration Mode:	♦Port ♦
SDB Ageing Time (HH:MM):	[0:30]
Spanning Tree:	♦Disable♦
Duplex Mode:	♦Half Duplex ♦
Backbone Port:	[24]
Default RMON Host/Matrix:	♦Disable♦
Plug-in Module Type:	Not Fitted
Transceiver Module Type:	Not Fitted
Power Supply:	Internal
OK CANCEL	

Figure 4-10 Unit Setup screen

- *Store and Forward* — Received packets are buffered in their entirety prior to forwarding. This ensures that only good frames are passed to their destination. The forwarding delay for this mode varies between 64 μ s and 1.2ms, depending on frame length. In this mode the latency, measured as the time between receiving the last bit of the frame and transmitting the first bit, is 8 μ s.
- *Intelligent* — The Switch monitors the amount of error traffic on the network and changes the forwarding mode accordingly. If the Switch detects less than 18 errors a second, it operates in Fast Forward mode. If the Switch detects more than 18 errors a second, it operates in Store and Forward mode until the number of errors returns to zero.

Intelligent Forwarding *Fast Forward / Store and Forward* This read-only field shows the forwarding state if the Forwarding Mode is set to Intelligent.

PACE Enable / Disable This field allows you to enable or disable PACE (Priority Access Control Enabled) for all ports on the Switch. PACE allows multimedia traffic to be carried over standard Ethernet and Fast Ethernet LANs by providing two features:

- **Implicit Class of Service** — When multimedia traffic is transmitted, it is given a higher priority than other data and is therefore forwarded ahead of other data when it arrives at the Switch. The Implicit Class of Service feature minimizes latency through the Switch and protects the quality of multimedia traffic.
- **Interactive Access** — When two-way multimedia traffic passes over an Ethernet network, interference can occur because access to the bandwidth is unequally allocated to traffic in one direction. The Interactive Access feature allocates the available bandwidth equally in both directions, therefore increasing the quality of the traffic.



Interactive Access should be enabled only on ports that connect to a single endstation, switch, bridge, or router. You should disable Interactive Access on a port if it is connected to a repeater. Also, Interactive Access should be enabled at only one end of a link.

For more information about disabling Interactive Access for a port, refer to "Setting Up the Switch Ports" on page 4-12.

VLAN Configuration Mode Port / AutoSelect This field allows you to specify how ports on the Switch are placed in VLANs:

- **Port** — The ports use Port VLAN Mode, which means that they are manually placed in the required VLAN. This is the default mode.
- **AutoSelect** — This option is not applicable for this device. Do not select this option.

SDB Ageing Time This field allows you to specify the ageing time (hours:minutes) for all non-permanent entries in the Switch Database of the unit. You can set an ageing time in the range 0 minutes to 277 hours, with a default of 30 minutes. If you enter 0:00, ageing is turned off. For more information about ageing times, refer to "Setting Up the Switch Database (SDB)" on page 4-16.

Spanning Tree Enable / Disable This field allows you to enable or disable the Spanning Tree Protocol (STP) on the Switch. For more information about STP, refer to "Spanning Tree Protocol" on page 5-10.

Duplex Mode Half Duplex / Full Duplex on 100M Ports / Full Duplex on All Ports This field allows you to set the duplex mode for ports that have Unit Default specified in the Duplex Mode field of the Port Setup screen. The default setting is Half Duplex. For more information about Duplex Mode, refer to "Setting Up the Switch Ports" on page 4-12.

Backbone Port 1 / 2 / 3 ... 24 / 25 / 26 If all the ports on the Switch belong to VLAN 1 and use Port VLAN Mode, this field allows you to specify a backbone port for the Switch. In all other situations, the field is not displayed.



On a new or initialized Switch, all ports belong to VLAN 1 and use Port VLAN Mode.

For more information about VLANs, refer to “Virtual LANs (VLANs)” on page 5-1. For more information about backbone ports and their role in VLAN functionality, refer to “Assigning a Port to a VLAN When Using Port VLAN Mode” on page 5-9.

Default RMON Host/Matrix *Enable / Disable*

This field allows you to specify whether Hosts and Matrix RMON sessions are defined on the default VLAN. The default setting for this field is Disable. For more information about RMON sessions, refer to “RMON” on page 5-20.

Plug-in Module Type This read-only field displays the type of Plug-in Module fitted to the rear of the unit, or displays Not Fitted.

Transceiver Module Type This read-only field displays the type of Transceiver Module fitted to the rear of the unit, or displays Not Fitted.

Power Supply *Internal / External* This read-only field displays External if the Switch is receiving power from a Redundant Power System. In all other cases, this field displays Internal.

Setting Up the Switch Ports

With the Switch Management screen displayed, choose the management level *Port*. Choose the appropriate port, then select the SETUP button.

The Port Setup screen is displayed as shown in Figure 4-11.



If the port is an ATM OC-3c Module port, the ATM Port Setup screen is displayed. For more information, refer to the “IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User’s Guide”.

The screen shows the following:

Port ID This read-only field shows the ID of the port you have chosen to setup.

Media Type This read-only field shows the media type of the link connected to this port.

Port Speed This read-only field shows the speed and Duplex Mode of the link; HD indicates half duplex, and FD indicates full duplex.

Port State *Enable / Disable* This field allows you to enable or disable the port. To prevent unauthorized access, we recommend that you disable any unused ports.

Link State *Present / Not Available* This read-only field shows the state of the link:

- *Present* — The port is operating normally
- *Not Available* — The link has been lost

IBM 8271 Nways Switch Port Setup			
Port ID:	1	Media Type:	10BASE-T
Port Speed:	10Mbps HD	Port State:	Enable
Link State:	Present	Lost Links:	0
Refer to the User Guide before changing the settings of these parameters.			
Intelligent Flow Management:		Enable	
Security:		Disable	
Disable Interactive Access:		No	
ULT mode:		Disable	
Duplex Mode:		Unit Default	
ULAN Configuration mode:		Unit Default	
Broadcast Storm Control			
Rising Threshold%:	[20]	Action:	blip port / notify
Falling Threshold%:	[10]	Action:	none
		OK	CANCEL

Figure 4-11 Port Setup screen

Lost Links This read-only field shows the number of times the link has been lost since the Switch was last reset. If the number in this field is not zero, you should check your cables and replace any that may be damaged.



The Lost Links counter increments each time an endstation goes through a power-off/on cycle.

Intelligent Flow Management *Enable / Disable* This field allows you to enable or disable Intelligent Flow Management (IFM). IFM minimizes packet loss which can occur with conventional switches.



IFM is not available on a port that has full duplex enabled:

- *If the Duplex Mode field in this screen is set to Full Duplex, the Intelligent Flow Management field is not displayed*

- *In all other cases where the port has full duplex enabled, IFM has no effect*

Security Enable / Disable When Security is enabled, the port enters single address learning mode. The Switch removes any address currently stored in the Switch Database against the port. The Switch then learns the source address from the first packet it receives on the port since Security was enabled.

Once the first address is learnt, no other endstation is permitted to access the network through the port. If an endstation with a different address attempts to transmit packets onto the network through the port, the port is automatically disabled and a trap is generated. The port remains disabled until it is enabled from the Port Setup screen or via SNMP management.

A more comprehensive set of security features is available through SNMP network management.



Security is not available on backbone ports. If the port has been defined as a backbone port, the Security field is not displayed.

Disable Interactive Access Yes / No This field allows you to disable the Interactive Access feature of PACE (Priority Access Control Enabled) on the current port. You should disable Interactive Access on a port if:

- The port is connected to a device with Interactive Access enabled
- The port is configured as a backbone port and is connected to a repeater

For more information about the Interactive Access feature, refer to "Setting Up the Switch Unit" on page 4-9.

VLT Mode Enabled / Disabled This field allows you to specify whether the port is a VLT (Virtual LAN Trunk) port. A Virtual Lan Trunk (or VLT) is a Switch-to-Switch link which carries traffic for all the VLANs on each Switch. To create a VLT, the ports on both ends of the link must be VLT ports. For more information about VLTs, refer to "VLANs and the Switch" on page 5-3.



If the port uses AutoSelect VLAN Mode (refer to the VLAN Configuration Mode field), you cannot specify that the port is a VLT port.

Duplex Mode Half Duplex / Full Duplex / Unit Default This field allows you to specify the duplex mode of the port:

- **Full Duplex** — Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link. In addition, full duplex also supports 100BASE-FX cable runs of up to 2km. You should only enable full duplex on a link between the Switch and another device with full duplex support.



Full duplex is not supported on the Transceiver Module port.

- **Half Duplex** — You should use half duplex if the device at the other end of the link does not support full duplex.

- **Unit Default** — The duplex mode of the port is defined by the Duplex Mode field in the Unit Setup screen. This is the default setting.

VLAN Configuration Mode *Port / AutoSelect / Unit Default* This field is not applicable for this device. It should not be changed from the default setting, Unit Default.

Broadcast Storm Control The Switch automatically creates an alarm on each of its ports to monitor the level of broadcast traffic on each port. The Broadcast Storm Control fields allow you to specify thresholds for the level of broadcast traffic on a port, and specify an action to take place if the threshold is exceeded.

Rising Threshold% This field allows you to specify the percentage of broadcast traffic on the current port which triggers the alarm for the port. The default is 20%.

Falling Threshold% This field allows you to specify the percentage of broadcast traffic on the current port required to reset the alarm for the port. The falling threshold prevents the rising threshold events being triggered continuously. The default is 10%.

Rising Action *none / event / disable port / disable port/notify / blip / blip port/notify* Use this field to specify the action for the alarm to take when it reaches the rising threshold:

- *none* — no action takes place
- *event* — an SNMP trap is generated
- *disable port*— the port is disabled
- *disable port/notify* — the port is disabled and an SNMP trap is generated
- *blip* — the broadcast and multicast traffic on the port is blocked for 5 seconds
- *blip port/notify* — the broadcast and multicast traffic on the port is blocked for 5 seconds, and an SNMP trap is generated



If user defined appears as an option in the Rising Action field, an unrecognized action has been specified using a MIB browser. You cannot select this option.

Falling Action *none / event / enable / event + enable* Use this field to specify the action for the alarm to take when it reaches the falling threshold:

- *none* — no action takes place
- *event* — an SNMP trap is generated
- *enable* — the port is enabled
- *event + enable* — the port is enabled and an SNMP trap is generated



If user defined appears as an option in the Falling Action field, an unrecognized action has been specified using a MIB browser. You cannot select this option.



You should be aware of the following points when using Broadcast Storm Control:

- *The Switch takes 5–7 seconds to recognize that a broadcast storm is occurring.*
- *Broadcast Storm Control calculates the average broadcast bandwidth over the previous 20-second interval. The average is based on four samples taken at 5-second intervals.*
- *When the average value exceeds the rising threshold value, the rising action is triggered. The action is not triggered again until the average broadcast bandwidth falls below the falling threshold level.*

Setting Up the Switch Database (SDB)

The Switch maintains a database of device addresses that it receives on its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered. The database holds up to a maximum of 104 entries (four entries per port); each entry consists of the MAC address of the device and an identifier for the port on which it was received.

Entries are added into the Switch Database in two ways:

- The Switch can learn entries. That is, the unit updates the SDB with the source MAC address, and the port identifier on which the source MAC address is seen. Addresses are not learned on the backbone port. Learning is affected by security — refer to the description for the Security field on page 4-13.
- The system administrator can enter and update entries using a MIB browser, an SNMP Network Manager or the Switch Database screen described in the following sections.

There are three types of entries in the SDB:

- **Ageing entries** — Initially, all entries in the database are ageing entries. Entries in the database are removed (aged out) if, after a period of time (ageing time), the device has not transmitted. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Ageing entries are deleted from the database if the Switch is reset or a power-off/on cycle occurs. For more information about setting an ageing time, refer to “Setting Up the Switch Unit” on page 4-9.
- **Non-ageing entries** — If the ageing time is set to 0:00, all ageing entries in the database are defined as non-ageing entries. This means that they do not age, but they are still deleted if the Switch is reset or a power-off/on cycle occurs. For more information about setting an ageing time, refer to “Setting Up the Switch Unit” on page 4-9.
- **Permanent entries** — Permanent entries do not age, and they are retained in the database if the Switch is reset or a power-off/on cycle occurs.

The Database View

The Unit Database View screen, as shown in Figure 4-12, allows you to view and configure the Switch Database. To access this screen, display the Switch Management screen, choose the management level *Unit*, then select the SDB button.

The Unit Database View screen shows the following:

Database Entries This read-only field shows the number of entries currently in the SDB. The database holds a maximum of 104 addresses (four entries per port).

MAC Address If you highlight an entry in the list-box and press [Return], this field shows the MAC address for the entry.

Port Number If you highlight an entry in the list-box, this field shows the port identifier for the entry.

Permanent *Yes / No* This field allows you to specify that the current entry is permanent. Refer to the previous section “Setting Up the Switch Database (SDB)” for a description of permanent and ageing entries.

A listbox containing three fields:

Port The port ID for the entry.

MAC Address The MAC address for the port currently stored in the database.

Permanent *Yes / No* Shows Yes if this entry is permanent, or No if this entry is ageing or non-ageing.

IBM 8271 Hways Switch Unit Database View			
	Port	MAC Address	Permanent
Database Entries: 19	10	08004e0849d1	No
	10	00805Fd23235	No
	10	080002057253	No
	10	08004e086330	No
	10	08004e0855ca	No
	10	08004e053cdb	No
	10	08004e105377	No
MAC Address: []	10	0020aF436438	No
Port Number: []	10	08004e0a4aF2	No
Permanent: <input type="radio"/> No <input type="radio"/>	10	08004e0747c9	No
	10	08004e0c9d1F	No
	10	08004e0bcbc0	No
<input type="button" value="FIND"/> <input type="button" value="REFRESH"/> <input type="button" value="INSERT"/> <input type="button" value="DELETE"/> <input type="button" value="CANCEL"/>			

Figure 4-12 Unit Database View screen

FIND This button lets you locate an entry in the database. Refer to “Searching the Switch Database” on page 4-18.

REFRESH This button refreshes the database so that it displays the latest information.

INSERT This button lets you insert an entry into the database.

DELETE This button allows you to delete entries from the database.

Searching the Switch Database

You can search the switch database in two ways: by MAC address or port number.

By MAC Address

To locate the port number against which a particular MAC address is entered in the SDB:

- 1 In the MAC Address field, type in the MAC address you are trying to locate.
- 2 Select FIND. The port ID is displayed in the Port Number field and the entry in the listbox is highlighted with an asterisk (*).

By Port

To locate the MAC addresses entered against a particular port ID in the SDB:

- 1 Clear the MAC Address field by moving into the field and pressing [Space].
- 2 In the Port Number field, enter the port ID for which you want MAC addresses displayed.
- 3 Select FIND. The listbox will show entries in the database for that port only.

Adding an Entry into the SDB

- 1 In the MAC Address field, type in the MAC address of the device.
- 2 In the Port field, type in the port identifier for this device.
- 3 Select whether the entry is permanent or not by specifying *Yes* or *No* in the Permanent field.
- 4 Select INSERT.

Deleting an Entry from the SDB

- 1 In the listbox, highlight the entry you want to delete and press [Return], or type the MAC address into the MAC Address field.
- 2 Select DELETE.

Specifying that an Entry is Permanent

- 1 In the listbox, highlight the entry you want to make permanent and press [Return], or type the MAC address into the MAC Address field.
- 2 In the Permanent field, specify *Yes*.
- 3 Select INSERT.

Setting Up Resilient Links

You can configure a Switch to provide resilient links to another device so that network disruption is minimized if a link fails. A *resilient link pair* consists of a main link and a standby link. You define a resilient link pair by specifying the main port and standby port at one end of the pair.

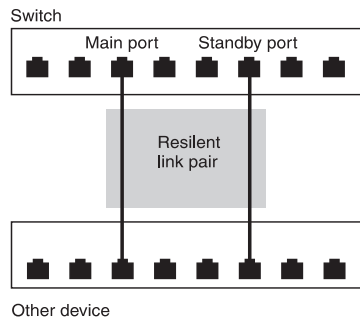


Figure 4-13 Resilient link pair

Under normal network operating conditions, the main link carries your data. The Receive Idle signal of a fiber link or the Test Pulse on an Ethernet twisted pair link is continually monitored by the Switch. If a signal loss is detected, the Switch immediately enables the standby port so that it carries the data. In addition, the main port is disabled.

If a main link has a higher bandwidth than its standby link, traffic is automatically switched back to the main link provided no loss of link is detected for two minutes. Otherwise, you need to manually switch traffic back to the main link.

When setting up resilient links, you should note the following:

- Up to 13 resilient link pairs can be configured on an 8271 Model 524 Switch.
- Resilient links cannot be set up if Spanning Tree (STP) is enabled on the Switch.
- Resilient links can only be set up on fiber or twisted pair links. The main and standby links in the same pair, however, can use any combination of these media.
- A resilient link pair can only be set up if:
 - The ports belong to the same VLAN.
 - The ports have an identical security setting.
 - Neither of the ports forms part of another resilient link pair.
- A backbone port can be configured as a main port in a resilient link pair. If a resilient backbone port fails, the standby port is immediately configured as a backbone port before it is enabled. A backbone port cannot be configured as a standby port.
- If the main port is a Virtual LAN Trunk (VLT) port, the standby port must also be a VLT port.
- A resilient link pair must be defined at only one end of the connection.
- You cannot disable any port that is part of a resilient link pair.

Configuring Resilient Links

With the Switch Management screen displayed, choose the port to be the main port in the resilient link pair, then select the RESILIENCE button.

The Port Resilience screen is displayed as shown in Figure 4-14. This screen allows you to set up, edit and delete resilient link pairs.

The screen shows the following:

Main Port ID This read-only field shows the ID of the main port.

Media Type *Twisted Pair / Fiber* This read-only field shows the media type connected to the main port.

Link State *Available / Not Available / Not Present* This read-only field shows the connection state of the main port:

- *Available* — The port is operating normally
- *Not Available* — The resilient link pair is disabled
- *Not Present* — The port is not present in the current hardware

Standby Port ID This field shows the current standby port ID and allows you to enter a new port ID. The standby port must be in the same VLAN as the main port.

Media Type *Twisted Pair / Fiber* This read-only field shows the standby port media type.

IBM 8271 Nways Switch Port Resilience

<p>Main Port ID: 1 Media Type: Twisted Pair Link State: Available</p> <p>Standby Port ID: [2] Media Type: Twisted Pair Link State: Not Available</p> <p>Pair State: Active Active Port: ↓Main Pair Enable: ↓Enabled</p>	<p style="text-align: center;">Standby Links Available</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th style="text-align: center;">Port ID</th> </tr> </thead> <tbody> <tr><td style="text-align: center;">2</td></tr> <tr><td style="text-align: center;">3</td></tr> <tr><td style="text-align: center;">4</td></tr> <tr><td style="text-align: center;">5</td></tr> <tr><td style="text-align: center;">6</td></tr> <tr><td style="text-align: center;">7</td></tr> <tr><td style="text-align: center;">8</td></tr> <tr><td style="text-align: center;">9</td></tr> <tr><td style="text-align: center;">10</td></tr> <tr><td style="text-align: center;">11</td></tr> </tbody> </table>	Port ID	2	3	4	5	6	7	8	9	10	11
Port ID												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												

APPLY DELETE **CANCEL**

Figure 4-14 Port Resilience screen

Link State *Available / Not Available / Not Present* This read-only field shows the connection state of the standby port:

- *Available* — The port is operating normally
- *Not Available* — The resilient link pair is disabled
- *Not Present* — The port is not present in the current hardware

Standby Links Available This listbox shows the ports that you can configure as standby.

Pair State *Active / Both Failed / Unknown / Not Available* This read-only field shows the current operating state of the resilient link pair:

- *Active* — The resilient link pair is enabled and operating normally with both main and standby port capable of carrying traffic.

- *Both Failed* — Although the resilient link pair is correctly configured, both links have failed. This could be due to loose connections or cable damage.
- *Unknown* — The network configuration has changed and the resilient link pair no longer conforms to the rules.
- *Not Available* — The resilient link pair is disabled.

Active Port *Main / Standby* If a main link does *not* have a higher bandwidth than its standby link, traffic is *not* automatically switched back to the main link when it recovers. Use this field to manually switch traffic back to the main link.

Pair Enable *Enabled / Disabled* Use this field to enable or disable the resilient link pair. Before you disable the resilient link pair, you must remove cabling from the ports to avoid creating loops in your network configuration.

Creating a Resilient Link Pair

- 1 Ensure that the port nominated as the standby port is not physically connected to the unit.
- 2 Ensure both ports have an identical port security mode configuration and that they are members of the same VLAN.
- 3 At the Switch Management screen, select the port to be configured as the main port in the link. Select the RESILIENCE button at the foot of the screen.
- 4 Select the standby port from the Standby Links Available listbox or enter the port ID in the Standby Port ID field.
- 5 Enable the pair in the Pair Enabled field. Select APPLY.
- 6 Connect the cabling for the standby port.

Deleting a Resilient Link Pair

To delete the resilient link set up on the port, select the DELETE button at the foot of the screen. The Port Resilience screen closes and the Switch Management screen is displayed.

Viewing the Resilient Links Setup

With the Switch Management screen displayed, choose the management level *Unit* and select the RESILIENCE button.

The Unit Resilience Summary screen is displayed as shown in Figure 4-15. This screen shows the current resilient link configuration for the unit, and allows you to access the Port Resilience screen for resilient link pairs.

The following information is displayed:

MAIN Port This read-only field displays the ID of the port configured as the main port for this resilient link pair.

STANDBY Port This read-only field displays the ID of the port configured as the standby port for this resilient link pair.

Pair State *Active / Both Failed / Unknown / Not Available* This read-only field displays the current state of this resilient link pair:

- *Active* — The resilient link pair is enabled and operating normally with both main and standby port capable of carrying traffic.
- *Both Failed* — Although the resilient link pair is correctly configured, both links have failed. Check for any loose connections or cable damage.
- *Unknown* — The network configuration has changed and the resilient link pair no longer conforms to the rules.
- *Not Available* — This resilient link pair is disabled.

IBM 8271 Nways Switch Unit Resilience Summary				
---MAIN---	--STANDBY--	Pair	Active	Pair
Port	Port	State	Port	Enable
01	02	Active	Main	Enabled
OK CANCEL				

Figure 4-15 Unit Resilience Summary screen

Active Port *Main / Standby / Both Failed* This read-only field displays which port in the resilient link pair is currently carrying traffic:

- *Main* — The pair is operating in its normal state with the main port carrying traffic.
- *Standby* — The main port has failed and the standby port is carrying the traffic. You should rectify the fault as soon as possible. If a main port has a higher bandwidth than the standby port, traffic is automatically switched back provided no loss of link is detected for 2 minutes. Otherwise, switch the traffic back manually by setting the Active Port field in the Port Resilience screen (described on page 4-20) to Main.
- *Both Failed* — Both ports of the resilient link pair have failed. This could be due to loose connections or cable damage.

Pair Enable *Enabled / Disabled* This read-only field displays whether the resilient link pair is currently enabled or disabled. You enable or disable a resilient link pair using the Port Resilience screen described in “Configuring Resilient Links” on page 4-20.

OK This button allows you to access the Port Resilience screen for the current resilient link pair.

Setting Up Traps

Traps are messages sent across the network to an SNMP Network Manager. They alert the network administrator to faults or changes at the Switch device.



Your Network Manager may automatically set up traps in the Switch Trap Table. Check the documentation accompanying your network management software.

To access the Trap Setup screen, select the SETUP TRAPS button from the Switch Management Setup screen (described in Chapter 3). The Trap Setup screen is shown in Figure 4-16.

The screen shows the following:

IP or IPX Address This field allows you to enter the IP or IPX address of the remote network management stations to which traps should be sent.

Community String This field allows you to enter community strings for each remote Network Manager, allowing a very simple method of authentication between the Switch and the remote Network Manager. The text string can be of 32 characters or less. If you want a Network Manager to receive traps generated by the device, you must enter the community string of the Network Manager into the trap table. The default community string is *public*.

IP or IPX Address:	Community String:	Throttle: (milli-secs)
[]	[public]	[100]
[]	[public]	[100]
[]	[public]	[100]
[]	[public]	[100]
[]	[public]	[100]
[]	[public]	[100]
[]	[public]	[100]
[]	[public]	[100]

OK CANCEL

Figure 4-16 Trap Setup screen

Throttle This field allows you to specify a throttle delay value for each remote Network Manager. Throttle delays are time periods placed between packets to prevent a remote Network Manager receiving too many traps at once. The unit of throttle is one thousandth of a second. The default value is 100, which gives a delay of one tenth of a second between each packet transmission.

Setting Up the Console Port

From the Switch Management Setup screen, described in Chapter 3, select the CONSOLE PORT button. The Console Port Setup screen is displayed as shown in Figure 4-17.

If you change any of the console port parameters, you terminate any existing sessions using the console port when you exit the screen. Ensure that the connected equipment's console port parameters are set to match the new configuration. This allows you to continue to access the management facility from the equipment after you change the console port parameters.

The screen shows the following:

Connection Type *Local / Remote* This field allows you to select the type of remote connection. Select *Remote* if you want to manage the Switch through a modem; DCD Control and DSR Control will be enabled. For all other cases, this field should be set to *Local*.

DCD Control *Enabled / Disabled* This field is only applicable to local connection types. It determines if DCD is required for a local connection, and whether the connection is closed if DCD is removed. Refer to your terminal or modem documentation if you are unsure of the correct setting.

IBM 8271 Hways Switch Console Port Setup	
Connection Type:	Local
DCD Control:	Disabled
DSR Control:	Disabled
Flow Control:	NONE
Auto Config:	Enabled
Speed:	9600
Char Size:	8
Parity:	NONE
Stop Bit:	1
OK CANCEL	

Figure 4-17 Console Port Setup screen

DSR Control *Enabled / Disabled* This field is only applicable to local connection types. It determines if DSR is required for a local connection, and whether the connection is closed if DSR is removed. Refer to your terminal or modem user documentation if you are unsure of the correct setting.

Flow Control *XON/XOFF / NONE / RTS-CTS Unidirectional / RTS-CTS Bidirectional* This field allows you to select the correct flow control option for your terminal or modem. Refer to your terminal or modem documentation if you are unsure of the correct setting.

Auto Config *Enabled / Disabled* The Switch can auto-configure the line speed (baud rate) of the console port to work with your VT100 terminal. This field allows you to specify whether auto-configuration is enabled.

Speed *1200 / 2400 / 4800 / 9600 / 19200*

This field allows you to select the correct line speed (baud rate) for your terminal or modem. If you have enabled auto-configuration, the line speed is set automatically.

Char Size *8* This read-only field displays the character bit (data bit) size for the Switch. You should set your terminal to the same value.

Parity *NONE* This read-only field displays the parity setting for the Switch. You should configure your terminal to the same setting.

Stop Bit *1* This read-only field displays the stop bit setting for the Switch. You should configure your terminal to the same setting.

Resetting the Switch

If you suspect a problem with the Switch, you can reset it.

- 1 From the Main Menu, select the RESET option.

The Reset screen is displayed, as shown in Figure 4-18.

- 2 Select OK.

Resetting the Switch in this way is similar to performing a power-off/on cycle. No setup information is lost.



ATTENTION: *Performing a reset may cause some of the data being transmitted at that moment to be lost.*

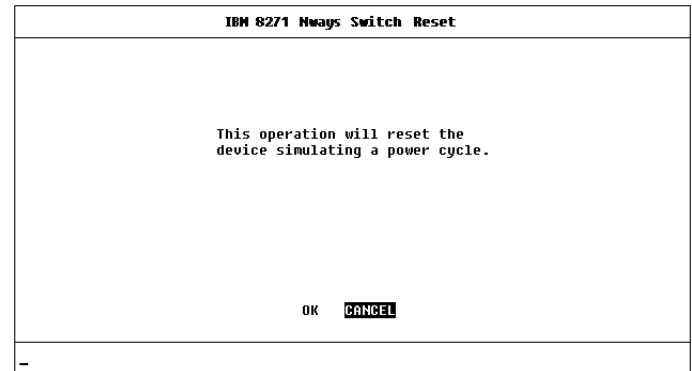


Figure 4-18 Reset screen

Initializing the Switch

This screen allows you to perform a reset as described in the previous section, and in addition, returns non-volatile data stored on the unit to its factory defaults (shown on page 1-12). Note that the IP address is not cleared. You should only initialize the Switch if:

- The configuration of the device no longer suits your network
- Other efforts to solve problems have not succeeded

To initialize the Switch:

- 1 From the Main Menu, select the INITIALIZE option.

The Initialize screen appears as shown in Figure 4-19.

- 2 Select OK.



ATTENTION: Use the Initialize option with great care. The Switch configuration is cleared from memory and cannot be recovered. After initialization, all user information is lost and only default users are available. All ports are set to their default values, and are therefore enabled and available to all users.

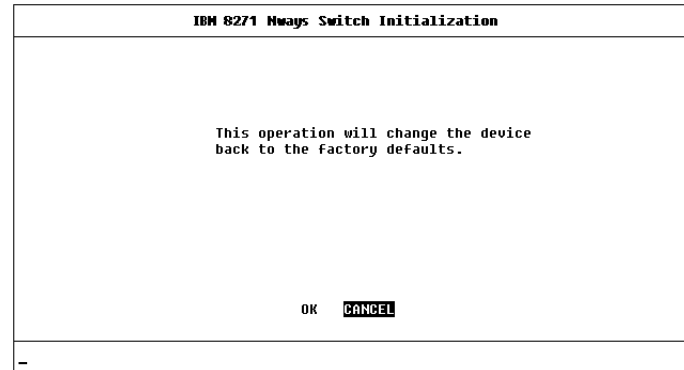


Figure 4-19 Initialize screen

When initializing the Switch, take particular note of the following:

- Network loops occur if you have set up resilient links. Before initializing the Switch, ensure you have disconnected the cabling for all your standby links.
- VLT ports fail and you are not able to manage the Switch if your management station communicates via the VLT. To avoid this:
 - a Remove the VLT configuration from both ends of the VLT link before you initialize the Switch. Note that the port furthest from your management station should have its VLT configuration removed first.
 - b Reconfigure the VLT once the initialization is complete.

Upgrading Software

When IBM issues a new version of the software image for the Switch, you can obtain it from IBM's electronic support services, as described in "Electronic Support" in Appendix F.



For upgrading the ATM OC-3c Module software, refer to the "IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User's Guide".

You use the Software Upgrade screen to download new software images. The protocol used for downloading software images is TFTP running over UDP/IP or IPX.



ATTENTION: Before attempting to download, note:

- The download only works over the network; it does not work through the console port.
- The download does not work over a Virtual LAN Trunk (VLT) if you have a Boot software version lower than version 2.0.
- The download does not work over an ATM link.



If a software download over IPX fails, enter the MAC or Ethernet address of your server into the Switch Database via the Unit Database View screen and then attempt the download again. Refer to "Searching the Switch Database" on page 4-18.

To upgrade Switch management software:

- 1 From the Main Menu, select SOFTWARE UPGRADE. The Software Upgrade screen is displayed, as shown in Figure 4-20.

IBM 8271 Nways Switch Software Upgrade		
Destination:	◆Switch	◆
File Name:	[3C16900.slx]
Server Address:	[]
This operation will reset the device once the upgrade has been completed.		
IP address format	d.d.d.d	
IPX address format	AABBCCDD:AABBCCDDEEFF	
OK CANCEL		

Figure 4-20 Software Upgrade screen

- 2 From the Destination field, select Switch (this is the default).
- 3 In the File Name field, enter the name of the file that contains the software image to be downloaded to the Switch.

You must place the image file where it is accessible to the TFTP load request. Check with your system administrator if you are unsure of where to place the image file.

- 4 In the Server Address field, enter the IP or IPX address of the server containing the software image to be loaded.
- 5 Select OK.

During the download, the MGMT LED flashes green and the screen is locked. When the download is complete, the Switch is reset.





ADVANCED MANAGEMENT

Virtual LANs (VLANs)

Setting up Virtual Local Area Networks (VLANs) on the Switch provides you with less time-consuming network administration and more efficient network operation.

The following sections explain more about the concept of VLANs and explain how they can be implemented on the Switch.

What are VLANs?

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 LAN segments are not restricted by the hardware which physically connects them; the segments are defined by flexible user groups that you create using software.

With VLANs, you can define your network according to:

- **Departmental groups** — For example, you can have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups** — For example, you can have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups** — For example, you can have one VLAN for users of e-mail, and another VLAN for users of multimedia.

Benefits of VLANs

Implementing VLANs on your network 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 endstation must be updated manually.

With a VLAN setup, if an endstation 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 which 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 which need to communicate with each other.

How VLANs Provide Extra Security

Devices within each VLAN can only communicate 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.

An Example

Figure 5-1 shows a network configured with three VLANs — one for each of the departments that access the network. 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.

Specific configurations using the Switch are shown later in this chapter.

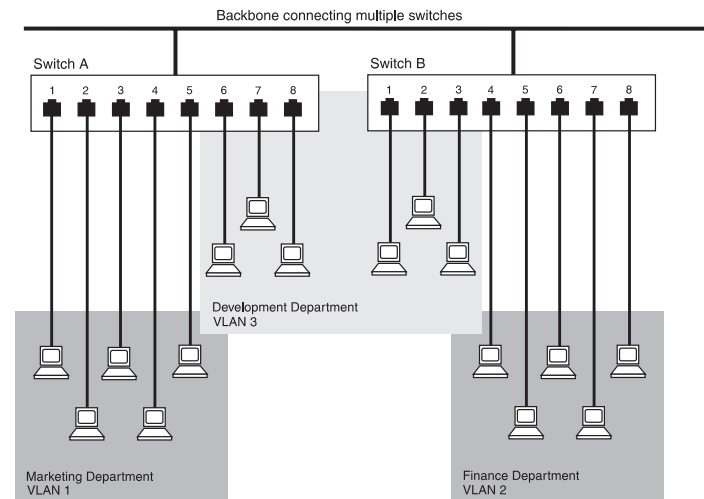


Figure 5-1 The concept of VLANs

VLANs and the Switch

The Switch supports VLANs which consist of a set of switch ports. Each switch port can only belong to one VLAN at a time, regardless of the device to which it is attached.

Each Switch can support up to 16 VLANs. However, you can have more than 16 VLANs in your entire network by connecting the 16 Switch VLANs to other VLANs using a router.

The Default VLAN and Moving Ports From the Default VLAN

On each Switch, VLAN 1 is the Default VLAN of the Switch; it has two properties:

- It contains all the ports on a new or initialized Switch
- It is the only VLAN which allows an SNMP Network Manager to access the management agent of the unit

By default, if a device is attached to a port in the Default VLAN and you want to move the device into another VLAN, you need to use the VLAN Setup screen to place the port in that VLAN. For more information about the VLAN Setup screen, refer to “Setting Up VLANs on the Switch” on page 5-7.

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. Communication between VLANs can only take place 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.

Connecting Common VLANs Between Switch Units

If you want to connect the VLANs on the 8271 Model 524 Switch with the same VLANs on another Switch unit, you can set up one link per VLAN. Alternatively, you can set up a single link for all the VLANs by creating a *Virtual LAN Trunk (VLT)*. A VLT is a Switch-to-Switch link which carries traffic for all the VLANs on each Switch. To set up a VLT, you configure the port at each end of the link.



VLTs can only be used for links between IBM 8271 Nways Ethernet Switch units. You cannot use VLTs for Switch-router links.

If you specify that a port on one VLAN is a VLT port, that port carries traffic for all the VLANs on the Switch. If you then disable the VLT function on that port, the port only carries traffic for the Default VLAN (VLAN 1).

Using Non-routable Protocols

If you are running non-routable protocols on your network (for example, DEC LAT or NET BIOS), 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, we recommend that you configure each network adapter with a unique MAC address.

Extending VLANs into an ATM Network

If the Switch has an ATM OC-3c Module installed, you can extend the VLANs you have defined in your existing network into an ATM network. For more information, refer to the "*IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User's Guide*".

VLAN Configurations

Example 1

The example shown in Figure 5-2 illustrates a simple VLAN configuration with a single Switch whose ports are divided between two VLANs. VLAN 1 is able to talk to VLAN 2 using the connection between each VLAN and the router.

To set up this configuration:

- 1 Use the VT100 screens:
 - a Place ports 1–6 and 13–18 in VLAN 1.
 - b Place ports 7–12 and 19–24 in VLAN 2.
- 2 Connect a port in VLAN 1 to the router.
- 3 Connect a port in VLAN 2 to the router.

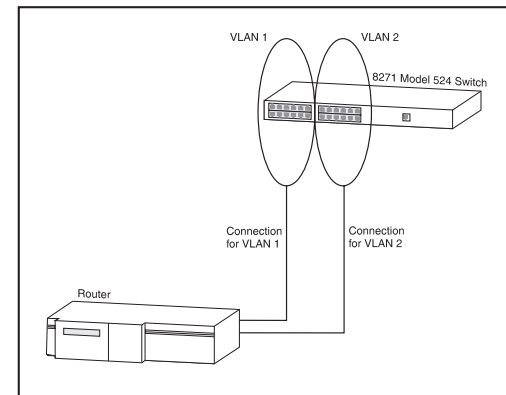


Figure 5-2 VLAN configuration with a single Switch unit

Example 2

The example shown in Figure 5-3 illustrates two VLANs spanning two Switch units. VLAN 1 is able to talk to VLAN 2 using the connection between each VLAN and the router. Ports within the same VLAN but on different Switches communicate using the VLT.

To set up this configuration:

- 1 Use the VT100 screens to:
 - a Place ports 1–6 and 13–18 of both Switch units in VLAN 1.
 - b Place ports 7–12 and 19–24 of both Switch units in VLAN 2.
- 2 Connect port 26 of the higher Switch to Server 1.
- 3 Connect port 26 of the lower Switch to Server 2.
- 4 Use the VT100 screens to:
 - a Place port 26 of the higher Switch in VLAN 2.
 - b Place port 26 of the lower Switch in VLAN 1.
- 5 Connect a port on the higher Switch to a port in the lower Switch.
- 6 Use the VT100 screens to specify that the Switch-to-Switch port on the higher Switch is a backbone port and a VLT port.
- 7 Use the VT100 screens to specify that the Switch-to-Switch port on the lower Switch is a VLT port.

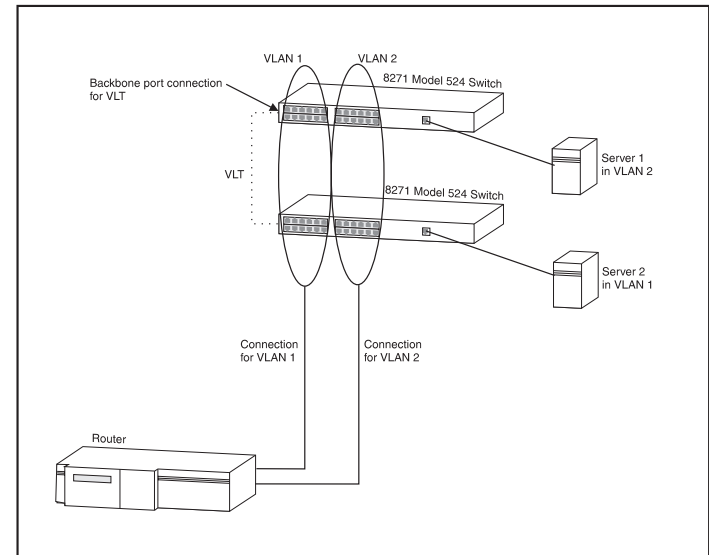


Figure 5-3 VLAN configuration with two Switch units

- 8 Connect a VLAN 1 port on the lower Switch to the router.
- 9 Connect a VLAN 2 port on the lower Switch to the router.

Example 3

The example shown in Figure 5-4 illustrates two VLANs spanning three 8271 Model 524 Switch units and a basement 8271 Model 712 Switch with a Plug-in Module. Each 8271 Model 524 Switch connects into the basement Switch using a VLT. The attached router allows the two VLANs to communicate with each other.

To set up this configuration:

- 1 Use the VT100 screens to:
 - a Place ports 1–6 and 13–18 of all the 8271 Model 524 Switch units in VLAN 1.
 - b Place ports 7–12 and 19–24 of all the 8271 Model 524 Switch units in VLAN 2.
- 2 Connect a port on each 8271 Model 524 Switch to a port in the 8271 Model 712 Switch.
- 3 Use the VT100 screens to:
 - a Specify that each 8271 Model 524 Switch port connected to the 8271 Model 712 Switch is a backbone port.
 - b Specify that each 8271 Model 524 Switch port connected to the 8271 Model 712 Switch is a VLT port.
 - c Specify that each 8271 Model 712 Switch port connected to a 8271 Model 524 Switch is a VLT port.
- 4 Connect port 1 of the 8271 Model 712 Switch to Server 1.
- 5 Connect port 2 of the 8271 Model 712 Switch to Server 2.

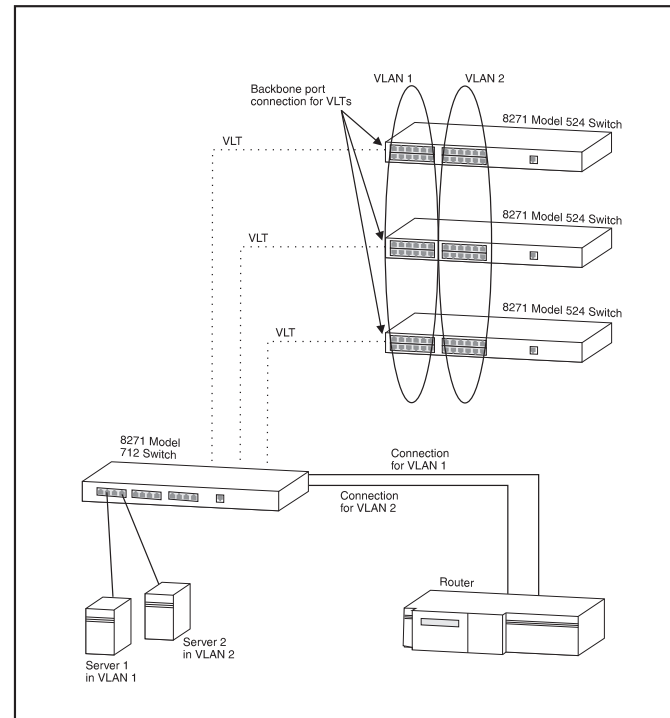


Figure 5-4 VLAN configuration with an 8271 Model 712 Switch

- 6 Use the VT100 screens to place port 1 of the 8271 Model 712 Switch in VLAN 1, and place port 2 of the 8271 Model 712 Switch in VLAN 2.
- 7 Connect two spare ports on the 8271 Model 712 Switch to the router.
- 8 Use the VT100 screens to specify that one 8271 Model 712 Switch port connected to the router is placed in VLAN 1, and the other is placed in VLAN 2.

Setting Up VLANs on the Switch

The VLAN Setup screen allows you to:

- Assign ports to VLANs, if those ports use Port VLAN Mode
- Define a backbone port for each VLAN
- View VLAN setup information for the Switch

To access the VLAN Setup screen:

- 1 From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
- 2 In the Management Level field, choose *VLAN*.
- 3 Choose the SETUP button. The VLAN Setup screen is displayed, as shown in Figure 5-5.

The screen shows the following:

A listbox containing three fields:

Port This field allows you to select the ID of the port that you want to set up.

Type *VLT / Bp / Standby / ATM*

This field displays information about the setup of the port:

- *VLT* — The port is a VLT port. A Virtual LAN Trunk (or VLT) is a Switch-to-Switch link which carries traffic for all the VLANs on each Switch. For more information about VLTs in general, refer to “VLANs and the Switch” on page 5-3. To specify that a port is part of a VLT, refer to “Setting Up the Switch Ports” on page 4-12.

The screenshot shows the 'IBM 8271 Nways Switch VLAN Setup' window. It contains a table with columns 'Port', 'Type', and 'VLAN Membership'. The 'VLAN Membership' column has 16 sub-columns numbered 1 through 16. Below the table are three fields: 'Port ID: 5', 'VLAN ID: [1]', and 'Backbone Port: No'. At the bottom are 'APPLY' and 'CANCEL' buttons.

Port	Type	VLAN Membership															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	ULT	1															
2			1														
3	Standby(2)																
4				1													
5					1												
6	AutoSelect					1											
7							1										
8	AutoSelect							1									
9									1								
10										1							

Port ID: 5 VLAN ID: [1] Backbone Port: No

APPLY CANCEL

Figure 5-5 VLAN Setup screen

- *Bp* — The port is the backbone port for the VLAN(s) specified in the VLAN Membership field.
A backbone port is used to connect each VLAN to the backbone of your network. Addresses received on the port are not stored in the Switch Database. Frames with unknown addresses received by the Switch are forwarded to the port.
- *Standby* — The port is the standby port of a resilient link pair. The main port of the pair is displayed in brackets. For more information about resilient links, refer to “Setting Up Resilient Links” on page 4-19.
- *ATM* — The port is an ATM OC-3c Module port. For more information, refer to the “IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User’s Guide”.

VLAN Membership This field displays the ID of the VLAN(s) to which the port belongs.

Port ID 1 / 2 / 3 ... 24 / 25 / 26 This field displays the ID of the port currently selected in the listbox.

VLAN ID 1 / 2 / 3 ... 16 If the port specified in the Port ID field uses Port VLAN Mode, this field allows you to enter the ID of the VLAN to which the port is to be assigned. By default, all ports use Port VLAN Mode and belong to the Default VLAN (VLAN 1). This field is not displayed if the port is a VLT port.



If you are using the Spanning Tree Protocol, you cannot use VLAN 16. This VLAN is used internally by the Switch and is therefore not available.

Backbone Port Yes / No If the port specified in the Port ID field uses Port VLAN Mode, this field allows you to specify whether the port is a backbone port. If the port is the standby port of a resilient link pair, you cannot specify that it is a backbone port.

Each VLAN can have one backbone port. By default, all ports belong to the Default VLAN (VLAN 1); because of this, an unconfigured Switch unit can only have one backbone port.

If you specify that an ATM OC-3c Module port is a backbone port, the port becomes a backbone port for all the VLANs on which it is active. It cannot be the backbone port for one VLAN and a standard port for another.



If you fit a Plug-in Module into a Switch with no specified backbone ports, the Module automatically becomes the backbone port for the Default VLAN when you power-up or initialize the Switch. If a Switch has no Plug-in Module, but you fit a Transceiver Module, this becomes the backbone port for the Default VLAN when you power-up or initialize the Switch.

APPLY This button applies any changes to the VLAN database.

ATM LEC Setup If the port is an ATM OC-3c Module port, this button allows you access the VLAN LEC Setup screen for extending your VLANs into an ATM network. For more information, refer to the "IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User's Guide".

Assigning a Port to a VLAN When Using Port VLAN Mode

- 1 In the Port ID field, enter the ID of the required port.
- 2 In the VLAN ID field, enter the ID of the required VLAN.
- 3 Select APPLY.



ATTENTION: Initially, all Switch ports belong to the Default VLAN (VLAN 1). This VLAN is the only one that allows an SNMP Network Manager to access the management agent of the unit. If you remove all ports from VLAN 1, then an SNMP Network Manager cannot manage the Switch.

Specifying a Backbone Port

- 1 In the Port ID field, enter the ID of the required port.
- 2 In the VLAN ID field, enter the ID of the required VLAN.
- 3 In the Select Port Type field, select Backbone Port.
- 4 Select APPLY.

Specifying that a Port is a VLT Port

To specify that a port is a VLT port, refer to “Setting Up the Switch Ports” on page 4-12.



To create a VLT link, the ports at both ends of the link must be VLT ports.

Spanning Tree Protocol

Using the Spanning Tree Protocol (STP) functionality of your Switch makes your network more fault tolerant.

The following sections explain more about STP and the STP features supported by the Switch.



STP is not currently supported over an Asynchronous Transfer Mode (ATM) network. Therefore, if you have an ATM OC-3c Module installed in your Switch, it does not join the STP system.

What is STP?



STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP more effectively, the 8271 Model 524 Switch will be defined 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

As an example, Figure 5-6 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 which cause the network to overload; however, STP allows you to have this configuration because it detects duplicate paths and immediately prevents, or *blocks*, one of them from forwarding traffic.

Figure 5-7 shows the result of enabling STP on the bridges in the configuration. The STP system has decided that traffic from LAN segment 2 to LAN segment 1 can only flow through Bridges C and A.

If the link through Bridge C fails, as shown in Figure 5-8, the STP system reconfigures the network so that traffic from segment 2 flows through Bridge B.

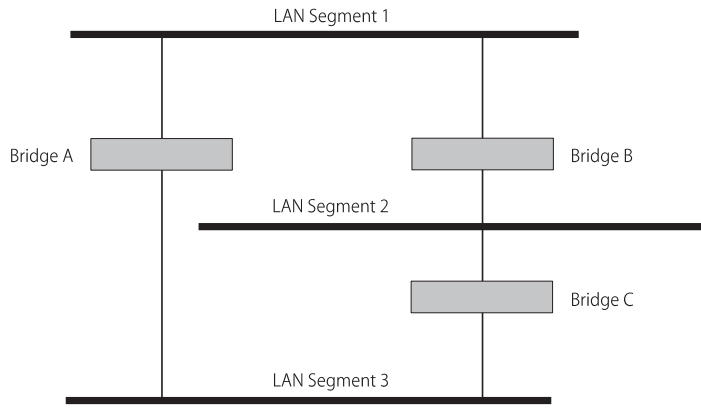


Figure 5-6 A network configuration that creates loops

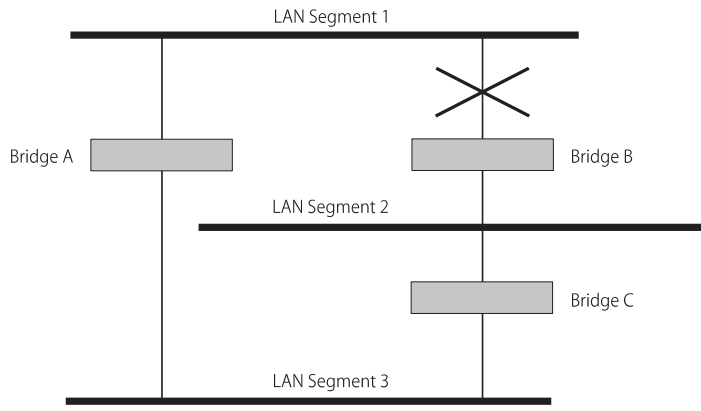


Figure 5-7 Traffic flowing through Bridges C and A

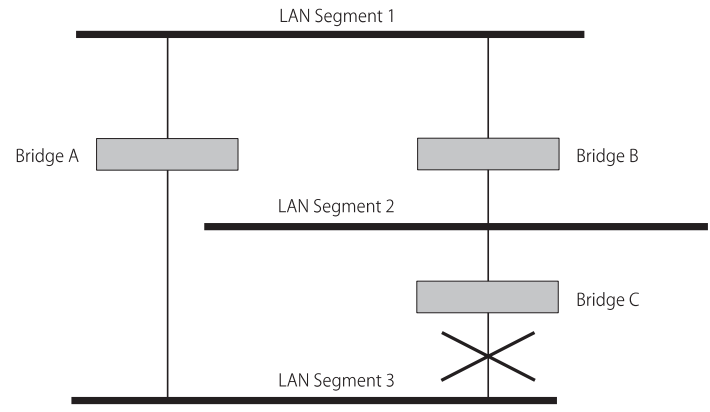


Figure 5-8 Traffic flowing through Bridge B

How STP Works

STP Initialization

Initially, the STP system requires the following 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 it 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 which 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.

Table 5-1 shows the default path costs for the Switch.

Table 5-1 Default path costs

Port Type	Duplex	Cost
100BASE-TX / 100BASE-FX (VLT)	Full	5
	Half	12
10BASE-T (VLT)	Full	24
	Half	25
100BASE-TX / 100BASE-FX	Full	150
	Half	300
10BASE-T	Full	650
	Half	700

- 2 After all the bridges on the network have determined the configuration of their ports, each bridge only forwards traffic 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.

An Example

Figure 5-9 illustrates 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 Bridge Identifier. Bridge C's port is chosen as the Designated Bridge Port for LAN C because it offers 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 (refer to "Configuring the STP Parameters of VLANs" on page 5-16) 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 (refer to "Configuring the STP Parameters of VLANs" on page 5-16).

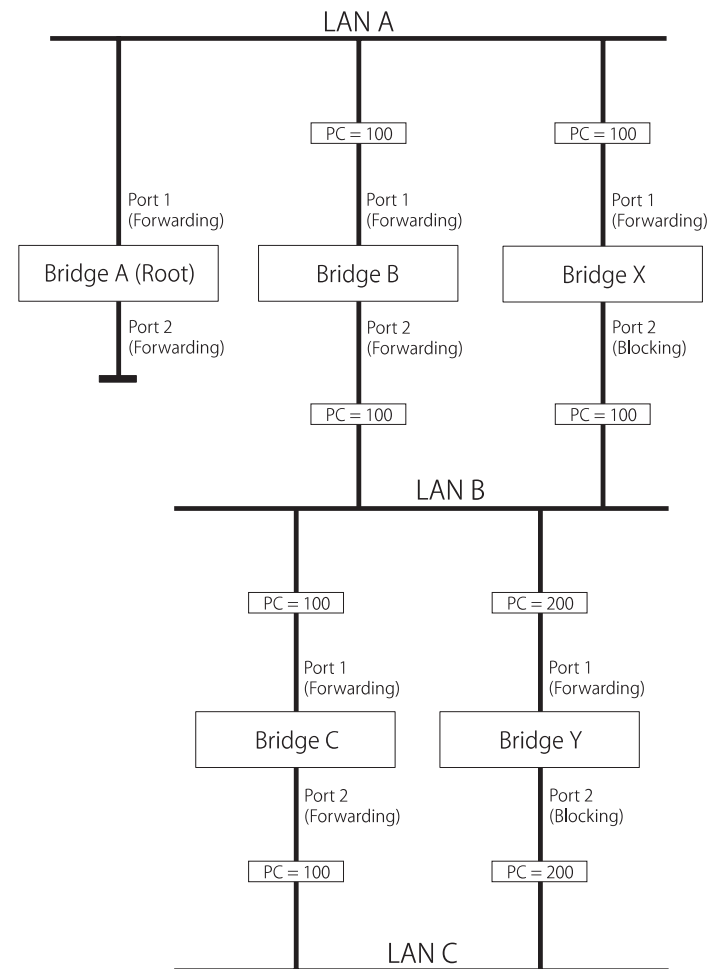


Figure 5-9 Port costs in a network

STP Configurations

Figure 5-10 shows two possible STP configurations using IBM 8271 Nways Ethernet LAN Switch units:

■ Configuration 1 — Redundancy for Backbone Link

In this configuration, an 8271 Model 524 Switch and an 8271 Model 712 Switch both have STP enabled and are connected by two Fast Ethernet links. STP discovers a duplicate path and disables one of the links. If the enabled link breaks, the disabled link becomes re-enabled, therefore maintaining connectivity.

■ Configuration 2 — Redundancy through Meshed Backbone

In this configuration, four 8271 Model 712 Switch units are connected such that there are multiple paths between them. STP discovers the duplicate paths and disables two of the links. If an enabled link breaks, one of the disabled links becomes re-enabled, therefore maintaining connectivity.

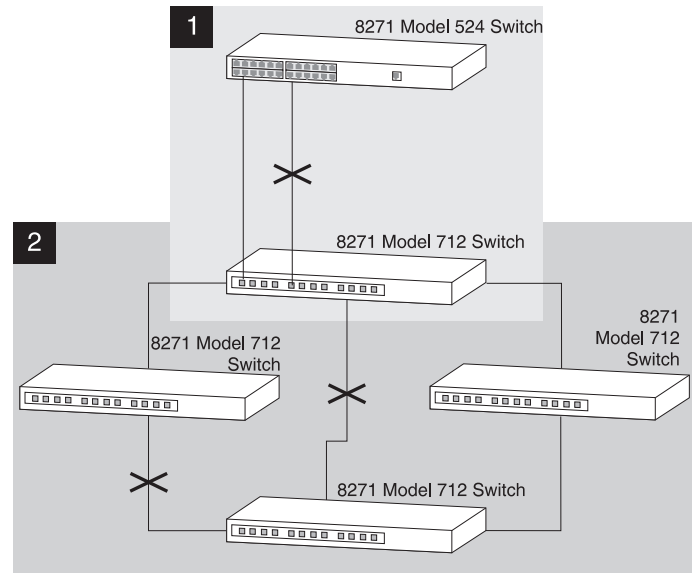


Figure 5-10 STP configurations

Enabling STP on the Switch

To enable STP on your Switch:

- 1 From the VT100 Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
- 2 In the Management Level field, choose *Unit*.
- 3 Choose the SETUP button. The Unit Setup screen is displayed, as shown in Figure 5-11.
- 4 In the Spanning Tree field, specify *Enable*.
- 5 Choose *OK*.



You cannot enable STP if you have set up resilient links on any of the Switch ports, or if you are using VLAN 16.



ATTENTION: *If STP is enabled on your 8271 Model 524 Switch, we recommend that you do not use STP for connections to another IBM 8271 Nways Ethernet LAN Switch, or a repeater. If you use STP for these connections, link losses may occur on your network.*

IBM 8271 Nways Switch Unit Setup	
Unit Name:	Desktop Switch]
sysName (Max 30 chars):	[Desktop Switch]
Forwarding Mode:	◆Fast Forward ◆
Intelligent Forwarding:	N/A
PACE:	◆Disable◆
ULAN Configuration Mode:	◆Port ◆
SDB Ageing Time (HH:MM):	[0:30]
Spanning Tree:	◆Disable◆
Duplex Mode:	◆Half Duplex ◆
Backbone Port:	[24]
Default RMON Host/Matrix:	◆Disable◆
Plug-in Module Type:	Not Fitted
Transceiver Module Type:	Not Fitted
Power Supply:	Internal
OK CANCEL	

Figure 5-11 Unit Setup screen

Configuring STP on the Switch



ATTENTION: You should not configure any STP parameters unless you have considerable knowledge and experience with STP.

Configuring the STP Parameters of VLANs

The Switch has a completely separate STP system for each VLAN that you have specified. Each VLAN has its own Root Bridge, Root Ports and BPDUs.

The VLAN STP screen allows you to set up and manage an STP system for each VLAN on the Switch. To access the VLAN STP screen:

- 1 From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
- 2 In the Management Level field, choose VLAN.
- 3 Choose the STP button. The VLAN STP screen is displayed, as shown in Figure 5-12.

The VLAN STP screen shows the following:

VLAN ID 1 / 2 / 3 ... 15 This field allows you to specify the VLAN to be configured.



If you are using STP, you cannot use VLAN 16. This VLAN is used internally by the Switch and is therefore not available.

IBM 8271 Hwags Switch VLAN STP			
VLAN ID:	[1]		
Topology Changes:	5	Max Age (s):	20
Designated Root:	8000:08004E09D247	Hello Time (s):	2
Root Cost:	850	Forward Delay (s):	15
Root Port:	1	Hold Time (s):	1
Time Since Topology Change:	9 Minutes, 7 Seconds		
Refer to the User Guide before changing the settings of these parameters.			
Bridge Priority:	[32768]		
Bridge Max Age (s):	[20]		
Bridge Hello Time (s):	[2]		
Bridge Forward Delay (s):	[15]		
APPLY		CANCEL	

Figure 5-12 VLAN STP screen

Topology Changes This read-only field shows the number of network topology changes that have occurred in the current VLAN.

Max Age 6 ... 40 This read-only field shows the time (in seconds) that the Switch waits before trying to re-configure the network. If the Switch has not received a BPDU within the time specified in this field, it will try to re-configure the network topology.

Designated Root This read-only field shows the Bridge Identifier of the designated Root Bridge.

Hello Time 1 ... 10 This read-only field shows the time delay (in seconds) between the transmission of BPDUs from the Switch.

Root Cost This read-only field shows the path cost from the Switch to the Root Bridge.

Forward Delay 4 ... 30 This read-only field shows the time (in seconds) that the ports on the Switch spend in the listening and learning states. For more information about these states, refer to “Configuring the STP Parameters of Ports” on page 5-18.

Root Port This read-only field shows the Root Port of the Switch.

Hold Time This read-only field shows the shortest time interval (in seconds) allowed between the transmission of BPDUs.

Time Since Topology Change This read-only field shows the time interval since the last topology change was detected.

Bridge Priority 0 ... 65535 This field 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 it is that the bridge will be the Root Bridge. The default setting for this field is 65535.



Do not change the priority of the Switch unless absolutely necessary.

Bridge Max Age 6 ... 40 This field allows you to specify the time (in seconds) that the Switch waits before trying to re-configure the network when it is the Root Bridge. If the Switch has not received a BPDU within the time specified in this field, it will try to re-configure the STP topology. The default setting for this field is 20 seconds.



The time must be greater than, or equal to, 2 x (Hello Time + 1), and less than, or equal to, 2 x (Forward Delay - 1).

Bridge Hello Time 1 ... 10 This field allows you to specify the time delay (in seconds) between the transmission of BPDUs from the Switch when it is the Root Bridge. The default setting for this field is 2 seconds.

Bridge Forward Delay 4 ... 30 This field allows you to specify the time (in seconds) that the ports on the Switch spend in the listening and learning states when the Switch is the Root Bridge. The default setting is 15 seconds. For more information about these states, refer to “Configuring the STP Parameters of Ports” on page 5-18.

APPLY This button applies any changes to the STP system.

Configuring the STP Parameters of Ports

The Port STP screen allows you to set up and manage the STP parameters of each port on the Switch. To access the Port STP screen:

- 1 From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
- 2 In the Management Level field, choose Port.
- 3 Choose the STP button. The Port STP screen is displayed, as shown in Figure 5-13.

The screen shows the following:

Port ID 1 / 2 / 3 ... 24 / 25 / 26 This read-only field shows the ID of the port to be configured.

STP State Disabled / Listening / Blocking / Learning / Forwarding This read-only field shows the current state of the port:

- **Disabled** — A port in this state does not forward packets, and does not participate in STP operation.
- **Listening** — A port in this state is preparing to forward packets, but has temporarily blocked to prevent a loop. During the Listening state, BPDUs are transmitted, received and processed.
- **Blocking** — A port in this state does not forward packets to prevent more than one active path existing on the network. The port is included in STP calculations, and BPDUs can be transmitted, received and processed.

IBM 8271 Hways Switch Port STP			
Port ID:	1		
STP State:	Forwarding	Designated Port:	80:01
Designated Root:	FFFF:08004e0a4af2	Designated Cost:	0
Designated Bridge:	FFFF:08004e0747c9	Fwd Transitions:	2
Refer to the User Guide before changing the settings of these parameters.			
Port Enable:	↕Enable↕		
Priority:	[128]		
Path Cost:	[700]		
Fast Start:	↕Enable↕		
OK		CANCEL	

Figure 5-13 Port STP screen

- **Learning** — A port in this state is preparing to forward packets, but has temporarily blocked to prevent a loop. During the Learning state, the Switch learns the addresses of all error-free packets. The port is included in STP calculations, and BPDUs can be transmitted, received and processed.
- **Forwarding** — A port in this state can forward packets. BPDUs can also be received and processed.

Designated Port This read-only field shows the ID of the Designated Bridge Port for the current port's segment.

Designated Root This read-only field shows the Bridge Identifier of the Root Bridge.

Designated Cost This read-only field shows the path cost from the Root Bridge to the Designated Bridge Port for the current port's segment.

Designated Bridge This read-only field shows the Bridge Identifier of the Designated Bridge for the current port's segment.

Fwd Transitions This read-only field shows the number of times that the current port has transitioned from the Learning state to the Forwarding state.

Port Enable *Enable / Disable* This field allows you to enable or disable the current port.

Priority *0 ... 255* This field 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 default setting for this field is 128.

Path Cost *0 ... 65535* This field allows you to specify the path cost of the port.



The Switch automatically assigns the default path costs shown in Table 5-1 on page 5-12. If you specify a new path cost in this field, this automatic system is disabled, and you can only re-enable it by initializing the Switch.

Fast Start *Enable / Disable* This field allows you to specify whether the port goes directly to the Forwarding state when a device is connected to it. Set this field to Enable if the port is directly connected to an endstation. The default setting for this field is Enable.



ATTENTION: *If you set the Fast Start field to Enable when the port is connected to multiple endstations, loops may occur in your network.*

RMON

Using the RMON (Remote Monitoring) capabilities of your Switch allows network administrators to improve their efficiency and reduce the load on their network.

The following sections explain more about the RMON concept and the RMON features supported by the Switch.



You can only use the RMON features of the Switch if you have an RMON management application.

What is RMON?

RMON is the common abbreviation for the Remote Monitoring MIB (Management Information Base), a system defined by the IETF documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely.

A typical RMON setup consists of two components:

- **The RMON probe** — an intelligent, remotely-controlled device or software agent that continually collects statistics about a LAN segment or VLAN, and transfers the information to a management workstation on request or when a pre-defined threshold is crossed.
- **The management workstation** — communicates with the RMON probe and collects the statistics from it. The workstation does not have to be on the same network as the probe and can manage the probe by in-band or out-of-band connections.

About the RMON Groups

The IETF define nine groups of Ethernet RMON statistics. This section describes these groups, and details how they can be used.

Statistics

The Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts and errors on a LAN segment or VLAN.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of your network.

History

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.

The group is useful for analysis of traffic patterns and trends on a LAN segment or VLAN, and to establish baseline information indicating normal operating parameters.

Alarms

The Alarms group provides a versatile, general mechanism for setting thresholds and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a vari-

able or its delta value. In addition, alarm thresholds may be autocalibrated or set manually.

Alarms are used to inform you of a network performance problem and they can trigger automated action responses through the Events group.

Hosts

The Hosts group specifies a table of traffic and error statistics for each host on a LAN segment or VLAN. Statistics include packets sent and received, octets sent and received, as well as broadcasts, multicasts, and error packets sent.

The group supplies a simple discovery mechanism listing all hosts that have transmitted. The next group, Hosts Top N, requires implementation of the Hosts group.

Hosts Top N

The Hosts Top N group extends the Hosts table by providing sorted host statistics, such as the top 20 nodes sending packets or an ordered list of all nodes according to the errors they sent over the last 24 hours.

Matrix

The Matrix group shows the amount of traffic and number of errors between pairs of devices on a LAN segment or VLAN. For each pair, the Matrix group maintains counters of the number of packets, number of octets, and error packets between the nodes.

The conversation matrix helps you to examine network statistics in more detail to discover who is talking to whom or if a particular PC is producing more errors when communicating with its file server, for example. Combined with Hosts Top N, this allows you to view the busiest hosts and their primary conversation partners.

Filter

The Filter group provides a mechanism to instruct the RMON probe to capture packets that match a specific criterion or condition.

Capture

The Capture group allows you to create capture buffers on the probe that can be requested and uploaded to the management workstation for decoding and presentation.

Events

The Events group provides you with the ability to create entries in an event log and/or send SNMP traps to the management workstation. Events can originate from a crossed threshold on any RMON variable. In addition to the standard five traps required by SNMP (link up, link down, warm start, cold start, and authentication failure), RMON adds two more: rising threshold and falling threshold.

Effective use of the Events group saves you time; rather than having to watch real-time graphs for important occurrences, you can depend on the Event group for notification. Through the SNMP traps, events can trigger other actions providing a mechanism for an automated response to certain occurrences.

Benefits of RMON

Using the RMON features of your Switch has three main advantages:

- **RMON improves efficiency**

Using RMON probes allows you to remain at one workstation and collect information from widely dispersed LAN segments or VLANs. This means that the time taken to reach a problem site, set up equipment, and begin collecting information is largely eliminated.

- **RMON allows proactive management**

If they are configured correctly, RMON probes deliver information before problems occur. This means that you can take action before they impact on users. In addition, probes record the behavior of your network, so that you can analyze the causes of problems.

- **RMON reduces the traffic load**

Traditional network management involves a management workstation polling network devices at regular intervals to gather statistics and identify problems or trends. As network sizes and traffic levels grow, this approach places a strain on the management workstation and also generates large amounts of traffic.

An RMON probe, however, autonomously looks at the network on behalf of the management workstation without affecting the characteristics and performance of the network. The probe reports by exception, which means that it only informs the management workstation when the network has entered an abnormal state.

RMON and the Switch

RMON requires one probe per LAN segment, and stand-alone RMON probes have traditionally been expensive. Therefore, an inexpensive RMON probe has been built into each Switch. This allows RMON to be widely deployed around the network without costing more than traditional network management.

A problem with stand-alone RMON probes is that they are passive; able to monitor and report, but nothing more. Placing probe functionality inside the network device allows integration of RMON with normal device management to allow proactive management.

For example, statistics can be related to individual ports and the Switch can take autonomous actions such as disabling a port (temporarily or permanently) if errors on that port exceed a pre-defined threshold. Also, since a probe needs to be able to see all traffic, a stand-alone probe has to be attached to a non-secure port. Implementing RMON in the Switch means all ports can have security features enabled.

RMON Features of the Switch

Table 5-2 details the RMON support provided by the Switch.

Table 5-2 RMON support supplied by the Switch

RMON Group	Support supplied by the Switch
Statistics	A new or initialized Switch has one Statistics session per port/VLAN.
History	<p>A new or initialized Switch has three History sessions on the 100BASE-TX port, backbone port and Default VLAN:</p> <ul style="list-style-type: none"> ■ 60-second intervals, 120 historical samples stored ■ 30-second intervals, 120 historical samples stored ■ 30-minute intervals, 96 historical samples stored
Alarms	<p>Although up to 700 alarms can be defined for the Switch, a new or initialized Switch has four alarms defined for each port:</p> <ul style="list-style-type: none"> ■ Bandwidth used ■ Broadcast bandwidth used ■ Percentage of packets forwarded ■ Errors per 10,000 packets <p>You can modify these alarms using an RMON management application, but you cannot create or delete them.</p> <p>For more information about the alarms setup on the Switch, refer to "About Alarm Actions" on page 5-25 and "About Default Alarm Settings" on page 5-26.</p>

Table 5-2 RMON support supplied by the Switch

RMON Group	Support supplied by the Switch
Hosts	<p>Although Hosts is supported by the Switch, there are no Hosts sessions defined on a new or initialized Switch by default.</p> <p>You can specify that a Hosts session is defined on the Default VLAN; for more information, refer to "Setting Up the Switch Unit" on page 4-9.</p>
Hosts Top N	Although Hosts Top N is supported by the Switch, there are no Hosts Top N sessions defined on a new or initialized Switch.
Matrix	<p>Although Matrix is supported by the Switch, there are no Matrix sessions defined on a new or initialized Switch by default.</p> <p>You can specify that a Matrix session is defined on the Default VLAN; for more information, refer to "Setting Up the Switch Unit" on page 4-9.</p>
Filter	The Filter group is not presently supported by the Switch.
Capture	The Capture group is not presently supported by the Switch.
Events	A new or initialized Switch has events defined for use with the default alarm system. Refer to "About Default Alarm Settings" on page 5-26 for more information.

When using the RMON features of the Switch, you should note the following:

- After the default sessions are created, they have no special status. You can delete or change them as required.
- The Switch can forward a very large volume of packets per second. The Statistics RMON group is able to monitor every packet, but the other groups sample a maximum of 6000 packets a second.
- The greater the number of RMON sessions, the greater the burden on the management resources of the Switch; however, the forwarding performance of the Switch is not affected.

About Alarm Actions

You can define up to 700 alarms for the Switch. The actions that you can define for each alarm are shown in Table 5-3.

Table 5-3 Alarm Actions

Action	High Threshold	Low Threshold
No action.		
Notify only.	Send Trap.	
Notify and blip port.	Send Trap. Block broadcast and multicast traffic on the port for 5 seconds.	
Notify and disable port.	Send Trap. Turn port off.	
Notify and enable port.		Send Trap. Turn port on.
Blip port.	Block broadcast and multicast traffic on the port for 5 seconds.	
Disable port.	Turn port off.	
Enable port.		Turn port on.
Notify and move resilient port.	Send Trap. If port is the main port of a resilient link pair then move to standby.	
Notify and blip device.	Send Trap. Block broadcast and multicast traffic on all ports for 5 seconds.	
Notify and disable device.	Send trap. Turn all ports on device off.	
Notify and enable device.		Send Trap. Turn ports back to original state.
Blip device.	Block broadcast and multicast traffic on all ports for 5 seconds.	
Disable device.	Turn all ports on device off.	
Re-enable device.		Turn ports back to original state.

About Default Alarm Settings

A new or initialized Switch has four alarms defined for each port:

- Bandwidth used
- Broadcast bandwidth used
- Percentage of packets forwarded
- Errors per 10,000 packets

The default values and actions for each of these alarms are given in Table 5-4.

Table 5-4 Initial settings for the default alarms

Statistic	High Threshold	Low Threshold Recovery	Samples per average	Period
Bandwidth used	Value: 85% No action	Value: 50% No action	4	60 secs
Broadcast bandwidth used	Value: 20% Notify and blip	Value: 10% No action	4	20 secs
Percentage of packets forwarded	Value: 85% No action	Value: 50% No action	4	60 secs
Errors per 10,000 packets	Value: 200 Notify	Value: 100 No action	4	60 secs

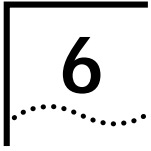
About the Audit Log

The Switch keeps an audit log of all management user sessions, providing a record of changes to any MIB including the RMON MIB. The log can only be read by users at the *security* access level using an SNMP Network Manager.

Each entry in the log contains information in the following order:

- Entry number
- Timestamp
- User ID
- Item ID (including qualifier)
- New value of item

There is a limit of 16 records on the number of changes stored. The oldest records are overwritten first.



STATUS MONITORING AND STATISTICS

This chapter describes how to view the current operating status of the Switch, how to display any error information in a fault log and how to carry out a remote poll to check the response of another network device.

It also describes the Statistics screens for the Switch, and advises you on actions to take if you see unexpected values for the statistics. Please note however, that as all networks are different, any actions listed are only recommendations.

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. This way, statistics can also help you get the best out of your network.

Summary Statistics

With the Switch Management screen displayed, choose the management level *Unit*, then select the STATISTICS button. The Summary Statistics screen is displayed, as shown in Figure 6-1.

The Summary Statistics screen lists values for the current counter against every port on the Switch and it is refreshed approximately every 2 seconds. Once values have reached approximately 4,000,000,000 they are reset to zero.

To view values for a particular counter, select the first button displayed at the foot of the Summary Statistics screen. Pressing [Space] toggles through the available counters and as soon as you move away from the button, the screen is refreshed to show values for that counter.

FRAMES RECEIVED Displays values for the Frames Received counter; the total number of frames that have been received by the current port, including fragments and frames with errors.

FRAMES TRANSMITTED Displays values for the Frame Transmitted counter; the total number of frames successfully transmitted by the current port, including fragments and frames with errors.

FRAMES FORWARDED Displays the total number of frames that were received by the current port and forwarded to other ports.

IBM 8271 Hways Switch Summary Statistics			
Port 1:	0	Port 2:	0
Port 3:	0	Port 4:	0
Port 5:	0	Port 6:	0
Port 7:	0	Port 8:	0
Port 9:	0	Port 10:	22724
Port 11:	0	Port 12:	0
Port 13:	0	Port 14:	0
Port 15:	0	Port 16:	0
Port 17:	0	Port 18:	0
Port 19:	0	Port 20:	0
Port 21:	0	Port 22:	0
Port 23:	0	Port 24:	0
Module(25):	Not Fitted	100BASE-TX(26):	0
◆ FRAMES RECEIVED ◆ CLEAR SCREEN COUNTERS CANCEL			

Figure 6-1 Summary Statistics screen

FRAMES FILTERED Displays the total number of frames that were filtered because the destination station was on the same segment (port) as the source station.

MULTI/BROADCAST (RX) Displays the total number of frames received by the current port that are addressed to a multicast or broadcast address.

MULTI/BROADCAST (TX) Displays the total number of frames transmitted by the current port that are addressed to a multicast or broadcast address.

ERRORS Displays the total number of errors which have occurred on the current port. Refer to the description of the Errors field on page 6-5.

CLEAR SCREEN COUNTERS Use this button to set all counters shown on the screen to zero. Use this button for analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device.

Port Statistics

With the Switch Management screen displayed, choose the management level *Port*, then select the STATISTICS button. The Port Statistics screen is displayed, as shown in Figure 6-2. As well as showing statistics for the port, this screen allows you access to traffic and error counter screens.



If the port is an ATM OC-3c Module port, the ATM Port Statistics screen is displayed. For more information, refer to the “IBM 8271 Nways Ethernet LAN Switch ATM OC-3c Module User’s Guide”.

The Port Statistics screen shows the following:

Port ID The ID of the port you are currently managing.

Bandwidth Used This counter provides a running average of the bandwidth used by the port, expressed as a percentage of the maximum bandwidth available for the port. A sampling period of 1 minute is used. The value gives an indication of the general traffic level of the network. A high utilization for single endstation segments is an indication that your network is operating efficiently. However, if multiple endstations are connected to this port and you see values of around 40% you should reconsider the topology of your network because each user will see degraded network performance.

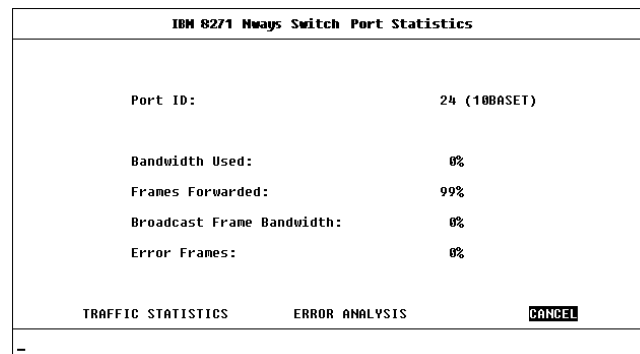


Figure 6-2 Port Statistics screen

Frames Forwarded This counter provides a running average of the proportion of the received frames that are forwarded, expressed as a percentage of all frames received by the port. A sampling period of 1 minute is used.

Broadcast Frame Bandwidth This counter provides a running average of the broadcast frame bandwidth used by the port, expressed as a percentage of the maximum bandwidth available for the port. A sampling period of 5 seconds is used.

Error Frames This counter provides a running average of the number of errors per 10,000 frames received by the port, expressed as a percentage. Refer to the field description for Errors on page 6-5.

TRAFFIC STATISTICS Select this button to access traffic counters for this port.

ERROR ANALYSIS Select this button to access error counters for this port.

Port Traffic Statistics

With the Port Statistics screen displayed, select the TRAFFIC STATISTICS button. The Port Traffic Statistics screen is displayed, as shown in Figure 6-3.

The Port Traffic Statistics screen shows the following:

Port ID The ID of the port you are currently managing.

Frames Received The number of valid frames received by the port, including fragments and frames with errors.

Frames Transmitted The number of frames that have been successfully transmitted by the port including fragments and frames with errors.

Octets Received The number of octets received by the port. The calculation includes the MAC header and Cyclical Redundancy Check (CRC), but excludes preamble/Start-of Frame-Delimiter (SFD). Octet counters are accurate to the nearest 256 octet boundary.

Octets Transmitted The number of octets transmitted by the port. The calculation includes the MAC header and CRC, but excludes preamble/SFD. Octet counters are accurate to the nearest 256 octet boundary.

IBM 8271 Mways Switch Port Traffic Statistics			
Port ID:	24 (100A5ET)		
Frames Received:	300780	Octets Received:	133551104
Frames Transmitted:	18136	Octets Transmitted:	1351424
Multicasts Received:	3214	Collisions:	7
Broadcasts Received:	266882	Fragments:	30
Frames Forwarded:	287704	Errors:	0
Frames Filtered:	13076	IFM Count:	0
Frame Size Analysis.			
64 Octets:	1 %	256 to 511 Octets:	73 %
65 to 127 Octets:	16 %	512 to 1023 Octets:	7 %
128 to 255 Octets:	2 %	1024 to 1518 Octets:	0 %
CLEAR SCREEN COUNTERS		CANCEL	

Figure 6-3 Port Traffic Statistics screen

Multicasts Received The number of frames successfully received that have a multicast destination address. This does not include frames directed to a broadcast address or frames received with errors.

Broadcasts Received The number of frames received that have a broadcast destination address. This does not include frames with errors.

Collisions An estimate of the total number of collisions that occurred when transmitting from the unit. Collisions are a normal part of Ethernet operation that occur when two devices attempt to transmit at the same time. A sudden sustained increase in the number of collisions may indicate a problem with a device or cabling on the network, particularly if this is not accompanied by an increase in general network traffic.

Fragments The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits, but including FCS octets).

Frames Forwarded The total number of frames which were received by the port and forwarded to their destination address.

Frames Filtered The total number of frames that were filtered because the destination address was on the same segment (port) as the source station.

Errors The total number of errors which have occurred on this port. Errors can be one of the following:

- CRC Alignment Errors
- Short Events
- Long Frames
- Late Events
- Jabbers

The value shown should be a very small proportion of the total data traffic.

IFM Count The number of times Intelligent Flow Management (IFM) has had to operate to minimize packet loss.

Frame Size Analysis The number of frames of a specified length as a percentage of the total number of frames of between 64 and 1518 octets. This indicates the composition of frames in the network.

The frame size ranges are:

- 64 octets
- 65–127 octets
- 128–255 octets
- 256–511 octets
- 512–1023 octets
- 1024–1518 octets

The composition of frames on your network may help you to analyze the efficiency of your network layer protocol.

CLEAR SCREEN COUNTERS Select this button to set all counters shown on the screen to zero. It is useful for trend analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device or affect counters at the network management workstation.

Port Error Analysis

With the Port Statistics screen displayed, select the ERROR ANALYSIS button. The Port Error Analysis screen is displayed, as shown in Figure 6-4.

The Port Error Analysis screen shows the following:

Port ID The ID of the port you are currently managing.

CRC Align Errors This counter is incremented by one for each frame with a CRC (Cyclic Redundancy Check) error or an alignment error. A CRC error occurs if a frame of valid length has an invalid CRC but does not have a framing error. It is likely that a bit has been corrupted in transmission. An alignment error occurs if a frame has a CRC error and the frame does not have an integral number of octets. Alignment errors may be caused by a fault at the transmitting device.

Check cables and connections for damage. Try changing the transceiver or adapter card of the device connected to the port at the source of the problem.

Short Events This counter is incremented by one for each carrier event whose duration is less than the short event maximum time. Short events are error frames smaller than the minimum size defined for Ethernet frames. They may indicate externally generated noise causing problems on the network. Check the cabling routing and re-route any cabling which may be affected by external noise sources.

IBM 8271 Mways Switch Port Error Analysis	
Port ID:	24 (10BASET)
CRC Align Errors:	0
Short Events:	0
Late Events:	0
Long Frames:	0
Jabbers:	0
CLEAR SCREEN COUNTERS CANCEL	

Figure 6-4 Port Error Analysis screen

Late Events This counter is incremented by one each time a collision occurs after the valid packet minimum time. A late event is an out-of-window collision that may occur if your Ethernet LAN exceeds the maximum size as defined in the IEEE standard. A late event is also counted as a collision.

Long Frames This counter is incremented by one each time a frame is received whose octet count is greater than the maximum frame size but less than Jabber frame size. Long Frames are frames that exceed the maximum size defined for Ethernet frames (1518 octets). If you see a high number of long frames on your network, you should isolate the source of these frames and examine the transceiver or adapter card at the device. Some protocols may generate these frames.

Jabbers The total number of packets received that were longer than 8K octets (excluding framing bits, but including FCS octets).

CLEAR SCREEN COUNTERS Select this button to set all counters shown on the screen to zero. It is useful for trend analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device or affect counters at the network management workstation.

Status Monitoring

The status screen provides read-only information about the Switch. This information may be useful for your technical support representative if you have a problem.

To access the screen, from the Main Menu, select the STATUS option. The Status screen is displayed, as shown in Figure 6-5.

The Status screen shows the following:

System Up Time The time the unit has been running since the last reset or power-off/on cycle.

Number Of Resets The total number of system resets since the Switch was first installed or initialized; either power on, manual reset or a watchdog expiry.

Last Reset Type *Other / Command / Watchdog / Power-reset / System-error* This field indicates the cause of the last reset. It may be due to management command, watchdog timeout expiry, power interruption, a manual reset or a system error.

Hardware Version The hardware version number of the Switch.

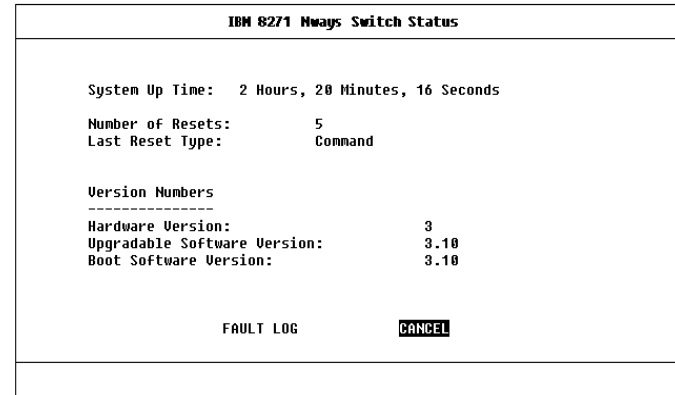


Figure 6-5 Status screen

Upgradable Software Version The version number of the agent software image stored in Flash EPROM. This version number is automatically updated when you download new software.

Boot Software Version This is the version number of the Boot software stored on the Switch.

FAULT LOG Select this button to display the Switch Fault Log, described the next section.

Fault Log

The Fault Log displays read-only information about the Switch which is updated whenever an abnormal condition is detected. This information is for internal use only. You may be asked to quote this information if reporting a fault to your supplier.

With the Status screen displayed, select the FAULT LOG button. The Fault Log is screen is displayed, as shown in Figure 6-6.

The Fault Log screen shows the following:

Reset Count The number of resets recorded at the time of the fault.

Time (seconds) The time elapsed since the last reset when the fault occurred.

Area This information may be used for fault diagnosis by your technical support representative.

Fault Number The hexadecimal number in this field indicates the type of fault. You should note this number and contact your technical support representative for advice.

IBM 8271 Nways Switch Fault Log			
Reset Count	Time (seconds)	Area	Fault Number
[Redacted]			
This information is for internal use only. You may be asked to quote the Area and Fault Number if reporting a problem to your supplier.			
CANCEL			

Figure 6-6 Fault Log screen

Remote Polling

The Remote Poll screen allows you to send a single frame to a remote device to see if that device is responding. This can help to locate the source of a network problem. It is also particularly helpful in locating devices that support IP, IPX and ping but are not manageable by SNMP.

To poll a device:

- 1 From the Main Menu, select Remote Poll. The Remote Poll screen is displayed, as shown in Figure 6-7.
- 2 In the Target Address field, enter the IP or IPX address of the device you want to poll.
- 3 Select the POLL button at the foot of the screen.

When the poll is complete, the Round Trip Time field shows the interval in milliseconds between sending the frame to the target device and receiving a response at the Switch. If the target device does not respond after approximately 10 seconds, this field displays *no reply*.

```
IBM 8271 Nways Switch Remote Poll

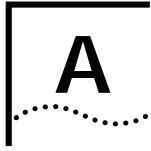
Target Address: [           ]
Round Trip Time: no reply

This operation will poll the target device.

IP address format d.d.d.d
IPX address format AABBCCDD:AABBCCDDEEFF

POLL  CANCEL
```

Figure 6-7 Remote Poll screen



SAFETY INFORMATION

You must read the following safety information before carrying out any installation or removal of components, or any maintenance procedures on the Switch.

Safety Notices

Safety notices are printed throughout this manual. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous.

World Trade Safety Information

Some countries require the safety information contained in publications to be presented in their national languages. Before using an English-language publication to set up, install, or operate this IBM product, you first should become familiar with the related 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.



Varning — livsfara: Innan du börja installera den här produkten bör du läsa säkerhetsinformationen i dokumentet *Varning: Säkerhetsföreskrifter – Läs detta först*, SD21-0030. Där beskrivs hur du på ett säkert sätt ansluter elektrisk utrustning.



Fare: Før du begynner å installere dette produktet, må du lese sikkerhetsinformasjonen i *Advarsel: Sikkerhetsinformasjon – Les dette først*, SD21-0030 som beskriver sikkerhetsrutinene for kabling og tilkobling av elektrisk utstyr.



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 de installatie van dit product, moet u eerst de veiligheidsinstructies lezen in de brochure *PAS OP! Veiligheidsinstructies – Lees dit eerst*, SD21-0030. Hierin wordt beschreven hoe u elektrische apparatuur op een veilige manier moet bekabelen en aansluiten.



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 Informtion – Read This First*, SD21-0030. In dit boekje vindt u veilige procedures voor het aansluiten van elektrische apparatuur.



Vorsicht: Bevor mit der Installation des Produktes begonnen wird, die Sicherheitshinweise in *Achtung: Sicherheitsinformationen – Bitte zuerst lesen*, IBM Form SD21-0030. Diese Veröffentlichung beschreibt die Sicherheitsvorkehrungen für das Verkabeln und Anschließen elektrischer Geräte.



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



Danger: Avant de procéder à l'installation de ce produit, lisez d'abord les consignes de sécurité dans la brochure *ATTENTION: Consignes de sécurité – A lire au préalable*, SD21-0030. Cette brochure décrit les procédures pour câbler et connecter les appareils électriques en toute sécurité.



Pericolo: prima di iniziare l'installazione di questo prodotto, leggere le informazioni relative alla sicurezza riportate nell'opuscolo *Attenzione: Informazioni di sicurezza – Prime informazioni da leggere* in cui sono descritte le procedure per il cablaggio ed il collegamento di apparecchiature elettriche.



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.



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.



Perigo: Antes de começar a instalar este produto, leia as informações de segurança contidas em *Cuidado: Informações Sobre Segurança – Leia Isto Primeiro*, SD21-0030. Esse folheto descreve procedimentos de segurança para a instalação de cabos e conexões em equipamentos elétricos.



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



Uwaga: Przed rozpoczęciem instalacji produktu należy zapoznać się z instrukcją: "Caution: Safety Information - Read This First", SD21-0030. Zawiera ona warunki bezpieczeństwa przy podłączeniu do sieci elektrycznej i eksploatacji.



Vigyázat: Mielőtt megkezdi a berendezés üzembe helyezését, olvassa el a *Caution: Safety Information – Read This First*, SD21-0030 könyvecskében leírt biztonsági információkat. Ez a könyv leírja, milyen biztonsági intézkedéseket kell megtenni az elektromos berendezés huzalozásakor illetve csatlakoztatásakor.



Pozor: Preden zaenete z instalacijo tega produkta prebertte poglavje: *'Opozorilo: Informacije o varnem rokovanju - preberi pred uporabo,'* SD21-0030. To poglavje opisuje pravilne postopke za kabliranje,



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。



Upozornění: než zahájíte instalaci tohoto produktu, přečtěte si nejprve bezpečnostní informace v pokynech „Bezpečnostní informace“ č. 21-0030. Tato brožurka popisuje bezpečnostní opatření pro kabeláž a zapojení elektrického zařízení.



위험: 이 제품을 설치하기 전에 반드시 "주의: 안전 정보-시작하기 전에" (SD21-0030) 에 있는 안전 정보를 읽으십시오.



ОСТОРОЖНО: Прежде чем устанавливать этот продукт, прочтите Инструкцию по технике безопасности в документе "Внимание: Инструкция по технике безопасности -- Прочсть 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.



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。



情報処理装置等電波障害自主規制協議会 (VCCI) 表示

この装置は、第一種情報装置(商工業地域において使用されるべき情報装置)で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(VCCI)基準に適合しております。

従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。

取扱説明書に従って正しい取り扱いをして下さい。



Opasnost: Prije nego sto počnete sa instalacijom produkta, pročitajte naputak o pravilima o sigurnom rukovanju u Upozorenje: Pravila o sigurnom rukovanju - Prvo pročitaj ovo, SD21-0030. Ovaj privitak opisuje sigurnosne postupke za priključivanje kabela i priključivanje na električno nabaianie.

Power Cords

A country-appropriate power cord must be ordered separately for each 8271 Ethernet LAN Switch. The feature numbers and part numbers to be used to order these power cords are listed below. Unless otherwise noted, all of the power cords listed below are 9 ft (2.8m), 250V/10A, unshielded power cords.

Country	Part Number (Feature Number)
U.S.A. and Canada	
Canada Mexico	United States 6952300 (FN 6851)
United States (6 ft. Chicago)	6952301 (FN 6852)
United States 220 VAC	1838574 (FN 6853)
Latin America	
Argentina Columbia	Paraguay Uruguay 6952291 (FN 6862)
Chile	14F0069 (FN 6858)

(continued)

Country	Part Number (Feature Number)
Bahamas	Guyana 1838574 (FN 6853)
Barbados	Haiti
Bolivia	Honduras
Brazil	Jamaica
Costa Rica	N. Antilles
Dominican R.	Panama
El Salvador	Peru
Ecuador	Trinidad
Guatemala	Venezuela

Europe, Middle East, and Africa

Albania	Macedonia	13F9979 (FN 6855)
Angola	Mozambique	
Austria	Netherlands	
Belarus	Norway	
Belgium	Poland	
Bosnia	Portugal	
Bulgaria	Romania	
Croatia	Russia	
Czechia	Saudi Arabia	
Egypt	Slovakia	
Finland	Slovenia	
France	Spain	
Germany	Sudan	
Greece	Sweden	
Hungry	Syrian Arab	
Iceland	Turkey	
Iran	Ukraine	
Kazakhstan	Yugoslavia	
Lebanon	Zaire	
Luxembourg		



(continued)









Country		Part Number (Feature Number)
Bahrain	Nigeria	14F0033 (FN 6856)
Cyprus	Oman	
Ghana	Quatar	
Iraq	Sierra Leone	
Ireland	Somalia	
Jordan	Tanzania	
Kenya	Uganda	
Kuwait	Un.Arab Emir.	
Libya	UK	
Malawi	Yemen	
Malta	Zambia	
Denmark		13F9997 (FN 6857)
Ethopia	Italy	14F0069 (FN 6858)
Israel		14F0087 (FN 6860)
Switzerland	Liechtenstein	14F0051 (FN 6859)
Namibia	Swaziland	14F0015 (FN 6861)
Pakistan	Zimbabwe	
South Africa		
Liberia		1838574 (FN 6853)
Asia Pacific		
Australia	New Zealand	13F9940 (FN 6854)
Brunei	Malaysia	14F0033 (FN 6856)
Hong Kong	China	
Macao	Singapore	

(continued)

Country		Part Number (Feature Number)
Japan	Taiwan	1838574 (FN 6853)
Philippines	Thailand	
Bangladesh	Sri Lanka	14F0015 (FN 6861)
Myanmar		
Indonesia	Korea (South)	13F9979 (FN 6855)

Important Safety Information

-  **DANGER:** U.K. only: The Switch is covered by OfTel General Approval, NS/G/12345/J/100003, for indirect connection to a public telecommunications system. This can only be achieved using the console port on the unit and an approved modem.
-  **DANGER:** Installation and removal of the unit must be carried out by qualified personnel only.
-  **DANGER:** L'installation et l'enlèvement de l'unité doivent être faits seulement par le personnel qualifié.
-  **DANGER:** Ein- und Ausbau des Gerätes ist **nur von Fachpersonal** vorzunehmen.
-  **Gevaar!** De eenheid mag alleen worden geïnstalleerd of verwijderd door bevoegde personen.
-  **Perigo:** A instalação e remoção da unidade deve ser feita apenas por pessoal especializado.
-  **Fare!** Installation og afmontering af enheden skal udføres afuddannet personale.
-  **Gevaar:** Installatie en verwijdering van de eenheid moet uitsluitend worden uitgevoerd door getraind personeel.
-  **Verra:** Yksikön saavat asentaa ja irrottaa vain tähän koulutetut henkilöt.

-  **Pericolo:** L'installazione e la rimozione dell'unità devono essere eseguite esclusivamente da personale specializzato.
-  **Fare:** Det er bare kvalifisert personale som kan installere og ta ut enheten.
-  **Perigo:** A instalação e a remoção da unidade devem ser efectuadas apenas por pessoal qualificado.
-  **Peligro:** La instalación y extracción de la unidad debe efectuarse únicamente por personal cualificado.
-  **Fara:** Installation och flyttning av enheten måste utföras av utbildad personal.
-  设备的安装和移动必须由有资格的人员来操作。
-  Postavljanje i demontažu ovog uređaja mora obaviti stručno osposobljena osoba.
-  Neodstra ujte desky modul , pokud je p ipojeno napájení.
-  Η εγκατάσταση και αφαίρεση της συσκευής πρέπει να γίνεται μόνο από ειδικευμένο προσωπικό.
-  Az egység telepítését és leszerelését csak szakképzett személyzet végezheti.



この装置の取り付け、取り外しはサービス技術員以外は実施しないでください。



장치를 설치하고 제거하는 것은 자격이 있는 사람이 수행해야 합니다.



Jednostkę może instalować i deinstalować jedynie wykwalifikowany personel.



Монтаж и демонтаж оборудования должен выполнять только квалифицированный персонал.



Inštalácia jednotky alebo jej premiestnenie musí byť uskutočnená za pomoci kvalifikovanej osoby.



Instalacija oziroma izklop naprave smejo izvajati samo usposobljene osebe.



安裝或移動本裝置的工作必須經由專業人員來執行。



DANGER: It is essential that the mains socket outlet is installed near to the unit and is accessible. You can only disconnect the unit by removing the appliance coupler from the unit.



DANGER: C'est essentiel que le socle soit installé près de l'unité et soit accessible. Vous pouvez seulement débrancher l'unité en enlevant la fiche d'alimentation de la prise de courant.



DANGER: Es ist wichtig, daß der Netzstecker sich in unmittelbarer Nähe zum Gerät befindet und leicht erreichbar ist. Das Gerät kann nur durch Herausziehen des Verbindungssteckers aus der Steckdose vom Stromnetz getrennt werden.



Gevaar: Het is van essentieel belang dat de contactdoos voor de stroomtoevoer in de nabijheid van de eenheid geïnstalleerd is en toegankelijk is. U kunt de eenheid alleen uitschakelen door de stroomtoevoer los te koppelen van de eenheid.



Perigo: É essencial que a tomada da parede esteja instalada próxima à unidade e esteja acessível. A unidade pode ser desconectada apenas após a remoção do engate.



Fare! Det er vigtigt, at hovedstikkontakten installeres i nærheden af enheden, og at der er fri adgang til den. Du kan kun afbryde enheden ved at fjerne opkoblingsenheden fra den.



Gevaar: Het is van essentieel belang dat de aansluiting voor het lichtnet zich dichtbij de eenheid bevindt en goed toegankelijk is. U kunt de eenheid uitsluitend ontkoppelen door het koppelstuk van de eenheid af te halen.



Vaara: On tärkeää, että pistorasia asennetaan lähelle yksikköä siten, että pistorasian luokse on esteetön pääsy. Voit katkaista yksiköstä virran vain irrottamalla pistokkeen yksiköstä.



Pericolo: E' essenziale che la presa di alimentazione sia installata in prossimità dell'unità e che sia accessibile. E' possibile scollegare l'unità soltanto rimuovendo la spina.



Fare: Det er viktig at hovedstikkkontakten er monteret i nærheten av enheten, og er tilgjengelig. Du kan bare frakoble enheten ved å trekke ut apparatledningen fra enheten.



Perigo: É essencial que a tomada elétrica seja instalada próximo da unidade e que seja facilmente acessível. Só é possível desligar totalmente a alimentação, retirando a ficha de ligação da unidade.



Peligro: Es muy importante que la toma de alimentación del zócalo esté instalada cerca de la unidad y que sea accesible. Sólo se puede desconectar la unidad extrayendo el acoplador del aparato de la unidad.



Fara: Det är viktigt att eluttaget sitter nära enheten och att det är lättåtkomligt. Du kan koppla ur utrustningen endast genom att ta bort kopplingsanordningen från enheten.



请将主插座安装在设备的附近, 以便使用. 您可从设备上移去电器。



Važnoje, da se izlazna mjesta glavne utičnice instaliraju blizu uređaja i da su pristupačna. Uređaj možete isključiti samo odspajanjem napajanja od uređaja.



Je nezbytné, aby si ová zásuvka byla instalována blízko za izeni a byla p ístupná. Za izení m žete odpojit pouze vytažením napájecího kabelu ze za izení.



Είναι σημαντικό η πρίζα παροχής ρεύματος να είναι εγκατεστημένη κοντά στη συσκευή και να είναι προσβάσιμη. Η αποσύνδεση της συσκευής γίνεται μόνο με αφαίρεση του συζεύκτη της συσκευής.



Lényeges, hogy a hálózati dugalj az egységhez közel és könnyen elérhető legyen. Az egységet csak a csatlakozódugó kihúzásával lehet feszültségmentesíteni.



電源コンセントは装置の近くに設置されいつでも取り扱えるようにしておくことが重要です。装置から電源接続器を取り外すことにより装置を切り離します。



주요 소켓 콘센트는 반드시 가까이에 설치되어서 접근하기 쉬워야 합니다. 연결 장치를 제거해야만 장치를 끌 수 있습니다.



Gniazdo, do którego podłączany jest kabel zasilania jednostki powinno być zainstalowane blisko jednostki, w łatwo dostępnym miejscu. Jednostkę można odłączyć jedynie wyjmując z niej kabel zasilający.



Очень важно, чтобы электрическая розетка находилась рядом с блоком, и чтобы она ничем не была загорожена. Блок можно отсоединить, только отсоединив от него шнур питания.



Je dôležité, aby sieťová zásuvka bola nainštalovaná v blízkosti zariadenia a bola prístupná. Zariadenie môžete vypnúť vytiahnutím sieťovej šnúry zo zariadenia.



Zelo pomembno je, da je glavna vtičnica blizu naprave in da je dostopna. Napravo je možno izključiti samo tako, da potegnete priključni vtič iz naprave.



很重要的，主要插座要安裝在本機器附近，且可供本機器使用。要將本機器斷電，唯一的方法是移除本機器的設備耦合器。



DANGER: This unit operates under SELV conditions (Safety Extra Low Voltage) according to IEC 950, the conditions of which are maintained only if the equipment to which it is connected is also operational under SELV.



DANGER: Cette unité marche sous les conditions SELV (Safety Extra Low Voltage) conformément à IEC 950, ces conditions sont maintenues seulement si le matériel auquel elle est branchée, est aussi en exploitation sous SELV.



DANGER: Das Gerät wird mit Sicherheits-Kleinspannung nach IEC 950 (SELV = Safety Extra Low Voltage) betrieben. Angeschlossen werden können nur Geräte, die ebenfalls nach SELV betrieben werden.



Gevarr: Deze eenheid werkt onder SELV (Safety Extra Low Voltage) volgens IEC 950, waarvan de voorwaarden alleen behouden blijven indien de apparatuur waarop het is aangesloten, ook onder SELV werkt.



Perigo: Esta unidade funciona sob condições SELV (Safety Extra Low Voltage) de acordo com IEC 950 mas, essa situação é mantida apenas se o equipamento ao qual ela está conectada também funcionar sob a condição SELV.



Fare! Denne enhed fungerer ved svagstrøm i henhold til betingelserne IEC 950. Disse betingelser overholdes kun, hvis det udstyr, enheden er sluttet til, også fungerer ved svagstrøm.



Gevaar: Deze eenheid werkt onder extra lage spanning (SELV, Safety Extra Low Voltage) volgens norm IEC 950. Er wordt uitsluitend aan deze norm voldaan zolang de apparatuur waarmee de eenheid is verbonden, ook werkt onder SELV.



Vaara: Tämä yksikkö sisältää kansainvälisen turva-standardin IEC 950 mukaisia SELV (Safety Extra Low Voltage) -suojajännitepiirejä. Yksikkö täyttää standardissa kuvatut ehdot vain, jos laite, johonyksikkö liitetään, käyttää SELV-piirejä.



Pericolo: Questa unità funziona in condizioni di bassissima tensione di sicurezza (SELV, Safety Extra Low Voltage) secondo l'IEC 950. Tali condizioni sono rispettate solo se anche l'apparecchiatura a cui l'unità è collegata funziona in SELV.



Fare: Dette utstyret drives med strøm fra kretser med ekstra lav spenning (SELV-kretser) i henhold til standarden IEC 950. Denne spenningen opprettholdes kun dersom utstyret som det er koblet til, også drives av såkalte SELV-kretser.



Perigo: Esta unidade funciona sob condições SELV (Safety Extra Low Voltage - Tensão Muito Baixa, de Segurança), de acordo com a norma IEC 950. O estabelecido nesta norma só poderá ser mantido se o equipamento ao qual a unidade for ligada também funcionar sob aquelas condições SELV.



Peligro: Esta unidad opera bajo condiciones SELV (Safety Extra Low Voltage / Voltaje Extra Bajo de Seguridad) de acuerdo a la norma IEC 950, si bien tales condiciones únicamente se mantienen si el equipo al que se conectan es asimismo operacional bajo SELV.



Fara: Den här enheten arbetar under villkoren för kyddsklenspanning (Safety Extra Low Voltage) enligt IEC 950. Dessa villkor uppfylls endast om utrustning till vilken enheten ansluts också arbetar med kyddsklenspanning.



设备遵守IEC 950 标准,在SELV(Safety Extra Low Voltage安全超低电压)条件下操作.设备所连接的并维持的条件也仅仅只能是在SELV条件下才可操作.



Ovaj uređaj radi pod SELV uvjetima (Safety Extra Low Voltage) prema propisu IEC 950. Stoga se ovaj uređaj može spajati samo sa drugim uređajem koji također radi pod SELV uvjetima.



设备遵守IEC 950 标准,在SELV(Safety Extra Low Voltage安全超低电压)条件下操作.设备所连接的并维持的条件也仅仅只能是在SELV条件下才可操作.



Η συσκευή αυτή λειτουργεί υπό συνθήκες SELV (Safety Extra Low Voltage) σύμφωνα με την προδιαγραφή IEC 950, οι συνθήκες της οποίας τηρούνται μόνο αν ο εξοπλισμός με τον οποίον συνδέεται λειτουργεί επίσης υπό συνθήκες SELV.



Ez az egység biztonsági feszültségű (SELV) áramköri feltételek alatt üzemel, az IEC 950 (MSZ EN 60950) szabványnak megfelelően. Ezek a feltételek csak akkor maradnak fenn, ha a kapcsolódó berendezés szintén biztonsági feszültségű (SELV) áramként működik.



この装置は I E C (国際電気標準会議) 9 5 0 の S E L V (Safety Extra Low Voltage) の条件のもとで稼働しますが、もし他の機器を接続した場合はその機器が S E L V の条件を満たしているときに限ります。



본 장치는 IEC 950에 따라 SELV 조건(Safety Extra Low Voltage) 하에서 작동하며, 연결된 장비도 SELV하에서 작동할 수 있는 경우에만 조건이 유지보수됩니다.



Jednostka pracuje pod napięciem SELV (Safety Extra Low Voltage - Bezpiecznie niskie napięcie), zgodnym z warunkami IEC 950, spełnionymi jedynie wówczas, gdy sprzęt do którego jest podłączona działa również pod tym napięciem.



Это устройство работает по стандарту IEC 950 в условиях Безопасно низкого напряжения (SELV) только при условии, что все оборудование в цепи отвечает стандартам SELV.



Táto jednotka pracuje pod bezpečným napätím podľa IEC 950, ale len v prípade, že zariadenie, ku ktorému je pripojená tak isto pracuje pod bezpečným napätím



Naprava deluje pod pogoji SELV zaščite (Zaščita z Varnostno Malo Napetostjo) vskladu z IEC 950. Pogoji delovanja so zagotovljeni samo v primeru, če naprava, na katero je priključena, deluje tudi pod zaščito z malo napetostjo.



本裝置必須在 SELV (安全特低壓) 的條件下操作。
(根據 IEC 950, 唯有連接本裝置的設備也在 SELV 的條件下操作, 方可確保本裝置的操作環境正確無誤。)



DANGER: To comply with European safety standards, a spare fuse must not be fitted to the appliance inlet. Only fuses of the same manufacturer, make and type should be used with the unit.



DANGER: Pour conformer aux normes de sécurité européennes, un fusible de rechange ne doit pas être ajusté à l'admission d'appareil. Seulement les fusibles du même fabricant, construit, et type doivent être utilisés avec l'unité.



DANGER: Um Übereinstimmung mit den europäischen Sicherheitsnormen zu gewährleisten, darf am Zuführungstecker des Gerätes keine Ersatzsicherung angebracht werden. Nur Sicherungen der gleichen Herstellung und Marke sowie des gleichen Typs für das Gerät verwenden.



Gevarr: Om te voldoen aan de Europese veiligheidsnormen mag de reservezekering niet in de buurt van de stroomtoevoer worden bewaard. Gebruik voor de eenheid alleen zekeringen van dezelfde fabrikant, dezelfde makelij en hetzelfde type.



Perigo: Para que esteja em conformidade com os padrões de segurança europeus, o fusível sobressalente não deve ser encaixado na entrada do aparelho. Apenas fusíveis do mesmo fabricante e do mesmo tipo devem ser utilizados com a unidade.



Fare! Pga. de europæiske sikkerhedsstandarder må du ikke indsætte en reservesikring i enheden. Du må kun bruge sikringer af samme producent, mærke og type sammen med enheden.



Gevaar: Om te voldoen aan Europese veiligheidsrichtlijnen dient u geen willekeurige zekering te monteren op de ingang van het toestel. Gebruik voor deze eenheid alleen zekeringen van dezelfde fabrikant, en van hetzelfde merk en type.



Verra: Eurooppalaiset turvastandardit edellyttävät, ettei varauslaketta asenneta laitteen verkkojohtoon. Laitteessa saa käyttää vain saman valmistajan sulakkeita, joiden merkki ja tyyppi ovat alkuperäisen mukaiset.



Pericolo: Per essere in conformità agli standard di sicurezza europei, nella presa dell'apparecchiatura non deve essere utilizzato un fusibile di scorta qualsiasi. Con questa unità devono essere utilizzati esclusivamente fusibili dello stesso costruttore, dello stesso modello e dello stesso tipo di quelli originali.



Fare: I henhold til europeiske sikkerhetskrav må du ikke sette inn en reservesikring i apparatinntaket. Du må bare bruke sikringer som er fra samme leverandør og av samme type og merke i enheten.



Perigo: Por forma a respeitar as normas de segurança Europeias, não deve ser instalado um fusível de reserva na entrada do aparelho. Só devem ser utilizados, com a unidade, fusíveis do mesmo fabricante, marca e tipo do original.



Peligro: Según los estándares de seguridad europeos, no debe ponerse un fusible de repuesto en el aparato. Sólo deben utilizarse fusibles del mismo fabricante, marca y tipo en esta unidad.



Fara: För att enheten ska uppfylla europeiska säkerhetsbestämmelser ska endast säkringar av samma typ och fabrikat användas.



为了遵守欧洲安全标准, 禁用其他的保险丝, 只能使用厂家, 品牌和型



Da bi se udovoljilo evropskim sigurnosnim standardima, rezervni osigurač ne smije biti montiran na uređaj. Sa aparatom se moraju koristiti samo osigurači istog proizvođača, izrade i vrst



V souladu s Evropskými bezpečnostními standardy nesmí být náhradní pojistka vložena do pívodu spotřebiče. V zaizení smí být používány pouze pojistky stejného výrobce, provedení a typu.



Σύμφωνα με τις Ευρωπαϊκές προδιαγραφές ασφάλειας, δεν πρέπει να τοποθετούνται εφεδρικές ασφάλειες στην αντίστοιχη υποδοχή της συσκευής. Πρέπει να χρησιμοποιούνται μόνο ασφάλειες του ίδιου κατασκευαστή, της ίδιας μάρκας και του ίδιου τύπου.



Az európai biztonsági szabványoknak való megfelelés érdekében tartalék biztosítót nem kell a dugaljba helyezni. Az egységhez csak az azonos gyártó által készített egyező típusú biztosítókat használjuk.



ヨーロッパの安全基準では、スペアのフューズは電源接続器の入力側に取付けてはなりません。フューズを交換する場合は、同一メーカーの同じタイプの製品を使用してください。



유럽 안전 표준을 따르려면 예비 퓨즈를 기구 입구에 맞추어서는 안됩니다. 같은 제조업체, 같은 유형의 퓨즈만이 장치에 사용되어야 합니다.



Zgodnie z europejskimi standardami bezpieczeństwa, zapasowy bezpiecznik nie może znajdować się we wkładanej oprawie. W jednostce można używać jedynie bezpieczników tego samego producenta, rodzaju i typu.



В соответствии с Европейскими стандартами по мерам безопасности запрещается вставлять запасной предохранитель на входе электроприбора. Для блока подходят только предохранители того же изготовителя, типа и модели.



Náhradná poistka nemôže byť nainštalovaná do zariadenia ak nie je schválená výrobcom zariadenia a ak nezodpovedá typu poistky určenej pre zariadenie.



Zaradi usklajenosti z evropskimi standardi v lezišce varovalke na napravi ni dovoljeno vstaviti poljubno izbrano varovalko. Uporabljajte samo varovalke istega tipa, proizvajalca in izdelave.



為符合歐洲安全標準，您不可在設備入口裝配備用保險絲。
本機器只應使用同一製造商、製造方法與類型的保險絲。



DANGER: Ensure that the power supply lead is disconnected before opening the IEC connector fuse cover or removing the cover of the unit.



DANGER: Assurer que l'entrée de la source d'alimentation soit débranchée avant d'ouvrir le couvercle de fusible du connecteur IEC ou d'enlever le couvercle de l'unité.



DANGER: Vorm Öffnen der Abdeckungsklappe der IEC Steckverbindungssicherung oder vorm Abnehmen der Gesamtabdeckung der Gerät sicherstellen, daß das Stromverbindungskabel vom Netzstrom getrennt ist.



Gevaar: Zorg ervoor dat het netsnoer losgekoppeld is voordat u de klep van de IEC-zekering opent of verwijdert.



Perigo: Antes de abrir a tampa do fusível do conector IEC, ou remover a tampa da unidade, certifique-se de que o fio da fonte de alimentação esteja desconectado.



Fare! Zorg ervoor dat het snoer van de voedingseenheid ontkoppeld is voordat u de afdekplaat van de zekeringen van de IEC-connectors opent of de kap van de eenheid verwijdert.



Gevaar: Kontrollér, at strømforsyningsledningene er afmonteret, før du åbner dækslet til IEC-stikkets sikring eller enhedens dæksel.



Varra: Varmista, että olet irrottanut verkkojohdon, ennen kuin avaat IEC-liittimen sulakekotelon kannen tai irrotat yksikön kannen.



Pericolo: Prima di aprire il coperchio del fusibile del connettore IEC oppure prima di rimuovere il coperchio dell'unità, accertarsi che il cavo dell'alimentatore sia scollegato.



Fare: Pass på at nettkabelen er frakoblet før du åpner dekslet til sikringsholderen eller tar av dekslet på enheten.



Perigo: Assegure-se de que o cabo de alimentação eléctrica está desligado, antes de abrir a tampa do compartimento de fusíveis do conector IEC ou de remover a cobertura da unidade.



Peligro: Asegúrese de que la línea de la fuente de alimentación esté desconectada antes de abrir la cubierta del fusible del conector IEC o extraer la cubierta de la unidad.



Fara: Se till att strömförsörjningskabeln är urkopplad innan du öppnar säkringslocket på IEC-kontakten eller tar bort enhetens kåpa.



在打开IEC连接器保险丝盖或移动设备盒盖以前，确保电源线已断开。



Provjerite da je kabel napajanja isključen prije promjene osigurača ili skidanja pokrova uređaja.



P ed otev enim krytu pojistky v IEC konektoru nebo odstran nim krytu za izení se ujist te, že je odpojena napájecí š ra sí ovéh o zdroje.



Βεβαιωθείτε ότι έχετε αποσυνδέσει το καλώδιο παροχής ρεύματος πριν ανοίξετε το κάλυμμα της ασφάλειας του συνδέσμου IEC ή αφαιρέσετε το κάλυμμα της συσκευής.



Biztosítsuk, hogy a hálózati csatlakozó kábel ki legyen húzva a dugaljából, mielőtt az IEC csatlakozó biztosítójának fedelét kinyitjuk vagy az egység fedelét levesszük.



IECコネクターのフューズのカバーを開けたり、装置のカバーを取り離す場合は、先に電源ケーブルを抜いてください。



IEC 커넥터 퓨즈 커버를 열거나 장치의 커버를 제거하기 전에 반드시 전원 공급 장치의 도선을 끊으십시오.



Przed otwarciem osłony gniazda bezpieczników IEC lub pokrywy urządzenia należy odłączyć kabel zasilający.



Перед тем, как открывать крышку предохранителя разъема IEC или снимать крышку блока, убедитесь, что подводящий электропровод отсоединен от сети.



Uistite sa, že napájacia šnúra je odpojená pred tým ako otvoríte IEC poistkový konektor alebo odstránite kryt zo zariadenia.



Preden odprete pokrov za varovalko na IEC vtiču ali odprete pokrov naprave, morate izkjučiti električno napajanje.



在打開 IEC 連接器保險絲蓋子或移除本機器的蓋子之前，請先確定電源導線已斷電。



DANGER: Ensure that the power is disconnected before opening the fuse holder cover. Only 5A Time Delay (anti-surge) fuses of the same type and manufacture as the original should be used.



DANGER: Assurer que l'alimentation soit débranchée avant d'ouvrir le couvercle du contenant du fusible. Seulement les fusibles de types 5A anti-transitoires du même type et fabricant que l'original doivent être utilisés.



DANGER: Vor dem Öffnen der Sicherungshalterung das Gerät vom Netzstrom trennen. Sicherungen nur durch gleichen Typ und Wert wie die Originalsicherung ersetzen. Sicherung auswechseln und die Klappe der Sicherungshalterung wieder schließen.



Gevaar: Zorg ervoor dat de stroomtoevoer afgesloten is voordat u de zekeringkast opent. Er mogen alleen zekeringen metvertraagde werking (anti-stroomstoot) van 5A worden gebruikt die van hetzelfde type en dezelfde makelij zijn als de originele zekeringen.



Perigo: Antes de abrir a tampa do prendedor do fusível, certifique-se de que a alimentação esteja desconectada. Devem ser utilizados apenas fusíveis 5A Time Delay (contra pico de energia) do mesmo tipo e fabricante originais.



Fare! Kontrollér, at strømmen er slukket, før du åbner sikringsholderens dæksel. Du må kun bruge træge 5A-sikringer (anti-surge) af samme type og producent som de originale sikringer.



Gevaar: Zorg ervoor dat de stroom is afgesloten voordat de afdekplaat van de zekeringhouder opent. Gebruik uitsluitend 5A zekeringen met tijdvertraging (anti-piek) van hetzelfde type en van dezelfde makelij als de originele zekeringen.



Vaara: Tarkista, että olet katkaissut virran, ennen kuin avaatsulakekotelon kannen. Laitteessa saa käyttää vain samantyyppisiä hitaita viiden ampeerin sulakkeita kuin alkuperäiset.



Pericolo: Accertarsi di togliere l'alimentazione prima di aprire il coperchio del porta-fusibili. Devono essere utilizzati soltanto fusibili da 5 A ad azione ritardata (anti-surge) dello stesso tipo e dello stesso costruttore di quelli originali.



Fare: Pass på at strømmen er slått av før du åpner dekselet til sikringsholderen. Bruk bare 5A sikringer (treg) av samme type og fabrikat som den originale sikringer.



Perigo: Assegure-se de que a alimentação eléctrica está desligada, antes de abrir a tampa do compartimento de fusíveis. Só devem ser utilizados fusíveis lentos (com atraso, anti-picos de corrente) de 5 Amperes, do mesmo tipo e fabricante do original.



Peligro: Asegúrese de que la alimentación esté desconectada antes de abrir la cubierta de soporte del fusible. Sólo deben usarse los fusibles 5A Time Delay (anti-surge) del mismo tipo y fabricante que el original.



Fara: Se till att strömmen är frånslagen innan du öppnar locket på säkringshållaren. Använd endast 5A tröga säkringar av samma typ och fabrikat som originalet.



危険：
在打开保险丝支架盖前，确保电源已断开。只能使用型号和厂家与最（ ）的保险（ ）

**OPASNOST**

Prije otvaranja pokrova osigurača provjerite da li je uređaj isključen iz električne mreže. Koristiti samo 5A osigurače sa vremenskim zaostajanjem (anti - surge) iste vrste i proizvođa

**Nebezpe i :**

P ed otev ení krytu držáku pojistky se ujist te, že je odpojen c napájení. Sm jí být používány pouze pojistky 5A s asovým zpožd ním (protipulzní) stejného typu a výrobce jako originál.

**Κίνδυνος:**

Βεβαιωθείτε ότι έχετε αποσυνδέσει την παροχή ρεύματος πριν ανοίξετε το κάλυμμα της ασφάλειας. Πρέπει να χρησιμοποιούνται μόνο ασφάλειες 5A θραδείας τήξεως (Time Delay) του ίδιου τύπου και κατασκευαστή με την αρχική ασφάλεια.

**VIGYÁZAT, VESZÉLY!**

Biztosítsuk, hogy feszültségmentes állapotban kerüljön sor a biztosítótartó fedelének nyitására. Csak 5 A-es késleltetett kiolvadású, az eredetivel egyező típusú és gyártmányú biztosítókat használjunk.

**危険：**

フューズ・ホルダーのカバーを開ける前に電源ケーブルを抜いてください。交換用フューズはそれまで使用されていたものと同一メーカーの同じタイプの5A(Time Delay, Anti-surge)のみを使用してください。



퓨즈함 커버를 열기 전에 전원을 끊었는지 확인하십시오. 원래의 퓨즈와 같은 유형의 5A Time Delay(반동요) 퓨즈만 사용해야 합니다.

**Niebezpieczeństwo:**

Przed otwarciem osłony gniazda bezpieczników należy sprawdzić, czy zasilanie jednostki zostało odłączone. Stosować można tylko bezpieczniki 5A Ze Zwłoką (antyprzepięciowe) wykonane przez tego samego producenta i tego samego typu, co oryginalne.

**Опасно:**

Перед тем, как открывать крышку гнезда предохранителя, убедитесь, что питание отключено. Следует использовать только предохранители 5A Time Delay (с защитой от бросков напряжения в сети) того же типа и изготовителя, что и у исходных.

**Nebezpečnostvo:**

Uistite sa, že napájacia šnúra je odpojená pred tým ako otvoríte ICE - poistkový konektor alebo odstránite kryt zo zariadenia.

**Nevarnost !**

Preden odprete pokrov ležišča varovalke se prepričajte, da je električno napajanje izklopljeno. Uporabljajte izključno 5A varovalke s časovno zakasnitvijo (prenapetostno o zaščito) istega tipa in proizvajalca kot so originalne.

**危険：**

在打開保險絲盒的蓋子之前，請先確定電源已切斷。您應該只能使用與原始保險絲同樣類型及製造商的「5A Time Delay」(反波動)保險絲。



DANGER: The sockets for a Redundant Power System are designed to only be used with a recommended RPS.



DANGER: Ces prises sont réservées exclusivement à une alimentation redondante (RPS) recommandée.



Gefahr: Diese Buchsen sind nur für den Einsatz mit einer empfohlenen redundanten Stromversorgung (RPS) vorgesehen.



Gevaar: Deze stekkerdozen zijn ontworpen om alleen te worden gebruikt met een extra voedingseenheid.



Perigo: Esses soquetes foram projetados para serem utilizados apenas com uma Fonte de Alimentação Redundante recomendada.



Fare! Disse sokler må kun bruges sammen med en anbefalet RPS (Redundant Power Supply).



Gevaar: Deze aansluitingen mogen alleen met een aanbevolen reservevoeding worden gebruikt.



Vaara: Näihin vastakeisiin saa kytkeä vain suositellun ylimääräisen jännitelähteen.



Pericolo: Queste prese sono progettate per essere utilizzate esclusivamente con il tipo di alimentatore addizionale raccomandato.



Fare: Disse uttakene skal kun brukes til en anbefalt e kstra strømforsyningsenhet.



Perigo: Estas tomadas foram concebidas para serem utilizadas apenas com uma Redundant Power Supply (Fonte de Alimentação de Reserva) recomendada.



Peligro: Estos zócalos han sido diseñados para ser utilizados sólo con un fuente de alimentación redundante recomendada.



Fara: De här uttagen är konstruerade för att endast användas tillsammans med det rekommenderade redundanta kraftsystemet.



危险：

这些插座设计为只能与推荐的电源一起使用。



OPASNOST

Te utičnice su izvedene samo za korištenje sa preporučenim dodatnim izvorom napajanja.



Nebezpečí:

Tyto zásuvky jsou navrženy pouze pro používání s doporučeným náhradním zdrojem napájení.



Κίνδυνος:

Οι υποδοχές αυτές είναι σχεδιασμένες να χρησιμοποιούνται μόνο με κάποια προτεινόμενη εφεδρική παροχή ρεύματος (Redundant Power Supply).



VIGYÁZAT!

Ezeket a foglalatokat kizárólag az ajánlott redundáns tápegység használatára tervezték!



危険：

これらのソケットは、推奨されたRPS（リダンダント電源装置）だけに使用するように設計されています。

**위험:**

이 소켓은 권장되는 Redundant Power Supply만 함께 사용되도록 설계되었습니다.

**Niebezpieczeństwo:**

Gniazda te zaprojektowano wyłącznie do użytku z zalecanym źródłem zasilania redundantnego.

**Опасно:**

Эти гнезда предназначены для использования только с рекомендованным дополнительным источником питания.

**Nebezpečnosť:**

Tieto zásuvky sú určené iba na použitie s odporúčaným zdrojom náhradného napájania (UPS).

**Nevarnost !**

Te vtičnice so namenjene samo za uporabo s priporočenim redundantnim napajalnikom

**危險：**

這些插座僅適用於建議的備援式電源供應器。



DANGER: The RJ45 ports are shielded RJ45 data sockets. They cannot be used as telephone sockets. Only connect RJ45 data connectors to these sockets. Either shielded or unshielded data cables with shielded or unshielded jacks can be connected to these data sockets.



DANGER: Ceux-ci sont les prises de courant de données RJ45 protégées. Ils ne peuvent pas être utilisés comme prises de courant téléphoniques. Brancher seulement les connecteurs RJ45 de données à ces prises de courant. Les câbles de données blindés ou non blindés, avec les jacks blindés ou non blindés, l'un ou l'autre, peuvent être branchés à ces prises de courant de données.



DANGER: Hierbei handelt es sich um abgeschirmte RJ45 Datenbuchsen, die nicht als Telefonbuchsen verwendbar sind. Nur RJ45 Datensteckverbinder an diese Buchsen anschließen. Diese Datenstecker können entweder mit abgeschirmten oder ungeschirmten Datenkabeln mit abgeschirmten oder ungeschirmten Klinkensteckern verbunden werden.



Gevaar: De RJ45-poorten zijn afgeschermd RJ45-contactdozen voor gegevens. Ze kunnen niet worden gebruikt als telefoonansluitingen. Op deze contactdozen mogen alleen RJ45-gegevensstekkers worden aangesloten. Er kunnen zowel afgeschermd als niet-afgeschermd gegevenskabels met al dan niet afgeschermd aansluitingen op deze gegevenscontactdozen worden aangesloten.



Perigo: As portas RJ45 são soquetes de dados RJ45 isolados. Não podem ser utilizados como soquetes de telefone. Ligue apenas conectores de dados RJ45 nesses soquetes. Cabos de dados isolados ou não com tomadas isoladas ou não podem ser conectados a esses soquetes de dados.



Fare! RJ45-portene er afskærmede RJ45-datasokler. De kan ikke bruges som telefonstik. Du må kun indsætte RJ45-datastik i disse sokler. Afskærmede eller uafskærmede datakabler med afskærmede eller uafskærmede jackstik kan tilsluttes disse datasokler.



Gevaar: Op deze datapoorten kunnen zowel afgeschermd als niet-afgeschermd datakabels metaafgeschermd of niet-afgeschermd pluggen worden aangesloten.



Vaara: RJ45-portit ovat suojattuja RJ45-datavastakkeita. Niitä ei voida käyttää puhelinvastakkeina. RJ45-datavastakkeeseen saa kytkeä vain RJ45-dataliitimiä. Näihin datavastakkeisiin voi kytkeä suojattuja taisyöjaamattomia datakaapeleita, joissa on suojattu tai suojaamaton pistoke.



Pericolo: Le porte RJ45 sono schermate e riservate alla trasmissione di dati; esse non possono essere utilizzate come prese telefoniche. Collegare a queste porte soltanto connettori per dati RJ45. A queste porte possono essere collegati sia cavi schermati che non schermati dotati di connettori schermati o non schermati.



Fare: RJ45-portene er skjærmede RJ45-datauttak, og kan ikke brukes som telefonuttak. Du må bare koble RJ45-datakontakter til disse uttakene. Du kan koble enten skjærmede eller ikke-skjærmede datakabler med skjærmede eller ikke-skjærmede jack-plugger til disse datauttakene.



Perigo: As portas RJ45 são tomadas de dados RJ45, blindadas. Não podem ser utilizadas como tomadas de telefone. Ligue unicamente fichas de dados RJ45 a estas tomadas. A estas tomadas de dados podem ser ligados cabos de dados blindados ou não, por intermédio de fichas blindadas ou não.



Peligro: Los puertos RJ45 son zócalos de datos RJ45 protegidos. No se pueden utilizar como zócalos telefónicos. Conecte sólo los conectores de datos RJ45 a estos zócalos. A estos zócalos de datos pueden conectarse tanto cables de datos protegidos como no protegidos con conectores protegidos o no protegidos.



Fara: RJ45-portarna är skærmede RJ45 datauttag och kan inte användas som telefonuttag. Anslut endast RJ45 datakontakter till dess uttag. Antingen skærmede eller oskærmede datakabler med skærmede eller oskærmede kontakter kan anslutas till datauttagen.



危险：
RJ45端口使用RJ45数据插座，不能用作电话插座。这些插座只能与RJ45数

的故

**OPASNOST**

Ulazi RJ45 su oklopljeni RJ45data utičnice, koji se ne mogu koristiti kao telefonske utičnice. Priključite samo RJ45 data konektore na te utičnice. Oklopljeni ili neoklopljeni kablovi za prijenos podataka

**Nebezpečí :**

Porty RJ45 jsou stíněné nebo datové zásuvky RJ45. Zásuvky nemohou být užívány jako telefonní. Do těchto zásuvek připojujte pouze datové konektory RJ45.

Do těchto datových zásuvek mohou být připojeny stíněné nebo nestíněné datové kabely se stíněnými nebo nestíněnými konektory.

**Κίνδυνος:**

Οι θύρες RJ45 είναι θωρακισμένες υποδοχές δεδομένων RJ45. Δεν μπορούν να χρησιμοποιηθούν ως υποδοχές τηλεφώνου. Στις υποδοχές αυτές πρέπει να συνδέονται μόνο σύνδεσμοι δεδομένων RJ45.

Σε αυτές τις υποδοχές δεδομένων μπορούν να συνδεθούν θωρακισμένα ή μη θωρακισμένα καλώδια δεδομένων με θωρακισμένα ή μη θωρακισμένα βύσματα.

**VIGYÁZAT, VESZÉLY!**

Az RJ45 típusú foglalatok adat csatlakozók, telefonálzatnak nem használhatók. Ezekbe a foglalatokba csak RJ45 típusú adat csatlakozókat dugaszoljunk.

Ezekbe a foglalatokba akár árnyékolt, akár árnyékoltatlan adat kábelek csatlakoztathatók, árnyékolt vagy árnyékoltatlan dugóval.

**危険：**

RJ45ポートはシールドされたRJ45データのソケットです。このポートは電話用ソケットとしては使えません。RJ45データ・コネクタだけを接続してください。接続するケーブルおよびジャックはそれぞれシールドされたものでもシールドされていないものでも使用できます。

**위험:**

RJ45 포트는 쉴드된 RJ45 데이터 소켓입니다. 전화 소켓으로는 사용할 수 없습니다. RJ45 데이터 커넥터만 이 소켓에 연결하십시오. 쉴드되거나 쉴드되지 않은 잭이 있는, 쉴드되거나 쉴드되지 않은 데이터 케이블들다 이 데이터 소켓에 연결될 수 있습니다.

**Niebezpieczeństwo:**

Porty RJ45 są ekranowanymi gniazdami danych RJ45. Nie można ich używać jako gniazd telefonicznych. Podłączać do nich można tylko złącza danych RJ45.

Do tych gniazd danych mogą być podłączane zarówno ekranowane, jak i nieekranowane kable danych z ekranowanymi lub nieekranowanymi wtyczkami.

**Опасно:**

Порты RJ45 представляют собой экранированные сигнальные гнезда RJ45. Их нельзя использовать в качестве телефонных гнезд. К этим гнездам можно подсоединять только сигнальные разъемы RJ45.

К этим сигнальным гнездам разрешается подсоединять экранированные или неэкранированные сигнальные кабели с экранированными или неэкранированными разъемами.



Nebezpečenstvo:

RJ45 porty sú tienené RJ45 dátové zásuvky. Nemôžu sa používať ako telefónne zásuvky. Zapoj iba RJ45 - dátové konektory do týchto zásuviek.

Iba tienené a netienené dátové káble s tieněných alebo netienených konektorov môžu byť zapojené do týchto dátových zásuviek.



Nevarnost!

Priključki RJ45 so oklopljene podatkovne vtičnice. Ne uporabljajte jih kot telefonske vtičnice. Vanje lahko priključujete samo podatkovne vtiče tipa RJ45.

Na podatkovne vtičnice lahko priključujete bodisi oklopljene ali neoklopljene kable z oklopljenimi ali neoklopljenimi konektori.



危險：

RJ45 埠是屏蔽的 RJ45 資料插座。它們不能當作電話插座使用。您只能將 RJ45 資料連接器連接至這些插座。

具有屏蔽或非屏蔽之插孔的屏蔽及非屏蔽資料電纜，都可以連接至這些資料插座。



DANGER: This unit cannot be powered from IT (impedance à la terre) supplies. If your supplies are of the IT type, this unit should be powered by 230V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to Earth (Ground).



DANGER: Cette unité ne peut pas être mise en marche des sources de courant IT (Impédance à la terre). Si vos sources de courant sont de type IT, cette unité doit être alimentée par 230V (2P+T) via un rapport de transformation d'isolation de 1:1, avec un point de connexion secondaire étiqueté Neutre, branché directement à la Terre (à la Masse).



Peligro: Esta unidad no puede alimentarse con fuentes IT (impedance áa la terre). Si sus fuentes son de tipo IT, esta unidad debería alimentarse a 230V (2P+T) utilizando un transformador de ratio 1:1, con el punto de conexión secundario etiquetado como Neutral y conectado directamente a tierra.



DANGER: The power cord set must be approved for the country where it will be used.

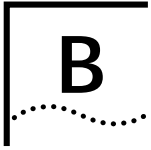


DANGER: La cordon d'alimentation surmoulé doit être approuvé pour le pays auquel il sera utilisé.



DANGER: Der Anschlußkabelsatz muß mit den Bestimmungen des Landes übereinstimmen, in dem er verwendet werden soll.





SCREEN ACCESS RIGHTS

The following table lists the rights assigned to each level of user for accessing and editing Switch screens via the VT100 interface.

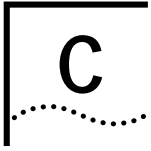
All access rights are read-and-write unless otherwise stated.

Screen	Available to access level...
Logon	Monitor
	Manager
	Security
Main Menu	Monitor
	Manager
	Security
Switch Management	Monitor
	Manager
	Security
Port STP	Monitor <i>read-only</i>
	Manager
	Security
Port Statistics	Monitor
	Manager
	Security

Screen	Available to access level...
Port Traffic Statistics	Monitor
	Manager
	Security
Port Error Analysis	Monitor
	Manager
	Security
Port Resilience	Monitor
	Manager
	Security
Port Setup	Monitor <i>read-only</i>
	Manager
	Security
Unit Statistics	Monitor
	Manager
	Security
Unit Database View	Monitor
	Manager
	Security
Unit Resilience	Monitor
	Manager
	Security
Unit Setup	Monitor <i>read-only</i>
	Manager
	Security

Screen	Available to access level...
VLAN STP	Monitor <i>read-only</i> Manager Security
VLAN Server	Monitor <i>read-only</i> Manager Security
VLAN Setup	Monitor <i>read-only</i> Manager Security
User Access Levels	Monitor Manager Security
Local Security	Security
Create User	Security
Delete Users	Security
Edit User	Monitor Manager Security
Status	Monitor Manager Security
Fault Log	Monitor Manager Security
Management Setup	Monitor <i>read-only</i> Manager Security

Screen	Available to access level...
Trap Setup	Monitor <i>read-only</i> Manager Security
Console Port Setup	Monitor <i>read-only</i> Manager Security
Software Upgrade	Security
Initialize	Security
Reset	Manager Security
Remote Poll	Manager Security



TROUBLESHOOTING

The following is a list of problems you may see when managing the Switch with suggested courses of corrective action to take. If you have a problem which is not listed here and you cannot solve it, please contact your local technical support representative.

LEDs

Power LED does not light:

Check that the power cable is firmly connected to the device and to the supply outlet.

Check the unit fuse. For information on changing the fuse, refer to “Power Socket and Fuse” in Chapter 1.

On powering-up, the MGMT LED lights yellow:

The unit has failed its Power On Self Test (POST) and you should contact your supplier for advice.

On powering-up, the MGMT LED flashes yellow:

The installed Plug-in Module has failed its Power On Self Test (POST). Try re-installing the Plug-in Module, ensuring it is properly seated. If the problem persists, contact your supplier for advice.

The Plug-in Module Status LED lights yellow:

If the MGMT LED is flashing yellow, the Module has failed its Power On Self Test; refer to the previous advice. Otherwise, the Module’s agent software is not installed correctly. Refer to the User Guide supplied with the Module.

The Plug-in Module Status LED flashes yellow:

The Module is not recognized. You may need to download a version of the Switch’s management agent software that recognizes the Module (refer to “Upgrading Software” on page 4-29), or remove the Module. Contact your supplier for further advice.

A link is connected and yet the Status LED does not light:

Check that:

- All connections are secure
- Fiber cables are free from damage
- The devices at both ends of the link are powered-up
- The connection uses cross-over cable if you are linking a 10BASE-T or 100BASE-TX port with a device which is MDIX-only

Using the VT100 Interface

The initial Main Banner screen does not display:

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

For console port access, you may need to press [Return] several times before the Main Banner appears.

Check the settings on your terminal or terminal emulator. The management facility's auto configuration works only with baud rates from 1200 to 19,200.

Screens are incorrectly displayed:

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

Check the settings on your terminal or terminal emulator. The management facility's autoconfiguration works only with baud rates from 1200 to 19,200.

Check that you are using a suitable font (for example, in HyperTerminal use the MS LineDraw font).

The SNMP Network Manager cannot access the device:

Check that the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Check that the device's IP address is correctly recorded by the SNMP Network Manager (refer to the user documentation for the Network Manager).

The Telnet workstation cannot access the device:

Check the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Ensure that you enter the IP address of the Switch correctly when invoking the Telnet facility.

Traps are not received by the SNMP Network Manager:

Check that the SNMP Network Manager's IP address and community string are correctly configured.

The SNMP Network Manager or Telnet workstation can no longer access the device:

Check that Remote Telnet access or Community-SNMP access is enabled.

Check that the port through which you are trying to access the device has not been disabled, refer to "Setting Up the Switch Ports" on page 4-12. If it is enabled, check the connections and network cabling at the port.

Check that the port through which you are trying to access the device is in VLAN 1 (the Default VLAN). Refer to “Setting Up VLANs on the Switch” on page 5-7.

Try accessing the device through a different port. If you can now access the device, a problem with the original port is indicated. Re-examine the connections and cabling.

There may be a network problem preventing you accessing the device over the network. Try accessing the device through the console port.

You forget your password and cannot log on:

If you are not one of the default users (monitor, manager or security), another user having ‘security’ access level can log on, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having ‘security’ access level can log in and initialize the device. This will return all configuration information, including passwords, to the initial values.

In the case where no-one knows a password for a security level user, contact your supplier.

Using the Switch

You see network problems and the Packet LED is on continuously with constant collisions (refer to “Port Traffic Statistics” on page 6-4):

You are using PACE equipped devices and have the Interactive Access feature of PACE enabled at both ends of the link. Interactive Access must only be enabled at one end of the Switch-device link. Disabling Interactive Access for a Switch port is described in “Setting Up the Switch Ports” on page 4-12.

You have configured a Switch port so that it ‘blips’ when a broadcast storm occurs, but the port does not blip properly:

The broadcast storms are occurring such that the average broadcast bandwidth cannot drop below the Falling Threshold value. This means that the blip only occurs once.

Try changing the following attributes in the Broadcast Storm Control section of the Port Setup screen:

- Rising Action to *disable port/notify*.
- Falling Action to *event + enable*.

For more information, refer to “Setting Up the Switch Ports” on page 4-12.

You have added the Switch to an already busy network, and response times and traffic levels have increased:

You may have added a group of users to one of the Switch ports via a repeater or switch, and not turned off IFM. Turn off IFM on any port that is connected to multiple devices. Refer to “Setting Up the Switch Ports” on page 4-12.

You have connected an endstation directly to the Switch and the endstation fails to boot correctly:

The Switch has STP enabled, and the endstation is booting before the STP initialization process is complete. Specify that the port has Fast Start enabled, and then reboot the endstation. For more information about specifying Fast Start for a port, refer to “Configuring the STP Parameters of Ports” on page 5-18.

The Switch keeps ageing out endstation entries in the Switch Database (SDB):

The Switch has STP enabled, and STP is instructing the Switch to age entries in the SDB faster because topology changes are occurring in the network.

- 1 Reduce the number of topology changes by enabling Fast Start for all ports which are directly connected to an endstation; refer to “Configuring the STP Parameters of Ports” on page 5-18.
- 2 Specify that the endstation entries are Non-ageing; refer to “Setting Up the Switch Database (SDB)” on page 4-16.
- 3 Consider disabling STP on the Switch, and using resilient links to provide network resilience; refer to “Enabling STP on the Switch” on page 5-15 and “Setting Up Resilient Links” on page 4-19.

You are trying to manage the Switch over a network which has STP, and you are losing contact with the management agent intermittently:

As shown in Figure C-1, there is an IBM 8271 Nways Ethernet LAN Switch unit (Switch A) between your management workstation and the Switch (Switch B). You have configured more than one VLAN on both Switch units, and there is a parallel STP path for each VLAN between the Switch units.

When Switch B transmits BPDUs across a VLAN other than VLAN 1, Switch A learns the MAC address of Switch B through the port on that VLAN. The management agent of Switch B is only accessible through VLAN 1, and so your management workstation cannot communicate with Switch B until it transmits BPDUs across VLAN 1. When that occurs, Switch A learns the MAC address of Switch B through the port on VLAN 1.

To avoid this situation, we recommend that you connect the two IBM 8271 Nways Ethernet LAN Switch units using a Virtual LAN Trunk (VLT). For more information about VLTs, refer to "Connecting Common VLANs Between Switch Units" on page 5-3.

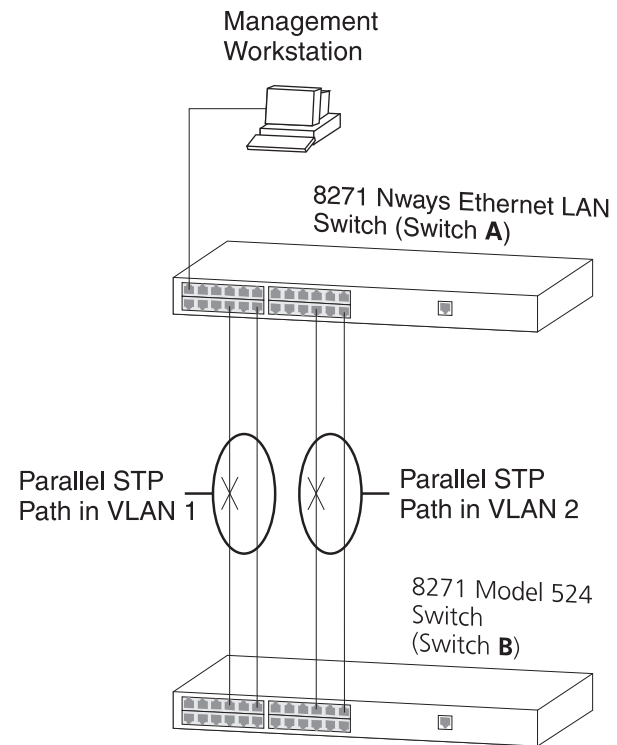
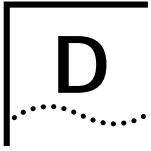


Figure C-1 Network configuration that results in loss of contact

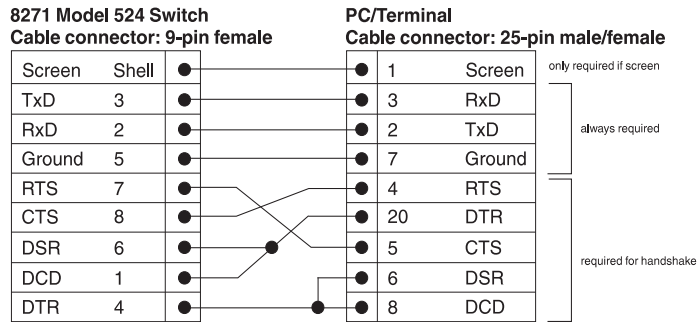




PIN-OUTS

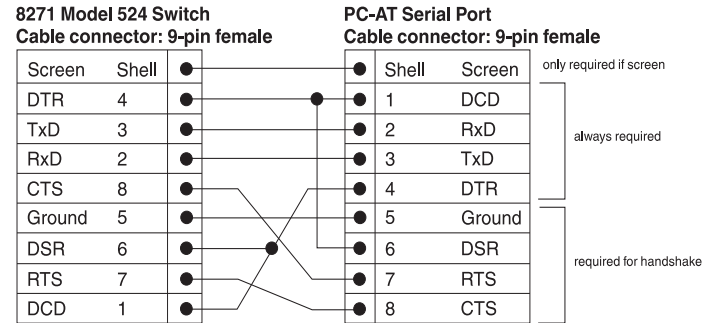
Null Modem Cable

9-pin to RS-232 25-pin



PC-AT Serial Cable

9-pin to 9-pin



Modem Cable

9-pin to RS-232 25-pin

8271 Model 524 Switch

Cable connector: 9-pin female

Screen	Shell	●
TxD	3	●
RxD	2	●
RTS	7	●
CTS	8	●
DSR	6	●
Ground	5	●
DCD	1	●
DTR	4	●

RS-232 Modem Port

Cable connector: 25-pin male

●	1	Screen
●	2	TxD
●	3	RxD
●	4	RTS
●	5	CTS
●	6	DSR
●	7	Ground
●	8	DCD
●	20	DTR

RJ45 Pin Assignments

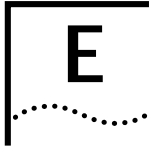
Pin assignments are identical for 10BASE-T and 100BASE-TX RJ45 connectors.

Ports configured as MDI

Pin Number	Signal	Function
1	TxD+ +	Transmit data
2	TxD- -	Transmit data
3	RxD+ +	Receive data
4	Not Assigned	
5	Not Assigned	
6	RxD- -	Receive data
7	Not Assigned	
8	Not Assigned	

Ports configured as MDIX

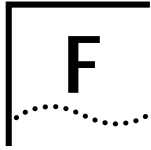
Pin Number	Signal	Function
1	RxD+ +	Receive data
2	RxD- -	Receive data
3	TxD+ +	Transmit data
4	Not Assigned	
5	Not Assigned	
6	TxD- -	Transmit data
7	Not Assigned	
8	Not Assigned	



SWITCH TECHNICAL SPECIFICATIONS

Physical Dimensions	Height: 76mm (3.0 in.) x Width: 483mm (19.0 in.) x Depth 300mm (12.0 in.) Weight: 4.4kg (9.7lbs)
Environmental Requirements	
Operating Temperature	0 to 50°C / 32 to 122°F
Storage Temperature	-10 to 70°C / 14 to 158°F
Operating Humidity	10-95% relative humidity, non-condensing
Standards	EN60068 (IEC68)
Safety	
Agency Certifications	UL 1950, EN60950, CSA 22.2 No. 950
AC Protection	5A Time Delay Fuse
Electromagnetic Compatibility	EN55022 Class B*, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class 2*, AS/NZS 3548 Class B*, EN 50082-1 * Category 5 screened cables must be used to ensure compliance with the Class B/Class 2 requirements of this standard. The use of unshielded cables (Category 5 for 100BASE-TX ports, and Category 3 or 5 for 10BASE-T ports) complies with the Class A/Class 1 requirements.
Heat Dissipation	100W maximum (341 BTU/hr maximum)
Power Supply	
AC Line Frequency	50-60 Hz
Input Voltage Options	100-120 / 200-240 VAC
Current Rating	3A (maximum) at 100 VAC / 2A (maximum) at 200 VAC

Standards Supported	SNMP	Protocols Used for Administration
	SNMP protocol (RFC 1157)	UDP (RFC 768)
	MIB-II (RFC 1213)	IP (RFC 791)
	Bridge MIB (RFC 1493)	ICMP (RFC 792)
	Repeater MIB (RFC 1516)	TCP (RFC 793)
	VLAN MIB (RFC 1573)	ARP (RFC 826)
	RMON MIB (RFC 1271 and RFC 1757)	TFTP (RFC 783)
	Terminal Emulation	BOOTP (RFC 951)
	Telnet (RFC 854)	



TECHNICAL SUPPORT AND SERVICE

This appendix provides contacts for help if you have questions about the IBM 8271 Nways Ethernet LAN Switch products or if the IBM 8271 Nways Ethernet LAN Switch products are not working correctly. It also explains how to access the IBM electronic sites to obtain the latest versions of microcode and release notes.

Electronic Support

This section explains how to access the IBM electronic site to obtain the latest version of microcode, drivers, and software by using the Internet World Wide Web, FTP, or the IBM BSS.

WWW

<http://www.networking.ibm.com/>

This is the IBM Networking home page. From here, you can access product announcements, publications, and other information regarding hardware and software updates, and a technical support information database. The direct path to the support area is:

<http://www.networking.ibm.com/nes/neshome.html>

FTP

[lansupport.raleigh.ibm.com](ftp://lansupport.raleigh.ibm.com)

IBM Bulletin Board System

Using a modem you can access the IBM BSS to obtain the latest versions of software. Set your modem and communications software to:

- 8 data bits
- no parity
- 1 stop bit

Dial one of the following numbers:

- United States: (919) 517-0001
- Toronto (905) 316-4255
- Vancouver: (604) 664-6464
- Montreal: (514) 938-3022

Voice Support

IBM Network Hardware support: 1-800-772-2227.
Follow the menu prompts for Network Hardware.

For support outside of the United States, please contact your IBM marketing representative or IBM reseller.





NOTICES, TRADEMARKS, AND WARRANTIES

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 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, 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.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

IBM, Nways

SmartAgent is a registered trademark, and PACE is a trademark, of 3Com Corporation.**

VT100 is a trademark of Digital Equipment Corporation.

Novell is a registered trademark of Novell, Incorporated. IPX is a trademark of Novell, Incorporated.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

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 your reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them. Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. If you have any questions, contact IBM or your reseller.

Machine: IBM 8271 Model 524 Nways Ethernet LAN Switch

Warranty Period*: 1 Year

*Contact your place of purchase for warranty service information.

Production Status

Each Machine is manufactured from new parts, or new and used 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 for Machines

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. The warranty period for a Machine is a specified, fixed period commencing on its 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, if authorized by IBM, 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.

For IBM or your reseller to provide warranty service for a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many of these transactions involve the removal of parts and their return to IBM. that are provided on an exchange basis. You represent that all removed parts are genuine and unaltered. A part that replaces a removed part will assume the warranty service status of the replaced part.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair or replace it with one that is at least functionally equivalent, without charge. The replacement may not be new, but it will be in good working order. If

IBM or your reseller is unable to repair or replace the Machine, you may return it to your place of purchase and your money will be refunded.

If you transfer a Machine to another user, warranty service is available to that user for the remainder of the warranty period. You should give your proof of purchase and this Statement to that user. However, for machines which have a life-time warranty, this warranty is not transferable.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at 1-800-IBM-SERV (426-7378). In Canada, call IBM at 1-800-465-6666. You may be required to present proof of purchase.

IBM or your reseller will provide certain types of repair and exchange service, either at your location or at IBM's or your reseller's service center, to restore a Machine to good working order.

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. You represent that all removed items are genuine and unaltered. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item. Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alter-

ations, and attachments not under warranty service. You also agree to ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange.

You agree to:

- 1 obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
- 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, and
 - c inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, a Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Extent of Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

The warranties may be voided by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, removal or alteration of Machine or parts identification labels, or failure caused by a product for which IBM is not responsible.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN THAT EVENT SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Limitation of Liability

Circumstances may arise where, because of a default on IBM's part 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 from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM is liable only for:

- 1 Damages for bodily injury (including death) and damage to real property and tangible personal property; and
- 2 The amount of any other actual direct damages or loss, up to the greater of US\$100,000 or the charges (if recurring, 12 months' charges apply) 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) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION 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.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications (DOC) Compliance Statement

This equipment does not exceed Class A limits per radio noise emissions for digital apparatus, set out in the Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps are necessary to correct the interference.

Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques pour les appareils numériques, telles que prescrites par le Règlement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécessaires pour en éliminer les causes.

European Community (CE) Mark of Conformity Statement for Unshielded Cable

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR22/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 Richtlinie 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 Corporation. Deutschland Informationssysteme GmbH, 70547 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 Warhinweis 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 Geräte in eine 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 authorized dealers. IBM cannot accept responsibility for any interference caused by using, other than recommended cables and connectors.

European Union (EU) Statement for Shielded Cable

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 CISPR22/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 Richtlinie 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 Corporation. 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 Geräte 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 authorized 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 Class A for Unshielded Cables

This is a Class A product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、第二種情報処理装置(住宅地域又はその隣接した地域において使用されるべき情報処理装置)で住宅地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(VCCI)基準に適合しております。

しかし、本装置をラジオ、テレビジョン受信機に近接してご使用になると、受信障害の原因となることがあります。

取扱説明書に従って正しい取り扱いをして下さい。

Japanese Voluntary Control Council for Interference (VCCI) Statement Class B for Shielded Cables

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this equipment is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

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B情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

Korean Communications Statement

Please note that this device has been approved for business purpose with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for a non-business purpose one.

대한민국 통신문

이 기기는 업무용으로 전자파 적합증을 받은 기기이므로 X까지 또는 사용자는 이 점을 주의하시기 바라며, 민원 접수 구입하였을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Information To The User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.



GLOSSARY

10BASE-T

The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

100BASE-FX

100Mbps Ethernet implementation over fiber.

100BASE-TX

100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

ageing

The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM

Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

backbone

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

backbone port

A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

bandwidth

Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate

The switching speed of a line. Also known as *line speed*.

BOOTP

The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge

A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast

A message sent to all destination devices on the network.

broadcast storm

Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port

The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD

Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching

The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet

100Mbps technology based on the Ethernet/CD network access method.

forwarding

The process of sending a frame toward its destination by an internetworking device.

full duplex

A system which allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

IFM

Intelligent Flow Management. A means of holding packets back at the transmit port of the connected endstation. Prevents packet loss at a congested switch port.

Intelligent Switching Mode

A packet forwarding mode, where the Switch monitors the amount of error traffic on the network and changes the method of packet forwarding accordingly.

IPX

Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

IP address

Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

LAN

Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency

The delay between the time a device receives a frame and the time the frame is forwarded out of the destination port.

line speed

See *baud rate*.

main port

The port in a resilient link that carries data traffic in normal operating conditions.

MDI / MDIX

Medium Dependent Interface. A type of Ethernet twisted pair port connection: MDI ports connect to MDIX (cross-over) ports using straight-through twisted pair cabling; MDI-to-MDI and MDIX-to-MDIX links use cross-over twisted pair cabling.

MIB

Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast

Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

PACE

Priority Access Control Enabled. An innovative technology which works in conjunction with a switch to control the latency and jitter associated with the transmission of multimedia traffic over Ethernet and Fast Ethernet.

POST

Power On Self Test. An internal test that the Switch carries out when it is powered-up.

protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link

A pair of ports that can be configured so that one will take over data transmission should the other fail. See also *main port* and *standby port*.

RJ-45

Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON

Remote Monitoring. Subset of SNMP MIB II which allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS

Redundant Power System. Provides a backup source of power when connected to the Switch.

server farm

A cluster of servers in a centralized location serving a large user population.

SLIP

Serial Line Internet Protocol. A protocol which allows IP to run over a serial line connection.

SmartAgent

Intelligent management agents in devices and logical connectivity systems that reduce the computational load on the network management station and reduce management-oriented traffic on the network.

SNMP

Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and endstation operation.

Spanning Tree Protocol (STP)

A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

standby port

The port in a resilient link that will take over data transmission if the main port in the link fails.

STP

See *Spanning Tree Protocol (STP)*.

switch

A device which filters, forwards and floods frames based on the frame's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP

A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet

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

TFTP

Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your Switch's local management capabilities.

UDP

User Datagram protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN

Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT

Virtual LAN Trunk. A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100

A type of terminal which uses ASCII characters. VT100 screens have a text-based appearance.



INDEX

Numerics

100BASE-TX port 1-2, 1-9
10BASE-T port 1-2, 1-9

A

Access Level field 4-3
access rights B-1
Active Port field 4-21, 4-22
ageing entries 4-16
ageing time, specifying 4-10
agent software version number 6-8
alarm actions 5-25
alarm settings, default 5-26
Alarms (RMON group) 5-21
Asynchronous Transfer Mode. *See* ATM
ATM 1-2
ATM Module 1-2
ATM networks, extending VLANs into 5-4
audit log 5-26
Auto Config field 4-25
auto configuration 4-25
auto logout 3-11
Auto Logout screen 3-11

B

backbone port 1-2, 5-7
 specifying 5-9
Backbone Port field 4-11, 5-8
baud rate. *See* line speed
boot software version number 6-8
BOOTP Select field 3-10
BOOTP server 3-6
BPDUs. *See* Bridge Protocol Data Units

Bridge Forward Delay field 5-17
Bridge Hello Time field 5-17
Bridge Identifier 5-12
Bridge Max Age field 5-17
Bridge Priority field 5-17
Bridge Protocol Data Units 5-12
Broadcast Storm Control field 4-14

C

cable
 maximum length 1-9, 2-2
 pin-outs D-1
Capture (RMON group) 5-22
Char Size field 4-26
Community String field 4-3, 4-5, 4-24
community strings
 changing 4-5
 entering 4-3
 role in trap setup 4-24
Community-SNMP field 4-6
Connection Type field 4-25
console port 1-11
 auto-configuration 4-25
 connecting equipment to 2-7
 connection type 4-25
 setting up 4-25
 speed 4-25
Console Port field 4-6
Console Port Setup screen 4-25
conventions
 notice icons, About This Guide 2
 text, About This Guide 2
counters
 Bandwidth Used (port) 6-3
 Broadcast Frame Bandwidth (port) 6-3
 Broadcast Received (port traffic) 6-4

Collisions (port traffic) 6-4
CRC Align Errors (port error) 6-6
Errors (port traffic) 6-5
Errors (port) 6-3
Errors (summary) 6-2
Fragments (port traffic) 6-5
Frame Size Analysis (port traffic) 6-5
Frames Filtered (port traffic) 6-5
Frames Filtered (summary) 6-2
Frames Forwarded (port traffic) 6-5
Frames Forwarded (port) 6-3
Frames Forwarded (summary) 6-2
Frames Received (port traffic) 6-4
Frames Received (summary) 6-2
Frames Transmitted (port traffic) 6-4
Frames Transmitted (summary) 6-2
IFM Count (port traffic) 6-5
Jabbers (port error) 6-6
Late Events (port error) 6-6
Long Frames (port error) 6-6
Multicasts Received (port traffic) 6-4
Multicasts Received (summary) 6-2
Multicasts Transmitted (summary) 6-2
Octets Received (port traffic) 6-4
Octets Transmitted (port traffic) 6-4
 resetting to zero 6-2, 6-5, 6-7
 Short Events (port error) 6-6
Create User screen 4-3

D

Data Link Protocol field 3-10
Database Entries field 4-17
database. *See* Switch Database
DCD Control field 4-25

default
 passwords 3-7
 router 3-10
 settings 1-12
 users 3-7
 Default RMON Host/Matrix field 4-11
 Default Router field 3-10
 Default VLAN 5-3, 5-8
 Delete Users screen 4-4
 Designated Bridge field 5-19
 Designated Bridge Port 5-12
 Designated Cost field 5-19
 designated downlink port. *See* backbone port
 Designated Port field 5-18
 Designated Root field 5-16, 5-18
 Destination field 4-29
 Device IP Address field 3-10
 Device Subnet Mask field 3-10
 Disable Interactive Access field 4-13
 Downlink Module. *See* Plug-in Module
 downlink port. *See* backbone port
 DSR Control field 4-25
 Duplex Mode field 4-10, 4-13

E

Edit User screen 4-5
 electronic emission notices G-5
 Ethernet address label 1-11
 Events (RMON group) 5-22

F

Falling Action field 4-15
 Falling Threshold% field 4-14
 Fast Boot tests 3-9
 Fast Ethernet configuration rules 2-2
 Fast Start field 5-19
 Fault Log screen 6-9
 Fault Log, interpreting 6-9
 fields
 Access Level 4-3
 Active Port 4-21, 4-22

Auto Config 4-25
 Backbone Port 4-11, 5-8
 BOOTP Select 3-10
 Bridge Forward Delay 5-17
 Bridge Hello Time 5-17
 Bridge Max Age 5-17
 Bridge Priority 5-17
 Broadcast Storm Control 4-14
 Char Size 4-26
 Community String 4-3, 4-5, 4-24
 Community-SNMP 4-6
 Connection Type 4-25
 Console Port 4-6
 Data Link Protocol 3-10
 Database Entries 4-17
 DCD Control 4-25
 Default RMON Host/Matrix 4-11
 Default Router 3-10
 Designated Bridge 5-19
 Designated Cost 5-19
 Designated Port 5-18
 Designated Root 5-16, 5-18
 Destination 4-29
 Device IP Address 3-10
 Device Subnet Mask 3-10
 Disable Interactive Access 4-13
 DSR Control 4-25
 Duplex Mode 4-10, 4-13
 Falling Action 4-15
 Falling Threshold% 4-14
 Fast Start 5-19
 File Name 4-29
 Flow Control 4-25
 Forward Delay 5-17
 Forwarding Mode 4-9
 Fwd Transitions 5-19
 Hello Time 5-16
 Hold Time 5-17
 Intelligent Flow Management 4-12
 Intelligent Forwarding 4-9
 IP or IPX Address 4-24
 IPX Network 3-10
 Link State 4-12, 4-20
 Lost Links 4-12
 MAC Address 4-17
 MAC address 3-9
 MAIN Port 4-22
 Main Port ID 4-20
 Management Level 4-7
 Max Age 5-16
 Node 3-10
 PACE 4-10
 Pair Enable 4-21, 4-23
 Pair State 4-20, 4-22
 Parity 4-26
 Password 4-3
 Path Cost 5-19
 Permanent 4-17
 Plug-in Module Type 4-11
 Port Enable 5-19
 Port Number 4-17
 Port Speed 4-12
 Port State 4-12
 Power On Self Test Type 3-9
 Power Supply 4-11
 Priority 5-19
 Remote Telnet 4-6
 Rising Action 4-14
 Rising Threshold% 4-14
 Root Cost 5-16
 Root Port 5-17
 SDB Ageing Time 4-10
 Security 4-13
 Server Address 4-29
 SLIP Address 3-10
 SLIP Subnet Mask 3-10
 Spanning Tree 4-10
 Speed 4-26
 Standby Links Available 4-20
 STANDBY Port 4-22
 Standby Port ID 4-20
 Stop Bit 4-26
 STP State 5-18
 sysName 4-9
 System Up Time 6-8
 Throttle 4-24
 Time Since Topology Change 5-17
 Topology Changes 5-16

Transceiver Module Type 4-11
Type 5-7
Unit Name 4-9
User Name 4-3, 4-5
VLAN Configuration Mode 4-10, 4-14
VLAN ID 5-8, 5-16
VLAN Membership 5-8
VLT Mode 4-13
File Name field 4-29
Filter (RMON group) 5-22
Flow Control field 4-25
Forward Delay field 5-17
forwarding 1-3
Forwarding Mode field 4-9
FTP, support site F-1
full duplex 1-4
 configuration rules 2-2
 enabling and disabling 4-10, 4-13
fuse, changing 1-11
Fwd Transitions field 5-19

H

hardware version number 6-8
Hello BPDUs 5-13
Hello Time 5-12
Hello Time field 5-16
History (RMON group) 5-21
Hold Time field 5-17
Hosts (RMON group) 5-21
Hosts Top N (RMON group) 5-21

I

IBM Bulletin Board System F-1
IFM. *See* Intelligent Flow Management
Initialization screen 4-28
initializing the Switch 4-28
installing the Switch 2-4
Intelligent Flow Management 1-4
Intelligent Flow Management field 4-12
Intelligent Forwarding field 4-9
Intelligent Switching Mode 1-4

Interactive Access, disabling 4-13
IP address
 default router 3-10
 device 3-10
 entering 1-13
 format 3-2
IP or IPX Address field 4-24
IP protocol 1-12
IPX address 1-13
IPX Network field 3-10
IPX protocol 1-12

K

keyboard shortcuts 3-5

L

LEDs 1-9
line speed 4-26
Link State field 4-12, 4-20
Local Security screen 4-6
logging off 3-11
logging on 3-7
Logon screen 3-7
Lost Links field 4-12

M

MAC Address field 3-9, 4-17
MAC address label 1-11
Main Banner screen 3-6
Main Menu screen 3-8
MAIN Port field 4-22
Main Port ID field 4-20
management agent version number 6-8
Management Level field 4-7
Management Setup screen 3-9
Matrix (RMON group) 5-22
Max Age 5-13
Max Age field 5-16

N

network configuration example 1-7
Node field 3-10
non-ageing entries 4-16
non-routable protocols
 limitations for VLAN-based networks 5-4

P

PACE 1-6
 disabling Interactive Access for a port 4-13
PACE field 4-10
packets, processing 1-3
Pair Enable field 4-21, 4-23
Pair State field 4-20, 4-22
Parity field 4-26
Password field 4-3
passwords
 changing 4-5
 default 3-7
 forgetting 4-5
 new 4-3
Path Cost field 5-19
path costs, default 5-12
permanent entries 4-16
 displaying 4-17
 specifying 4-17, 4-18
Permanent field 4-17
pin assignments
 modem cable D-2
 null modem cable D-1
 RJ45 D-2
 serial cable D-1
pin-outs D-1
Plug-in Module 1-2
Plug-in Module slot 1-11
Plug-in Module Type field 4-11
port
 100BASE-TX 1-2, 1-9
 10BASE-T 1-2, 1-9
 backbone 1-2, 5-7, 5-8
 console 1-11

- enabling and disabling 4-12
- speed 4-12
- state 4-12
- statistics 6-3
- Port Enable field 5-19
- Port Error Analysis screen 6-6
- Port Number field 4-17
- Port Resilience screen 4-20
- Port Setup screen 4-12
- Port Speed field 4-12
- Port State field 4-12
- Port Statistics screen 6-3
- Port STP screen 5-18
- Port Traffic Statistics screen 6-4
- Power On Self Test Type field 3-9
- power supply 1-11
- Power Supply field 4-11
- powering-up 2-6
- Priority field 5-19
- problem solving C-1

Q

- quick start for SNMP users 1-13

R

- rack mounting 2-4
- Redundant Power System. *See* RPS
- Remote Monitoring. *See* RMON
- Remote Poll screen 6-10
- remote polling 6-10
- Remote Telnet field 4-6
- reset button 1-11
- Reset screen 4-27
- reset, time since last 6-8
- resets
 - number of 6-8
 - type 6-8
- resetting the Switch 4-27
- resilient link pair 4-19
- resilient links 1-5, 4-19
 - configuring 4-20

- creating 4-21
- deleting 4-21
- rules 4-19, 4-24
- viewing 4-22
- Rising Action field 4-14
- Rising Threshold% field 4-14
- RMON 5-20
 - alarm actions 5-25
 - benefits 5-23
 - default alarm settings 5-26
 - enabling and disabling Hosts and Matrix 4-11
 - features supported 5-24
 - groups supported 5-24
 - probe 5-20
- Root Bridge 5-12
- Root Cost field 5-16
- Root Path Cost 5-12
- Root Port field 5-17
- RPS 1-11
 - connecting 2-6

S

- safety information
 - English A-6
- screens 4-1
 - access rights B-1
 - Auto Logout 3-11
 - Console Port Setup 4-25
 - Create User 4-3
 - Delete Users 4-4
 - Edit User 4-5
 - Fault Log 6-9
 - Initialization 4-28
 - Local Security 4-6
 - Logon 3-7
 - Main Banner 3-6
 - Main Menu 3-8
 - Management Setup 3-9
 - Port Error Analysis 6-6
 - Port Resilience 4-20
 - Port Setup 4-12
 - Port Statistics 6-3
 - Port STP 5-18
 - Port Traffic Statistics 6-4
 - Remote Poll 6-10
 - Reset 4-27
 - Software Upgrade 4-29
 - Status 6-8
 - Summary Statistics 6-2
 - Switch Management 4-7
 - Trap Setup 4-24
 - Unit Database View 4-17
 - Unit Resilience Summary 4-22
 - Unit Setup 4-9
 - User Access Levels 4-2
 - VLAN Server 4-8
 - VLAN Setup 5-7
 - VLAN STP 5-16
- SDB Ageing Time field 4-10
- security 1-5
- Security field 4-13
- serial number, location on unit 1-9
- serial port. *See* console port
- Server Address field 4-29
- service, technical F-1
- SLIP Address field 3-10
- SLIP Subnet Mask field 3-10
- SNMP 1-12, 3-6
 - Community 4-6
 - quick start 1-13
- socket
 - power 1-11
 - RPS 1-11
- Software Upgrade screen 4-29
- software version number 6-8
- Spanning Tree field 4-10
- Spanning Tree Protocol. *See* STP
- specifications, system E-1
- Speed field 4-26
- standards supported E-2
- Standby Links Available field 4-20
- STANDBY Port field 4-22
- Standby Port ID field 4-20

- statistics 6-1
 - counters. *See* counters
 - port 6-3
 - port error 6-6
 - port traffic 6-4
 - summary 6-2
 - Statistics (RMON group) 5-21
 - Status screen 6-8
 - Stop Bit field 4-26
 - STP 1-6, 5-10
 - Bridge Identifier 5-12
 - Bridge Protocol Data Units 5-12
 - configurations 5-14
 - configuring port properties 5-18
 - configuring VLAN properties 5-16
 - default path costs 5-12
 - Designated Bridge Port 5-12
 - enabling and disabling 4-10, 5-15
 - Hello BPDUs 5-13
 - Hello Time 5-12
 - Max Age 5-13
 - Root Bridge 5-12
 - Root Path Cost 5-12
 - STP State field 5-18
 - subnet mask, device 3-10
 - Summary Statistics screen 6-2
 - support, technical F-1
 - Switch 1-1
 - desktop configuration 1-7
 - dimensions E-1
 - features 1-1
 - front view 1-8
 - initializing 4-28
 - installing 2-4
 - LEDs 1-9
 - logging off 3-11
 - logging on 3-7
 - management setup 3-9
 - port setup 4-12
 - powering-up 2-6
 - rack mounting 2-4
 - rear view 1-10
 - size E-1
 - stacking with other units 2-4
 - unit defaults 1-12
 - unit setup 4-9
 - upgrading software 4-29
 - wall mounting 2-5
 - weight E-1
 - Switch Database 4-16
 - adding an entry 4-18
 - ageing entries 4-16
 - configuring 4-17
 - deleting an entry 4-18
 - non-ageing entries 4-16
 - permanent entries 4-16
 - searching 4-18
 - Switch Management screen 4-7
 - sysName field 4-9
 - System Up Time field 6-8
 - system, specifications E-1
-
- T**
- Technical support and service F-1
 - Telnet 3-2, 4-6
 - terminal emulator, connecting 2-7
 - terminal, connecting 2-7
 - Throttle field 4-24
 - Time Since Topology Change field 5-17
 - Topology Changes field 5-16
 - Transceiver Module 1-2
 - Transceiver Module slot 1-11
 - Transceiver Module Type field 4-11
 - Trap Setup screen 4-24
 - traps
 - community strings 4-24
 - setting up 4-24
 - throttle 4-24
 - trouble-shooting C-1
 - Type field 5-7
-
- U**
- Unit Database View screen 4-17
 - unit defaults 1-12
 - Unit Name field 4-9
 - Unit Resilience Summary screen 4-22
 - Unit Setup screen 4-9
 - upgradable software version number 6-8
 - upgrading software 4-29
 - User Access Levels screen 4-2
 - User Name field 4-3, 4-5
 - users
 - access levels 4-6
 - changing names 4-5
 - creating 4-3
 - default 3-7
 - deleting 4-4
 - editing 4-5
 - names 4-3
 - passwords 4-3
 - setting up 4-2
-
- V**
- version number
 - boot software 6-8
 - hardware 6-8
 - upgradable software 6-8
 - Virtual LAN Trunks. *See* VLTs
 - Virtual LANs. *See* VLANs
 - VLAN Configuration Mode field 4-10, 4-14
 - VLAN ID field 5-8, 5-16
 - VLAN Membership field 5-8
 - VLAN Server screen 4-8
 - VLAN Setup screen 5-7
 - VLAN STP screen 5-16
 - VLANs 1-5, 5-1
 - assigning ports 5-9
 - Default 5-3, 5-8
 - extending into an ATM network 5-4
 - setting up 5-7, 5-9
 - using non-routable protocols 5-4
 - using unique MAC addresses 5-4
 - VLTs 5-7
 - VLT Mode field 4-13
 - VLTs 5-3, 5-7
 - Voice support F-1

VT100 interface
 accessing 3-1
 definition 1-12
 logging on 3-7
 navigating 3-4
VT100 terminal, connecting 2-7

W

wall mounting 2-5
World Wide Web (WWW)
 IBM Networking home page F-1

Z

zeroing screen counters 6-2, 6-5, 6-7