8271 Nways Ethernet LAN Switch Models E12 and E24

User's Guide

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 (July, 1998)

This edition applies to the IBM 8271 Nways Ethernet LAN Switch Models E12 and E24 with agent software version 1.0.

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.

CONTENTS

2 INSTALLING THE SWITCH

3 SETTING UP FOR MANAGEMENT

II MANAGING THE SWITCH

4 WORKING WITH THE WEB INTERFACE

SAFETY NOTICES

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 not 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 säkerhetsinformtionen 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. Vejiedningen beskriver den fremgangsmåde, du skal bruge ved tilslutning af kabier og udstyr.

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

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 appratuur.

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 elktrischer 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 *Attenzion: 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 podłączaniu do sieci elektrycznej
i eksploatacji.

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

Pozor: Preden zaènete 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 инсталлировать этот продукт, прочтите Инструкцию по технике безопасности в документе "Внимание: Инструкция по технике безопасности -- Прочесть в первую очередь", SD21-0030. В этой брошюре описаны безопасные способы каблирования и подключения электрического оборудования.

Nebezpečenstvo: Pred inštaláciou výrobku si prečítajte bezpečnosté predpisy v
Výstraha: Bezpeč osté predpisy - Prečítaj ako prvé, SD21 0030. V tejto brožúrke sú opísané bezpečnosté postupy pre pripojenie elektrických zariadení.

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。

危険： 導入作業を開始する前に、安全に関する小冊子SD21-0030 の「最初にお読みください」(Read This First)の項をお読みください。
この小冊子は、電気機器の安全な配線と接続の手順について説明しています。

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 napajanje.

ОПАСНОСТ
Пред да почнете да го инсталирате овој продукт, прочитајте ја информацијата за безбедност:
"Предупредување: Информација за безбедност: Прочитајте го прво ова", SD21-0030.
Оваа брошура опишува безбедносни процедури за каблирање и вклучување на електрична опрема.

ABOUT THIS GUIDE

This guide provides all the information you need to install and manage the IBM 8271 Nways Ethernet LAN Switch Models E12 and E24.

This 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 LANs (Local Area Networks).

This guide is intended for use with both E12 and E24 models:

- *02L0876 — 12 10BASE-T ports*
- *02L0877 — 24 10BASE-T ports*

All pictures and example screens show the 24-port model, however, all procedures also apply to the 12-port model.

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

Finding Specific Information in This Guide

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

If you are looking for...	Turn to...
A summary of key features, some examples of how the Switch can be used in your network, or a list of unit default settings	Chapter 1
Recommendations on where to site the Switch, procedures for installing the Switch, information on stacking Switches, or a description of the power-up sequence	Chapter 2
An overview of management methods and required setup, or a description of default user names	Chapter 3
Procedures for accessing the web interface, information on navigating the web pages, or a full description of how to manage the stack using the web interface	Chapter 4

(continued)

If you are looking for...	Turn to...
Procedures for accessing the command line interface, information on navigating the menu structure, or a full description of how to configure the Switch using the command line interface	Chapter 5
A description of the Spanning Tree Protocol	Chapter 6
A description of RMON in the Switch	Chapter 7
Advice for solving problems	Chapter 8
Safety information, information on using the Serial Interface Utility, pin-out diagrams, technical specification details, advice on obtaining technical support, warranty, trademark, and other reference information	Appendices and Index
List of terms used in this guide	Glossary

Conventions

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

Table 1 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

Table 2 Text Conventions

Convention	Description
`Commands`	Commands that you enter are shown in a **`bold Courier`** typeface. The word "command" means you must enter the command exactly as shown in text and press [Return] or [Enter]. Example: To change your password, enter: **`system password`**

(continued)

Table 2 Text Conventions

Convention	Description
`Screen displays`	Information as it appears on the screen is shown in a `Courier` typeface.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press [Return] or [Enter]. Do not press the Return or Enter key when an instruction simply says "type."
underlined text	Text that is underlined indicates a default configuration setting

Related Documentation

The Switch document set includes:

- *IBM 8271 Nways Ethernet LAN Switch Models E12 and E24 Quick Reference Guide*, Part Number 02L0886
- *IBM 8271 Nways Ethernet LAN Switch Models E12 and E24 Quick Installation Guide*, Part Number 02L0885
- *IBM 8271 Nways Ethernet LAN Switch Models E12 and E24 Release Notes*, Part Number 02L0887

Other publications you may find useful:

- Documentation accompanying the *IBM 8271 Nways Ethernet LAN Switch Models F12 and F24*.
- Documentation accompanying *IBM 8271 Nways Ethernet LAN Switch* Expansion Modules.
- Documentation accompanying the Advanced Redundant Power System.

I GETTING STARTED WITH THE SWITCH

1 INTRODUCING THE SWITCH

This chapter introduces the IBM 8271 Nways Ethernet LAN Switch Models E12 and E24. It covers the following topics:

- About the Switch
- Switch — Front View Detail
- Switch — Rear View Detail
- Switch Features Explained
- Unit Defaults
- Managing the Switch
- Building the Switch into your Network
- Configuration Rules for Fast Ethernet

About the Switch

The 8271 range of products solves the problem of growth in dynamic network environments and provides everything you need for successful workgroup networking.

As part of the 8271 range, the Switch Models E12 and E24 meet the challenge of modern LANs and allow you to add features and expand capacity as your network grows.

Summary of Features

The Switch has the following features:

- 12 or 24 switched 10BASE-T ports
- Two Fast Ethernet 10BASE-T/100BASE-TX ports
- Matrix port for interconnecting up to four units in a single stack
  - Any combination of Switch Models E12 and E24 and Switch Models F12 and F24 units may be stacked
- Slot for a high-speed expansion module or matrix module
- Transceiver module slot (10 Mbps Ethernet)
- Support for up to 6000 endstations (one MAC address per endstation)
- Four packet forwarding modes
- Flow control
  - 802.3x
  - Intelligent Flow Management
- Full duplex on all ports (not transceiver module)
- Security
- Resilient links
- Spanning Tree Protocol (STP)
- Hardware ready for VLANs, automatic configuration of multicast filters (GARP and IGMP Snooping) and Fast IP
- A choice of management methods:
  - A graphical web interface
  - A simple-to-use command line interface
  - SNMP-compliant management over the network
- Connects to Redundant Power System/Uninterruptable Power System
- Integrated network management
- 19-inch rack or stand-alone mounting

Switch — Front View Detail

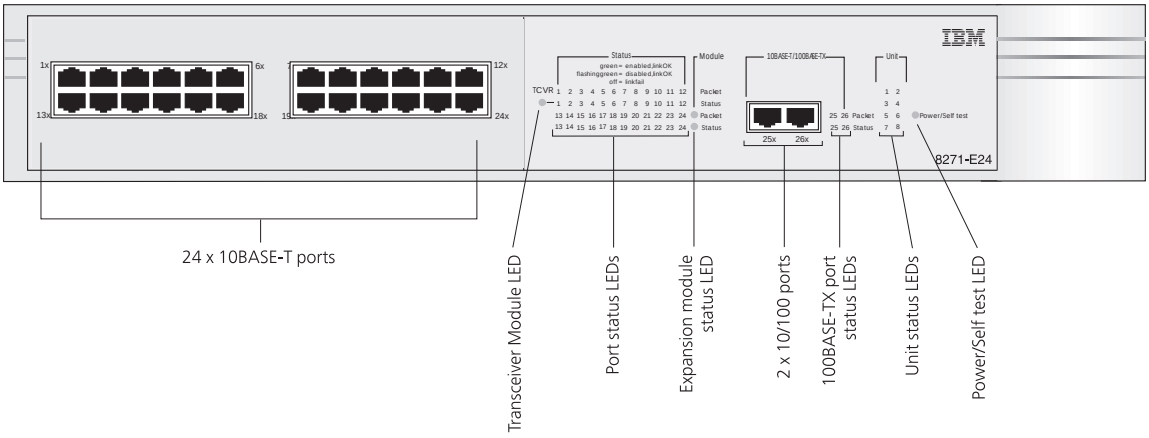


Figure 1-1 Switch — Front view

Port Connections

10BASE-T Ports

Twenty-four (or 12) 10BASE-T ports with RJ-45 sockets, each allow a full 10 Mbps bandwidth to attached endstations. The maximum segment length is 100m (328ft) over category 3, 4, or 5 UTP cable. With full duplex enabled, bandwidth is doubled.

These ports are configured as MDIX (cross-over). See "Choosing the Correct Cables" *on page 2-9 for further information.*

10BASE-T/100BASE-TX Ports

Two 10BASE-T/100BASE-TX connections with RJ-45 sockets, can be set to 10BASE-T, 100BASE-TX, or with auto-negotiation enabled, they can automatically detect the speed of a link and provide a 10 Mbps connection to Ethernet devices or a 100 Mbps connection to Fast Ethernet devices. The maximum segment length is 100m (328ft) over category 5 twisted pair cable. With full duplex enabled, bandwidth is doubled.

As these ports are configured as MDIX (cross-over). See "Choosing the Correct Cables" *on page 2-9 for further information.*

LEDs

Table 1-1 lists the LEDs on the front of the Switch and their states according to color. Information on using the LEDs for problem solving can be found in Chapter 8, "Problem Solving".

Table 1-1 LED colors

LED	Color	Indicates
TCVR	Yellow	Port 1 is a transceiver module fitted to the rear of the unit.
	Off	Port 1 operating as a 10BASE-T port.
Port Status LEDs 1–26*		
Packet	Yellow	Packets are being transmitted/received on this port.
	Off	No traffic on this port.
Status	Green	Link is present; port enabled.
	Green flashing	Link is present; port is disabled.
	Off	Link not present.
Expansion Module		
Packet	Yellow	Packets are being transmitted/received on an expansion module port.
	Off	No traffic on the expansion module.
Status	Yellow	A valid expansion module is installed.
	Yellow flashing	A non-supported expansion module is installed.
	Off	No expansion module is installed.
Power/Self Test		
	Green	The Switch is powered on.
	Green flashing	Power On Self Test (POST) or software download in progress.
	Off	The power supply is faulty.
	Yellow	The Switch has failed its Power On Self Test.
Unit LEDs		
1–8	Green	Indicates the position of the Switch in the stack and that the link is OK. Note that only four Switch units can be stacked at present.
	Off	The Switch is not configured into a stack.

* If your Switch has 24 10BASE-T ports, ports 1–24 are 10BASE-T ports, ports 25 and 26 are 10BASE-T/100BASE-TX ports. If your Switch has 12 10BASE-T ports, ports 1–12 are 10BASE-T ports, and ports 13 and 14 are 10BASE-T/100BASE-TX ports. For both models, ports supplied through an expansion module are numbered sequentially from the last fixed port on the front of the unit.

Switch — Rear View Detail

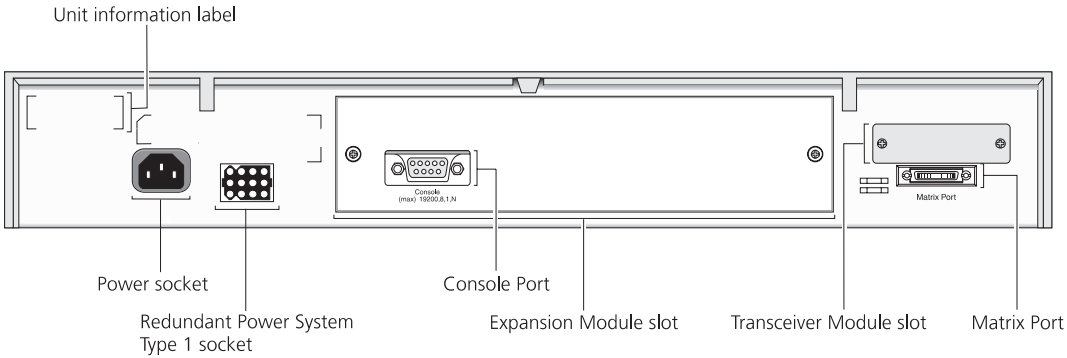


Figure 1-2 Switch — Rear view

Unit Information Label This label displays the unique MAC address and serial number of the Switch. You may need this information for fault reporting purposes.

Power Socket The Switch automatically adjusts to the supply voltage ranging from 90 to 240V AC.

Redundant Power System Socket To protect against internal power supply failure, you can use this Type 1 socket to connect a Redundant Power System (RPS) to the Switch. See "Connecting a Redundant Power System (RPS)" on page 2-8.

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.

Expansion Module Slot Use this slot to install one of the expansion modules available for the Switch. You could install an expansion module that provides a high-speed link to the rest of your network, or a matrix module that provides four matrix ports for stacking units together. There is a range of suitable expansion modules; contact your supplier for availability.

When an expansion module is not installed, ensure the blanking plate is secured in place.

Transceiver Module

A slot at the rear of the unit allows you to install an Ethernet (10 Mbps) transceiver module: either an AUI Trainsceiver Interface Module or a 10BASE-FL Transceiver Interface Module. When a transceiver module is fitted, port 1 automatically switches to become the transceiver module port. The transceiver module can provide a 10 Mbps link (half duplex mode only) to the rest of your network using various media such as fiber and coaxial cabling.

When a transceiver module is not installed, ensure the blanking plate is secured in place.

Matrix Port

The matrix port allows you to connect two Switch units back-to-back (both Switches must support the matrix feature) or to connect the Switch to the high-speed Matrix Module.

Switch Features Explained

The following sections explain in more detail the Switch features listed in "Summary of Features" on page 1-2.

Forwarding Mode

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

- *Fast Forward* — Packets are forwarded as soon as the destination address is received and verified. The forwarding delay, or latency, for all packets in this mode is just 35µs, but with the lack of error checking, any error packets received are propagated through the switch.
- *Fragment Free* — A minimum of 512 bits of the received packet is buffered prior to the packet being forwarded. This ensures that collision fragments are not propagated through the network. The forwarding delay, or latency, for all packets in this mode is 64µs.
- *Store and Forward* — Received packets are buffered in their entirety prior to forwarding. This ensures that only good packets are passed to their destination. The forwarding delay for this mode varies between 64µs and 1.2ms, depending on packet length and port speed. In Store and Forward mode, latency is measured as the time between receiving the last bit of the packet and transmitting the first bit. For the Switch Model E12 and E24, this is 7µs.
- *Intelligent* — The Switch monitors the amount of error traffic on the network and changes the forwarding mode accordingly. If the Switch detects *less* than 20 errors a second, it will operate in Fast Forward mode. If the Switch detects *more* than 20 errors a second, it will

operate in Store and Forward mode until the number of errors returns to 0.

Flow Control

Flow control is provided for all ports in the stack, including expansion module ports. It is a congestion control mechanism built into the Switch that should be enabled on that unit if it is connected to another switch, or an endstation. By default, flow control is enabled on half-duplex links; by default, it is disabled on full duplex links. If the Switch is connected to a repeated segment with local traffic, flow control should be disabled.

Congestion is caused by one or more devices sending traffic to an already congested port on the Switch. If a port on the Switch is connected to another switch or endstation, flow control will prevent packet loss and inhibit the device from generating more packets until the period of congestion ends.

In the Model E12 and E24, flow control is implemented in two ways:

- 802.3x standards-based for ports operating in full duplex
- Intelligent Flow Management (IFM) for ports operating in half duplex

Full Duplex

The Switch provides full duplex support for all its fixed Ethernet and Fast Ethernet ports and any installed expansion module ports. Full duplex allows packets to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link. In addition, full duplex also supports IEEE 802.3x flow control and 100BASE-FX cable runs of up to 2km.

Full duplex must always be enabled at both ends of a link. On twisted pair connections, this is done automatically by the Switch; on fiber connections, both ends must be manually set to full duplex mode.

***ATTENTION**: If Auto-negotiation is disabled, do not manually enable full duplex on a connection to a hub or repeater.*

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. This helps to prevent unauthorized users attaching devices to the network.

Resilient Links

The resilient link feature in the Switch enables you to protect critical links and prevent network downtime should that link 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. Resilient links are fast to set up, you have full control over their configuration, and the port at the other end of the resilient link does not have to support a particular resilience feature.

Resilient links and Spanning Tree cannot be set up on the same unit or stack.

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

STP is beneficial for large parts of your network for which you want to automatically set up redundancy.

Spanning Tree and resilient links cannot be set up on the same unit or stack.

Unit Defaults

Table 1-2 shows the factory settings for the Switch. If you initialize the Switch, it will be returned to these defaults.

Table 1-2 Unit Default Settings

Port Status	Enabled
Forwarding Mode	Intelligent
Full Duplex Flow Control	Auto
Half Duplex Flow Control (IFM)	Enabled
Auto-negotiation	Enabled
Spanning Tree (STP)	Disabled
Security	Disabled

Table 1-2 Unit Default Settings

System Alarm — broadcast bandwidth	Enabled: High threshold — 20% Low threshold — 10%
System Alarm — % errors per minute	Enabled: High threshold — 20 errors per second Low threshold — 1 error per second

Managing the Switch

Management software embedded in the Switch allows you a choice of management methods:

- You can access the web interface using any Java®-enabled web browser. Using the web interface is described in Chapter 4, "Working With the Web Interface".
- You can access the command line interface using a terminal or a workstation running terminal emulation connected directly to the Switch's console port, or over the network using Telnet. Using the command line interface is described in Chapter 5, "Working With The Command Line Interface".
- For more powerful management, you can use SNMP-based network management software. This is the most convenient method of management if you have a large network with multiple devices to set up.

Building the Switch into your Network

The following sections give more information on how you can make best use of the Switch in your network.

Server Connections

When connecting servers to the Switch, use the following rules to ensure that the Switch is operating at maximum efficiency:

- Ideally, any local server should be connected to the Switch using a 100 Mbps port.
- If that is not possible, connect the local server to a dedicated 10 Mbps port.
- If that is not possible and the local server is connected to a repeated segment where the traffic is mainly local to that segment, disable Flow Control on the port to which the repeater is connected.

If your network is running a peer-to-peer protocol and you have multiple endstations connected to the Switch via a repeater, we recommend that you disable Flow Control on the port to which the repeater is connected.

Network Configuration Examples

The following illustrations show some examples of how the Switch can be placed on your network.

Network Segmentation I

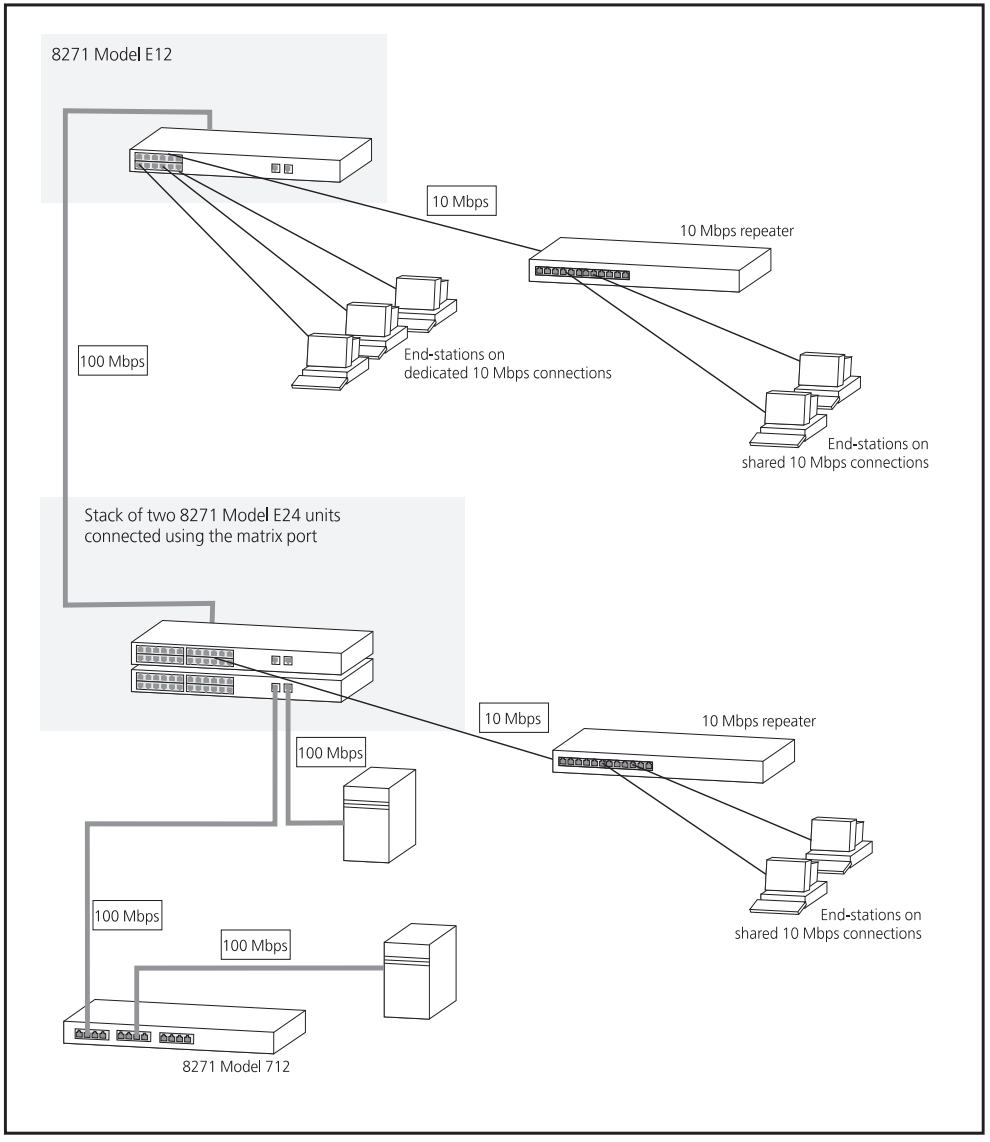


Figure 1-3 Using the Switch to segment your network

Figure 1-3 shows how the Switch fits into a large corporate network with a Fast Ethernet infrastructure. A Switch is positioned on each floor and servers are centralized in the basement.

Network Segmentation II

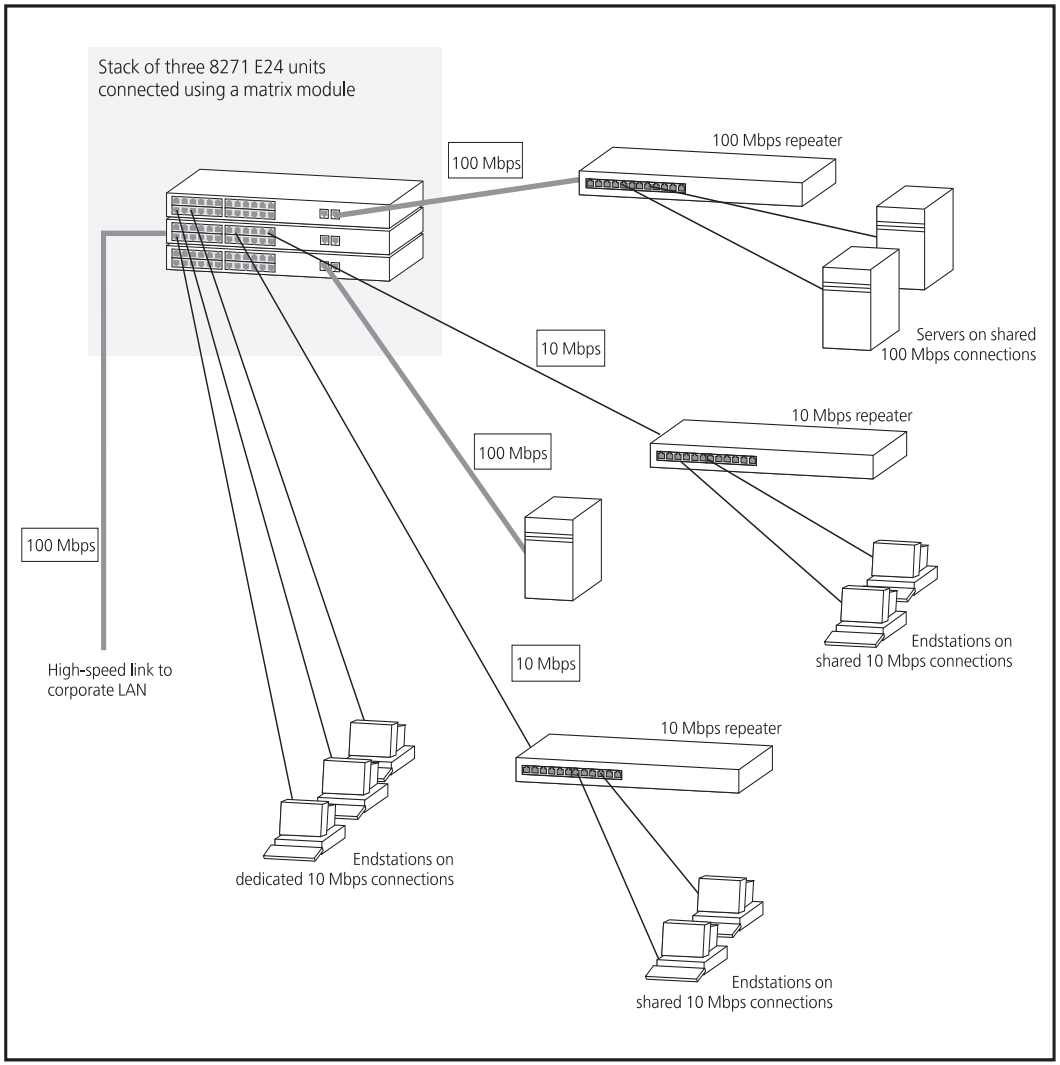


Figure 1-4 Using the Switch to segment your network

Figure 1-4 shows the Switch in a second workgroup situation. This setup could be that of a small office within a large corporation, or part of a larger corporate network. Most of the switch ports have multiple endstations.

Desktop Switching

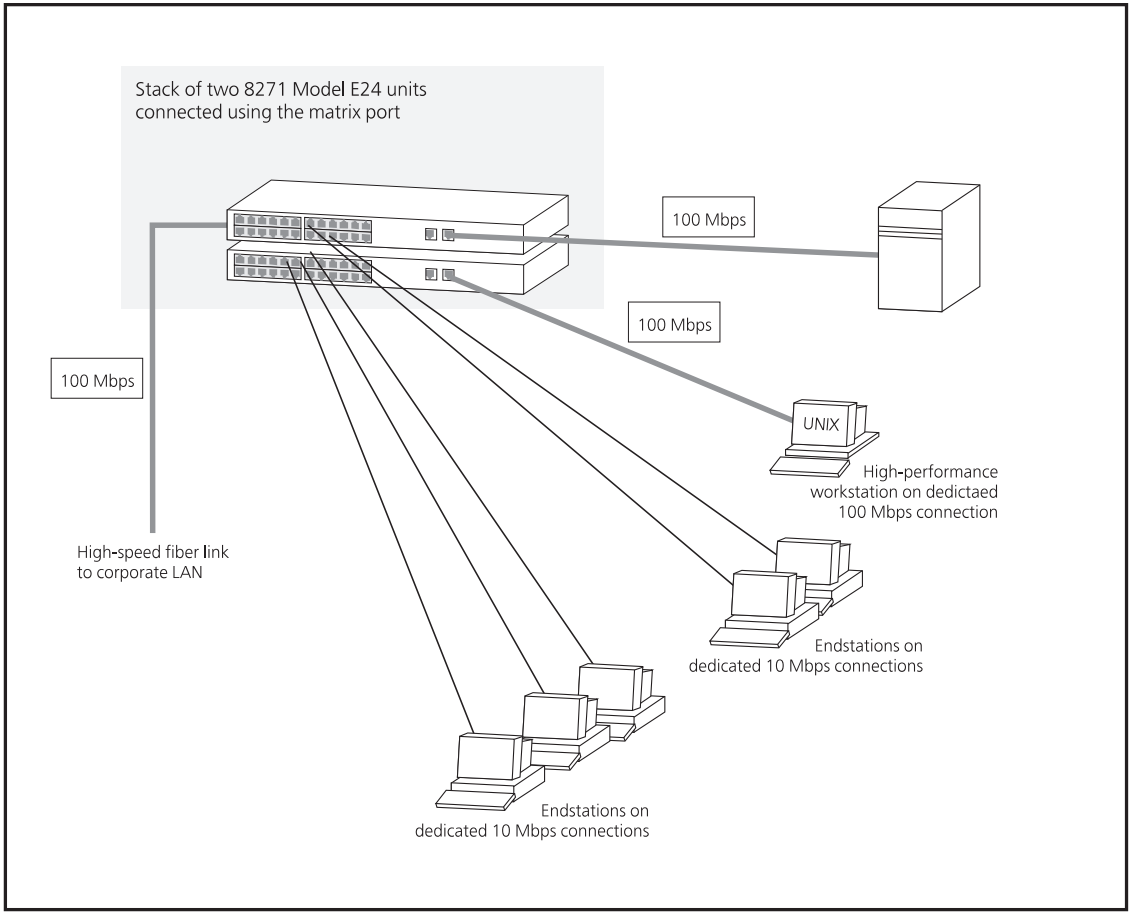


Figure 1-5 Using the Switch in a desktop environment

Figure 1-5 shows the Switch used for a group of heavy-traffic users in a large corporate network. Here switching is brought to the desktop with a single endstation per switch port. Local servers are connected via the 100 Mbps Fast Ethernet link.

Configuration Rules for Fast Ethernet

The topology rules for Fast Ethernet (100 Mbps) are slightly different to those for 10 Mbps Ethernet. Figure 1-6 illustrates the key topology rules and provides examples of how they allow for large-scale Fast Ethernet networks.

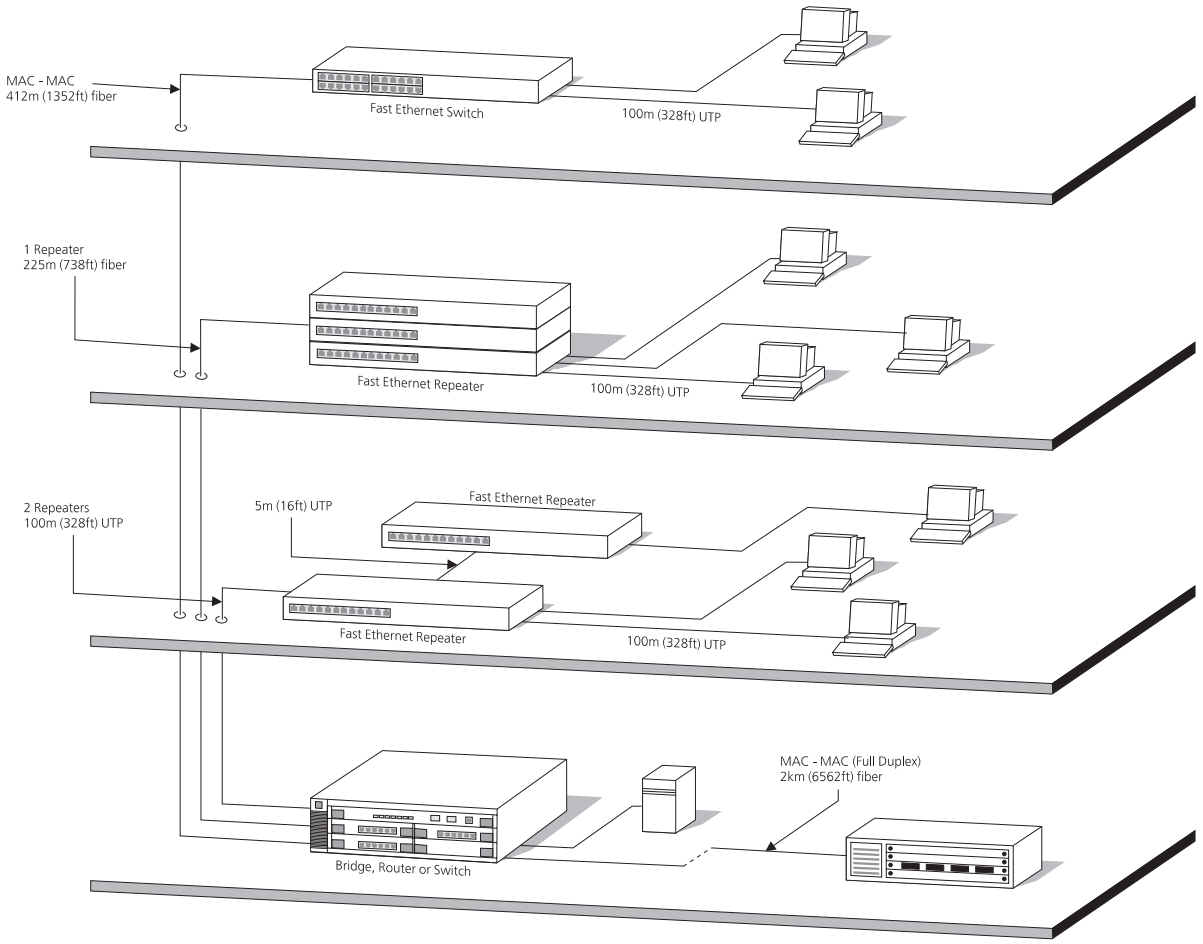


Figure 1-6 Fast Ethernet configuration rules

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 standards-compliant 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 100m (328ft) UTP run from a repeater out to the desktops.

Configuration Rules with Full Duplex

The Switch provides full duplex support for all its fixed Ethernet and Fast Ethernet ports and ports provided through an expansion module. Full duplex allows packets 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.

2 INSTALLING THE SWITCH

This chapter contains all the information you need to install and set up the Switch. It covers the following topics:

- Installing the Switch
- Stacking Units
- The Power-up Sequence
- Choosing the Correct Cables
- Getting Started

Installing the Switch

The following sections describe how to site and install your Switch.

Following Safety Information

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

Choosing a Suitable Site

The Switch is suited for use in an office environment 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-mounting/rack-mounting kit, containing two mounting brackets and six screws, is supplied with the Switch.

When deciding where to position the unit, ensure that:

- You will be 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 (1 in.) clearance.
- No objects are placed on top of the unit.
- If the units are free standing, not more than four units can be placed on top of one another.

Rack Mounting

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

ATTENTION: *Disconnect all cables from the Switch before continuing. Remove all self adhesive pads from the underside of the unit, if 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 2-1.

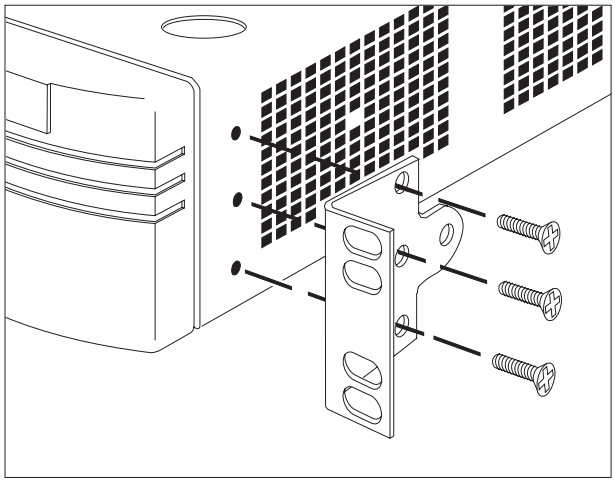


Figure 2-1 Fitting the mounting bracket

3. Insert the three screws and fully tighten with a suitable screwdriver.

You must use the screws supplied with the mounting brackets. Damage caused to the unit by using incorrect screws will invalidate your warranty.

4. Repeat the two previous steps 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 the ventilation holes face sidewards and the front panel faces upwards.
6. Connect cables.

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

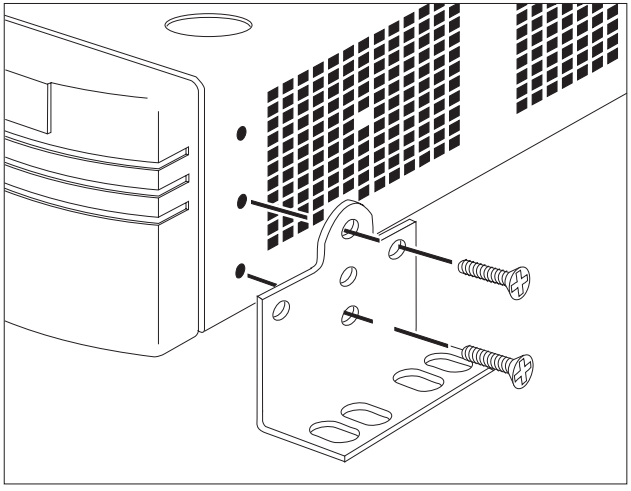


Figure 2-2 Wall mounting the Switch

3. Insert the two screws and tighten with a suitable screwdriver.

You must use the screws supplied with the mounting brackets. Damage caused to the unit by using incorrect screws will invalidate your warranty.

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 sidewards 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 all cables.

Free-standing Units

You do not have to rack or wall-mount the Switch, it can be left free-standing. You can have a maximum of four units positioned one on top of the other. If mixing a variety of units, the smaller units must be positioned at the top.

If you are placing units one on top of the other, you must use the four self-adhesive rubber pads supplied. Apply the pads to the underside of the unit, stick one 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.

Stacking Units

Model E12 and E24 units can be connected together to form a stack. This stack can then treated as a single manageable unit with one IP address.

The Model E12 and E24 can be configured into a stack with Model F12 and F24 units. For information on configuring the Models F12 and F24, refer to the user guide that accompanies it or to the help system which covers both Switches.

You can connect units together in two ways:

- A matrix port on the rear of the Switch allows you to connect two units back-to-back. For this you will need a matrix cable. Contact your supplier for details.
- A slot at the rear of the unit allows you to install a Matrix Module. The Matrix Module provides four ports and allows you to interconnect up to a maximum of four Switch units using Matrix Cables.

Stacking Two Units

To stack two units you do not need any additional modules, just one Matrix Cable. The units can be rack-mounted or free-standing. If you choose to have them free-standing, remember to position the rubber feet supplied with the unit, as detailed in "Free-standing Units". When positioning units you should bear in mind that matrix cables are 1m (3.28ft) long.

Connect one end of the cable to the matrix port of the top unit, and the other end to the matrix port on the lower unit. See Figure 2-3.

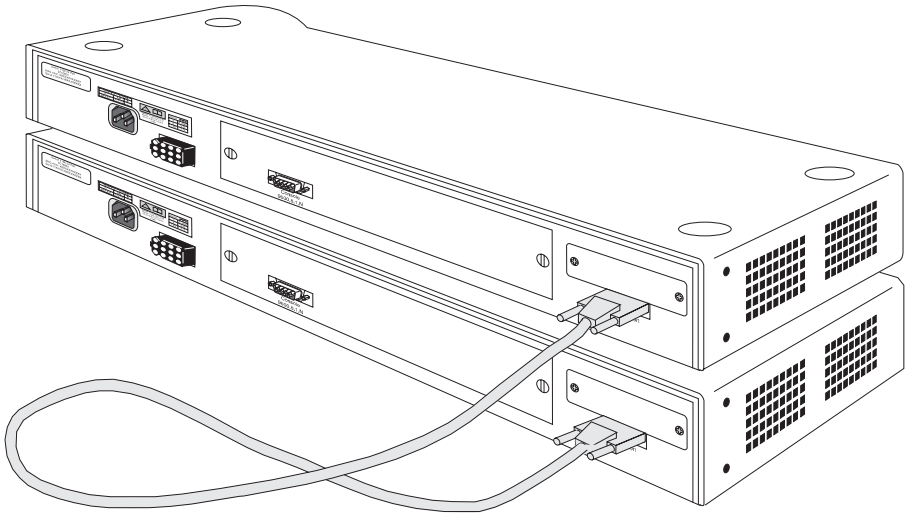


Figure 2-3 A stack of two units

Stacking Multiple Units

You can connect up to four Switch units to form a stack. If you connect more than two units, you will need a Switch Matrix Module and the appropriate number of matrix cables.

You only need to install one Matrix Module which leaves the slots in the other units free for further expansion modules.

1. Arrange your units as required. They can be rack-mounted or free standing. If you choose to have them free-standing, remember to position the rubber feet supplied with the unit, as detailed in "Free-standing Units" on page 2-5. When positioning units you should bear in mind that matrix cables are 1m (3.28ft) long.
2. Into one of the units, install the Matrix Module. You can find instructions for doing this in the documentation that accompanies the Matrix Module. We recommend that for ease of configuration, you install the Matrix Module in the bottom unit.
3. Connect Matrix Cables, see Figure 2-4:
   a. Connect a cable to the port marked Unit 1 on the Matrix Module. Connect the other end of this cable to the matrix port located on the unit itself.

b Connect a second matrix cable to the port marked Unit 2 on the Matrix Module. Connect the other end of this cable to the matrix port located on the second unit.

c Repeat steps **a** and **b** for any additional units.

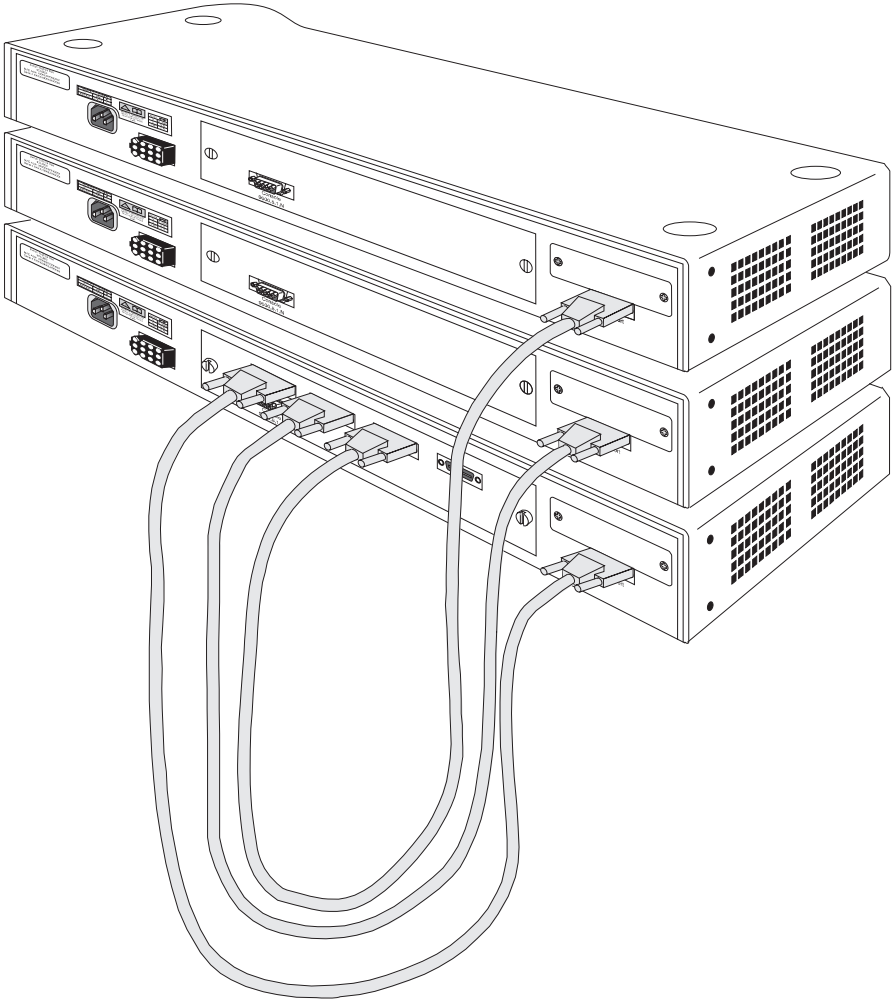


Figure 2-4 A stack of multiple units

The Power-up Sequence

The following sections describe how to get your Switch powered up and ready for operation.

Connecting a Redundant Power System (RPS)

You can connect a Redundant Power System (RPS) to the Switch. The RPS is designed to maintain the power to your Switch if an internal power supply failure occurs.

At +5V, the current requirement for the Switch is 4.8A, including any transceiver module that might be fitted, but excluding an expansion module. Check the documentation supplied with your expansion module for power consumption figures.

If the current consumption of the Switch plus any installed expansion module exceeds the capability of the RPS (8.5A), you need an Advanced RPS with one Advanced RPS 100W Module. Contact your supplier for details.

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

For further information, see the user guide that accompanies the RPS.

Powering up the Switch

Use the following sequence of steps to power-up the Switch.

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.*

1. Plug the power cord into the power socket at the rear of the Switch.
2. Plug the other end of the power cord into your power outlet.

   The Switch will power-up and run through its 12-second Power On Self Test (POST).

Checking for Correct Operation

During the POST, all ports on the Switch are disabled and the LEDs light in the following sequence:

- all unit LEDs light
- TCVR and Module LEDs light
- port Status LEDs light in a rapid cycle

When the POST has completed, observe the Power/Self Test LED to check that your Switch is operating correctly. Table 2-1 shows possible colors for the LED.

Table 2-1 LED colors

Color	State
Green	Unit is receiving power and operating normally
Yellow	A fault has occurred during the POST. The Switch fails its self test if any of the ports fail during power-up.
Off	Power supply is faulty

If there is evidence of a problem, refer to Chapter 8, "Problem Solving".

Choosing the Correct Cables

All of the ports on the front of the Switch are configured as MDIX (cross-over). If you want to make a connection to another MDIX port, you will need a "cross-over" cable. If you want to make a connection to an MDI port on for example, a Network Interface Card (NIC), you will need to use standard "straight-through" cable. This is illustrated in Figure 2-5.

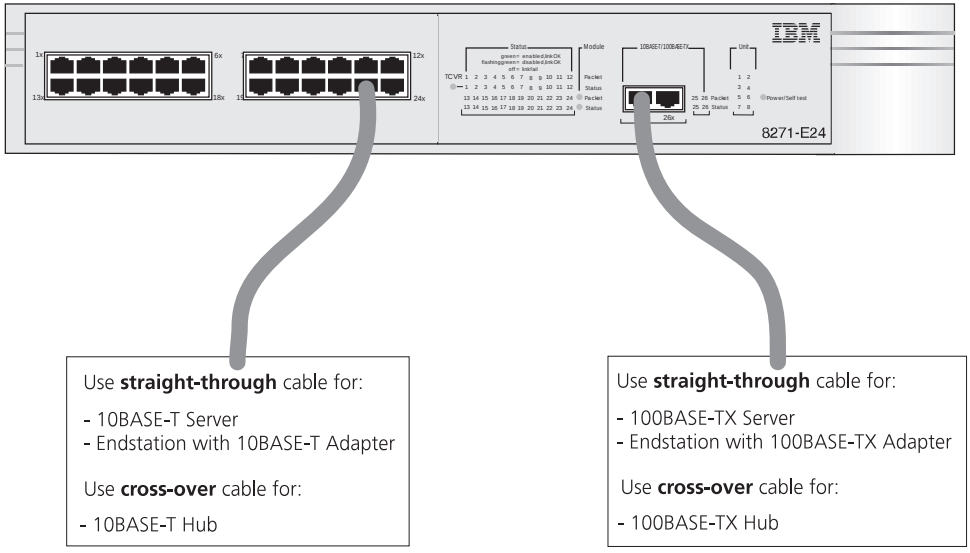


Figure 2-5 Connecting other devices to the Switch

Getting Started

If you want to manage the Switch over the network, you must assign it a unique IP address. You can do this using the command line interface or the web interface.

For multiple units connected in a stack, you need only assign an IP address to one unit in the stack. This IP address is then used to communicate to the whole stack.

Using the command line interface:

1. Connect a management workstation to the console port of the Switch, see "Through the Console Port" on page 3-6.
2. Log on to the command line interface, see "Accessing the Interface" on page 5-2.
3. Use the **`ip interface define`** command to enter a suitable IP address for the Switch, see "Setting the IP Configuration" on page 5-9.

Using the web interface:

1. Connect a management workstation to the console port of the Switch and run the Serial Web Utility, see "Through the Console Port" on page 3-6.
2. Use the Getting Started pages or the IP Setup page to enter a suitable IP address for the Switch, see "The Getting Started Pages" on page 4-4 or "Setting Up IP Information" on page 4-15.

3 SETTING UP FOR MANAGEMENT

This chapter explains the various ways of managing the Switch and details the steps you need to take before you can begin configuring it to suit the needs of your network. It covers the following topics:

- Why Manage the Switch?
- Methods of Managing the Switch
- Setting Up Web Interface Management
- Setting Up Command Line Interface Management
- SNMP Management
- Managing the Stack Over the Network
- Logging in as a Default User

Why Manage the Switch?

Network management is not required to get the Switch working, but if you do use it, you can change and monitor the way it works. By doing this, you could improve the way the Switch operates in your network.

Throughout this chapter, the term stack *refers to a number of Switches that are managed as a single unit. A stack can also contain a single Switch.*

If the stack is connected and configured as recommended, the bottom Switch in the stack is Unit 1, the next Switch up is Unit 2 and so on. Check the Unit LEDs on the front of the Switch.

Methods of Managing the Switch

You can manage the Switch in any of the following ways:

- Using the web interface.
- Using the command line interface.
- Using SNMP-compliant network management software.

The setup you require for each of these methods is illustrated in Figure 3-1.

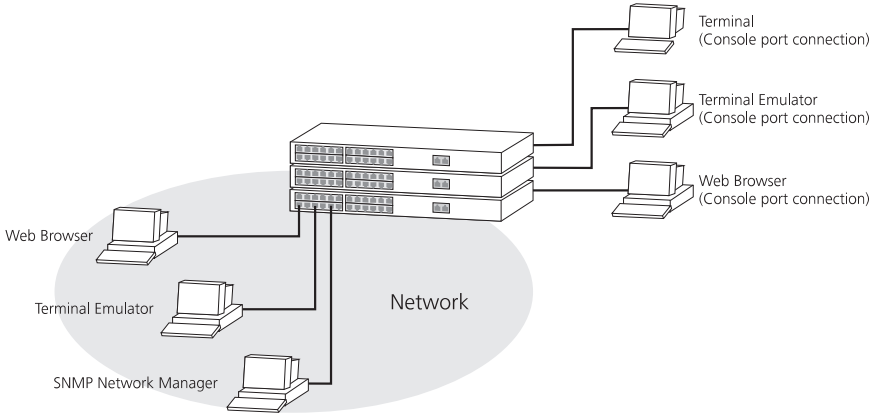


Figure 3-1 Management connections

Setting Up Web Interface Management

You can access the web interface using:

- A management workstation connected to the Switch over an IP network
- A management workstation connected to the console port of a Switch, running the Serial Line Internet Protocol (SLIP).

While multiple users can access the web interface at any one time, too many users may cause a slow response time for the web pages. You may see the error message "document contains no data". We therefore recommend that you limit the number of users with access to 3.

Over the Network

To manage the stack using the web interface over an IP network:

1. You must set up the stack with IP information; refer to "Managing the Stack Over the Network" on page 3-7.
2. You must have an IP stack correctly installed on your management workstation. You can check this by trying to browse the Web; if you can browse, an IP stack is available on your workstation.

   In addition, each Switch unit in the stack has online help and online documentation that you can set up if required. For more information, refer to "Installing Online Documentation and Help" on page 3-4.

Through the Console Port

To manage the Switch through the console port using the web interface:

1. The management workstation must be connected directly to the Switch console port using a standard null modem cable. The console port of the Switch has a male 9-pin d-type connector. You can find a pin-out diagram for the cable in Appendix D, "Pin-outs". To connect the cable:
   - **a** Attach the female connector on the cable to the male connector on the Switch's console port.
   - **b** Tighten the retaining screws on the cable to prevent it from being loosened.
   - **c** Connect the other end of the cable to your terminal or terminal emulator.

2 The management workstation must be running the Serial Line Interface Protocol (SLIP) and SLIP parameters (address and subnet mask) must be setup correctly. To do this you must install, configure and run the Serial Web Utility described in Appendix B.

In addition, each Switch unit in the stack has online help and online documentation that you can set up if required.

Installing Online Documentation and Help

The CD-ROM supplied with the your Switch contains online help and online documentation that can be used with the web interface.

- The online help system is in a HTML (HyperText Markup Language) format so that when it is launched, it appears in a secondary window in your Web browser.
- The online documentation is an online version of this User Guide in two formats, HTML and PDF (Portable Document Format).

To set up the online help and documentation:

1 Decide where the files are to be stored:

- On a local drive of your management workstation (recommended)
- On the CD-ROM, inserted into the CD-ROM drive of your management workstation
- On a network server
- On the CD-ROM, inserted into the CD-ROM drive of a networked CD-ROM server
- On a Web server

If several users are using the web interface, we recommend that you copy the files onto a server, or insert the CD-ROM into a networked CD-ROM server.

2 If the files are to be accessed from the CD-ROM, insert the CD-ROM into the relevant CD-ROM drive.

3 If the files are to be accessed from a local drive or server, copy the files from the CD-ROM to the relevant directory:

- The help files are stored in the `\Agent\IBM01_00\Help\` directory on the CD-ROM. The help files are accessed using the `Index.htm` file.

Help files for the Switch Model E12 and E24 are the same as those supplied with the Switch Model F12 and F24. If you have already installed help files for the Switch Models F12 and F24, you do not need to install the files supplied with the Switch Model E12 and E24.

- The documentation files are stored in the `\Agent\IBM01_00\Docs\` directory on the CD-ROM:
  - Both versions of the documentation can be accessed using the `\Agent\IBM01_00\Docs\Index.htm`
  - The HTML version of the user guide can be accessed directly using `\Agent\IBM01_00\Docs\E24TX\Index.htm`
  - The PDF version of the user guide can be accessed directly using `\Agent\IBM01_00\Docs\E24TX\E24TX.pdf`

We recommend that you copy the entire `\Agent\IBM01_00\Docs\` directory to your local drive or server to maintain the structure of the files.

If you have already installed documentation files for the Model F12/F24 on your local drive or server, copy the `\Agent\IBM01_00\Docs\E24TX\` *directory into the Model F12/F24* `docs` *directory. You can then access the documentation for both units from the Model F12/F24* `\Docs\Index.htm` *file.*

Choosing a Suitable Web Browser

To access the web interface correctly, your Web browser must support:

- Java®
- Frames
- HTML 3.2

Recommended Web browsers are:

- Netscape® Navigator™ Version 3.0 or above
- Microsoft® Internet Explorer Version 3.0 or above

Setting Up Command Line Interface Management

You can access the command line interface using:

- A terminal or terminal emulator connected over the network using Telnet
- A terminal or terminal emulator directly connected to the console port of a Switch in the stack or connected through a modem to the console port of a Switch in the stack

Over the Network

To manage the stack using the command line interface over a network using Telnet:

1. You must set up the stack with IP information; refer to "Setting the IP Configuration"on page 5-9.
2. If you are using a terminal emulator, you must have an IP stack correctly installed on the terminal emulator.
3. To open the Telnet session, you must specify the IP address of the stack. Check the documentation supplied with the Telnet facility if you are unsure how to do this.

Through the Console Port

To manage the stack using the command line interface through the console port:

1. You must connect the terminal or terminal emulator to the console port correctly. If you are connecting directly to the console port, you need a standard null modem cable. If you are using a modem in your setup, you need a standard modem cable.The console port of the Switch has a male 9-pin d-type connector. You can find a pin-out diagram for the cables in Appendix D, "Pin-outs". To connect the cable:
   a. Attach the female connector on the cable to the male connector on the Switch's console port.
   b. Tighten the retaining screws on the cable to prevent it from being loosened.
   c. Connect the other end of the cable to your terminal or terminal emulator.
2. The terminal or terminal emulator connected to the console port must use the same settings as the console port:
   - 8 data bits
   - no parity
   - 1 stop bit

To configure the settings of the terminal, refer to the terminal documentation. If auto-configuration for the Switch containing the console port is *enabled* (default), the line speed (baud) of the terminal is detected automatically. The Switch can auto-detect a maximum line speed of 19,200 baud.

SNMP Management

Any Network Management Software running the Simple Network Management Protocol (SNMP) can manage a stack, provided the MIB (Management Information Base) is installed correctly on the management workstation.

Managing the Stack Over the Network

When managing your stack over the network, you must remember the following, regardless of your chosen method:

- Before you can manage the Switch or stack over a network, you must set up its IP parameters using the command line interface or the web interface. To do this, you must connect a management workstation to the console port and then follow the procedure described in "Setting the IP Configuration" on page 5-9.

For your network to operate correctly, each stack must have a unique IP address. If you need to know more about IP addressing, refer to "IP Addresses" *on page 3-7.*

- Any IP information configured for a Switch in a stack can be used to manage the entire stack.
- IP must be configured correctly on your management station.

IP Addresses

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

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: 192.128.40.120

Consider the IP address in two parts:

- The first part (192.128 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 within your organization only, you may use any arbitrary IP address, as long as each address for each device is unique. We suggest you use addresses in the series 192.100.X.Y, where X and Y are numbers between 1 and 254. Use 192.101.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 time of publication:

Network Solutions
Attn: InterNIC Registration Service
505, Huntmar Park Drive
Herndon
VA22070
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 URL **`http://www.internic.net`** into your web browser.

Subnets and Using a Subnet Mask

You can divide your IP network into sub-networks or subnets. Support for subnets is important because the number of bits assigned to the device part of an IP address limits the number of devices that may be addressed on any given network. For example, a Class C address is restricted to 254 devices.

If you have a small network (less than 254 devices), you may decide not to have subnets.

A subnet mask is used to divide the device part of the IP address into two further parts:

- The first part identifies the subnet number.
- The second part identifies the device on that subnet.

The bits of the subnet mask are set to 1 if the device is to treat the corresponding bit in the IP address as part of the original network number or as part of the subnet number. These bits in the mask are set to 0 if the device is to treat the bit as part of the device number.

If you are unsure about what mask to use, we suggest that you use a general mask, 255.255.0.0, which corresponds to the example address used in the previous sections.

Logging in as a Default User

Whether you manage your switch using the web interface or the command line interface, you will need to log on correctly with a user name and password.

Default User Names

The Switch is set up with four default user names and appropriate passwords. Each of these users has a certain level of access. These default users are listed in Table 3-1.

Table 3-1 Default Users

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

To protect your switch from unauthorized access, we recommend that you change the default passwords as soon as possible.

II MANAGING THE SWITCH

4 Working With the Web Interface

This chapter describes how to access and use the web interface to manage your stack. It covers the following topics:

- Accessing the Web Interface
- The Getting Started Pages
- The Main Web Interface
- Configuring the Current Switch
- Changing the Management Settings for the Stack
- Configuring the Stack
- Viewing Statistics for the Current Switch

Throughout this chapter, the term stack *refers to a number of Switches that are managed as a single unit. A stack can also contain a single Switch.*

This chapter applies to the Switch Model E12 and E24 only. If you have a Switch Model F12 and F24 in your stack, please see the user guide that accompanies it, or refer to the help files which cover both Switches.

Accessing the Web Interface

You can access the web interface from a management station over the network or from a management station connected to the console port.

To access the web interface through the console port, you must install, configure and run the Serial Web Utility described in Appendix B.

To access the web interface over the network, follow these steps:

1. Ensure your network is correctly set up for management using the web interface. For more information, see "Setting Up Web Interface Management" on page 3-3.
2. Open your Web browser.
3. In the *Location* field of the browser, enter the URL of the stack. This must be in the format:

   `http://`*`nnn.nnn.nnn.nnn`*`/`

   where ***`nnn.nnn.nnn.nnn`*** is the IP address of the stack

   When the browser has located the stack, a user name and password dialog is displayed as shown in Figure 4-1.

Figure 4-1 User name and password dialog

If the user name and password dialog is not displayed, see Chapter 8, "Problem Solving"*.*

4 Enter your user name and password:

- If you have been assigned a user name and password, enter those details.
- If you are accessing the web interface for the first time, enter a user name and a password. The defaults are described in "Logging in as a Default User" on page 3-9. If you are setting up the stack for management, we suggest that you log on as *admin* (which has no default password).

To prevent unauthorized configuration of the stack, we recommend that you change the default passwords as soon as possible. To do this using the web interface, you need to log in as each default user and then follow the steps described in "Changing Your Password" on page 4-20.

If you forget your password while logged out of the web interface, see Chapter 8, "Problem Solving"*.*

Once you have entered a correct user name and password, one of two events occur:

- If you are accessing the web interface for the first time, a set of Getting Started pages is displayed. These are described in "The Getting Started Pages" on page 4-4.
- If you have accessed the web interface before, the Unit pages of the web interface are displayed. For information about the interface in general, see "The Main Web Interface" on page 4-6. For information about the Unit pages specifically, see "Configuring the Current Switch" on page 4-12.

If you are unable to access the web interface, see Chapter 8, "Problem Solving".

While you are managing the stack, you can view other Web pages using your browser, and then simply use the Back *button to reload the web management pages. You do not need to re-enter your username and password.*

Exiting the Web Interface

You can exit the web interface at any time; to do this, close your Web browser. For security reasons, you should always close your browser after a management session.

The Getting Started Pages

When you access the web interface for the first time or after a power-off/on cycle, a set of Getting Started pages is displayed. The first Getting Started page is shown in Figure 4-2.

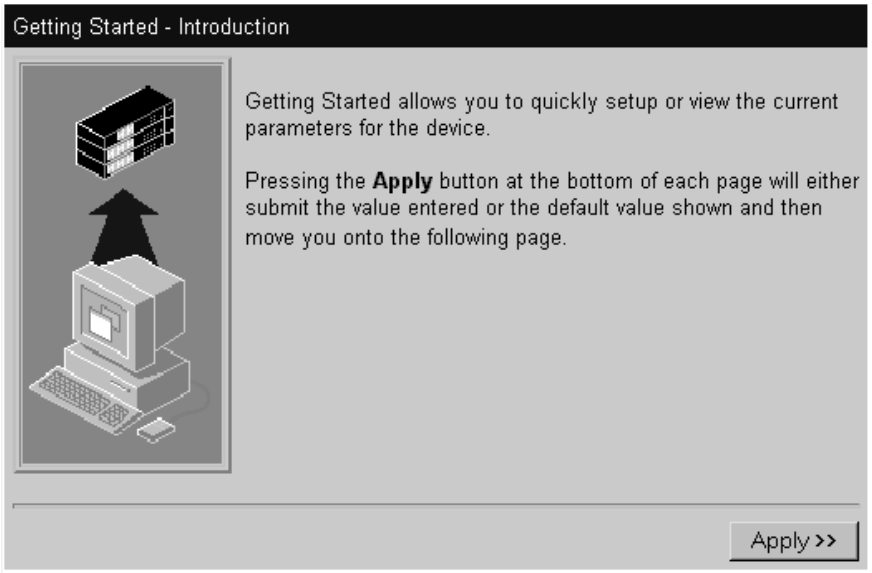


Figure 4-2 The Getting Started - Introduction page

The Getting Started pages allow you to enter basic setup information for the stack.

If you are using the web interface over the network, this IP information is already configured.

As you go through the pages, you are asked to enter:

1. A descriptive name for the stack.
2. Whether you want to allocate IP information for the stack, or whether you want a BOOTP server (if you have one) to allocate the information automatically.

   If you choose to allocate IP information yourself, you are prompted to enter the following information:

   - An IP address for the stack. For more information about IP addresses, see "Managing the Stack Over the Network" on page 3-7.

- A subnet mask for the stack. For more information about Subnet Masks, see "IP Addresses" on page 3-7.
- An IP address for the default router, if one exists on your network.

If you choose BOOTP, you are taken straight to the next page.

3 The URL or file path of the online help and online documentation for the stack. If the files are stored on a web server, you must begin the URL with **`http://`**. If the files are installed on your management workstation, you must begin the file path with **`file://`**. If you do not know where the online help and online documentation is stored, see "Installing Online Documentation and Help" on page 3-4.

4 A new password for the current user (enter the existing password if you want to leave the password unchanged).

Once you have completed the Getting Started pages, the Unit pages of the main web interface are displayed. For general information about the web interface, see "The Main Web Interface" on page 4-6. For information about the Unit pages specifically, see "Configuring the Current Switch" on page 4-12.

The Getting Started pages are available from the web interface at any time. For more information, see "Changing the Management Settings for the Stack" *on page 4-20.*

The Main Web Interface

Illustrated in Figure 4-3, the main web interface is made up of three areas:

- **The Banner**

  This is always displayed at the top of the browser window. It displays the name of the current Switch in the stack, and contains several external link icons that allow you to access information outside of the web interface. For more information about the external links, see "The External Link Icons" on page 4-7.

- **The Side-bar**

  This is always displayed down the left side of the browser window. It contains management icons that allow you to display Web pages in the page area. For more information, see "The Management Icons" on page 4-7.

- **The Page**

  This is always displayed in the center of the browser window. It contains the various Web pages that allow you to manage the stack. For more information, see "The Pages" on page 4-8.

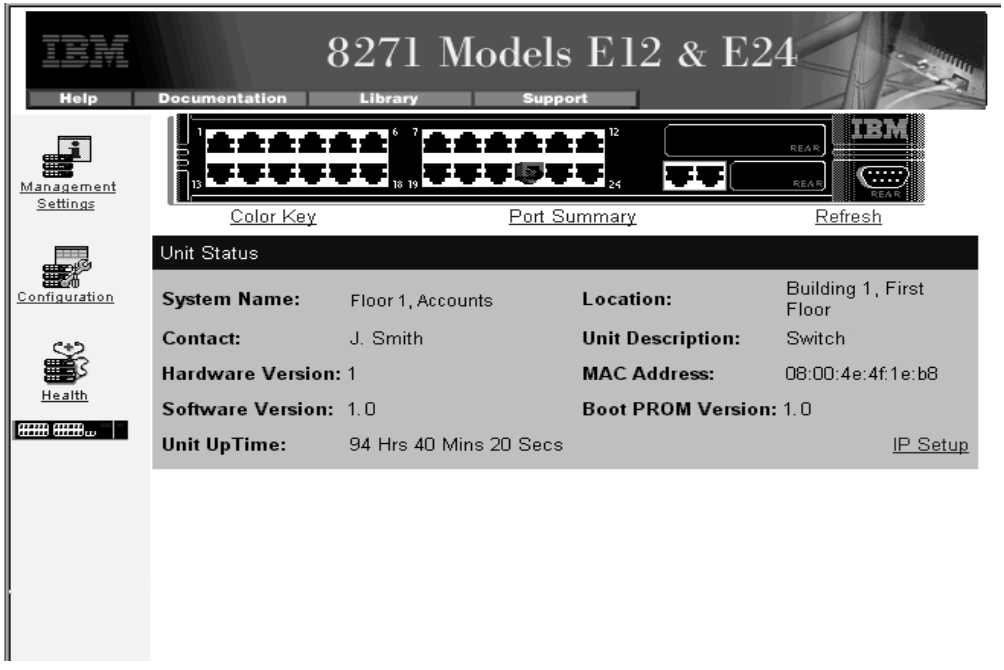


Figure 4-3 Main parts of the web interface page

The External Link Icons

The banner of the main web interface contains several external link icons that allow you to access information outside of the interface; these are shown in Table 4-1. These links are displayed on the banner at all times.

Table 4-1 External Link icons and their actions

External Link Icon	Action
Help	If you have set up the online help, click the Help icon to display the help for the web interface in a second browser window. See "Installing Online Documentation and Help" on page 3-4 for further information.
Documentation	If you have set up the online documentation, click the Documentation icon to display this user guide. See "Installing Online Documentation and Help" on page 3-4 for further information.
Library	If your management workstation has access to the World Wide Web, click the Library icon to display the Online Library of the IBM Web site.
Support	If your management workstation has access to the World Wide Web, click the Support icon to display support information from the IBM Web site.

The Management Icons

The side-bar of the main web interface displays management icons that allow you to access the Web pages; these are shown in Table 4-2.

Table 4-2 Management Icons and their actions

Management Icon	Action
	**Management Settings** — Click on this icon to display Management Settings pages for the stack.
	**Configuration** — Click on this icon to display Configuration pages for the stack.
	**Health** — Click on this icon to display Health pages for the stack.
	**Unit** — This icon represents the current stack. Click a unit to display its Unit pages.

The Pages

The map of the web interface in Figure 4-4 shows how you can access each of the pages and the links between them.

- **Unit Pages** — These pages allow you to view and change information specific to the current Switch in the stack and the ports on that Switch:
  - Switch Graphic — A graphical representation of the Switch is always displayed above the other Unit pages.
  - Unit Status — Contains information about the status of the Switch.
  - IP Setup —Allows you to set up IP information for the Switch.
  - Port Setup — Allows you to configure individual ports on the Switch.
  - Console Port Setup — Allows you to configure the console port of the Switch.
  - Port Summary — Allows you to display speed and duplex settings for all ports on the Switch.

  For more information, see "Configuring the Current Switch" on page 4-12.

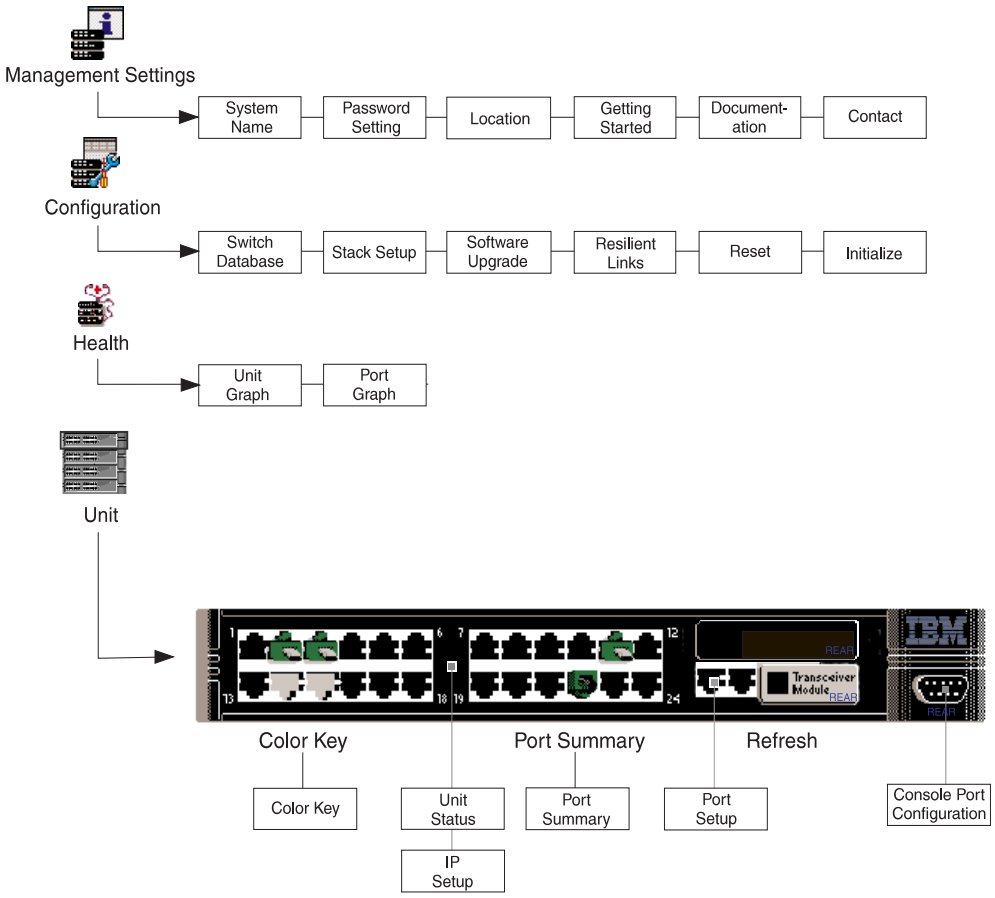


Figure 4-4 Web interface map

- **Management Settings Pages** — These pages allow you change the management settings for the stack:
  - System Name — Allows you to specify a descriptive name for the stack.
  - Password Setting — Allows you to change your password.
  - Location — Allows you to specify the location of this Switch.
  - Getting Started — Allows you to access the Getting Started pages for the stack.
  - Documentation — Allows you to specify the location of the online help and documentation for the stack.

- Contact — Allows you to enter the name of a person responsible for the Switch.

For more information, see "Changing the Management Settings for the Stack" on page 4-20.

- **Configuration Pages** — These pages allow you to view and change information specific to the stack:
  - Switch Database — Allows you to configure the Switch Database of the stack.
  - Stack Setup — Allows you to configure operating modes for the stack.
  - Software Upgrade — Allows you to upgrade management software for all Switches in the stack.
  - Resilient Links — Allows you to set up resilient links across the stack.
  - Reset —Allows you to reset all Switches in the stack.
  - Initialize — Allows you to initialize all Switches in the stack.

  For more information, see "Configuring the Stack" on page 4-24.
- **Health Pages** — This category contains pages that allow you to view statistics for the current Switch in the stack:
  - Unit Graph — This page allows you to display statistics for all the ports on the Switch.
  - Port Graph — This page allows you to display statistics for a specific port on the Switch.

  For more information, see "Viewing Statistics for the Current Switch" on page 4-34.

Navigating the Page Area

To access the first page in each group of pages, click on the relevant icon on the side-bar; to access the remaining pages in the group, click on the underlined hotlinks displayed at the top of each page.

Making Changes in the Page Area

If you change any setting on a page, you *must* click the *Apply* button at the foot of the page to make the change to the stack.

Changes made on a page are only applied when you click Apply. *If you make changes on a page but do not wish to apply them, click the* Back *button in your browser to exit the page.*

The Switch Graphic

A graphical representation of the Switch is always shown at the top of the Unit pages. A typical example of a graphic is shown in Figure 4-5.

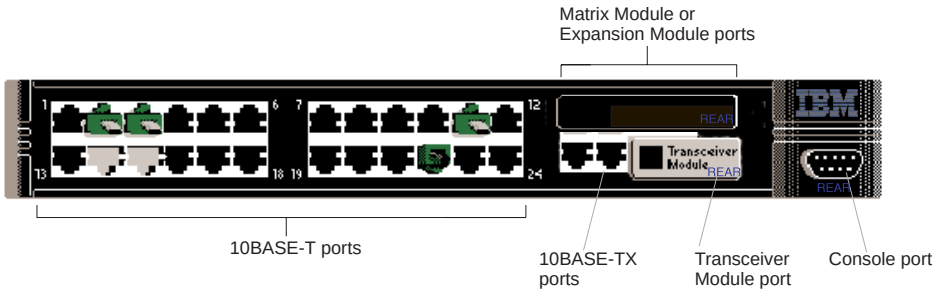


Figure 4-5 The Switch graphic

Any ports located on the rear of the physical Switch are shown on this graphic for convenience. By clicking on parts of the graphic, you can access the relevant configuration pages.

If you click on:

- The unit (but not a port) — the Unit Status page is displayed.
- A 10BASE-T, 100BASE-TX or transceiver module port — the Port Setup page is displayed
- The console port — the Console Port Configuration page is displayed.

The graphic also indicates the status of the ports. See "Viewing Port Status" on page 4-12.

If you have a Matrix Module installed, the expansion module area states Matrix Module. *You cannot configure matrix ports.*

Configuring the Current Switch

The Unit pages allow you to:

- View the status of the ports on the Switch
- View information about the status of the Switch
- Set up IP information for the Switch
- Configure individual ports on the Switch
- Configure the console port of the Switch

To access the Unit pages, click the unit icon on the sidebar.

Viewing Port Status

The ports on the Switch graphic are color-coded to show their status:

- Green — Enabled, connected
- Black — Enabled, disconnected
- Gray (with connection) — Disabled, connected
- Gray (without connection) — Disabled, disconnected

To display this color-coding convention, click the Color Key hotlink.

Refreshing the Switch Graphic

The Switch graphic does not update itself automatically — if you make a change to the status of a port, you need to click the Refresh hotlink positioned under the Switch graphic. If, after clicking Refresh, the Switch graphic does not update, you may need to make a small change to your Web browser, see "Using the Serial Web Utility" on page 8-6.

Viewing the Port Speed and Duplex

To display the speed and duplex mode for each port on the Switch, click the *Port Summary* hotlink located beneath the Switch graphic. A typical port summary page is displayed in Figure 4-6.

Port Summary

Port	Speed	Duplex	Port	Speed	Duplex
1	10	Half	14	---	---
2	10	Half	15	---	---
3	10	Half	16	---	---
4	---	---	17	---	---
5	---	---	18	---	---
6	---	---	19	---	---
7	---	---	20	---	---
8	10	Half	21	---	---
9	---	---	22	---	---
10	---	---	23	---	---
11	---	---	24	---	---
12	10	Full	25	100	Full
13	10	Full	26	100	Full

Figure 4-6 The Port Summary page

If you have an expansion module fitted to your Switch, these port numbers will following on sequentially from the number of fixed ports on the front of the unit.

Viewing Administration Information

The Unit Status page displays general administration information that has been setup for this Switch. A typical Unit Status page is displayed in Figure 4-7.

Unit Status

System Name:	Floor 1, Accounts	**Location:**	Building 1, First Floor
Contact:	J. Smith	**Unit Description:**	Switch
Hardware Version:	1	**MAC Address:**	08:00:4e:4f:1e:b8
Software Version:	1.0	**Boot PROM Version:**	1.0
Unit UpTime:	94 Hrs 40 Mins 20 Secs		IP Setup

Figure 4-7 The Unit Status page

The Unit Status page contains the following elements:

System Name
Displays the name given to the Switch during the Getting Started procedure.

Location
Displays the physical location of the Switch.

Contact
Displays the details of a person to contact about the Switch.

Unit Description
Displays the product name of the Switch.

Hardware Version
Displays the version number of the Switch hardware.

MAC Address
Displays the factory-set MAC (Ethernet) address assigned to the Switch.

Software Version
Displays the version number of the management software currently installed on the Switch.

Boot PROM Version
Displays the version of Boot PROM software installed on the Switch.

Unit Uptime
Displays the time that has elapsed since the Switch was last reset, initialized or powered-up.

IP Setup
This hotlink displays the IP Setup page.

Setting Up IP Information

You can set up IP information for the Switch using the IP Setup page.

To access the page, click the *IP Setup* hotlink on the Unit Status page. The IP Setup page is displayed as shown in Figure 4-8.

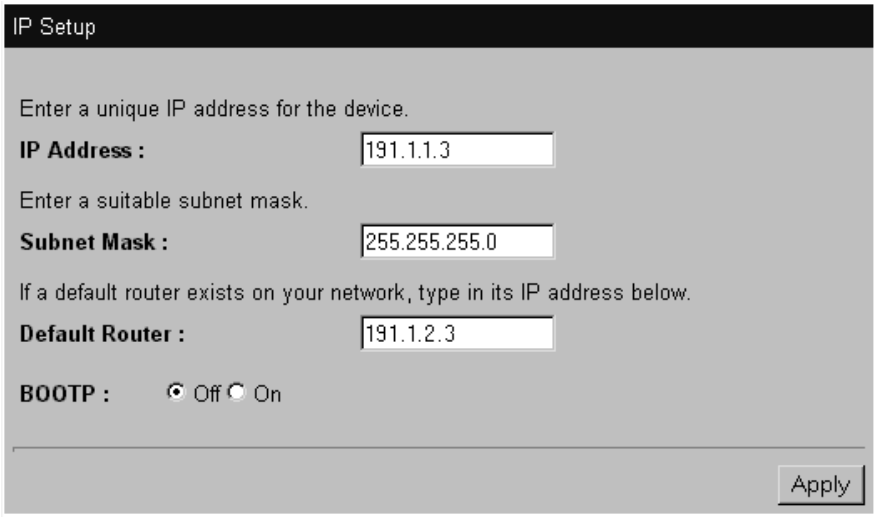


Figure 4-8 The IP Setup page

The IP Setup page contains the following elements:

IP Address

Allows you to enter a unique IP address for the Switch. If you change the IP address of the Switch, your web browser will no longer recognize it. You must retype the new IP address into the location window of your browser. For more information about IP addresses, see "Managing the Stack Over the Network" on page 3-7.

Subnet Mask

Allows you to enter a subnet mask for the Switch. For more information about subnet masks, see "Subnets and Using a Subnet Mask" on page 3-8.

Default Router

Allows you to enter the IP address of the default router if your network contains one or more routers. For more information about IP addresses, see "Managing the Stack Over the Network" on page 3-7.

BOOTP *On* / *Off*
If you have a BOOTP server on your network, these radio buttons allow you to specify whether the server allocates IP information for the Switch automatically.

Configuring a Port

You can configure individual ports on the Switch using the Port Setup page.

To access the page, click the relevant port on the Switch graphic. The Port Setup page is displayed as shown in Figure 4-9.

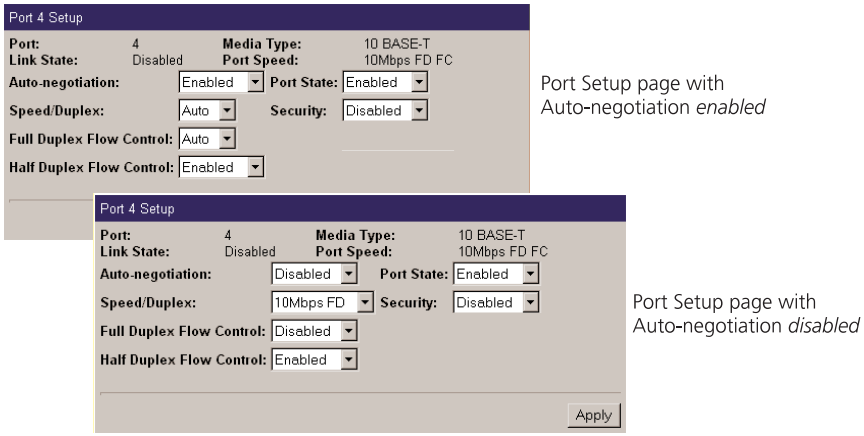


Figure 4-9 The Port Setup page

The Port Setup page contains the following read-only elements:

Port
Displays the number of the selected port.

Link State
States whether the link is enabled or disabled.

Media Type
Displays the media type of the link connected to the port.

Port Speed
Displays the current operational speed of this port and indicates the duplex mode. *FC* indicates that Flow Control is enabled.

Using this page, you can set the following:

Auto-negotiation *Enabled* / *Disabled*
Allows you to specify whether auto-negotiation is enabled:

- If auto-negotiation is enabled on the 10BASE-T/100BASE-TX ports, their speed and duplex mode is automatically detected and set accordingly.
- If auto-negotiation is enabled on the 10BASE-T ports, the duplex mode only is automatically detected and set accordingly.
- If you disable auto-negotiation, you can manually set the speed and duplex mode of the port using the Speed/Duplex drop-down listbox.

Fiber ports are not auto-negotiating. If you chose to setup a fiber port provided through an expansion module, Auto-negotiation is set to Disabled *and you cannot change it.*

With auto-negotiation enabled, the Speed/Duplex *and* Full Duplex Flow Control *fields display* Auto *and cannot be set manually.*

ATTENTION: *The duplex mode of a link is not detected if the port on the other end of the link is not auto-negotiating. In this case, the Model E12 or E24 port is set to operate in half duplex:*

- *If you want the link to operate in full duplex, set the Switch port to operate in full duplex using the Speed/Duplex drop-down listbox.*
- *If you want the link to operate in half duplex, set the port on the other end of the link to half duplex.*

Speed/Duplex *100 Mbps FD / 100 Mbps HD / 10 Mbps FD / 10 Mbps HD /* *Auto*
If auto-negotiation is enabled, this field shows *Auto* and you cannot change it manually. If auto-negotiation is disabled, or if the device at the other end of the link does not support auto-negotiation, this field allows you to:

- Specify full duplex mode (*FD*) or half duplex mode (*HD*) for 10BASE-T ports or 100BASE-FX ports provided through an expansion module.
- Specify speed and full duplex mode (*FD*) or half duplex mode (*HD*) for 10BASE-T/100BASE-TX ports.

Full Duplex Flow Control *Enabled* / *Disabled* / *Auto*
If auto-negotiation is enabled, this field shows *Auto* and you cannot change it manually. If auto-negotiation is disabled and the link is full duplex, this field allows you to enable or disable IEEE 802.3x flow control. Flow control minimizes any packet losses that may occur on congested ports.

For Flow Control to operate correctly, you must manually enable it at both ends of the Switch—endstation link.

Flow control should be disabled if the port is connected to multiple devices using a repeater.

Half Duplex Flow Control *Enabled* / *Disabled*
For half duplex links, allows you to enable the Intelligent Flow Management (IFM) system of flow control. Flow control minimizes any packet losses that may occur on congested ports.

Port State *Enabled* / *Disabled*
Allows you enable or disable the port.

Security *Enabled* / *Disabled*
Allows you to specify whether the port uses Security to guard against unauthorized users connecting devices to your network. When Security is enabled on a port, it enters Single Address Learning Mode. In this mode, the Switch removes all the MAC (Ethernet) addresses stored for the port in the Switch Database and then learns the address of the first packet it receives on the port.

Once the first address is learned, no other endstation is allowed to access the network through the port. If an endstation with a different address attempts to transmit packets through the port, the port is automatically disabled until it is enabled using the *Port State* field.

Configuring the Console Port

By default, the console port is configured for direct connection to a terminal. You only need to change this configuration if you are connecting a modem to the port. You can configure the console port of the Switch using the Console Port Setup page.

To access the page:

1. Click the Unit icon on the side-bar.
2. Click the console port on the Switch graphic. The Console Port Configuration page is displayed as shown in shown in Figure 4-10.

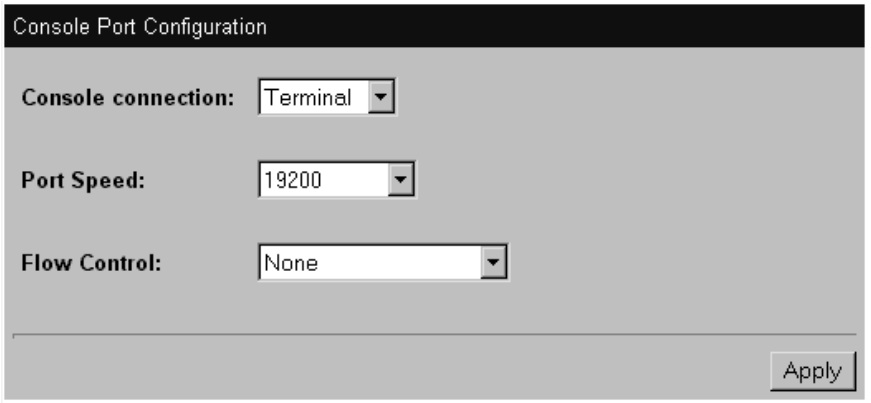


Figure 4-10 The Console Port Configuration page

The Console Port Configuration page contains the following elements:

Console connection *Terminal / Modem*
Allows you to specify the device that you are connecting to the console port.

Port Speed *AutoConfig / 1200 / 2400 / 4800 / 9600 / 19200*
Allows you to specify the line speed (baud rate) of the console port. If you select *AutoConfig*, the line speed of the port is automatically set to the line speed of the terminal or modem.

Flow Control *None / Hardware RTS/CTS*
Allows you to specify the flow control option suitable for your terminal or modem. Refer to the documentation accompanying your terminal or modem if you are unsure of the correct setting.

Changing the Management Settings for the Stack

The Management Settings pages allow you to:

- Specify a descriptive name for the stack.
- Change your password.
- Access the Getting Started pages for the stack.
- Specify the location of the online help and documentation for the stack.

Specifying a Name for the Stack

You can specify a descriptive name for the stack using the System Name page.

To access the page, click the Management Settings icon on the side-bar. The System Name page is displayed as shown in Figure 4-11.

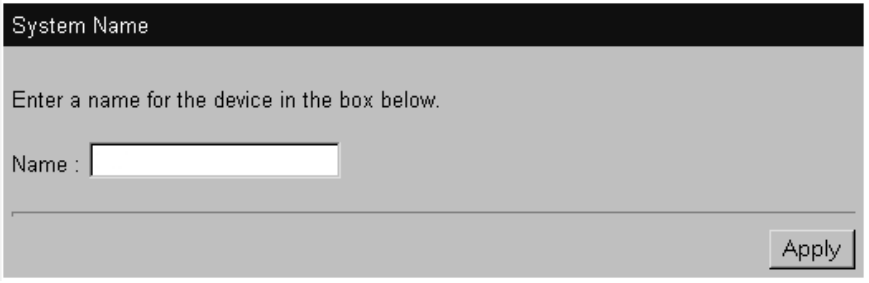


Figure 4-11 The System Name page

The Name field allows you to enter a descriptive name for the stack up to 20 characters in length.

Changing Your Password

You can change the password for your user using the Password Setting page.

To access the page, click the Management Settings icon on the side-bar and click the password setting hotlink. The Password Setting page is displayed as shown in Figure 4-12.

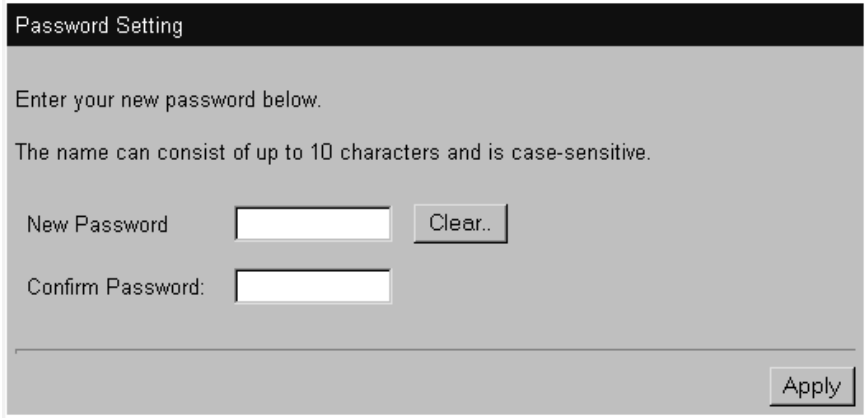


Figure 4-12 The Password Setting page

The Password Setting page contains the following elements:

New Password
Allows you to enter a new password for your user. The password can be a maximum of 10 characters.

Confirm Password
You must re-enter the new password for confirmation.

Specifying a Location for the Stack

You can specify the location of the Switch using the Location page. You could enter for example, the building number if you are on a campus, floor number, or name of the wiring closet.

To access the page, click the Management Settings icon on the side-bar and click the *Location* hotlink. The Location page is displayed as shown in Figure 4-13.

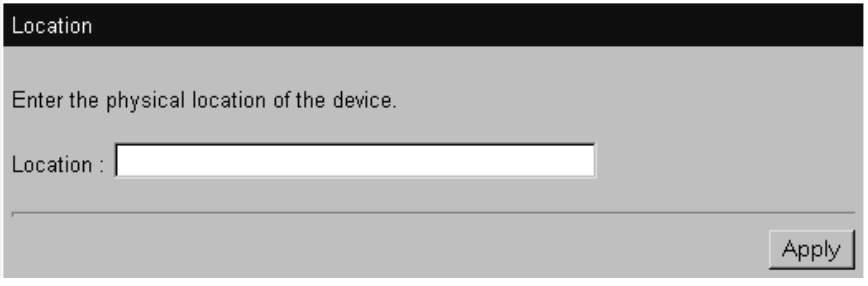


Figure 4-13 The Location page

Accessing the Getting Started Pages

You can use the Getting Started pages at any time to enter and change basic setup information for the stack.

To access the Getting Started pages, click the Management Settings icon on the side-bar and click the *Getting Started* hotlink.

Using these pages is described in "The Getting Started Pages" on page 4-4.

Specifying a Contact for the Stack

You can enter the name of a contact for this stack using the Contact page.

To access the Contact page, click the Management Settings icon on the side-bar and click the Contact hotlink. The Contact page is displayed as shown in Figure 4-14.

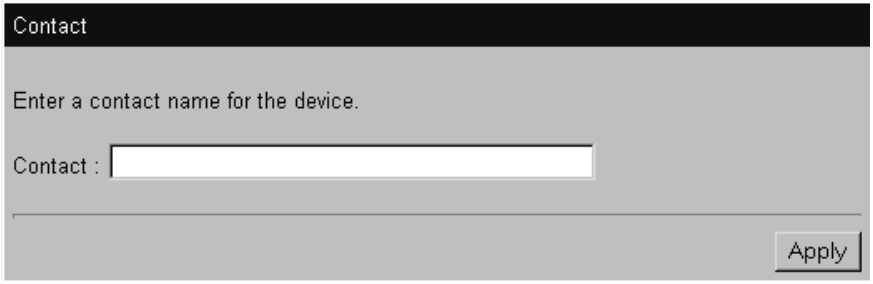


Figure 4-14 The Contact page

Specifying the Location of Online Help and Documentation

The documentation page allows you to specify the location of the online help and documentation for the stack.

To access the Documentation page, click the Management Settings icon on the side-bar and click the *Documentation* hotlink. The Documentation page is displayed as shown in Figure 4-15.

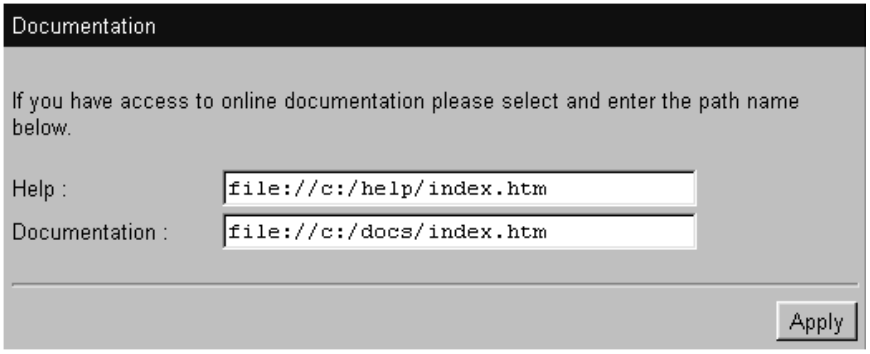


Figure 4-15 The Documentation page

The Documentation page contains the following elements:

Help
This field allows you to specify the URL or file path of the online help. If the files are stored on a web server, you must begin the URL with **`http://`**. If the files are installed on you management workstation, you must begin the file path with **`file://`**. If you do not know where the online help is stored, see "Installing Online Documentation and Help" on page 3-4.

Documentation
This field allows you to specify the URL or file path of the online documentation for the stack. If the files are stored on a web server, you must begin the URL with **`http://`**. If the files are installed on you management workstation, you must begin the file path with **`file://`**. If you do not know where the online documentation is stored, see "Installing Online Documentation and Help" on page 3-4.

Configuring the Stack

The Configuration pages allow you to:

- Configure the operating modes for the stack
- Configure the Switch Database of the stack
- Set up resilient links across the stack
- Reset the all units in the stack
- Initialize all units in the stack
- Upgrade management software for the stack

To access the Configuration pages, click the Configuration icon on the side-bar.

Configuring Stack Operating Modes

You can specify operating modes for the stack using the Advanced Stack Setup page. To access the page, click the Configuration icon on the side-bar. The Advanced Stack Setup page is displayed as shown in Figure 4-16.

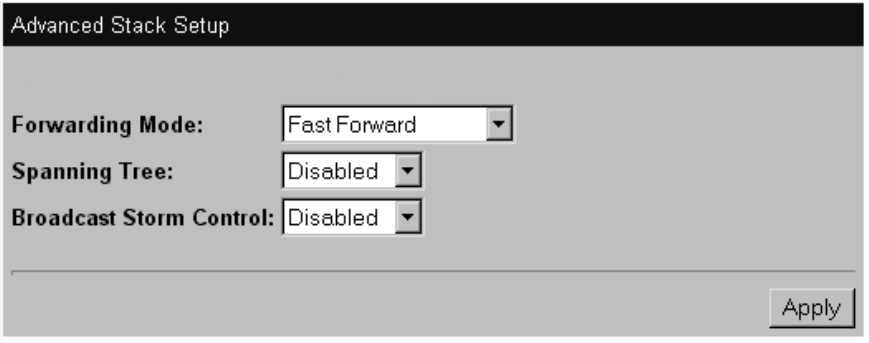


Figure 4-16 The Advanced Stack Setup page

The Advanced Stack Setup page contains the following elements:

Forwarding Mode *Fast Forward* / *Fragment Free* / *Store and Forward* / *Intelligent*
Allows you to set the Forwarding Mode for the stack:

- *Fast Forward* — Packets are forwarded as soon as the destination address is received and verified. The forwarding delay, or latency, for all packets in this mode is 35µs but with the lack of error checking, error packets are propagated onto the network.
- *Fragment Free* — A minimum of 512 bits of the received packet is buffered before to the packet is forwarded. This ensures that collision fragments are not propagated through the network. The forwarding delay, or latency, for all packets in this mode is 64µs.
- *Store and Forward* — Received packets are buffered entirely before they are forwarded. This ensure that only good packets are forwarded to their destination. The forwarding delay for this mode varies between 64µs and 1.2ms, depending on packet length and port speed. In Store and Forward mode, latency is measured as the time between receiving the last bit of the packet and transmitting the first bit. For the Model E12 and E24, this is 7µs.
- Intelligent — The stack monitors the amount of error traffic on the network and changes the Forwarding Mode accordingly. If the stack detects less than 20 errors a second, the Forwarding Mode is set to Fast Forward. If the stack detects 20 or more errors a second, the Forwarding Mode is set to Store and Forward until the number of errors a second returns to zero.

Spanning Tree *Enabled* / *Disabled*
Allows you to specify whether the stack uses the Spanning Tree Protocol (STP). STP improves your network's tolerance to faults; for more information, see Chapter 6, "Spanning Tree Protocol".

Storm Control *Enabled* / *Disabled*
Allows you to specify whether the stack uses Broadcast Storm Control. If Broadcast Storm Control is enabled, the stack automatically creates an alarm for each port to monitor the level of broadcast traffic on that port. If over 20% of the total traffic on a port is broadcast traffic, the broadcast traffic on the port is blocked until the broadcast traffic returns to 20%.

Configuring the Switch Database

You can configure the Switch Database for the stack using the Switch Database page.

To access the page, click the Configuration icon on the side-bar and click the Switch Database hotlink. The Switch Database page is displayed as shown in Figure 4-17.

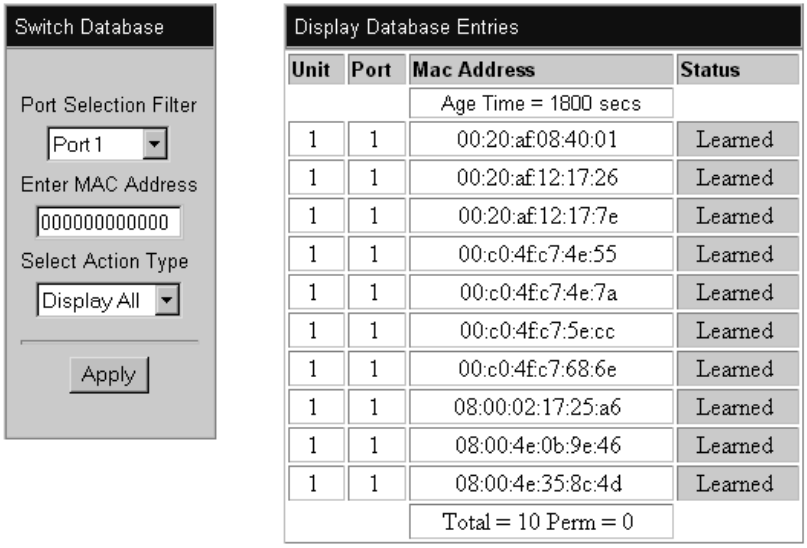


Figure 4-17 The Switch Database page

What is the Switch Database?

The Switch Database is used by the stack to determine if a packet should be filtered or forwarded, and which port should forward the packet if it is to be forwarded.

The database contains a list of entries, each containing two items:

- The MAC address information from each endstation that sends packets to the port.
- The port in the stack that receives packets from that endstation.

The maximum number of entries the database can hold is 6000 multiplied by the number of Model E12 and E24 units in the stack. The maximum number of entries the Model F12 and F24 database can hold is 12,000 addresses per unit.

Databases entries can have two states:

- *Learned* — The stack has placed the entry into the Switch Database when a packet was received. Learned entries are removed (aged out) from the Switch Database if the stack does not receive packets from that endstation for 30 minutes. This prevents the Switch Database from becoming full with obsolete entries by ensuring that when an endstation is removed from the network, its entry is also removed from the database. Learned entries are also removed from the Switch Database if the Switch that submitted the entry is reset or powered-off.
- *Permanent* — The entry has been placed into the Switch Database using the Switch Database page. Permanent Entries are not removed from the Switch Database unless they are deleted using the Switch Database page.

Displaying the Switch Database

The Display Database Entries table shown on the Switch Database page displays the Switch Database entries for the stack:

- **Unit** *1 / 2 / 3 / 4*
  This column displays the Switch unit in the stack that contains the port for the entry.
- **Port**
  This column displays the port for the entry.
- **MAC Address**
  This column displays the MAC address for the entry.
- **Status** *Learned / Permanent*
  This column displays the state of the entry.

To display a subset of the entries:

1. From the *Port Selection Filter* drop-down listbox, select a port that has submitted the relevant entries.
2. In the *Enter MAC Address* field, enter the first few characters of the MAC (Ethernet) address for the relevant entries.
3. From the *Select Action Type* drop-down listbox, select *Search*.
4. Click *Apply*.

To display the entire list of entries:

1. From the *Select Action Type* drop-down listbox, select *Display All*.
2. Click *Apply*.

Inserting Permanent Entries into the Switch Database

The Switch Database page allows you to insert permanent entries into the Switch Database. To insert a permanent entry:

1. In the *Port Selection Filter* drop-down listbox, select a port.
2. In the *Enter MAC Address* field, enter the MAC (Ethernet) address for the entry.
3. From the *Select Action Type* drop-down listbox, select Insert.
4. Click *Apply*.

The Display Database Entries table is not automatically updated with the new entry. To update the table:

a *From the Select Action Type drop-down listbox, select Display All.*

b *Click* Apply.

Deleting Entries from the Switch Database

The Switch Database page allows you to delete entries from the Switch Database. To delete an entry:

1. In the *Enter MAC Address* field, enter the MAC (Ethernet) address for the entry.
2. From the *Select Action Type* drop-down listbox, select Delete.
3. Click *Apply*.

The Display Database Entries table is not automatically updated with the deletion. To update the table:

a *From the Select Action Type drop-down listbox, select Display All.*

b *Click* Apply.

Setting Up Resilient Links for the Stack

You can set up resilient links for the stack using the Resilient Links page.

To access the page, click the Configuration icon on the side-bar and click the Resilient Links hotlink. The Resilient Links page is displayed as shown in Figure 4-18.

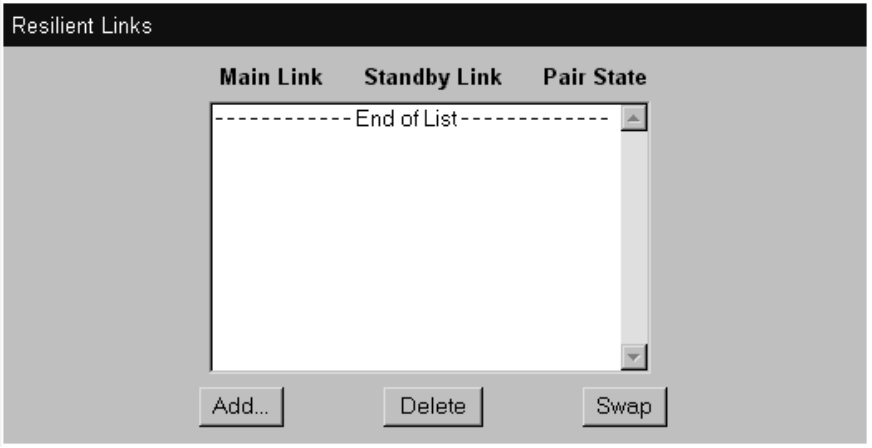


Figure 4-18 The Resilient Links page

What are Resilient Links?

The Resilient Link feature enables you to protect critical links and prevent network downtime if those links fail. A resilient link comprises of a *resilient link pair* containing a main link and a standby link. If the main link fails, the standby link immediately and automatically takes over the task of the main link.

The resilient link pair is defined by specifying a main port and a standby port at one end of the link. If the main link fails, the main port is disabled and the standby port is enabled. If the main port has a higher bandwidth than the standby port, the main port is automatically re-enabled if no link failure is detected for 2 minutes. Otherwise, you need to re-enable the main port manually.

When setting up resilient links, note the following:

- Resilient link pairs should not be set up if the stack uses the Spanning Tree Protocol (STP).
- Resilient link pairs can only be set up using fiber or twisted pair ports. The main and standby ports in the same pair, however, can use any combination of these media.
- A resilient link pair can only be set up if:
  - The ports is not a secure port.
  - Neither of the ports belong to another resilient link pair.
- A resilient link pair must only be defined at one end of the link.
- Ports that are part of a resilient link pair cannot be disabled unless a link failure occurs.

Displaying Resilient Link Pairs

The Resilient Links page displays the resilient link pairs that are set up for the stack:

- **Main Link** *Unit 1 Port 1 / Unit 1 Port 2 / ...*
  This column displays the port in the stack that is the main port of the resilient link pair, and the state of the link on that port.
- **Standby Link** *Unit 1 Port 1 / Unit 1 Port 2 / ...*
  This column displays the port in the stack that is the standby port of the resilient link pair, and the state of the link on that port.
- **Pair State** *Operational / Not Operational*
  This column displays whether the resilient link pair is operational or not. When the pair is operational, either the main port or the standby port can forward traffic.

Creating a Resilient Link Pair

1. Click *Add...* The Add Resilient Links page is displayed. If there is more than one Switch in your stack, you are asked to choose the main unit and standby unit. Click *Next*.
2. Select the main port and click *Next*.
3. Select the standby unit and click *Next*.
4. Click *Next...* The Resilient Links page is displayed showing the new resilient link pair.

Deleting a Resilient Link Pair

1. Click the resilient link pair.
2. Click the *Delete* button.

Swapping the Main and Standby Ports of a Resilient Link Pair

1. Click the resilient link pair.
2. Click the *Swap* button.

Resetting all Switches in the Stack

The Reset page allows you to reset all units in the stack.

To access the Reset page, click the Configuration icon on the side-bar and click the *Reset* hotlink. To reset the stack, choose Yes and click *Apply*.

What Happens During a Reset?

Resetting the stack simulates a power-off/on cycle for each of the Switches in the stack. You may want to do this if you need to:

- Remove all the Learned entries in the Switch Database (SDB).
- Reset the statistic counters of the stack.

ATTENTION: *Resetting the stack may cause some of the traffic being transmitted over the network to be lost. It also clears all Learned entries from the Switch Database.*

The stack takes about 10 seconds to reset. While the stack is resetting, the Web browser cannot communicate with the stack.

Initializing all Switches in the Stack

The Initialize page allows you to initialize all units in the stack.

To access the page, click the Configuration icon on the side-bar and click the Initialize hotlink. To initialize the stack, choose *Yes* and click *Apply*.

What Happens During Initialization?

Initializing the Switch units in the stack returns them to their default (factory) settings. You should only initialize the stack if the stack has been previously used in a different part of the network and the configuration does not suit the new environment.

ATTENTION: *Use great care when initializing the stack — it removes all configuration information, including security, resilient links and passwords. However, IP and SLIP information is retained to ensure that you can continue managing the stack.*

Network loops occur if you have set up resilient links. Before initializing the stack, ensure you have disconnected the cabling for all standby links.

The stack takes about 10 seconds to initialize. While the stack is initializing, the Web browser cannot communicate with the stack.

Upgrading Management Software

The Software Upgrade page allows you to install new versions of management software onto your stack.

To access the Software Upgrade page, click the Configuration icon on the side-bar and click the *Software Upgrade* hotlink. The Software Upgrade page is displayed as shown in Figure 4-19.

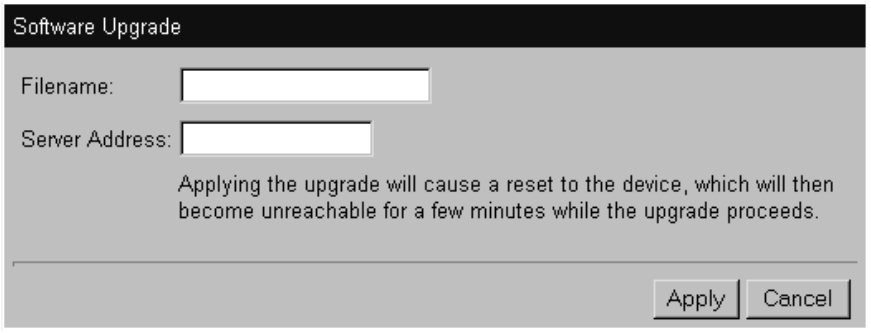


Figure 4-19 The Software Upgrade page

To upgrade the management software:

1. Copy the software upgrade file into an appropriate directory on a TFTP server. For information on using a TFTP server, refer to the documentation that accompanies it.
2. Enter the name of the software upgrade file in the *Filename* field. The file name format is:

   `nws`*`xx_yy`*`.bin`

   where xx_yy is the version of management software.
3. Enter the IP address of the TFTP server in the *Server Address* field.
4. Click *Apply*. During the upgrade, the Power/Self Test LED flashes green and the web interface is locked. The upgrade takes about 5 minutes; when the upgrade is complete, the units in the stack are reset.

ATTENTION: *During the upgrade, do not power down or reset the Switch.*

Viewing Statistics for the Current Switch

You can view statistics for the current Switch in the stack using the Health pages. These pages allow you to:

- Display a range of statistics for a specific port on the Switch.
- Display a range of statistics for all the ports on the Switch.

Displaying Port Statistics

You can display a range of statistics for a specific port on the Switch using the Port Graph page.

To access the page, click the Health icon on the side-bar. The graphs that can be displayed are shown in Figure 4-20.

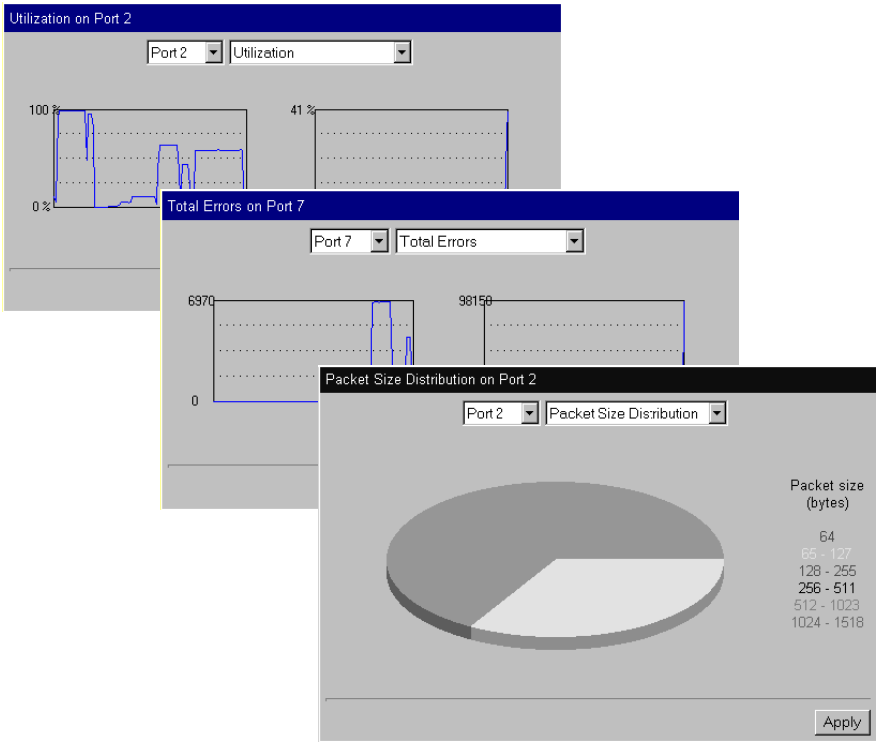


Figure 4-20 Port Graph pages

The Port Graph page allows you to display a range of statistics for a chosen port. You can choose to display a graph for *Utilization, Total Errors* or *Packet Size Distribution*.

To display the Utilization graph — From the first drop-down listbox, choose a port. From the second drop-down listbox, choose *Utilization*. Click *Apply*.

To display the Total Errors graph — From the first drop-down listbox, choose a port. From the second drop-down listbox, choose *Total Errors*. Click *Apply*.

To display the Packet Size Distribution graph — From the first drop-down listbox, choose a port. From the second drop-down listbox, choose *Packet Size Distribution*. Click *Apply*.

Interpreting the Statistics

The Utilization graph scales automatically to show the percentage bandwidth used on the port, over the last hour and last 48 hours:

- A bandwidth utilization of 0 – 25% indicates that the ports are dealing with a light traffic load.
- A bandwidth utilization of 26 – 80% indicates that the ports are dealing with a heavy traffic load.
- A bandwidth utilization of 81 – 100% indicates that the ports are dealing with a very heavy traffic load. This could be caused by an fault in your network, or an inadequate network configuration.

The Total Errors graph scales automatically to show the total number of packets with errors that have been seen on the port over the last hour and 48 hours.

The Packet Size Distribution graph displays the proportion of packets of certain sizes seen by the port over the last 30 seconds:

- 64 bytes and less
- 65 – 127 bytes
- 128 – 255 bytes
- 256 – 511 bytes
- 512 – 1023 bytes
- 1024 – 1518 bytes

Displaying Unit Statistics

You can display a range of statistics for all the ports on the Switch using the Unit Graph page.

To access the page, click the Health icon on the side-bar. Click the *Unit Graph* hotlink. The graphs that can be displayed are shown in Figure 4-21.

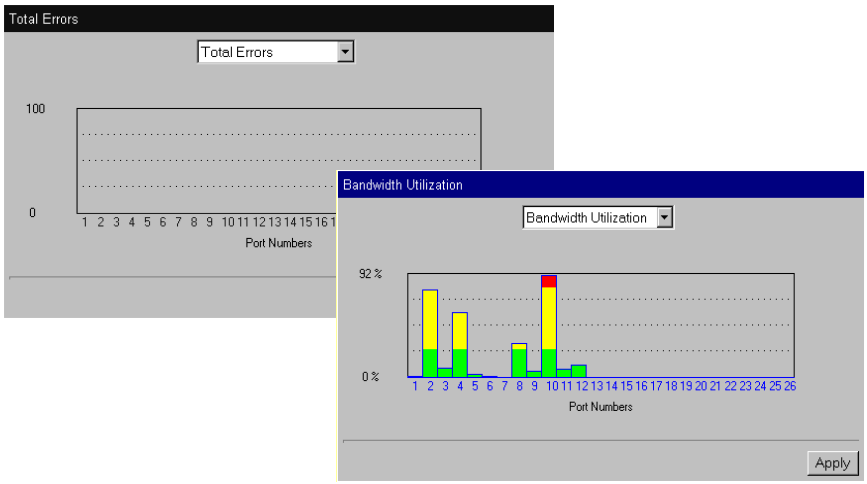


Figure 4-21 Unit Graph pages

If you click a port on one of these graphs, the graph for that port is displayed.

The Unit Graph page allows you to display a range of statistics for the Switch as a whole. You can choose to display a graph for *Bandwidth Utilization* or *Total Errors*.

To display the Bandwidth Utilization graph — Choose *Bandwidth Utilization* from the drop-down listbox. Click *Apply*.

To display the Total Errors graph — Choose *Total Errors* from the drop-down listbox. Click *Apply*.

Interpreting the Statistics

The Utilization graph scales automatically to display the percentage of bandwidth used on all ports across the Switch over the last 30 seconds:

- A bandwidth utilization of 0 – 25% (green bar on the graph) indicates that the ports are dealing with a light traffic load.
- A bandwidth utilization of 26 – 80% (yellow bar on the graph) indicates that the ports are dealing with a heavy traffic load.
- A bandwidth utilization of 81 – 100% (red bar on the graph) indicates that the ports are dealing with a very heavy traffic load. This could be caused by an fault in your network, or an inadequate network configuration.

The Total Errors graph scales automatically to show the total number of packets with errors that have been seen on all ports across the Switch over the last 30 seconds.

5 WORKING WITH THE COMMAND LINE INTERFACE

This chapter details switch management that can be accessed and changed using the command line interface. It covers the following topics:

- Accessing the Interface
- Using the Command Line Interface Menus
- A Quick Guide to the Commands
- Switch Administration
- Configuring the Switch
- Viewing the Configuration
- Enabling And Disabling Remote Access
- Initializing the Switch
- Resetting the Switch
- Upgrading Management Software
- Pinging Other Devices

This chapter applies to the Switch Model E12 and E24 only. If you have Switch Model F12/F24 in your stack, please see the user guide that accompanies it.

Accessing the Interface

The following steps describe how you access the command line interface:

1. Set up your network for command line interface management; for more information, see "Setting Up Command Line Interface Management" on page 3-6. The login sequence for the command line interface begins as soon as a relevant Switch in the stack detects a connection to its console port, or as soon as a Telnet session is started.

If the login sequence does not begin immediately, press the [Return] key a few times until it does begin. If the sequence still does not begin, see on "Using the Command Line Interface" *on page 8-5.*

2. At the login and password prompts, enter your user name and password:

   - If you have been assigned a user name and password, enter those details.
   - If you are accessing the command line interface for the first time, enter a default user name and password to match your access requirements. The defaults are described in "Logging in as a Default User" on page 3-9. If you are setting up the stack for management, we suggest that you log in as `admin` (which has no default password).

   If you have logged on correctly, the top-level menu of the command line interface is displayed, see "Using the Command Line Interface Menus" on page 5-3. If you have *not* logged on correctly, the message `Incorrect password` is displayed and the login sequence starts again.

   To prevent unauthorized configuration of the stack, we recommend that you change the default passwords as soon as possible. To do this using the command line interface, you need to log in as each default user and then follow the steps described in "Setting and Changing Passwords" on page 5-7.

Exiting the Command Line Interface

To exit the command line interface, enter the command **`logout`**. The management session is terminated.

The **`logout`** *command can be used at any menu level of the interface.*

A management session will be terminated if there is period of inactivity lasting longer than 15 minutes. After the session has terminated, the first key that you press will return you to the login prompt.

Using the Command Line Interface Menus

Once you logged onto the command line interface correctly, you will see the top-level menu, an example of which is shown in Figure 5-1.

```
Menu options:------------ IBM 8271 Nways Model E24 ---------------------------------
   system                  - Administer system-level functions
   ethernet                - Administer Ethernet ports
   ip                      - Administer IP
   logout                  - Logout of the command line interface

Type ? for help.
--------------------------Top floor/Marketing (Unit 1)-----------------------------
Select menu option:
```

Figure 5-1 Top-level menu

Use the command line interface by selecting options from this menu and from the others below it. Each menu option is accompanied by a brief description of what that option does.

Command Line Interface Menu Structure

Figure 5-2 shows the menu/command structure for the command line interface.

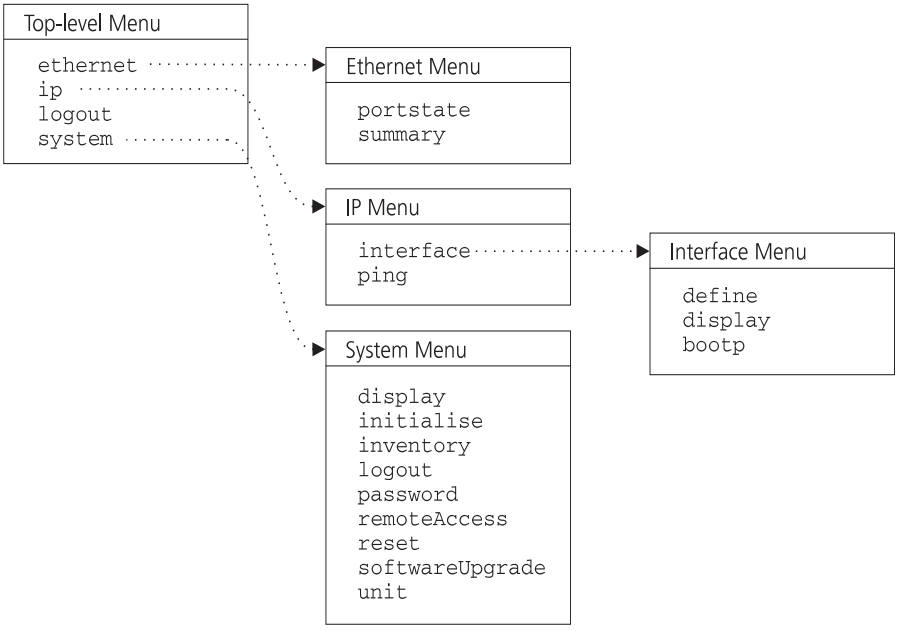


Figure 5-2 Command line interface menu structure

From the top-level menu, you can access three sub-menus.

- **System Menu** — from here, you can view system configuration, configure command line interface parameters, change your password, reset and initialize the Switch.
- **Ethernet Menu** — from here, you can view information for and name Ethernet ports.
- **IP Menu** — from here, you can configure IP parameters and ping other devices.

Navigating the Menus and Entering Commands

You can navigate the menus using any of the following methods:

- **Following the menu hierarchy** — at the `Select menu option:` prompt, type your selected menu name and press [Return]. The screen changes to show the next level of menus available or the list of commands available within your selected menu.

- **Entering multiple menu names on the same line** — if you are familiar with the menu structure you can enter successive menus on the same line at the `Select menu option:` prompt. For example, to display the system configuration, the command line interface would read:

  ```
  Select menu option: system display
  ```

- **Abbreviated commands** — for speedy navigation of the menus, you need only enter enough characters to uniquely identify the menu you want at the prompt. For example, to display system configuration, the command line interface would read:

  ```
  Select menu option: sy di
  ```

As you navigate through the menus, the prompt will change to display your current position in the hierarchy. For example, if you are in the interface sub-menu of the `ip` menu, ready to enter your next option, the prompt reads:

```
Select menu option (ip/interface):
```

Entering Commands

When you reach the menu level containing the specific command you want to enter, you are prompted for a value.

Commands can also be entered at the end of the menu string. If you do this, the task is completed and you are returned to the previous menu. For example to display IP information for a unit, from the top-level menu, enter:

```
Select a menu option: ip interface display
```

Where applicable, default values for commands are shown in parenthesis after the prompt.

Returning to the Previous Menu

You can return to the previous menu, by entering **q** at the prompt.

Returning to the Top-level Menu

You can return to the top-level menu by pressing the Escape key or [Esc].

Obtaining Help

You can get help at any time by entering **?** at the prompt.

A Quick Guide to the Commands

Table 5-1 lists all of the commands available from the command line interface and tells you briefly what each one does.

Table 5-1 Commands available through the command line interface

Command	What does it do?
(system)display	Shows administration information for the Switch
(system)initialise	Configures the unit back to factory defaults
(system)inventory	Lists units in the stack
(system)password	Sets/changes a password
(system)reset	Simulates a power off/on cycle
(system)softwareUpgrade	Allows new management software to be downloaded to the Switch
(system)unit	Changes the focus of the command line interface from one unit in the stack to another
(system)remoteAccess	Enables/disables all forms of remote access to the Switch
(ethernet)portState	Enables/disables an Ethernet port
(ethernet)summary	Displays port statistics
(ip)(interface)bootp	Enables/disables BOOTP
(ip)(interface)define	Sets IP and SLIP parameters
(ip)(interface)display	Displays IP and SLIP parameters
(ip)ping	Sends a PING request to another specified device on the network
logout	Ends a management session (can be used anywhere within the menu structure)

Switch Administration

The following sections detail general management functions that can be carried out from the command line interface.

Selecting a Unit for Configuration

The **`unit`** command allows you to change the focus of the command line interface from one Switch to another in a stack. This allows you to move between Switches in your stack quickly and easily.

1 At the top level menu, enter:

```
system unit
```

The command line interface asks you to enter a unit number.

2 Enter the number of the unit you wish to manage. Currently, you can have up to four Switches in one stack. If you have installed and setup your stack as recommended, unit 1 is the bottom unit in the stack.

To finish the session on this switch and return to the previous, enter the command **`logout`**.

Setting and Changing Passwords

We recommend that setting a password is the first task you carry out on the Switch. Setting a password prevents unauthorized access to the command line interface.

If you forget your password while logged out of the Switch, contact your local support representative for advice.

To set a new password or change an existing password:

1 At the top-level menu of the command line interface, enter:

```
system password
```

2 You are prompted for your old password:

```
old password
```

If this is the first time you are setting a password, press [Return] without entering any text. If you already have a password set up, then enter this password.

3 The prompt changes to show:

```
Enter new password
```

Enter your new password. The prompt asks you to confirm your new password by entering it again.

The command line interface displays a message to tell you that your password has successfully changed.

Configuring the Switch

The following sections detail the parameters you can set through the command line interface.

Enabling and Disabling a Port

By default, all ports on the Switch are enabled.

To enable or disable a port:

1. At the top-level menu, enter:

   `ethernet port`

   The prompt changes to show:

   `Select Ethernet port(s) (1-26|all):`

2. Enter the number of the port you wish to enable or disable.

   The prompt shows you the current port state in square parenthesis, and asks you to enter the new state:

   `Enter new value (enabled, disabled) [enabled]:`

3. Enter **`disabled`** or **`enabled`** as required.

In a stack of units, you can only apply this command to the current unit. If you wish to alter port states on another unit, you will need to connect to it using the **`unit`** *command, see* "Selecting a Unit for Configuration" *on page 5-7.*

Enabling and Disabling BOOTP

The **`bootp`** command allows you to enable or disable BOOTP for the Switch.

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.

By default, BOOTP is disabled.

To enable or disable BOOTP:

1. At the top-level menu, enter:

   `ip interface bootp`

   The prompt asks you to enter the new state:

   `Enter new value (enabled, disabled) [enabled]:`

2. Enter **`disabled`** or **`enabled`** as required.

Setting the IP Configuration

Before you can manage the Switch over the network, you must assign it an IP address. You may also wish to use a subnet mask and enter a default gateway address. This command also allows you to set an address and subnet mask for SLIP.

1. At the top-level menu of the command line interface, enter:

   `ip interface define`

   The prompt changes to show:

   `Enter IP address [0.0.0.0]:`

2. Enter a valid IP address for the Switch. The prompt changes to show:

   `Enter subnet mask [255.255.255.0]:`

   Enter a new subnet mask if you wish.

3. You are prompted for a default gateway address:

   `Enter default gateway [0.0.0.0]:`

   Press [Return] if you do not need a gateway address.

4. You are prompted for a SLIP address:

   `Enter SLIP address [0.0.0.0]:`

   Press [Return] if you do not need a SLIP address.

5. Finally, you are prompted for a SLIP subnet mask:

   `Enter SLIP subnet mask [255.255.255.0]:`

   Press [Return] if you do not need a SLIP subnet mask.

Viewing the Configuration

The following sections detail the ways in which you can view switch and stack configuration information using the command line interface.

Displaying the Port Summary

You can use the summary command to display the state of the ports on a switch and also the number of packets, octets and errors received on each of the ports since the last reset, initialization or power-off/on cycle.

From the top level menu, enter:

```
ethernet summary
```

The command line interface shows a screen of information similar to the following:

```
Port     State        Rx Packets     Rx Octets      Errors
1        Enabled      163542         65439864       4
2        Disabled     0              0              0
3        Enabled      639263         83636219       4
4        Disabled     0              0              0
5
...
26       Enabled      645232         23142514       0
```

The statistics that are displayed are accumulative over the time interval since the last reset, initialization or power-off/on cycle. If the display requires more than 24 lines, press Return to see the remaining data.

Displaying the Switch Configuration

You can use the **display** command to show current configuration information for your switch.

From the top-level menu, enter:

```
system display
```

The command line interface shows a screen of information similar to this example:

```
IBM 8271 Nways Ethernet LAN Switch Model E24
Unit Name: Development
Location: Wiring closet, Floor 2
Contact: Joe Bloggs
Time since reset: 2 days, 3 hours, 10 minutes
Operational Version: 1.00    Boot Version: 1.0
Hardware Version: 1.00
Serial Number: 2103332
```

This information is read-only. If a problem occurs and you need advice from your support representative, you may be asked for some of the information shown on this screen.

Displaying the Stack Configuration

You can use the **`inventory`** command to view the arrangement of switches in the stack.

From the top-level menu, enter:

```
system inventory
```

The screen displays the stack configuration, similar to this example:

```
Select menu option: system inventory
Position    Description          Name             State
1           8271 Model E12       Accounts         Operational
2           8271 Model E24       Development      Operational
3           8271 Model F12       Accounts         Loading
4           8271 Model F24       Accounts         Operational
```

where:

- **`Position`** — the position of the unit in the stack
- **`Description`** — the type of device
- **`Name`** — the name you assigned to this unit
- **`State`** — current operating state of the unit:
  - **`Operational`** — indicates the unit is operating normally
  - **`Loading`** — indicates that there is a process taking place, for example a software upgrade.

Displaying the IP Configuration

At the prompt, enter the command:

```
ip interface display
```

The command line interface displays the IP address, subnet mask, default router address, SLIP address and SLIP subnet mask for this Switch.

Enabling And Disabling Remote Access

As a basic security measure, you can prevent unauthorized remote access to the management software using the **remoteAccess** command.

When remote access is disabled, you will not be able to:

- access the Switch over the network using the web interface
- access the Switch command line interface over the network
- access the Switch using SNMP-based network management software

You will only have access to the web-based interface and the command line interface using a direct connection the Switch's console port.

When set to enabled, you can access the management software using all methods.

To disable remote access:

1. At the top-level menu, enter:

   system remoteAccess

2. Enter **enabled** or **disabled** as required.

Resetting the Switch

The **reset** command allows you to reset the Switch.

What Happens During a Reset?

Resetting the stack simulates a power-off/on cycle for each of the Switches in the stack. You may want to do this if you need to:

- Remove all the Learned entries in the Switch Database (SDB).
- Reset the statistic counters of the stack.

ATTENTION: *Resetting the stack may cause some of the traffic being transmitted over the network to be lost. It also clears all Learned entries from the Switch Database.*

The stack takes about 10 seconds to reset. While the stack is resetting, the Web browser cannot communicate with the stack.

1 At the top-level menu, enter:

```
system reset
```

2 The command line interface asks you to confirm the reset. Enter **y** if you wish to proceed, or **n** if you want to stop the reset.

Initializing the Switch

The **`initialise`** command allows you to initialize the Switch.

What Happens During Initialisation?

Initializing the Switch returns it to default (factory) settings. You should only initialize the Switch if:

- It is a new Switch that you are adding to an existing stack
- The configuration of the Switch no longer suits yout network
- Other efforts to solve a problem have not succeeded.
- You are advised to do so by an IBM technical support representative.

ATTENTION: *Use great care when initializing the stack — it removes all configuration information, including security, resilient links and passwords. However, IP and SLIP information is retained to ensure that you can continue managing the stack.*

Network loops occur if you have set up resilient links. Before initializing the stack, ensure you have disconnected the cabling for all standby links.

The stack takes about 10 seconds to initialize.

To initialize the Switch:

1 At the top-level menu, enter:

```
system initialise
```

2 The command line interface asks you to confirm the initialize. Enter **y** if you wish to proceed. Enter **n** if you do not want to initialize the Switch.

Upgrading Management Software

You can use the **softwareUpgrade** command to download a new software image. The protocol used for downloading software images is TFTP running over UDP/IP and it will work over the network or through the console port using SLIP.

1 From the top-level menu, enter:

```
system softwareUpgrade
```

The prompt changes to show:

```
TFTP Server Address [0.0.0.0]:
```

Enter the IP address of the TFTP server that holds the new file to be downloaded. The file must be stored somewhere where it is accessible to the TFTP load request. Check with your system administrator if you are unsure where to place the image file.

2 The prompt asks you for the name of the file:

```
File name [nwsxx_yy.bin]:
```

Enter the name of your software image file (where xx_yy is the version of agent software).

During the download, the Power/Self Test LED flashes green and the command line interface is locked. When the download is complete, the Switch is reset and the command line interface displays the message `Installation complete`.

Pinging Other Devices

The **ping** command allows you to send out a ping request and test that a device on your network is functioning correctly. You can use ping to ensure that the Switch is installed correctly, and that your network connections are good.

1 At the top-level menu, enter:

```
ip ping
```

The prompt changes to show:

```
Enter destination IP address:
```

2 Enter the IP address of the device you want to ping.

3 It will then display a message similar to the following when the action is complete and the ping is successful:

```
Starting ping, resolution of displayed time is 10 milli-sec
response from 191.1.1.2: 3 router hops. time = 10ms
```

If there is no response from the device being polled, you will see:

```
no answer from 191.1.1.2
```

III ADVANCED NETWORKING FEATURES

6 SPANNING TREE PROTOCOL

This chapter describes the Spanning Tree Protocol and how it is implemented in the Switch. It covers the following topics:

- What is STP?
- How STP Works

STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP more effectively, the Switch will be treated as a 2-port bridge in this chapter.

What is STP?

Using the Spanning Tree Protocol (STP) makes your network more fault tolerant. It 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 6-1 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 is illegal, as it 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 6-2 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 6-3, the STP system reconfigures the network so that traffic from segment 2 flows through Bridge B.

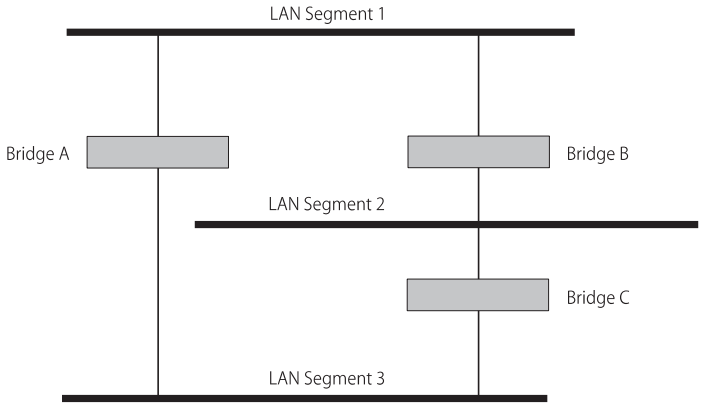


Figure 6-1 Network with an illegal topology

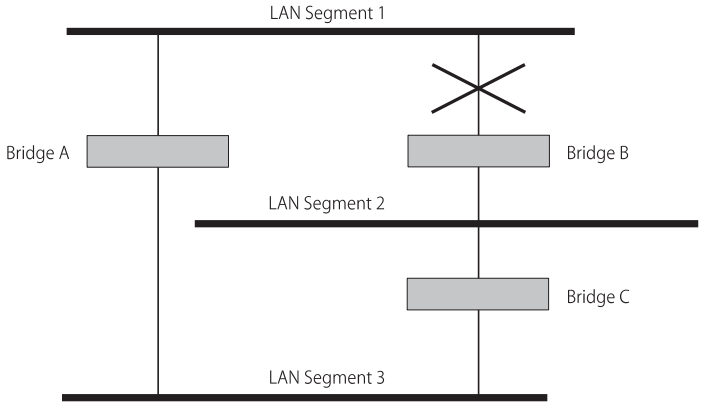


Figure 6-2 Traffic flowing through Bridges C and A

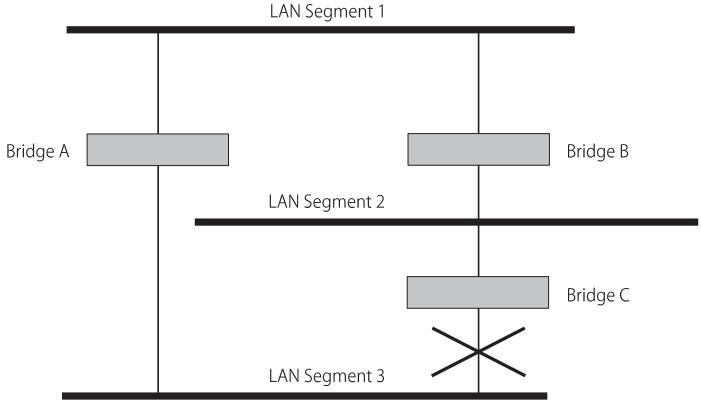


Figure 6-3 Traffic flowing through Bridge B

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:

- 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 6-1 shows the default path costs for the Switch.

Table 6-1 Default path costs

Port Type	Duplex	Cost
10BASE-T	Full	650
	Half	700
100BASE-TX/100BASE-FX	Full	150
	Half	300

- 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 6-4 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 have 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 expires before receiving a Hello BPDU, it assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. It initiates a reconfiguration of the network topology.

You can adjust timers to determine how quickly a network reconfigures and therefore how rapidly the network recovers from a path failure.

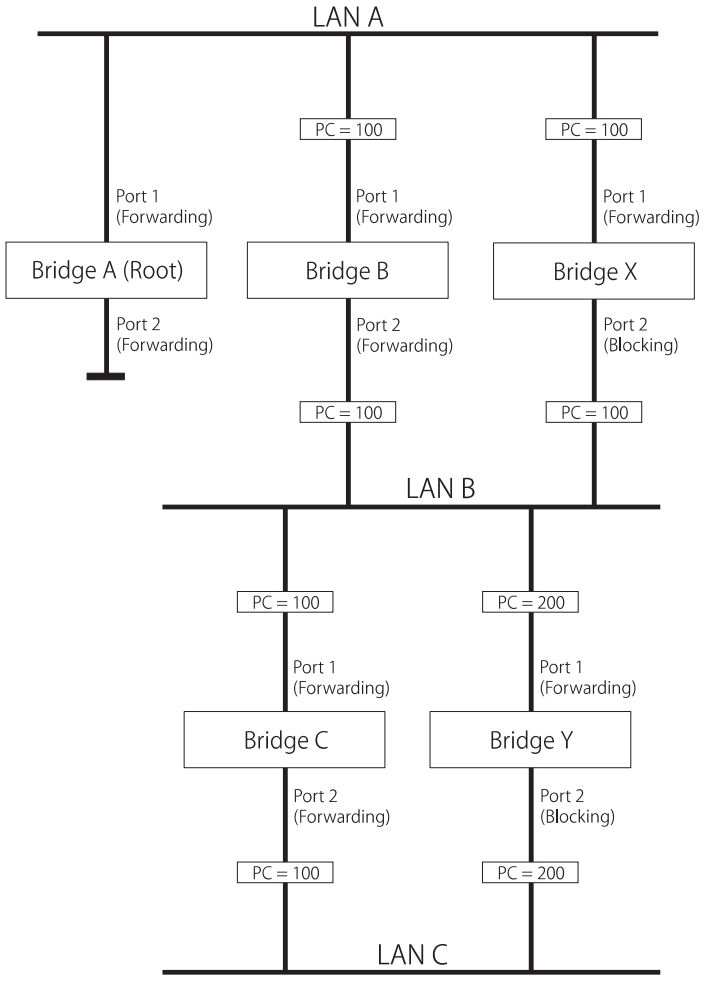


Figure 6-4 Port costs in a network

STP Configurations

Figure 6-5 shows three possible STP configurations using IBM 8271 Nways Switches:

- **Configuration 1 — Redundancy for backbone link**

  In this configuration, a Model E24 and a Model F24 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 Model F24 units are connected such that there are multiple paths between each one. 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.

- **Configuration 3 — Redundancy for cabling error**

  In this configuration, a Model E24 has STP enabled and is accidentally connected to a repeater using two links. STP discovers a duplicate path and disables one of the links, therefore avoiding a loop.

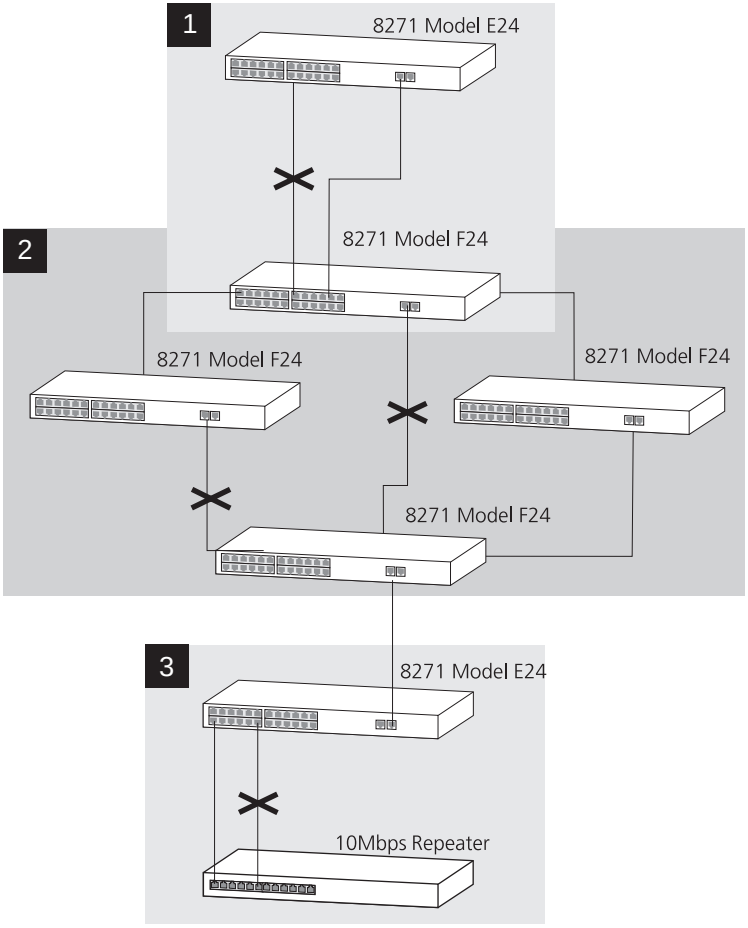


Figure 6-5 STP configurations

7 RMON

This chapter describes the concept of RMON and how it is implemented in the Switch. It covers the following topics:

- What is RMON?
- Benefits of RMON
- RMON and the Switch

What is 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, or using a MIB browser.

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, 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.

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.

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, 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 variable 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. 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. 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 (not supported in this release)

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

Capture (not supported in this release)

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:

- **It improves your efficiency**

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

- **It allows you to manage your network in a more proactive manner**

  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.

- **It reduces the load on the network and the management workstation**

  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.

One other 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.

As an 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 7-1 details the RMON support provided by the Switch.

Table 7-1 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.
History	A new or initialized Switch has two History sessions per port. These sessions provide the data for the web interface unit and port graphs: ■ 30 second intervals, 10 historical samples stored ■ 30 minute intervals, 10 historical samples stored
Alarms	Although up to 200 alarms can be defined for the Switch, a new or initialized Switch has two alarms defined for each port: ■ Broadcast bandwidth used ■ Errors over one minute You can modify these alarms using an RMON management application, but you cannot create or delete them. For more information about the alarms setup on the Switch, see "Alarm Events" on page 7-7 and "Default Alarm Settings" on page 7-8.
Hosts	Although Hosts is supported by the Switch, there are no Hosts sessions defined on a new or initialized Switch.
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	Although Matrix is supported by the Switch, there are no Matrix sessions defined on a new or initialized Switch.
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, see "Default Alarm Settings" on page 7-8 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 200,000 packets a second.
- The greater the number of RMON sessions, the greater the burden on the management resources of the Switch. The forwarding performance of the Switch is not affected, however with a large number of RMON sessions, you may experience slow response times from the web interface.

If you need the filter or capture groups or if you want to use RMON II, the roving analysis port may be used to monitor traffic from any port within the stack.

Alarm Events

You can define up to 200 alarms for the Switch. The events that you can define for each alarm are shown in Table 7-2:

Table 7-2 Alarm Events

Event	Action
No action.	
Notify only.	Send Trap.
Notify and filter port.	Send Trap. Block broadcast and multicast traffic on the port. Recovers with the *unfilter port* event.
Notify and disable port.	Send Trap. Turn port off.
Notify and enable port.	Send trap. Turn port on.
Disable port.	Turn port off.
Enable port.	Turn port on.
Notify and switch resilient port.	Send Trap. If port is the main port of a resilient link pair then move to standby.
Notify and unfilter port.	Send trap. Unblock broadcast and multicast traffic on the port.
Set forwarding mode to *Store and Forward.*	
Set forwarding mode to *Fast Forward.*	

Default Alarm Settings

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

- Broadcast bandwidth used
- Errors

The default values and actions for each of these alarms are given in Table 7-3.

Table 7-3 Values and actions for the default alarms

Statistic	High Threshold	Low Threshold Recovery	Period
Broadcast bandwidth used	Value: 20%	Value: 10%	20 secs
	Action: Notify and filter	Action: Notify and unfilter	
Errors	Value: 20 errors per second	Value: 1 error per second	60 secs
	Action: Set forwarding mode to *Store and Forward*	Action: Set forwarding mode to *Fast Forward*	

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.

IV Problem Solving

8 PROBLEM SOLVING

This chapter lists problems you may see when managing the Switch and gives suggested courses of corrective action to take. It covers the following topics:

- LED Indications
- Using the Command Line Interface
- Using SNMP Network Management
- Using the Serial Web Utility
- Using the Serial Web Utility
- Using the Management Software Upgrade Utility

If you have a problem which is not listed here and you cannot solve it, please contact your local technical support representative or refer to Appendix F.

LED Indications

This section details problems that are indicated by the LEDs on the front of the unit.

Power LED does not light. Check that the power cable is firmly connected to the device and to the supply outlet.

On powering-up, the Power/Self Test LED lights yellow. The unit has failed its Power On Self Test (POST) and you should contact your supplier for advice.

The Module Status LED flashes yellow. The expansion module installed in the Switch is not recognized. You may need to download a version of the Switch's management software that recognizes the Module, 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.
- 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.

The Packet LED for a 10BASE-T port is lit, but the Status LED for that port is off. You have connected a 100 Mbps link which does not support auto-negotiation or has auto-negotiation disabled, to a 10 Mbps port. Do one of the following:

- If possible, enable auto-negotiation on the 100 Mbps link, or set the speed to 10 Mbps if this feature is supported.
- Disconnect the 100 Mbps endstation from this port and connect it to a port that supports 100BASE-TX.

The Packet LED for an Expansion Module is flashing even though there is no external traffic on this link. If you have a Matrix Module installed into your Switch, this is normal operation. Management software in the stack passes packets between units even if there is no other traffic activity.

Using the Web Interface

This section details problems you may see when using the web interface.

The Web browser cannot access the stack. Check that:

- IP information for the stack is correctly configured. See "Setting Up IP Information" on page 4-15 or "Setting the IP Configuration" on page 5-9.
- Remote access to the stack is enabled if you are managing over the network. Access the Switch through its console port and see "Enabling And Disabling Remote Access" on page 5-12.
- The port through which you are accessing the stack has not been disabled. Access the Switch through its console port and see "Displaying the Port Summary" on page 5-10.

The Web browser cannot access the stack over a serial link from a management workstation running Windows 95. You must access the stack using the Serial Web Utility (SLIP Driver) available on the CD-ROM supplied with the Switch. See Appendix B, "Using the Serial Web Utility".

The web interface is not displaying correctly. This could be due to large amounts of traffic on the network. Reload the web page.

The web interface is slow to respond to commands, and "Document contains no data" messages are displayed. Too many users are accessing the web interface at the same time. We recommend that you restrict the number of users with access to three.

A "URL not found" message is displayed when you click the Help or Documentation icon. The web interface cannot access the Help or Documentation files. See "Installing Online Documentation and Help" on page 3-4.

A "URL not found" message is displayed when you click the IBM Library, IBM Contacts or IBM Support icon. Your management station cannot access the World Wide Web. Contact your network administrator.

The Switch graphic shown on the web interface does not refresh automatically. You may need to make one small configuration change to your web browser, so that it always downloads the latest version of a web page from the web interface.

To do this for Netscape Navigator™ version 3.0:

1. Start Netscape Navigator.
2. From the Options menu, select *Network Preferences*.

   The Preferences dialog box appears.
3. Select the Cache tab, and in the Verify Documents field, choose *Every Time*.
4. Click *OK*.

To do this for Microsoft Internet Explorer Version 3.0:

1. Start Microsoft Internet Explorer.
2. From the View menu, select *Options*.

   The Options dialog box appears.
3. Select the Advanced tab, and in the Advanced property sheet choose *Settings*.
4. Check *Every visit to the page*.
5. Click OK.

You forget your password while logged out of the web interface. Ask another user with a Security access level to log in and initialize the stack. The implications of initializing the stack are described in "Initializing all Switches in the Stack" on page 4-32.

If no-one knows a password for a user with a Security access level, contact your supplier.

A management software upgrade has failed, and you can no longer manage the stack using the web interface. Try accessing the command line interface and upgrading the stack again. If this is not possible, separate each Switch from the stack and upgrade using the Management Software Upgrade Utility described in Appendix C.

Using the Command Line Interface

This section details problems you may see when using the command line interface.

The terminal or terminal emulator cannot access the stack. Check that:

- Your terminal is configured correctly with the settings:
  - 8 data bits
  - no parity
  - 1 stop bit

  Auto-configuration only works with line speeds from 1200 to 19,200 baud.
- You have tried pressing [Return] several times.
- Remote access to the stack is enabled if you are trying to access the stack over the network. Access the Switch through the console port, and see "Enabling And Disabling Remote Access" on page 5-12.
- The port through which you are trying to access the stack over the network, has not been disabled. Access the Switch through the console port and see "Viewing Port Status" on page 4-12.

If the login sequence still does not display, reset the stack The implications of resetting the stack are described in "Resetting all Switches in the Stack" on page 4-31 and "Resetting the Switch" on page 5-12.

You forget your password while logged out of the command line interface. Ask another user with a Security access level to log in and initialize the stack. The implications of initializing the stack are described in "Initializing all Switches in the Stack" on page 4-32.

If no-one knows a password for a user with a Security access level, contact your supplier.

A management software upgrade has failed and you can no longer access the command line interface. Try accessing the web interface and upgrading the stack again. If this is not possible, separate each Switch from the stack and upgrade using the Management Software Upgrade Utility described in Appendix C.

Using SNMP Network Management

Traps are not received by the SNMP Network Management Software. Check that the SNMP Network Management Software's IP address and community string are correctly configured.

The management station can no longer access the stack. Check that:

- Remote access to the stack is enabled.
- The port through which you are trying to access the stack has not been disabled.

Try accessing the stack through a different port. If you can now access the stack, a problem with the original port is indicated. Re-examine the connections and cabling.

There may be a network problem preventing you accessing the stack over the network. Try accessing the stack through the console port.

Using the Serial Web Utility

This section details problems you may see when using the Serial Web Utility described in Appendix B.

You are unable to connect to the Switch's web interface. It may be that:

- The Switch is not powered on.
- You are not using a proper null modem cable. Pin-outs are detailed in Appendix D.
- The following settings are different on your Switch and management station:
  - Flow control.
  - Line speed (baud).
- The Switch has automatically configured its communication speed, but you have subsequently changed the speed configured on your

management station (the device only automatically configures the speed the first time it connects).

- You have selected the wrong COM port on your management station.

You can change some of the settings for the management station using the Advanced Configuration Parameters dialog box. To display this, select the Serial Web Setup program item in the Serial Web program group.

Using the Management Software Upgrade Utility

This section describes the problems you may see when using the Management Software Upgrade Utility described in Appendix C.

An error occurred when the utility tried to connect through the PC's serial port. The serial port being used is not the same as the serial port specified in the upgrade command. Retry the command ensuring that you specify a value of '1' or '2' for the serial port.

An error occurred when the utility tried to communicate with the Switch. There could be a number of reasons for this:

- The Switch was not powered on within 5 seconds of pressing [Return].
- The null modem cable is not connected to the Switch's console port.
- The null modem cable is not connected to the PC's serial port, or the serial port being used is not the same as the serial port specified in the upgrade command.
- The Switch was not powered off and on as directed.

Retry the command ensuring that you follow all the steps.

An error occurred when the utility tried to open the management software file for reading. There could be two reasons for this:

- The file specified in the upgrade command does not exist or is in a different directory to the one given. Check the filename and its location.
- You do not have read access for the file. Check the file's properties using Explorer (in Windows 95) or File Manager (in other versions of Windows).

The error message `USAGE: update [-c comport] filename` **is returned.** You have not specified the correct number of parameters for the upgrade command. Retry with the correct parameters.

An error occurred when the utility tried to transfer the file. There could be a number of reasons for this:

- The null modem cable has become disconnected from the hub or the PC during the file transfer. Reconnect the cable and start again.
- Power to the Switch has been disrupted during the file transfer. Check the power connection to the Switch and start again.
- An incorrect file has been specified and transferred to the Switch. Check the filenames and start again.

V Appendices and Index

A 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.

Power Cords

A country-appropriate power cord must be ordered separately for each 8271 Ethernet LAN Switch. The feature codes 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 Code)
U.S.A. and Canada		
Canada Mexico	United States	6952300 (F/C 6851)*
United States (6 ft. Chicago)		6952301 (F/C 6852)*
United States 220 VAC		1838574 (F/C 6853)
Latin America		
Argentina Columbia	Paraguay Uruguay	6952291 (F/C 6862)
Chile		14F0069 (F/C 6858)

(continued)

* 125V/10A

Country		Part Number (Feature Code)
Bahamas	Guyana	1838574 (F/C 6853)
Barbados	Haiti	
Bolivia	Honduras	
Brazil	Jamaica	
Costa Rica	N. Antilles	
Dominican R.	Panama	
El Salvador	Peru	
Equador	Trinidad	
Guatemala	Venezuela	
Europe, Middle East, and Africa		
Albania	Macedonia	13F9979 (F/C 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		
Bahrain	Nigeria	14F0033 (F/C 6856)
Cyprus	Oman	
Ghana	Qatar	
Iraq	Sierra Leone	
Ireland	Somalia	
Jordan	Tanzania	
Kenya	Uganda	
Kuwait	Un.Arab Emir.	
Libya	UK	
Malawi	Yemen	
Malta	Zambia	
Denmark		13F9997 (F/C 6857)

(continued)

Country		Part Number (Feature Code)
Ethiopia	Italy	14F0069 (F/C 6858)
Israel		14F0087 (F/C 6860)
Switzerland	Liechtenstein	14F0051 (F/C 6859)
Namibia Pakistan South Africa	Swaziland Zimbabwe	14F0015 (F/C 6861)
Liberia		1838574 (F/C 6853)
Asia Pacific		
Australia	New Zealand	13F9940 (F/C 6854)
Brunei Hong Kong Macao	Malaysia China Singapore	14F0033 (F/C 6856)
Japan Philippines	Taiwan Thailand	1838574 (F/C 6853)
Bangladesh Myanmar	Sri Lanka	14F0015 (F/C 6861)
Indonesia	Korea (South)	13F9979 (F/C 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 doorbevoegde personen.

Perigo: A instalação e remoção da unidade deve ser feita apenas porpessoal 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 efectuarseúnicamente por personal cualificado.

Fara: Installation och flyttning av enheten måste utföras av utbildad personal.

危险 ：

这些插座设计为只能与推荐的电源一起使用.

Postavljanje i demontažu ovog uređaja mora obaviti stručno osposobljena osoba.

Neodstraňujte desky modulů, pokud je připojeno 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.

Instalacijo 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。

Инсталацијата и отстранувањето на единицата мора да биде извршено само од квалификуван кадар.

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 hovedstikkontakten er montert i næ rheten av enheten, og er tilgjengelig. Du kan bare frakoble enheten ved å trekke ut apparatledningen fra enheten.

Perigo: É essencial que a tomada eléctrica 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 nezbytne, aby síťová zásuvka byla instalována blízko zařízení a byla přístupná. Zařízení můžete odpojit pouze vytažením napájecího kabelu ze zařízení.

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 끊을 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 dôlelžité, aby sieťová zásuvka bola nainštalovaná v blízskosti zariadenia a bola prístupná. Zariadenie môžete vypnúť vytiahnutírr 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.

很重要的是，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。

Битно е, главниот електричен приклучок да е пристапен и да е инсталиран близу до единицата. Вие можете да ја одвоите единицата само со отстранување на делот за спојување од единицата.

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 oequipamento ao qual ela est conectada também funcionar sob a condição SELV.

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

Gervaar: 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 turvastandardin IEC 950 mukaisia SELV (Safety Extra LowVoltage) -suojajännitepiirejä. Yksikkö täyttää standardissa kuvatut ehdot vain, jos laite, johonyksikkö liitetään, käyttää SELV-piirejä.

Pericolo: Questa unità funziona in condizioni di bassissima tensionedi sicurezza (SELV, Safety Extra Low Voltage) secondo l'IEC 950.Tali condizioni sono rispettate solo se anche l'apparecchiaturaa 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 LowVoltage - Tensão Muito Baixa, de Segurança), de acordo com anorma IEC 950. O estabelecido nesta norma só poderá ser mantidose o equipamento ao qual a unidade for ligada também funcionarsob 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, sibien tales condiciones únicamente se mantienen si el equipo alque se conectan es asimismo operacional bajo SELV.

Fara: Den här enheten arbetar under villkoren för kyddsklenspänning (Safety Extra Low Voltage) enligt IEC 950. Dessa villkor uppfylls endast

om utrustning till vilken enheten ansluts också arbetar med skyddsklenspänning.

设备遵守IEC 950 标准,在SELV(Satety 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(Satety 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) áramkörként működik.

この装置はＩＥＣ（国際電気標準会議）９５０のＳＥＬＶ(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ＳＥＬＶ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 jenotka 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。)

Оваа единица работи под SELV услови (сигурносен екстра низок напон) согласно со IEC 950, кои услови се одржуваат само ако опремата на која е приклучена исто така работи под SELV.

DANGER: Ensure that the power supply lead is disconnected before 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 voorda u de afdekplaat van de zekeringen van de IEC-connectors opent of de kap van de eenheid verwijdert.

Gevaar: Kontrollér, at strømforsyningsledningen 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 dekselet til sikringsholderen eller tar av dekselet 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.

Před otevřenim krytu pojistky v IEC konektoru nebo odstranēnim krytu zařízení se ujistěte, že je odpojena napájecí šňůra síťového 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 dugaljból, 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 vtičnici ali odprete pokrov naprave, morate izključiti 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。

Осигурете дека доводот до склопот за снабдување со ел. енергија е одвоен, пред да го отворите капакот од IEC приклучокот со осигурувач(и) или пред отстранувањето на поклопецот од единицата.

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 unc alimentation redondante (RPS) recommandée.

Gefahr: Diese Buchsen sind nur für den Einstaz 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 paraserem utilizados apenas com uma Fonte de Alimentação Redundante recomendada.

Fare! Disse sokler må kun bruges sammen med enanbefalet RPS (Redundant Power Supply).

Gevaar: Deze aansluitingen mogen alleenmet een aanbevolen reservevoeding worden gebruikt.

Vaara: Näihin vastakkeisiin 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 utilizadasapenas com uma Redundant Power Supply (Fonte de Alimentaçãode 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.

Nezebzpečenstvo:
Tieto zásuvky sú určene ıba na použitie s odporučaným 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。

Опасност:

Овие втичници се дизајнирани да се употребуваат само со некој препорачан резервен склоп за снабдување со ел. енергија.

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 unabgeschirmten Datenkabeln mit abgeschirmten oder unabgeschirmten Klinkensteckern verbunden werden.

Gevaar: De RJ45-poorten zijn afgeschermde RJ45-contactdozen voor gegevens. Ze kunnen niet worden gebruikt alstelefoonaansluitingen. Op deze contactdozen mogen alleenRJ45-gegevensstekkers worden aangesloten. Er kunnen zowel afgeschermde als niet-afgeschermde gegevenskabelsmet al dan niet afgeschermde aansluitingen op deze gegevenscontactdozen worden aangesloten.

Perigo: As portas RJ45 são soquetes de dados RJ45 isolados. Não podem ser utilizados como soquetes de telefone. Ligueapenas conectores de dados RJ45 nesses soquetes. Cabos de dados isolados ou não com tomadas isoladas ou não podemser conectados a esses soquetes de dados.

Fare! RJ45-portene er afskærmede RJ45-datasokler. De kan ikke bruges somtelefonstik. 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 afgeschermde als niet-afgeschermde datakabels metafgeschermde of niet-afgeschermde pluggen worden aangesloten.

Vaara: RJ45-portit ovat suojattuja RJ45-datavastakkeita. Niitä ei voikäyttää puhelinvastakkeina. RJ45-datavastakkeeseen saa kytkeävain RJ45-dataliittimiä. Näihin datavastakkeisiin voi kytkeä suojattuja

taisuojaamattomia datakaapeleita, joissa on suojattu tai suojaamatonpistoke.

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 connettoriper dati RJ45. A queste porte possono essere collegati sia cavischermati che non schermati dotati di connettori schermati onon schermati.

Fare: RJ45-portene er skjermede RJ45-datauttak,og kan ikke brukes som telefonuttak. Du må bare kobleRJ45-datakontakter til disse uttakene. Du kan koble enten skjermede eller ikke-skjermede datakabler medskjermede eller ikke-skjermede 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 intermãdio 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 skärmade RJ45 datauttag och kan inte användas som telefonuttag. Anslut endast RJ45 datakontakter till dessauttag. Antingen skärmade eller oskärmade datakablar med skärmade eller oskärmade 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
的数

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 podatak

Nebezpečí:

Porty RJ45 jsou stíněné 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 i nestíněné datové kabely se stíněnými i 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, telefonaljzatnak nem használhatók. Ezekbe a foglalatokba csakRJ45 típusú adat csatlakozókat dugaszoljunk.

Ezekbe a foglalatokba akár árnyékolt, akár árnyékolatlan adat kábelek csatlakoztathatók, árnyékolt vagy árnyékolatlan 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・コネクター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 케이블 둘다 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 telefone zásuvky. Zapoj iba RJ45 - datové konenktory do týchto zásuviek.

Iba tienené a netienené datové káble s tieneých alebo netienených konektorov môžu byť zapojené do týchto datových zásuviek.

Nevarnost !

Priključki RJ45 so oklopljene podatkovne vtičnice. Ne uporabljajte jih kot telefonske vtičnice. Vanje lahko priključujete samo podakovne vtiče tipa RJ45.
Na podatkovne vtičnice lahko priključujete bodisi oklopljene ali neoklopljene kable z oklopljenemi ali neoklopljenemi konektorji.

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。

Опасност:

Комуникациските приклучоци RJ45 се заштитени RJ45 втичници за пренос на податоци. Тие не можат да бидат употребени како телефонски втичници. Приклучувајте само RJ45 конектори за комуникација на овие втичници.

На овие втичници за пренос на податоци, можат да бидат приклучени било заштитени или незаштитени кабли за комуникација со заштитени или незаштитени џекови.

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.

Gevaar:

Het netsnoer moet in overeenstemming zijn met de geldende veiligheidsvoorschriften in het land waar het wordt gebruikt.

Perigo:

O cabo de alimentação deve ser aprovado no país em que será utilizado.

Opasnost:

Energetski kabelski priključak treba imati atest za državu u kojoj se upotrebljava.

危险：

电源线必须具有可用于该国家的认可。

危險：

所使用的電纜線組須經當地政府的認可。

Nebezpečí:

Napájecí šňůra musí být schválena pro zemi použití.

Fare!

Netledningen skal være godkendt i det land, hvor den skal anvendes.

Gevaar:

Het netsnoer moet goedgekeurd zijn voor het land waarin het wordt gebruikt.

VAARA:

Verkkoliitäntäjohdon tulee olla käyttömaassaan hyväksytty.

Achtung:

Die Netzkabel müssen für das Land zugelassen sein, in dem sie verwendet werden.

Κίνδυνος:

Το καλώδιο ρεύματος θα πρέπει να είναι εγκεκριμένο για τη χώρα στην οποία πρόκειται να χρησιμοποιηθεί.

VESZÉLY

Az országban engedélyezett hálózati kábeleket használjon.

PERICOLO:

Il cavo di alimentazione deve essere approvato nel paese in cui verrà utilizzato.

危険：

電源ケーブルおよびコネクターは国の関連法規に適合していることが必要です。

위험:

전원 코드 세트는 반드시 사용될 국가에서 승인한 것이어야 합니다.

Опасност:

Кабелот за електрично напојување мора да биде одобрен во земјата каде ќе се користи.

Fare:

Nettkabelen må være godkjent i det landet den skal brukes i.

Nebezpieczeństwo:

Kabel zasilający musi być dopuszczony do użytku w kraju, w którym będzie użyty.

Perigo:

O cabo de alimentação e peças acessórias têm de estar aprovados no país onde irão ser utilizados.

Atenţie:

Ansamblul cordonului de alimentare trebuie certificat pentru ţara de utilizare.

Опасно:

Следует использовать шнур питания, отвечающий требованиям, предъявляемым к шнурам питания в вашей стране.

Nebezpečenstvo

Napájací kábel musí byť schválený krajinou, v ktorej bude použitý.

Nevarnost:

Komplet priključnih vrvic mora biti odobren za državo, kjer se bo uporabljal.

Peligro:

El juego de cables de alimentación ha de estar autorizado por el país en el que se utilizará.

FARA:

Nätkablarna måste vara godkända i det land där de ska användas.

危險：

所使用的電纜線組須經當地政府的認可。

B USING THE SERIAL WEB UTILITY

Introduction

If you are using a management station running Microsoft Windows 95 and you want to access the web interface through the Switch's console port, you must use the serial web utility (SLIP driver) included on the CD-ROM supplied with the Switch. You can find it in the directory:

```
\Win95\Drivers\Slip\
```

Every time you want to access the web interface, use the serial web utility to set up the connection to the web interface; it launches your web browser and accesses the web interface using SLIP for you.

If you have any problems accessing the Switch's web interface using the serial web utility, see "Using the Serial Web Utility" in Chapter 8.

Installing the Serial Web Utility

The serial web utility can be installed on to a management station that already has other management applications installed on it.

The default directory into which the serial web utility is installed is `C:\Program Files\IBM\IBM Serial Web`
This can be changed during the installation if required.

The installation program is a standard Windows-based installation.
To install the serial web utility:

1. Start Windows 95.

If you already have an existing management application running, ensure that it is closed down.

2. Insert the CD-ROM into your CD-ROM drive.
3. Select *Run* from the *Start* menu.

4 In the *Run* dialog box, type ***drive*:\Win95\Drivers\Slip\SETUP** (where ***drive*** is the letter of your CD-ROM drive) and click *OK*.

The installation program starts and checks your system configuration; enter any information that's requested.

If the setup program cannot find specific files on your management station, it asks you to insert you Windows 95 CD-ROM. If it still cannot find the files, you must obtain them directly from Microsoft. Contact Microsoft for more information.

5 When the installation program has ensured all the relevant files are installed, it asks you to select the COM port. This is the serial port on your management station that you are going to use when connecting to the Switch's console port.

If you click *Advanced*, the Advanced Configuration Parameters dialog box is displayed, showing all of the settings the serial web utility will use when it is run. These default settings are already correct for connection to the Switch so you should not need to change them:

Connection name Allows you to enter a name for the connection.

Modem name Allows you to enter a name for the modem connection.

PC SLIP Address The SLIP address that is to be allocated to the management station. The default address is '192.168.101.2'.

Device URL The URL that the serial web utility uses to access the Switch, which includes the Switch's SLIP address. For example, the default SLIP address for the Switch is '192.168.101.1' so the URL is:
http://192.168.101.1/

Flow Control *None* / *XON/XOFF* / *Hardware RTS/CTS*
Allows you to specify the flow control that the management station is to use.

Data bits, **Stop bits** and **Parity** are all fixed.

Speed *1200* / *2400* / *4800* / *9600* / *19200*
Allows you to specify the baud rate that the management station is to use.

You can change the *PC SLIP Address*, *Device URL*, *Flow Control* and *Speed settings* after the installation is complete.

6 When you have finished, the final installation dialog box is displayed informing you that the serial web utility has been installed on your management station. Click *Finish* to close the dialog box.

7 You are asked if you want to restart Windows 95 so that it can use the new settings you have configured. You must restart Windows 95 before running the serial web utility.

When you return to your Windows 95 desktop, the serial web utility shortcut ('Serial Web Management') created by the installation program is visible. The utility also has its own program group called 'Serial Web' under the default program group specified during the install, which contains:

- Serial Web Management — Launches the serial web utility.
- Serial Web Setup — Displays the Advanced Configuration Parameters dialog box, which allows you to view and change some of the settings the serial web utility uses when it is run.
- License agreement.

Using the Serial Web Utility

Every time you want to access the web interface through a serial link, make your management connection (see "Setting Up Web Interface Management" on page 3-3) and use the serial web utility to set up your connection:

1 Either:

- Double-click on the Serial Web Management shortcut.
- Select the Serial Web Management program item in the Serial Web program group.

2 The serial web utility opens and asks you if you want to use the URL that has been set up. The URL includes the Switch's SLIP address. For example, if the SLIP address for the Switch is '192.168.101.1', the URL is:
`http://192.168.101.1/`

If you want to change the URL, click *URL*. If the URL is correct, click *OK*.

3 The serial web utility attempts to establish a connection.

If successful, the standard Windows 95 Dial-Up Networking dialog box is displayed, showing the various connection details. Your default web browser is then launched with the specified URL.

The connection is complete if the web interface's user and password dialog is displayed. You are now ready to manage the Switch or stack; see Chapter 4.

C MANAGEMENT SOFTWARE UPGRADE UTILITY

The CD-ROM supplied with the Switch includes an agent upgrade utility that can be used for upgrading new versions of management software to the Switch. You can find it in the directory:

`Agent/Update/`

Only use this utility if a previous software upgrade has failed and you are unable to communicate with your Switch using the web interface. At all other times you should use the web interface to upgrade your Switch.

If you have any problems using the management software upgrade utility, refer to "Using the Management Software Upgrade Utility" on page 8-7.

Using the Upgrade Utility

The upgrade utility works from an MS-DOS prompt. It upgrades one Switch at a time.

Upgrading a switch may take up to 5 minutes.

To upgrade the management software for a Switch:

1. Connect your PC's serial (COM) port to the Switch's console port, using a null modem cable.
2. If you are using Microsoft Windows, close it down so that you are at the MS-DOS prompt. Under Windows 95, you can run this utility from an MS-DOS window.
3. At the MS-DOS prompt, change to your CD-ROM drive and go to the directory `Agent/Update`.

4. Enter the upgrade command:

   update nws*xx_yy***.bin**

   where **xx_yy** is the version of management software..

   You can also use the following parameter with the upgrade command to specify the serial (COM) port to use for the PC (COM 1) or (COM 2). The default for this is COM 1:

   -c 1 or **-c 2**

   An example of the upgrade command with this parameter is:

   update -c 1 nws*xx_yy***.bin**

5. Power off the Switch.
6. At your PC, press [Return].
7. Power on the Switch immediately (within 5 seconds).

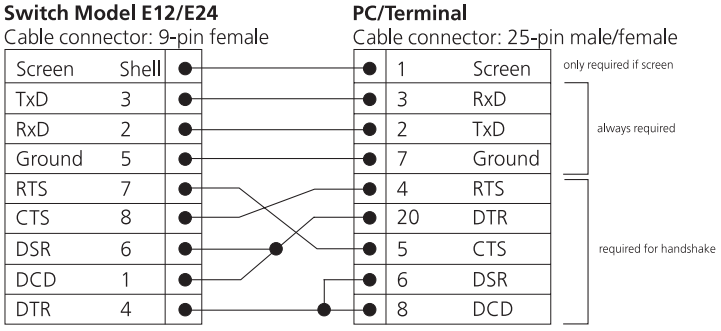
   The utility transfers the management software to the Switch.

8. Repeat all of the steps for any other Switches that need upgrading.

D PIN-OUTS

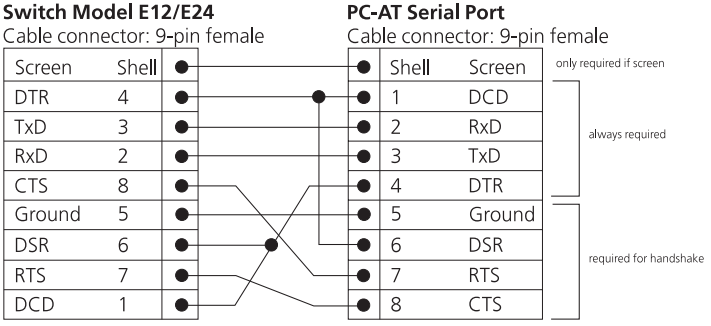
Null Modem Cable

9-pin to RS-232 25-pin



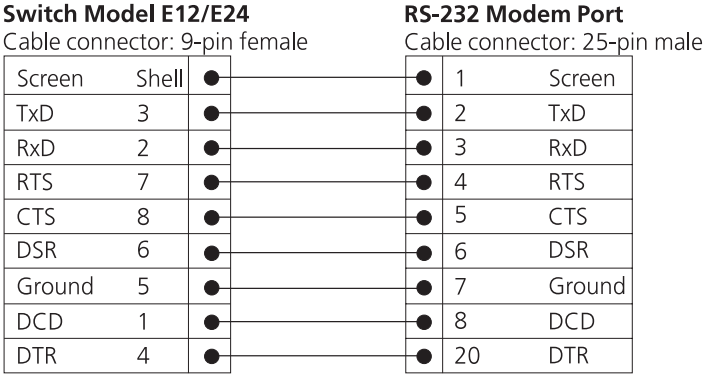
PC-AT Serial Cable

9-pin to 9-pin



Modem Cable

9-pin to RS-232 25-pin



RJ45 Pin Assignments

Pin assignments are identical for 10BASE-T and 100BASE-TX RJ45 connectors

Table D-1 Pin assignments

Pin Number	Signal	Function
Ports configured as MDI		
1	TxData +	Transmit data
2	TxData –	Transmit data
3	RxDta +	Receive Data
4	Not assigned	
5	Not assigned	
6	RxData –	Receive data
7	Not assigned	
8	Not assigned	
Ports configured as MDIX		
1	RxDta +	Receive Data
2	RxData –	Receive Data
3	TxData +	Transmit data
4	Not assigned	
5	Not assigned	
6	TxData –	Transmit data
7	Not assigned	
8	Not assigned	

E 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,
EMC	
Emissions	When STP cables are used: EN55022 Class B*, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class B*, AS/NZS 3548 Class B* * Category 5 shielded cables must be used to ensure compliance with the Class B requirements of this standard. When UTP cables are used: EN55022 Class A*, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class A*, AS/NZS 3548 Class A* * Unshielded cables Category 3 or 5 for 10BASE-T ports or Category 5 for 100BASE-TX ports may be used for Class A compliance. * see Electronic Emission Notices in Appendix G.
Immunity	EN50082-1
Heat Dissipation	117 watts maximum (400 BTU/hour maximum)
Power Supply	
AC Line Frequency	50/60 Hz
Input Voltage Options	90 – 240 VAC
Current Rating	3 amps (maximum)

(continued)

Standards Supported	SNMP	Terminal Emulation
	■ SNMP protocol (RFC 1157)	■ Telnet (RFC 854)
	■ MIB-II (RFC 1213)	**Protocols Used for Administration**
	■ Bridge MIB (RFC 1493)	■ UDP (RFC 768)
	■ Repeater MIB (RFC 1516)	■ IP (RFC 791)
	■ VLAN MIB (RFC 1573)	■ ICMP (RFC 792)
	■ RMON MIB (RFC 1271)	■ TCP (RFC 793)
	■ BOOTP (RFC 951)	■ ARP (RFC 826)
		■ TFTP (RFC 783)

F 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 or FTP.

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/support`

FTP

1. Access the IBM Networking Environment anonymous FTP site:
   `ftp.networking.ibm.com/pub/products/lanprods/switch`
2. Login as *anonymous*.
3. Enter your entire e-mail address as your password.
4. Locate and download the desired files.

Voice Support

IBM Network Hardware support: 1-800-IBM-SERV. Follow the menu prompts for Network Hardware.

For support outside of the United States, please contact your IBM marketing representative or IBM reseller.

G 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

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft 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

International Business Machines Corporation
Armonk, NY 10504

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 Nways Ethernet LAN Switch Models E12 and E24

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 and Canada, call IBM at **1-800-IBM-SERV (426-7378)**. 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, alterations, 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 for Shielded Twisted Pair (STP) Cable

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

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformite aux normes du ministere des Communications du Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

European Community (CE) Mark of Conformity 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.

WARNING: This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Zulassungsbesheinigung laut dem Deutshen Gesetz über die elektromagnetische Veträglichkeit von Geräten (EMVG) vom 30, August 1995 (bzw. der EMC EG Richlinie 89/336)

Dieses Gerät ist berechtigt in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantworlich 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 B.

EN 55022 Klasse B Geräte müssen mit folgendem Warhinweis versehen werden:

"Warnung: dies ist eine Einrichtung der Klasse B. Diese Einrichtung kann im Wohnbereich Funkstorungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maβbnahmen durchzufuhren und dafur 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 verößern.

Anmerkung:

Um die Einhaltung des EMVG sicherzusellen sind die Geräte, wie in den IBM Handüchern angegeben, zu installieren und zu betreiben.

CISPR22 Compliance Statement for Shielded Cable

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 commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Japanese Voluntary Control Council for Interference (VCCI) Statement

This product is a Class B Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Technology Equipment (VCCI). This product is aimed to be used in a domestic environment. When used near a radio or TV receiver, it may become the cause of radio interference. Read the Instructions for correct handling.

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。

Taiwanese Class A Warning Statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

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 전자파적합등록을 받은 기기이오니 X메지 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못 구입하였을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Electronic Emission Notices for Unshielded Twisted Pair (UTP) Cable

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.

IBM is not responsible for any radio or television interference caused 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

Industry Canada Class A Emission Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformite aux normes du ministere des Communications du Canada

Cet appareil numérique de la classe A est conform à la norme NMB-003 du Canada.

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.

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.

Zulassungsbesheinigung laut dem Deutshen Gesetz über die elektromagnetische Veträglichkeit von Geräten (EMVG) vom 30, August 1995 (bzw. der EMC EG Richlinie 89/336)

Dieses Gerät ist berechtigt in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantworlich 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 Funkstorungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maβbnahmen durchzufuhren und dafur 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 veröβern.

Anmerkung:

Um die Einhaltung des EMVG sicherzusellen sind die Geräte, wie in den IBM Handüchern angegeben, zu installieren und zu betreiben.

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

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Technology Equipment (VCCI). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Class A Warning Statement

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策•

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 전자파적합등록을 받은 기기이오니 X매장 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못 구입하였을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

GLOSSARY

10BASE-T The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

100BASE-FX 100 Mbps Ethernet implementation over fiber.

100BASE-TX 100 Mbps 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.

auto-negotiation A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an endstation that also supports auto-negotiation, the link can self-detect its optimum operating setup.

bandwidth Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10 Mbps, the bandwidth of Fast Ethernet is 100 Mbps.

baud 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 10 Mbps using CSMA/CD to run over cabling.

Fast Ethernet 100 Mbps 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.

half duplex Data transmission that can occur in two directions over a single line, but only one direction at a time. Contrast with *full duplex*.

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.

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 Medium Dependent Interface. An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X Medium Dependent Interface Cross-over. An Ethernet port connection where the internal transmit and receive lines are crossed.

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.

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 console port connection.

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.

switch A device that 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.

INDEX

T

U

V

W