



# **8271 Nways Ethernet LAN Switch Models F12 and F24**

---

*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 Model F12 and F24 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.

© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION 1998. ALL RIGHTS RESERVED.

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

# CONTENTS

---

## SAFETY NOTICES

- Safety Notices 1
  - World Trade Safety Information 1

---

## ABOUT THIS GUIDE

- Finding Specific Information in This Guide 7
- Conventions 8
- Related Documentation 9

## I GETTING STARTED WITH THE SWITCH

---

### 1 INTRODUCING THE SWITCH

- About the Switch 1-2
  - Summary of Hardware Features 1-2
  - Summary of Software Features 1-2
- Switch — Front View Detail 1-4
  - 10BASE-T/  
100BASE-TX Ports 1-4
  - LEDs 1-4
- Switch — Rear View Detail 1-6
  - Unit Information Label 1-6
  - Power Socket 1-6
  - Redundant Power System Socket 1-6
  - Console Port 1-6
  - Expansion Module Slot 1-6
  - Matrix Port 1-7
- Switch Software Features Explained 1-7
  - Full Duplex 1-7
  - Flow Control 1-7

Security	1-8
Resilient Links	1-8
Spanning Tree Protocol	1-9
Management	1-9
Default Settings for the Switch	1-10
Network Configuration Examples	1-11
Configuration Rules for Fast Ethernet	1-14
Configuration Rules with Full Duplex	1-15

---

## **2 INSTALLING THE SWITCH**

Installing the Switch	2-2
Following Safety Information	2-2
Choosing a Suitable Site	2-2
Rack-mounting	2-3
Wall-mounting	2-4
Placing Units On Top of Each Other	2-5
Stacking Units	2-5
Stacking Two Units	2-5
Stacking Multiple Units	2-6
The Power-up Sequence	2-8
Connecting a Redundant Power System	2-8
Powering-up the Switch	2-8
Checking for Correct Operation	2-8
Choosing the Correct Cables	2-9
Assigning IP Information	2-10

---

## **3 SETTING UP FOR MANAGEMENT**

Why Manage the Stack?	3-2
Methods of Managing a Stack	3-2
Setting Up Web Interface Management	3-3
Through the Console Port	3-3
Over the Network	3-4
Installing Online Help and Documentation	3-4
Choosing a Suitable Browser	3-5
Setting Up Command Line Interface Management	3-6
Through the Console Port	3-6
Over the Network	3-7

Setting Up SNMP Management	3-7
Managing the Stack Over the Network	3-7
IP Addresses	3-8
Subnets and Using a Subnet Mask	3-8
Logging in as a Default User	3-9

## **II MANAGING THE SWITCH**

---

### **4 WORKING WITH THE WEB INTERFACE**

Accessing the Web Interface	4-2
Exiting the Web Interface	4-3
About The Getting Started Pages	4-4
About the Main Web Interface	4-6
The External Link Icons	4-7
The Management Icons	4-8
The Page Area	4-8
Configuring the Current Switch	4-12
Viewing the Status of the Ports	4-12
Viewing the Administration Details of the Switch	4-14
Setting Up IP Information for the Switch	4-15
Configuring a Port on the Switch	4-16
Configuring the Console Port of the Switch	4-19
Changing the Management Settings for the Stack	4-21
Specifying a Descriptive Name for the Stack	4-21
Changing Your Password	4-22
Specifying the Physical Location of the Stack	4-23
Accessing the Getting Started Pages	4-23
Specifying the Location of the Online Help and Documentation	4-24
Specifying a Contact for the Stack	4-25
Configuring the Stack	4-26
Configuring the Switch Database of the Stack	4-26
Configuring the Operating Modes of the Stack	4-29
Setting Up Resilient Links for the Stack	4-31
Resetting All the Units in the Stack	4-33
Initializing All the Units in the Stack	4-34
Upgrading the Management Software of the Stack	4-35

Viewing Statistics for the Current Switch	4-36
Displaying Unit Statistics	4-36
Displaying Port Statistics	4-37

---

## **5 WORKING WITH THE COMMAND LINE INTERFACE**

Accessing the Interface	5-2
Exiting the Interface	5-3
How Many Users Can Access the Interface?	5-3
About the Interface Menus	5-3
Entering Commands	5-4
Displaying Menus	5-5
Obtaining Help	5-5
A Quick Guide to the Commands	5-6
Viewing and Changing Information About Ports in the Stack	5-7
Enabling and Disabling Ports	5-7
Viewing Port Status Information	5-8
Viewing and Changing IP-related Information	5-8
Specifying IP and SLIP Information	5-9
Displaying IP and SLIP Information	5-10
Specifying Whether the Switch Uses BOOTP	5-10
Pinging Other Devices On Your Network	5-11
Viewing and Changing Information About the Stack	5-12
Moving the Focus of the Command Line Interface	5-12
Displaying Configuration Information About the Current Switch	5-13
Displaying Summary Information About the Switch Units in the Stack	5-14
Changing Your Password	5-15
Enabling and Disabling Remote Access to the Stack	5-16
Resetting the Switch Units in the Stack	5-17
Initializing the Switch Units in the Stack	5-17
Upgrading the Management Software of the Stack	5-18

## **III ADVANCED NETWORKING FEATURES**

---

### **6 SPANNING TREE PROTOCOL**

What is STP?	6-2
--------------	-----

How STP Works	6-4
STP Initialization	6-4
STP Stabilization	6-4
STP Reconfiguration	6-5
An Example	6-5
STP Configurations	6-6
Enabling STP on a Stack	6-8

---

## **7 RMON**

What is RMON?	7-2
The RMON Groups	7-2
Benefits of RMON	7-4
RMON and the Stack	7-5
RMON Features of the Stack	7-6
About Alarm Actions	7-7
About Default Alarm Settings	7-8
About the Audit Log	7-8

## **IV PROBLEM SOLVING**

---

### **8 PROBLEM SOLVING**

Solving Problems Indicated by LEDs	8-2
Solving Problems That Occur When Using the Web Interface	8-2
Solving Problems That Occur When Using the Command Line Interface	8-5
Solving Problems That Occur When Using an SNMP Network Manager	8-6
Solving Problems With the Serial Web Utility	8-7
Solving Problems With the Management Software Upgrade Utility	8-8
Solving Other Problems	8-9

## **V APPENDICES AND INDEX**

---

### **A SAFETY INFORMATION**

- Power Cords A-1
  - Important Safety Information A-3
- 

### **B USING THE SERIAL WEB UTILITY**

- Introduction B-1
  - Installing the Serial Web Utility B-1
  - Using the Serial Web Utility B-3
- 

### **C MANAGEMENT SOFTWARE UPGRADE UTILITY**

- Using the Upgrade Utility C-1
- 

### **D PIN-OUTS**

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

### **E SWITCH TECHNICAL SPECIFICATIONS**

---

### **F TECHNICAL SUPPORT AND SERVICE**

- Electronic Support F-1
    - WWW F-1
    - FTP F-1
  - Voice Support F-1
- 

### **G NOTICES, TRADEMARKS, AND WARRANTIES**

- Trademarks G-1
- Statement of Limited Warranty G-2
  - Production Status G-2
  - The IBM Warranty for Machines G-2



Warranty Service	G-3
Extent of Warranty	G-4
Limitation of Liability	G-4
Electronic Emission Notices for Shielded Twisted Pair (STP) Cable	G-5
Federal Communications Commission (FCC) Statement	G-5
Canadian Department of Communications (DOC) Compliance Statement	G-6
Avis de conformité aux normes du ministère des Communications du Canada	G-6
European Community (CE) Mark of Conformity Statement for Shielded Cable	G-6
CISPR22 Compliance Statement for Shielded Cable	G-7
Japanese Voluntary Control Council for Interference (VCCI) Statement	G-7
Taiwanese Class A Warning Statement	G-8
Korean Communications Statement	G-8
Electronic Emission Notices for Unshielded Twisted Pair (UTP) Cable	G-8
Federal Communications Commission (FCC) Statement	G-8
Canadian Department of Communications (DOC) Compliance Statement	G-9
Avis de conformité aux normes du ministère des Communications du Canada	G-9
European Community (CE) Mark of Conformity Statement for Unshielded Cable	G-9
Japanese Voluntary Control Council for Interference (VCCI) Statement Class A for Unshielded Cables	G-10
Taiwanese Class A Warning Statement	G-11
Korean Communications Statement	G-11

---

## **GLOSSARY**

---

## **INDEX**



# 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 nor extremely hazardous.

## World Trade Safety Information

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



**DANGER:** Before you begin to install this product, read the safety information in *Caution: Safety Information – Read This First*, SD21-0030. This booklet describes safe procedures for cabling and plugging in electrical equipment.



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



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



**Fare:** Før du installerer dette produkt, skal du læse sikkerhedsforskrifterne i *NB: Sikkerhedsforskrifter – Læs dette først*,

SD21-0030. Vejledningerne beskriver den fremgangsmåde, du skal bruge ved tilslutning af kabler 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 elektrische apparatuur op een veilige manier moet bekabelen en aansluiten.



**Gevarr:** Voordat u begint met het installeren van dit produkt, dient u eerst de veiligheidsrichtlijnen te lezen die zijn vermeld in de publikatie *Caution: Safety Information – Read This First*, SD21-0030. In dit boekje vindt u veilige procedures voor het aansluiten van elektrische apparatuur.



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



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



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



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



**Perigo:** Antes de iniciar a instalação deste produto, leia as informações de segurança *Cuidado: Informações de Segurança – Leia Primeiro*, SD21-0030. Este documento descreve como efectuar, de um modo seguro, as ligações eléctricas dos equipamentos.



**Peligro:** Antes de empezar a instalar este producto, lea la información de seguridad en *Atención: Información de Seguridad – Lea Esto Primero*,

SD21-0030. Este documento describe los procedimientos de seguridad para cablear y enchufar equipos eléctricos.



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



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



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



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



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



危險：安裝本產品之前，請先閱讀  
"Caution: Safety Information--Read  
This First" SD21-0030 手冊中所提  
供的安全注意事項。這本手冊將會說明  
使用電器設備的纜線及電源的安全程序。



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



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



**ОСТОРОЖНО:** Прежде чем устанавливать этот продукт, прочтите Инструкцию по технике безопасности в документе "Внимание: Инструкция по технике безопасности -- Прочсть в первую очередь", SD 21-0030. В этой брошюре описаны безопасные способы каблирования и подключения электрического оборудования.



Nebezpečenstvo: Pred inštaláciou výrobku si prečítajte bezpečnostné predpisy v  
Výstraha: Bezpečnostné predpisy - Prečítaj ako prvé,  
SD21 0030. V tejto brožúrke sú opísané bezpečnostné 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 što 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 oriključivanie kabela i priključivanie na električno nabaianie.



### 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 Switch Models F12 and F24.

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 F12 and F24 models:*

- 02L0878 — 12 10BASE-T/100BASE-TX ports
- 02L0879 — 24 10BASE-T/100BASE-TX 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.

<b>If you are looking for...</b>	<b>Turn to...</b>
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)

<b>If you are looking for...</b>	<b>Turn to...</b>
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	Appendix
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

<b>Icon</b>	<b>Notice Type</b>	<b>Alerts you to...</b>
	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

<b>Convention</b>	<b>Description</b>
Screen displays	Text with this typeface represents information as it appears on the screen.
<b>Commands</b>	When you see text with this typeface you must enter the command exactly as it shown and then press the Return or Enter key. For example: <p style="margin-left: 40px;">To change your password, enter:</p> <p style="margin-left: 80px;"><b>system password</b></p>

(continued)

**Table 2** Text Conventions (continued)

Convention	Description
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type".
[Key] names	Key names appear in text in one of two ways: <ul style="list-style-type: none"> <li>■ Referred to by their labels, such as "the Return key" or "the Escape key"</li> <li>■ Written with brackets, such as [Return] or [Esc].</li> </ul>
<i>Menu commands</i> and <i>buttons</i>	Menu commands or button names appear in italics. For example:  From the <i>Help</i> menu, select <i>Contents</i> .
Words in <i>italics</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text.
Words in <b>bold</b>	Bold text denotes key features.

---

## Related Documentation

The Switch document set includes:

- *IBM 8271 Nways Ethernet Switch Models F12 and F24 Quick Reference Guide*, Part Number 02L0890
- *IBM 8271 Nways Ethernet Switch Models F12 and F24 Quick Installation Guide*, Part Number 02L0889
- *IBM 8271 Nways Ethernet Switch Models F12 and F24 Release Notes*, Part Number 02L0891

Other publications you may find useful:

- Documentation accompanying the *IBM 8271 Nways Ethernet Switch Models E12 and E24*.
- Documentation accompanying *IBM 8271 Nways Ethernet Switch Expansion Modules*.
- Documentation accompanying the Advanced Redundant Power System.





# GETTING STARTED WITH THE SWITCH

- Chapter 1 Introducing the Switch
- Chapter 2 Installing the Switch
- Chapter 3 Setting Up for Management



# 1

## INTRODUCING THE SWITCH

This chapter contains introductory information about the IBM 8271 Nways Ethernet LAN Switch Model F12 and F24 and how it can be used in your network. It covers the following topics:

- About the Switch
- Switch — Front View Detail
- Switch — Rear View Detail
- Switch Software Features Explained
- Default Settings for the Switch
- Network Configuration Examples
- Configuration Rules for Fast Ethernet
- Configuration Rules with Full Duplex

---

**About the Switch**

The 8271 Models F12 and F24 aggregate your existing 10 Mbps devices, connects high-performance workgroups with a 100 Mbps backbone or server connection, and connects power users to dedicated 100 Mbps ports — all in one switch.

**Summary of Hardware Features**

The Switch has the following hardware features:

- 12 or 24 Fast Ethernet auto-negotiating 10BASE-T/100BASE-TX ports
- Matrix port for interconnecting F12/F24 or E12/E24 units in a single stack:
  - Connect two units back-to-back using a single Matrix Cable
  - Connect up to four units using Matrix Cables linked to a Matrix Module
- Slot for an Expansion Module or Matrix Module
- Connects to Redundant Power System/Uninterruptible Power System
- 19-inch rack or stand-alone mounting

**Summary of Software Features**

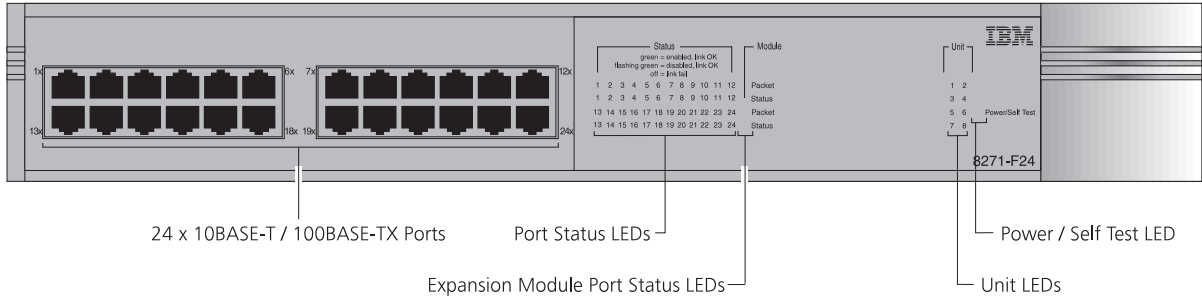
The Switch has the following software features:

- Support for up to 12,000 endstations (one MAC address per endstation)
- Stack management for up to four units
- Store-and-Forward forwarding mode
- Full duplex on all ports
- Flow control on all ports:
  - IEEE 802.3x on full duplex links
  - Intelligent Flow Management on half duplex links
- Security
- Resilient Links
- Spanning Tree Protocol (STP)
- Multicast filtering
- Future support for VLANs, automatic configuration of multicast filters (GARP and IGMP snooping) and Fast IP



- A choice of management methods:
  - Web-based management
  - Command line interface management
  - SNMP management

## Switch — Front View Detail



**Figure 1-1** Switch — front view

### 10BASE-T/ 100BASE-TX Ports

The Switch has 12 or 24 auto-negotiating 10BASE-T/100BASE-TX ports configured as MDIX (cross-over). These ports can be set to 10BASE-T half duplex, 10BASE-T full duplex, 100BASE-TX half duplex, 100BASE-TX full duplex, or they can automatically detect the speed and Duplex Mode of a link and provide the appropriate connection. The maximum segment length is 100m (328ft) over category 5 twisted pair cable.



*As these ports are configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only. See “Choosing the Correct Cables” on page 2-9 for more information.*

### LEDs

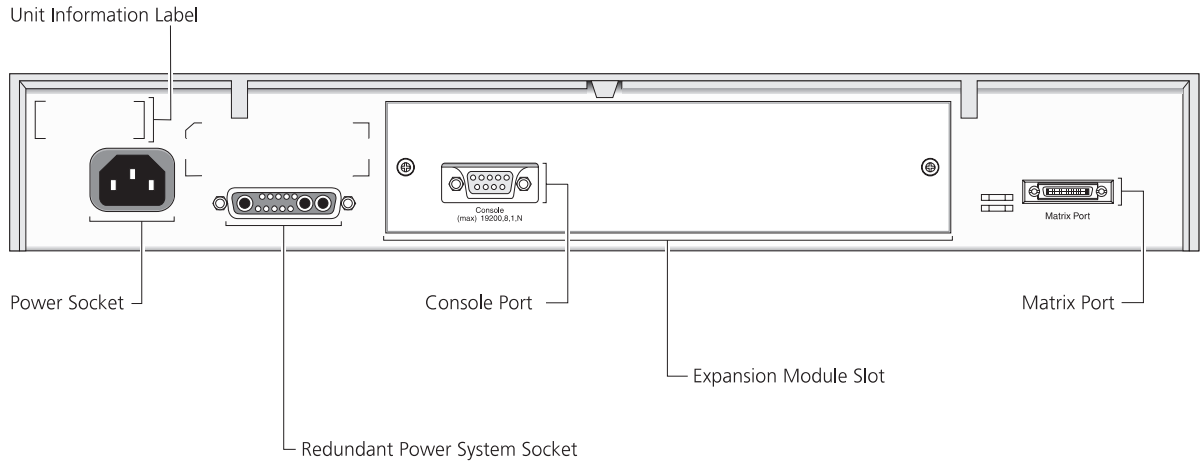
Table 1-1 lists the LEDs visible on the front of the Switch, and their states according to color. For information on using the LEDs for problem solving, see “Solving Problems Indicated by LEDs” on page 8-2.

**Table 1-1** LED behavior

LED	Color	Indicates
<b>Port Status LEDs*</b>		
Packet	Yellow	Packets are being transmitted/received on the port.
	Off	No packets are being transmitted/received on the port.
Status	Green	A link is present, and the port is enabled.
	Green flashing	A link is present, but the port is disabled.
	Off	No link is present.
<b>Expansion Module Port Status LEDs</b>		
Packet	Yellow	Packets are being transmitted/received on the Expansion Module or Matrix Module port(s).
	Off	No packets are being transmitted/received on the Expansion Module or Matrix Module port(s).
Status	Yellow	A valid Expansion Module or Matrix Module is installed in the Switch.
	Yellow flashing	An unrecognized Expansion Module or Matrix Module is installed in the Switch.
	Off	No Expansion Module or Matrix Module is installed in the Switch.
<b>Unit LEDs</b>		
1 – 8	Green	Indicates the position of the Switch in the stack and that a link is present. Note that although there are eight LEDs, only four Switch units can be stacked at present.
1 – 8	Off	The Switch is stand-alone.
<b>Power/Self Test LED</b>		
	Green	The Switch is powered on.
	Green flashing	The Switch is either downloading software or is initializing (which includes running a Power On Self Test).
	Yellow	The Switch has failed its Power On Self Test.
	Off	The Switch is not receiving power.

\* If your Switch has 24 10BASE-T/100BASE-TX ports, these ports are numbered 1 to 24. If your Switch has 12 10BASE-T/100BASE-TX ports, these ports are numbered 1 to 12. 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 its power setting to any supply voltage in the range 90–240V A.C.

### Redundant Power System Socket

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

### Console Port

The console port allows you to connect a terminal and perform remote or local out-of-band management. The console port uses standard null modem cable and is set to auto-baud, 8 data bits, no parity and 1 stop bit.

### Expansion Module Slot

You can use this slot to 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 Switch 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.*

### Matrix Port

The matrix port allows you to:

- Stack the Switch with another Model F12/F24 or Model E12/E24 unit using a single Matrix Cable
- Stack the Switch with up to three other Model F12/F24 or Model E12/E24 units, if one of the units has a Matrix Module installed

## Switch Software Features Explained

The following sections explain in more detail the software features listed in “Summary of Software Features” on page 1-2.



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

### Full Duplex

Full duplex support is provided for all ports in the stack, including 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 supports 100BASE-FX cable runs of up to 2km (6562ft).

Full duplex must always be enabled at both ends of a link. If the link uses an auto-negotiating twisted pair connection, this is done automatically. If the link uses a fiber connection or a connection that is not auto-negotiating, both ends must be set to full duplex mode manually.



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



*For more information about enabling full duplex on a port, see “Configuring a Port on the Switch” on page 4-16.*

### Flow Control

Flow control is a congestion control mechanism that is provided for all ports in the stack, including Expansion Module ports. Congestion is caused by one or more devices sending traffic to an already congested port on the Switch. Flow control prevents packet loss and inhibits the devices from generating more packets until the period of congestion ends.

In the Model F12 and F24, Flow Control is implemented in two ways:

- IEEE 802.3x standard for ports operating in full duplex.
- Intelligent Flow Management (IFM), a method of flow control for ports operating in half duplex. IFM should only be enabled if the port is connected to another switch, or an endstation. If the port is connected to a repeated segment with local traffic, IFM should be disabled.



*For information about enabling flow control on a port, see “Configuring a Port on the Switch” on page 4-16.*

### Security

Each port in the stack can use a Security feature that guards 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 port learns a single MAC (Ethernet) address; once this is learned, the port is disabled if a different address is seen on the port. Until Security is disabled, no other address can be learned.



*For more information about enabling Security on a port, see “Configuring a Port on the Switch” on page 4-16.*

### Resilient Links

The Resilient Link feature of the stack enables you to protect critical links and prevent network downtime should those links fail. Setting up resilience ensures that if a main communication link fails, 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 a simple method of creating redundancy that provides you with an instant reaction to link failure. Resilient Links are quick 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.



**ATTENTION:** *Resilient links and Spanning Tree cannot be set up on the same stack.*



*For more information about Resilient Links, see “Setting Up Resilient Links for the Stack” on page 4-31.*

## Spanning Tree Protocol

The stack 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 designed to set up automatic redundancy and protection against network loops across the whole of your network.



**ATTENTION:** *Spanning Tree and resilient links cannot be set up on the same stack.*



*For information about STP, see “Spanning Tree Protocol” on page 6-1. For information about enabling STP, see “Configuring the Operating Modes of the Stack” on page 4-29.*

## Management

Each Switch unit in the stack contains management agent software that allows you to manage the stack using three methods:

- *Web interface management* — Each Switch unit in the stack has an internal set of web pages that allow you to manage the stack using any Java<sup>®</sup>-enabled Web browser. You can access the web interface using:
  - A management workstation connected over the network
  - A management workstation connected to the console port of a Switch unit in the stack, running the Serial Line Internet Protocol (SLIP)
- *Command line interface management* — Each Switch unit in the stack has a command line interface that allows you to perform limited 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 connected to the console port of a Switch unit in the stack
- *SNMP management* — You can manage the stack using any Network Manager running the Simple Network Management Protocol (SNMP).



For information about management of the stack, see “Setting Up for Management” on page 3-1.

## Default Settings for the Switch

Table 1-2 shows the default settings of the Switch. If you initialize the Switch, it is returned to these defaults.

**Table 1-2** Default settings

<b>Port Status</b>	Enabled
<b>Port Speed</b>	10BASE-T/100BASE-TX ports are auto-negotiated
<b>Duplex Mode</b>	10BASE-T/100BASE-TX ports are auto-negotiated
<b>Flow Control</b>	Enabled in half duplex (IFM), auto-negotiated in full duplex
<b>Spanning Tree (STP)</b>	Disabled
<b>System Alarm (broadcast bandwidth used)</b>	Enabled <ul style="list-style-type: none"> <li>■ High threshold: 20% — Notify and filter</li> <li>■ Low threshold: 10% — Notify and unfilter</li> </ul>
<b>System Alarm (errors over 1 min)</b>	Enabled <ul style="list-style-type: none"> <li>■ High threshold: 20 errors per second — Notify</li> <li>■ Low threshold: 1 error per second — No action</li> </ul>

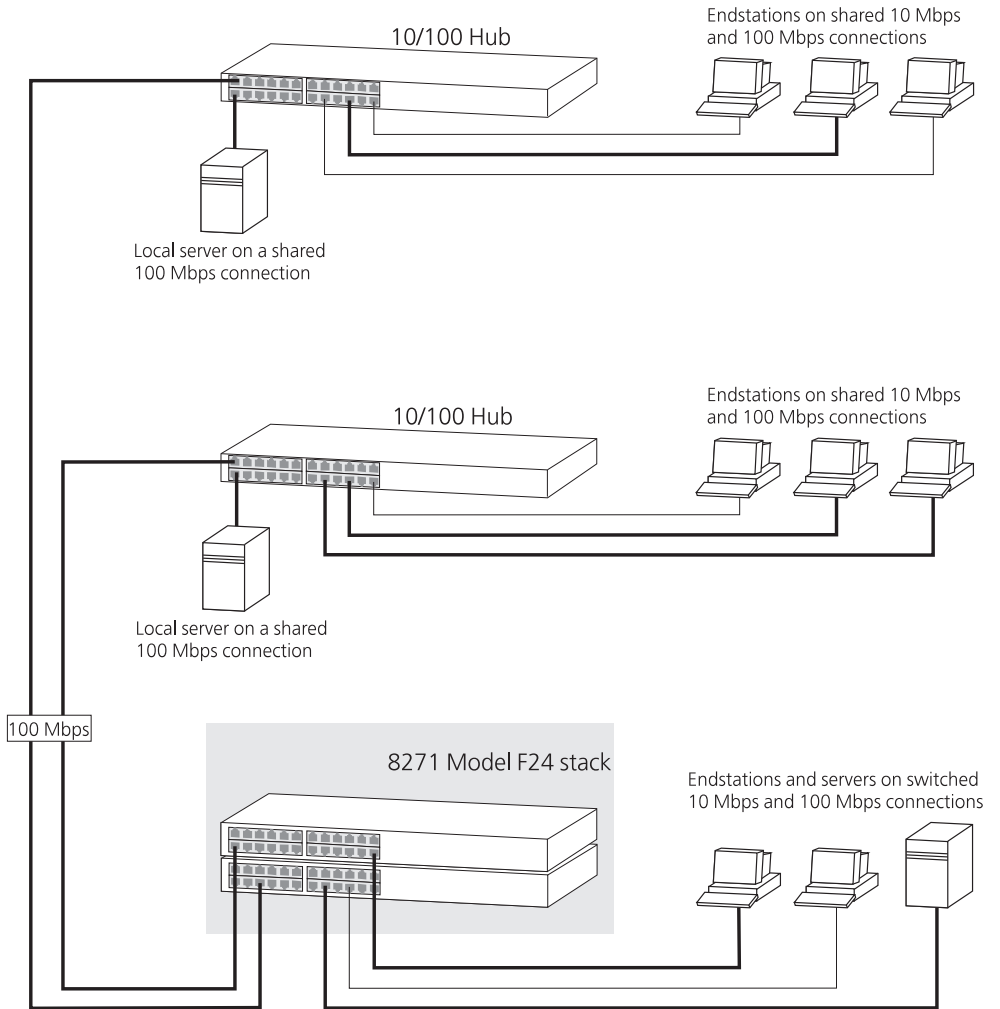


**Network Configuration Examples**

The following illustrations show some examples of how the Switch can be used in your network.

**The Model F24 as a Segmentation Switch**

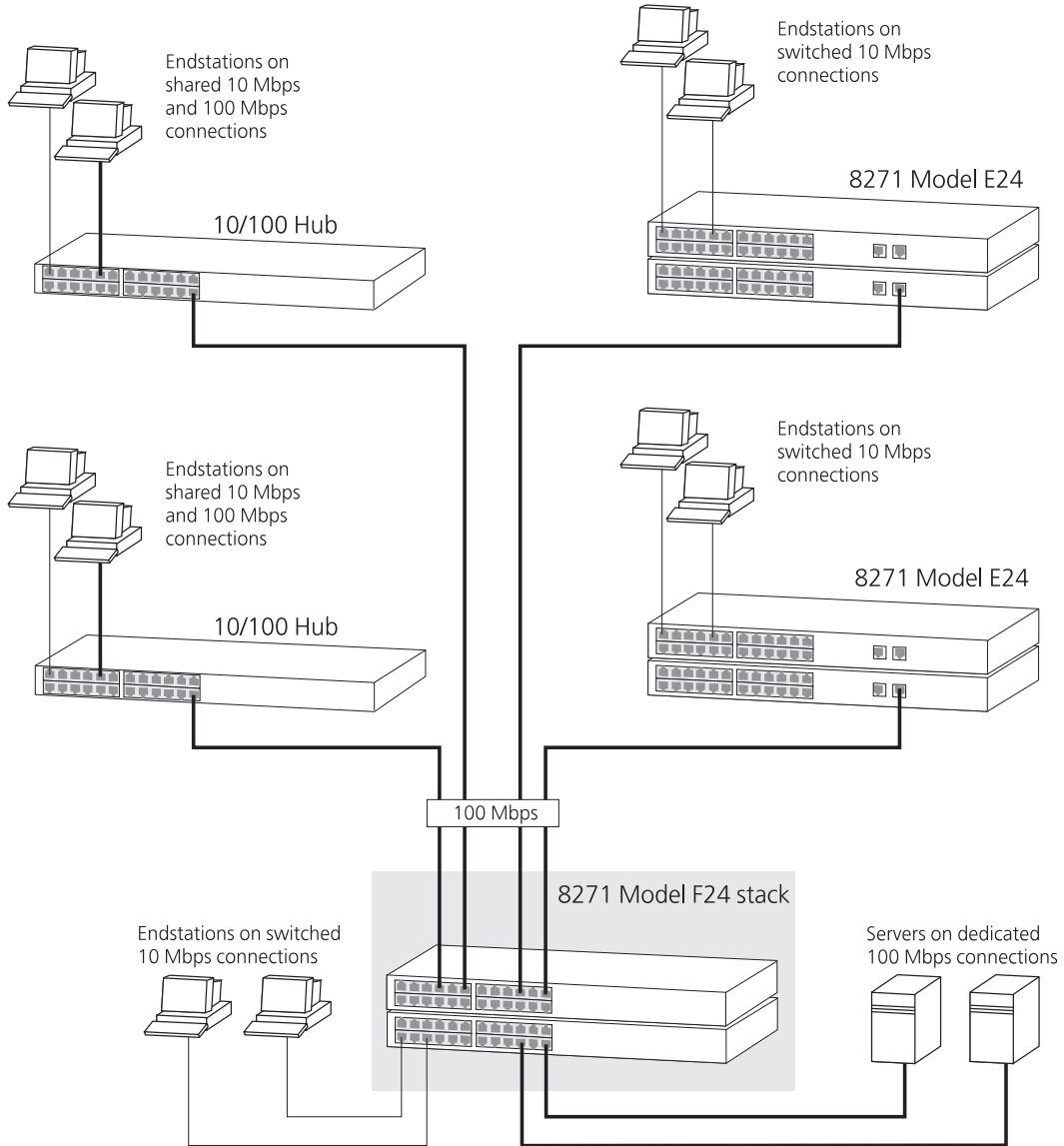
The example in Figure 1-3 shows how the Switch can segment a network of shared 10 Mbps and 100 Mbps connections. There is a 10/100 shared segment on each floor, and these segments are connected to the Switch which is positioned in the basement.



**Figure 1-3** Using the Switch to segment your network

### The Model F24 as a Collapsed Backbone Switch

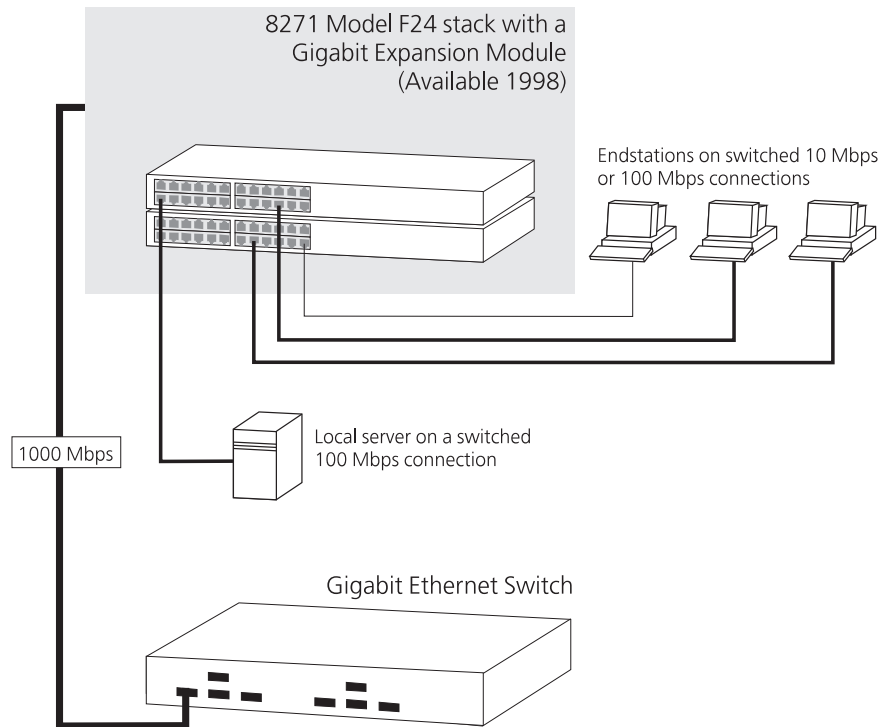
The example in Figure 1-4 shows how the Switch can act as a backbone for both shared and switched network segments.



**Figure 1-4** Using the Switch as a collapsed backbone

### The Model F24 as a Desktop Switch

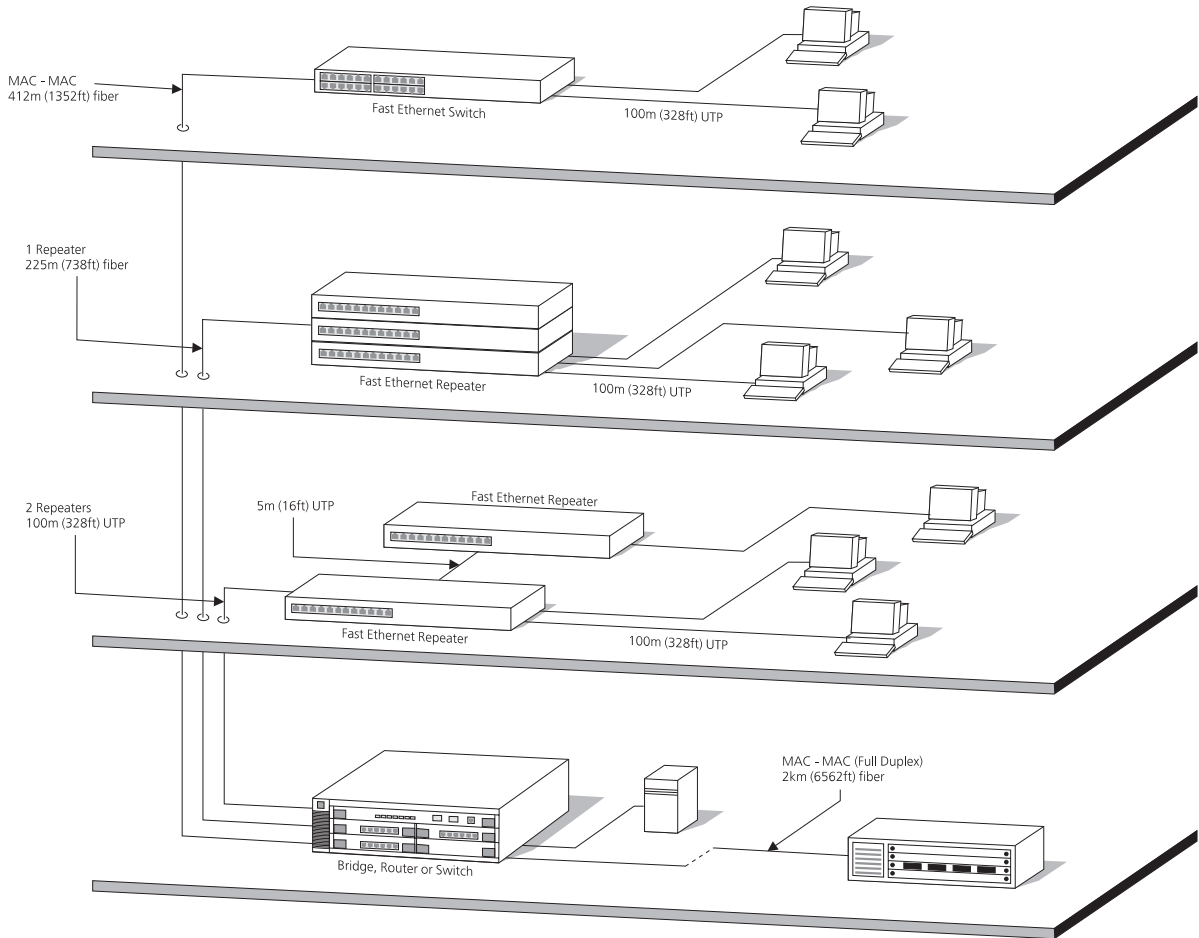
The example in Figure 1-5 shows how the Switch can be used for a group of heavy-traffic users that require dedicated 10 Mbps or 100 Mbps connections to the desktop. The Model F24 has a Gigabit Ethernet Expansion Module that allows it to provide a Gigabit link to a Gigabit Ethernet Switch in the basement.



**Figure 1-5** Using the Switch in a desktop environment

## Configuration Rules for Fast Ethernet

The topology rules for 100 Mbps Fast Ethernet 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 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 link from a repeater to a router or switch, plus 100m (328ft) UTP run from a repeater out to the endstations.

---

## **Configuration Rules with Full Duplex**

The Switch provides full duplex support for all its ports, including Expansion Module ports. 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 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
- Assigning IP Information

---

## 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 Switch 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 Switch, ensure that:

- You are able to meet the configuration rules detailed in “Configuration Rules for Fast Ethernet” on page 1-14 and “Configuration Rules with Full Duplex” on page 1-15.
- The Switch 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 Switch.
- Air-flow is not restricted around the Switch or through the vents in the side of the Switch. We recommend that you provide a minimum of 25mm (1in.) clearance.
- No more than four Switch units are placed on top of one another, if the units are free standing.

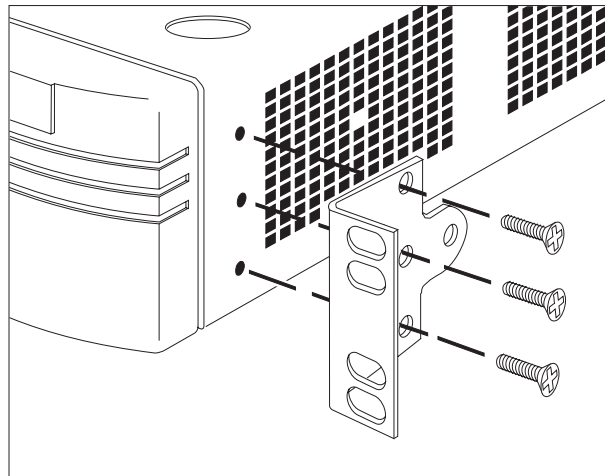


**Rack-mounting** The Switch is 1.5U high and fits in most standard 19-inch racks.



**ATTENTION:** *Disconnect all cables from the Switch before continuing. Remove all self adhesive pads from the underside of the Switch if they have been fitted.*

- 1 Place the Switch 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 Switch, as shown in Figure 2-1.



**Figure 2-1** Fitting a bracket for rack mounting

- 3 Insert the three 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 invalidates your warranty.*

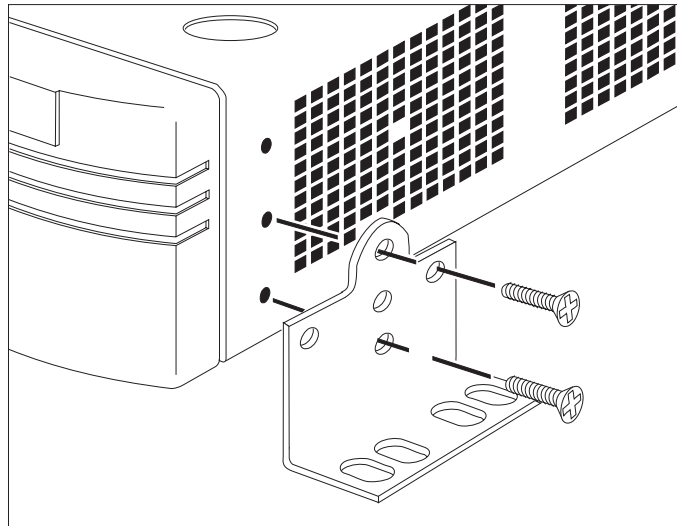
- 4 Repeat steps 2 and 3 for the other side of the Switch.
- 5 Insert the Switch into the 19-inch rack and secure with suitable screws (not provided). Ensure that the ventilation holes face sideways and the front panel faces upwards.
- 6 Connect network cabling.

**Wall-mounting** A single Switch can be wall-mounted.



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

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



**Figure 2-2** Fitting a bracket for wall-mounting

- 3 Insert the two screws and tighten with a suitable screwdriver.
- 4 Repeat steps 2 and 3 for the other side of the Switch.
- 5 Ensure that the wall you are using 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.
- 6 Mount the Switch as follows:
  - a Position the base of the Switch against the wall (or plywood) ensuring that the ventilation holes face sideways and the front panel faces upwards. Mark the position of the screw holes in both wall brackets on the wall. Drill the four holes.

- b Using suitable fixings and screws (not provided), attach the Switch securely to the wall or plywood.
- c Connect network cabling.

### **Placing Units On Top of Each Other**

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

If you are placing Switch units one on top of the other, you must use the self-adhesive rubber pads supplied. Apply the pads to the underside of each Switch, sticking one in the marked area at each corner. Place the Switch 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**

Switch units can be stacked together and then treated as a single manageable unit with one IP address.

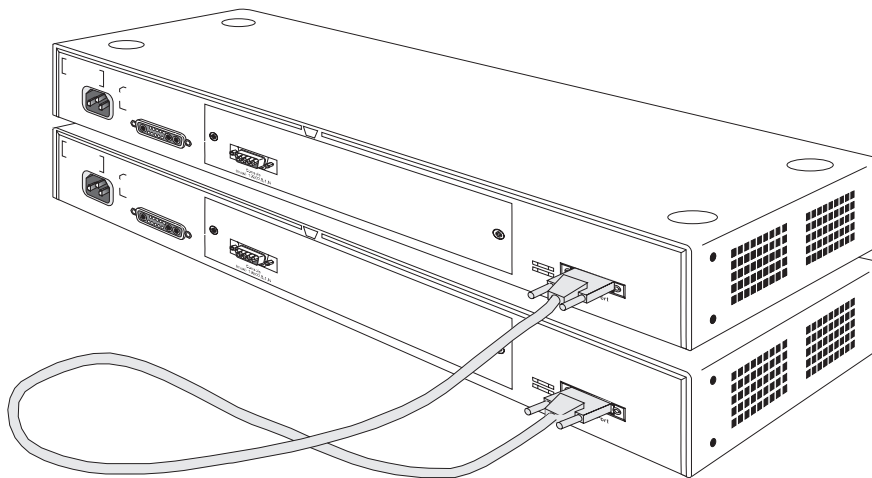
You can stack Switch units together in two ways:

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

### **Stacking Two Units**

To stack two Switch units, you only need one Matrix Cable. The Switch units can be rack-mounted or free-standing; if you choose to have them free-standing, remember to position the rubber feet as detailed in “Placing Units On Top of Each Other” above. When positioning Switch units, note that Matrix Cables are 1m (3.28ft) long.

As shown in Figure 2-3, connect one end of the Matrix Cable to the matrix port of the top Switch, and the other end to the matrix port of the lower Switch.



**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 need a Switch Matrix Module and the appropriate number of Matrix Cables.

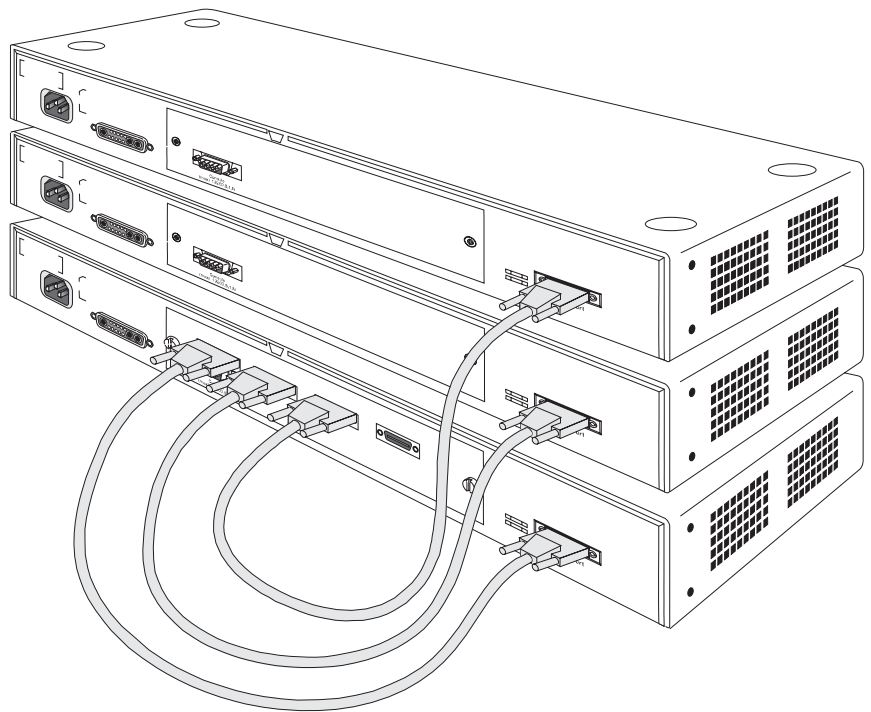


*You only need one Matrix Module for each stack.*

To stack multiple Switch units:

- 1 Arrange your Switch 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 as detailed in “Placing Units On Top of Each Other” on page 2-5. When positioning Switch units, note that Matrix Cables are 1m (3.28ft) long.
- 2 Install the Matrix Module into one of the Switch units. You can find instructions for doing this in the documentation that accompanies the Matrix Module. We recommend that for ease of configuration, the Matrix Module should be installed in the *bottom* Switch of your stack.

- 3 Connect the Matrix Cables, as shown in Figure 2-4:
  - a Connect a Matrix Cable to the port marked Unit 1 on the Matrix Module. Connect the other end of this cable to the matrix port of the Switch that contains the Matrix Module.
  - 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 of the second Switch.
  - c Repeat steps **a** and **b** for any additional Switch 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

You can connect an Advanced Redundant Power System to the Switch. This unit, which is also known as an RPS, is designed to maintain the power to your Switch if a power supply failure occurs.

For normal redundancy, the unit requires one Type 2 Power Module.

For full redundancy, the unit requires two Type 2 Power Modules combined using a Type 2 Y-Cable. Contact your supplier for details.



**ATTENTION:** *The Switch can only use an Advanced Redundant Power System output.*

### 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 powers-up and runs through its Power On Self Test (POST), which takes approximately 12 seconds.

### Checking for Correct Operation

During the Power On Self Test, all ports on the Switch are disabled and the LEDs light in the following sequence:

- All unit LEDs light
- Module LEDs light
- Port Status LEDs light in a rapid cycle

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

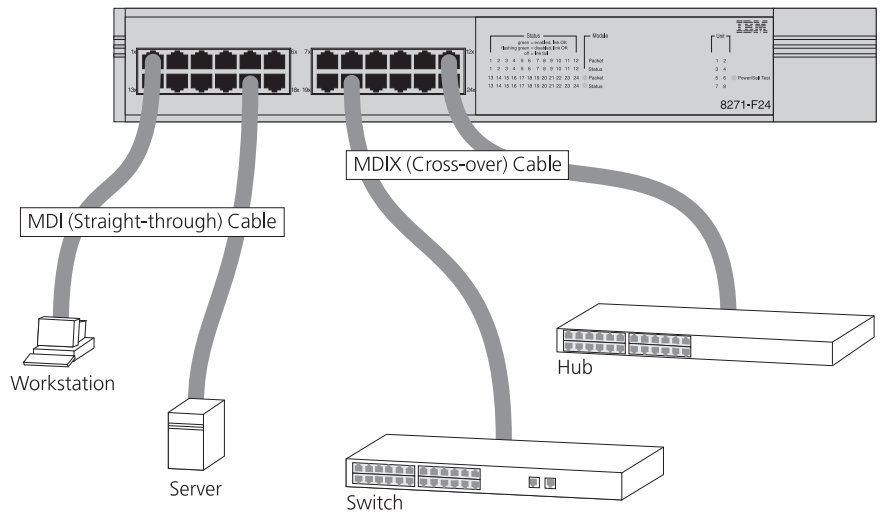
**Table 2-1** LED colors

Color	State
Green	The Switch is powered-up and operating normally
Yellow	The Switch has failed its Power On Self Test. This occurs if any of the ports fail during power-up.
Off	The Switch is not receiving power.

If there is evidence of a problem, see “Solving Problems Indicated by LEDs” on page 8-2.

### 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 need a *cross-over* cable. Many ports on workstations and servers are configured as MDI (straight-through). If you want to make a connection to an MDI port, you need to use a standard *straight-through* cable. This is illustrated in Figure 2-5.



**Figure 2-5** Connecting other devices to the Switch

## Assigning IP Information

Before using the Switch on your network, we recommend that you assign IP information to the Switch. If you do this, you can manage the Switch over the network.



*If you have multiple units connected in a stack, you only need to assign IP information to one unit in the stack. This IP information is then used to manage the whole stack.*

For more information about IP, see “Managing the Stack Over the Network” on page 3-7. For details about assigning IP information to the Switch using the web interface, see “Over the Network” on page 3-4. For details about assigning IP information to the Switch using the command line interface, see “Over the Network” on page 3-7.



# 3

## SETTING UP FOR MANAGEMENT

This chapter explains the various ways of managing a stack, and details the steps required before you can configure a stack to suit the needs of your network. It covers the following topics:

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



*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.*

## Why Manage the Stack?

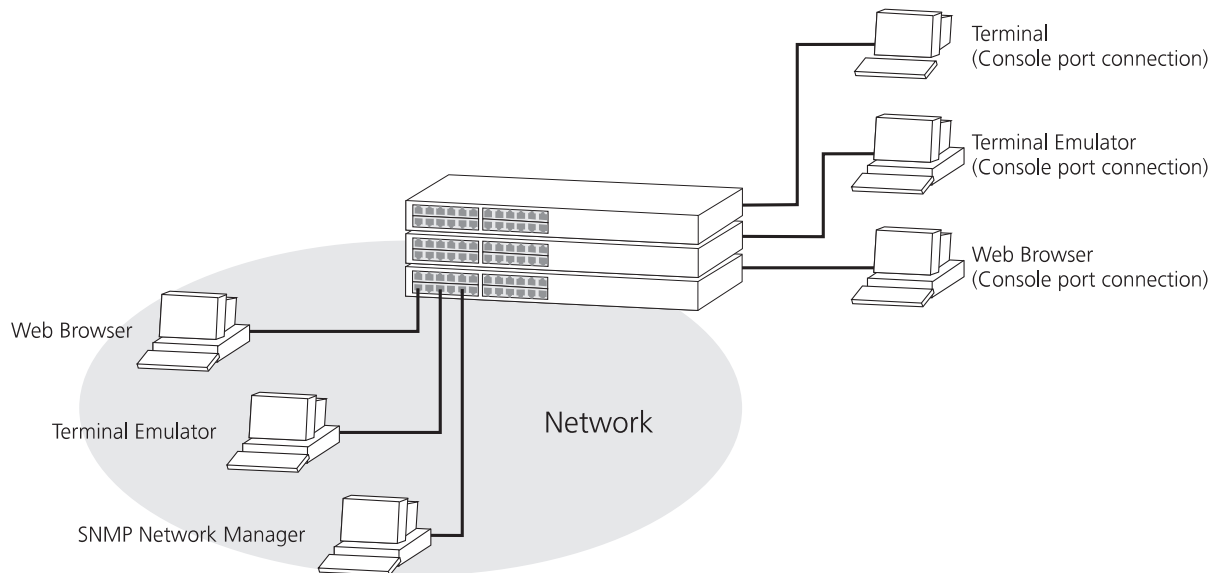
Network management is not required to get the stack working, but if you do use it, you can change and monitor the way the stack works. By doing this, you may improve the efficiency of the stack and therefore improve the performance of your network.

## Methods of Managing a Stack

You can manage a stack using one of the following methods:

- *Web interface management* — Each Switch unit in the stack has an internal set of web pages that allow you to manage the stack using a Java<sup>®</sup>-enabled Web browser.
- *Command line interface management* — Each Switch unit in the stack has a command line interface that allows you to perform limited management.
- *SNMP management* — You can manage the stack using any Network Manager running the Simple Network Management Protocol (SNMP).

Figure 3-1 shows each of the management methods.



**Figure 3-1** Management methods

---

## Setting Up Web Interface Management

You can access the web interface using:

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



*While multiple users can access the web interface at any one time, too many users may result in a slow response time for the web pages and the error message “document contains no data”. We therefore recommend that you allow only three users access to the interface.*

## Through the Console Port

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

- 1 You must connect the management workstation to the console port directly 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 [“Pin-outs”](#) on page D-1.

To connect the cable:

- a Attach the female connector on the cable to the male connector on the console port of the Switch.
  - b Tighten the retaining screws on the cable to prevent it from being loosened.
  - c Connect the other end of the cable to your management workstation.
- 2 The management workstation must be running the Serial Line Interface Protocol (SLIP), and the SLIP parameters (address and subnet mask) of the Switch need to be configured correctly. To do this, you must install, configure and run the Serial Web Utility described in “Using the Serial Web Utility” on page B-1.
  - 3 Install the online help and online documentation for the web interface, if required. For more information, see “Installing Online Help and Documentation” on page 3-4.
  - 4 Access the web interface using the correct user name and password. Default user names and passwords are described in “Logging in as a Default User” on page 3-9.

**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. To do this:
  - a Access the web interface of the stack through a console port. See “Through the Console Port” on page 3-3.
  - b Use the Getting Started pages or IP Setup page to enter suitable IP information for the Switch.
 

For more information about IP, see “Managing the Stack Over the Network” on page 3-7. For more information about the Getting Started pages, see “About The Getting Started Pages” on page 4-4. For more information about the IP Setup page, see “Setting Up IP Information for the Switch” on page 4-15.
- 2 You must have an IP stack correctly installed on your management workstation. You can check this by trying to browse the World Wide Web; if you can browse, an IP stack is installed.

### Installing Online Help and Documentation

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

- The online help system is in an HTML (HyperText Markup Language) format.
- 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.



*The help files for Switch Model F12/F24 are the same as the help files for the Switch Model E12/E24. If you have already installed the help files for a Switch Model E12/E24, you do not need to install any Switch Model F12/F24 help files.*

- 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 `\agent\IBM01_00\docs\index.htm`
  - The HTML version can be accessed directly using `\agent\IBM01_00\docs\F24TX\index.htm`
  - The PDF version can be accessed directly using `\agent\IBM01_00\docs\F24TX\F24TX.pdf`

We recommend that you copy the `\agent\IBM01_00\docs\` directory as a whole to maintain the structure of the files.



*If you already have documentation files for a Model E12/E24 on your local drive or server, copy the `\agent\IBM01_00\docs\F24TX\` directory into the Model E12/E24 `\docs\` directory. By doing this, you can access the documentation for both units from the Model E12/E24 `\docs\index.htm` file.*

### Choosing a Suitable Browser

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

- Java<sup>®</sup>
- Frames
- HTML 3.2

Suitable Web browsers are:

- Netscape<sup>®</sup> Navigator™ Version 3.0 or above
- Microsoft<sup>®</sup> 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 to the console port of a Switch directly, or through a modem
- A terminal or terminal emulator connected to a Switch over an IP network using Telnet

### 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 connecting to the console port using a modem, you need a standard modem cable. The console port of the Switch has a male 9-pin d-type connector. You can find pin-out diagrams for both cables in ["Pin-outs"](#) on page D-1.

To connect the cable:

- a Attach the female connector on the cable to the male connector on the console port of the Switch.
  - 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, terminal emulator, or modem.
- 2 The terminal, terminal emulator, or modem must use the same settings as the console port:
    - 8 data bits
    - no parity
    - 1 stop bit

To configure the settings of the terminal, terminal emulator, or modem, see the documentation that accompanies it. If the Switch containing the console port has auto-configuration enabled (default), the line speed (baud) is detected automatically. The Switch can auto-detect a maximum line speed of 19200 baud.

- 3 Access the command line interface using the correct user name and password. Default user names and passwords are described in "Logging in as a Default User" on page 3-9.

**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. To do this:
  - a Access the command line interface of the stack through a console port. See “Through the Console Port” on page 3-6.
  - b Use the **ip interface define** command to enter suitable IP information for the Switch.

For more information about IP, see “Managing the Stack Over the Network” on page 3-7. For more information about the **ip interface define** command, see “Specifying IP and SLIP Information” 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.

---

## Setting Up SNMP Management

Any network management application running the Simple Network Management Protocol (SNMP) can manage a stack, provided the correct MIBs (Management Information Bases) are installed on the management workstation.

For information about using an SNMP network management application to manage the stack, see the documentation supplied with the software.

---

## Managing the Stack Over the Network

When managing your stacks over the network, each stack must be correctly configured with the following IP information:

- An IP address — for more information, see “IP Addresses” on page 3-8.
- A subnet mask — for more information, see “Subnets and Using a Subnet Mask” on page 3-8.

**IP Addresses** 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, for example 191.128.40.120:

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

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

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

### **Obtaining a Registered IP Address**

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

Network Solutions  
Attn: InterNIC Registration Service  
505, Huntmar Park Drive  
Herndon  
VA 22070  
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 [www.internic.net](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

If you manage a stack using the web interface or the command line interface, you need to log on with a correct user name and password. The stack has four default user names, each with a different password and level of access. These default user names are listed in Table 3-1.

**Table 3-1** Default Users

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

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





# MANAGING THE SWITCH

Chapter 4 Working With the Web Interface

Chapter 5 Working With the Command Line Interface



# 4

## WORKING WITH THE WEB INTERFACE

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

- Accessing the Web Interface
- About The Getting Started Pages
- About 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 Model F12/F24 only. If you have a Model E12/E24 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 through the console port or over the network.

To access the web interface through the console port, you must install, configure and run the Serial Web Utility described in “Using the Serial Web Utility” on page B-1.

To access the web interface over the network, take the following steps:

- 1 Ensure that 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 “Solving Problems That Occur When Using the Web Interface” on page 8-2.*

- 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 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 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 4-22.



*If you forget your password while logged out of the web interface, see “Solving Problems That Occur When Using the Web Interface” on page 8-2.*

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 are displayed. These are described in “About The Getting Started Pages” on page 4-4.
- If you have accessed the web interface before, the main web interface is displayed. For information about the interface, see “About the Main Web Interface” on page 4-6.

If you are unable to access the web interface, see “Solving Problems That Occur When Using the Web Interface” on page 8-2.



**ATTENTION:** *While multiple users can access the web interface at any one time, too many users may result in a slow response time for the web pages, or the error message “document contains no data”. We therefore recommend that you limit the number of users with access.*



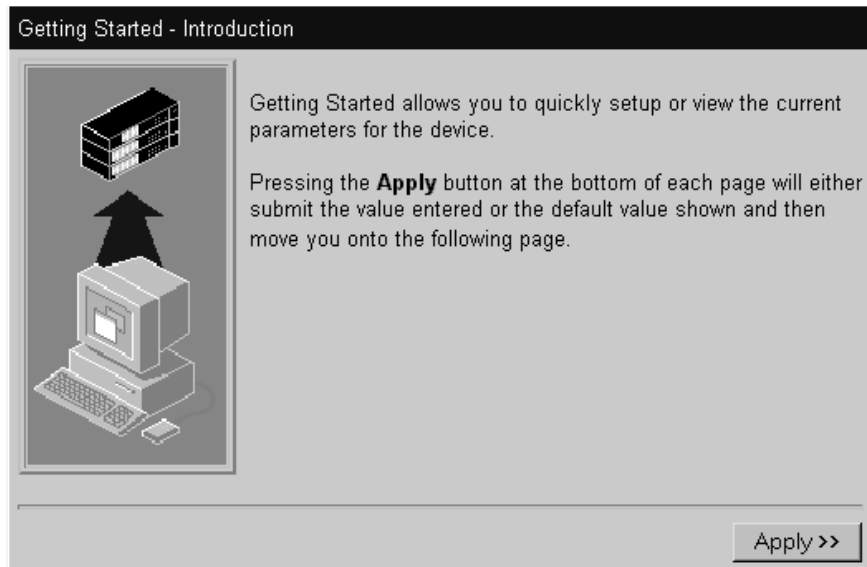
*While you are managing the stack, you can view other web pages using your browser, and then simply use the Back button to reload the web management pages. You do not need to re-enter your username and password.*

## 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 Web browser after a management session.

## About 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 are displayed. The first Getting Started page, Getting Started - Introduction 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. 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 "Subnets and Using a Subnet Mask" on page 3-8.
- An IP address for the default router, if one exists on your network.



If you choose to allocate IP information using a BOOTP server, no prompts are displayed.

- 3 The URL or file path of the online help and online documentation for the stack.
  - If the files are installed on your management workstation, on the CD-ROM, or on a network server, you must begin the file path with **file://**.
  - If the files are stored on a Web server, you must begin the URL with **http://**.

If you do not know where the online help and online documentation is stored, see "Installing Online Help and Documentation" 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 main web interface is displayed. For information about the interface, see "About the Main Web Interface" on page 4-6.



*The Getting Started pages are available from the main web interface at any time. For more information, see "Changing the Management Settings for the Stack" on page 4-21.*

## About the Main Web Interface

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 (below). For more information, see “The Management Icons” on page 4-8.

- **The Page Area**

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 Page Area” on page 4-8.

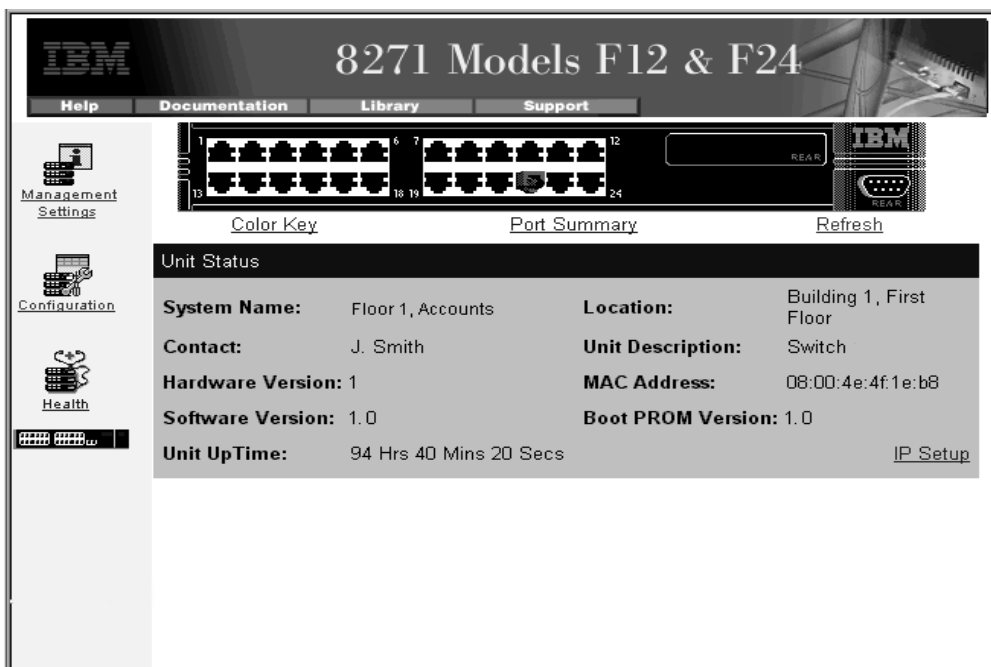


Figure 4-3 Main parts of the web interface page

## 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.





**Table 4-1** External Link icons and their actions

External Link Icon	Action
<b>Help</b>	<p>If you have set up the online help, clicking the Help icon displays the help for the web interface in a second browser window.</p> <p>For information about setting up the online help, see “Installing Online Help and Documentation” on page 3-4.</p>
<b>Documentation</b>	<p>If you have set up the online documentation, clicking the Documentation icon allows you to access the User Guides for the stack in a second browser window.</p> <p>For information about setting up the online documentation, see “Installing Online Help and Documentation” on page 3-4.</p>
<b>Library</b>	<p>If your management workstation has access to the World Wide Web, clicking the Library icon displays the Online Library of the IBM World Wide Web site in a second browser window.</p>
<b>Support</b>	<p>If your management workstation has access to the World Wide Web, clicking the Support icon displays support information from the IBM World Wide Web site in a second browser window.</p>

## The Management Icons

The side-bar of the main web interface contains several Management Icons that allow you to display web pages in the page area; these are shown in Table 4-2.

**Table 4-2** Management Icons and their actions .

Management Icon	Action
	<b>Management Settings</b> — Click on this icon to display the Management Settings pages for the stack.
	<b>Configuration</b> — Click on this icon to display the Configuration pages for the stack.
	<b>Health</b> — Click on this icon to display the Health pages for the stack.
	<b>Unit</b> — Click on this icon to display the Unit pages for the current Switch unit in the stack. To display the Unit pages for a specific unit in a stack, click on that unit in the Unit icon.

For an overview of the pages accessed using these icons, see “The Page Area” on page 4-8.

## The Page Area

The page area of the main web interface contains web pages that allow you to manage the stack. The web pages are grouped into four categories:

- **Unit Pages** — These pages allow you to configure the current Switch in the stack and the ports on that Switch:
  - **Switch Graphic** — This page contains a graphic of the Switch that allows you to view the status of the ports. It is always displayed above the other Unit pages.
  - **Color Key** — This page allows you to view the color-coding information used by the Switch Graphic page.
  - **Port Summary** — This page allows you to view the speed and Duplex Mode of the ports shown in the graphic on the Switch Graphic page.

- **Unit Status** — This page allows you to view the general administration details of the Switch.
- **IP Setup** — This page allows you to set up IP information for the Switch.
- **Port Setup** — This page allows you to configure individual ports on the Switch.
- **Console Port Configuration** — This page allows you to configure the console port of the Switch.

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

- **Management Settings Pages** — These pages allow you to change the management settings for the stack:
  - **System Name** — This page allows you to specify a descriptive name for the stack.
  - **Password Setting** — This page allows you to change your password.
  - **Location** — This page allows you to specify the physical location of the stack.
  - **Getting Started** — This page allows you to access the Getting Started pages for the stack.
  - **Documentation** — This page allows you to specify the location of the online help and documentation for the stack.
  - **Contact** — This page allows you to specify the details of a person to contact about the stack.

For more information, see “Changing the Management Settings for the Stack” on page 4-21.

- **Configuration Pages** — These pages allow you to configure the stack:
  - **Switch Database** — This page allows you to configure the Switch Database of the stack.
  - **Advanced Stack Setup** — This page allows you to configure the operating modes of the stack.
  - **Software Upgrade** — This page allows you to upgrade the management software of the Switch units in the stack.

- **Resilient Links Setup** — This page allows you to set up resilient links for the stack.
- **Reset** — This page allows you to reset the Switch units in the stack.
- **Initialize** — This page allows you to initialize the Switch units in the stack.

For more information, see “Configuring the Stack” on page 4-26.

- **Health Pages** — These pages allow you to view statistics for the current Switch in the stack:
  - **Unit Graph** — This page allows you to display a range of statistics for all the ports on the Switch.
  - **Port Graph** — This page allows you to display a range of statistics for a specific port on the Switch.

For more information, see “Viewing Statistics for the Current Switch” on page 4-36.

### Navigating the Page Area

To access the first page of each category, click on the relevant Management Icon on the side-bar; to access the remaining pages in the category, click on the underlined hotlinks that are displayed at the top of each page.



*There are four exceptions to the navigation system. The Color Key page, Port Summary page, Port Setup page and Console Port Configuration page are accessed from the Switch Graphic page.*

Figure 4-4 shows you how to access each of the web pages.

### Making Changes in the Page Area

If you change any setting on a page in the page area, you *must* click the *Apply* button at the bottom right of the page to make the change to the stack. The change is only made when you click the *Apply* button.



*If you make changes on a page but do not wish to apply them, click the Back button in your Web browser to exit the page.*

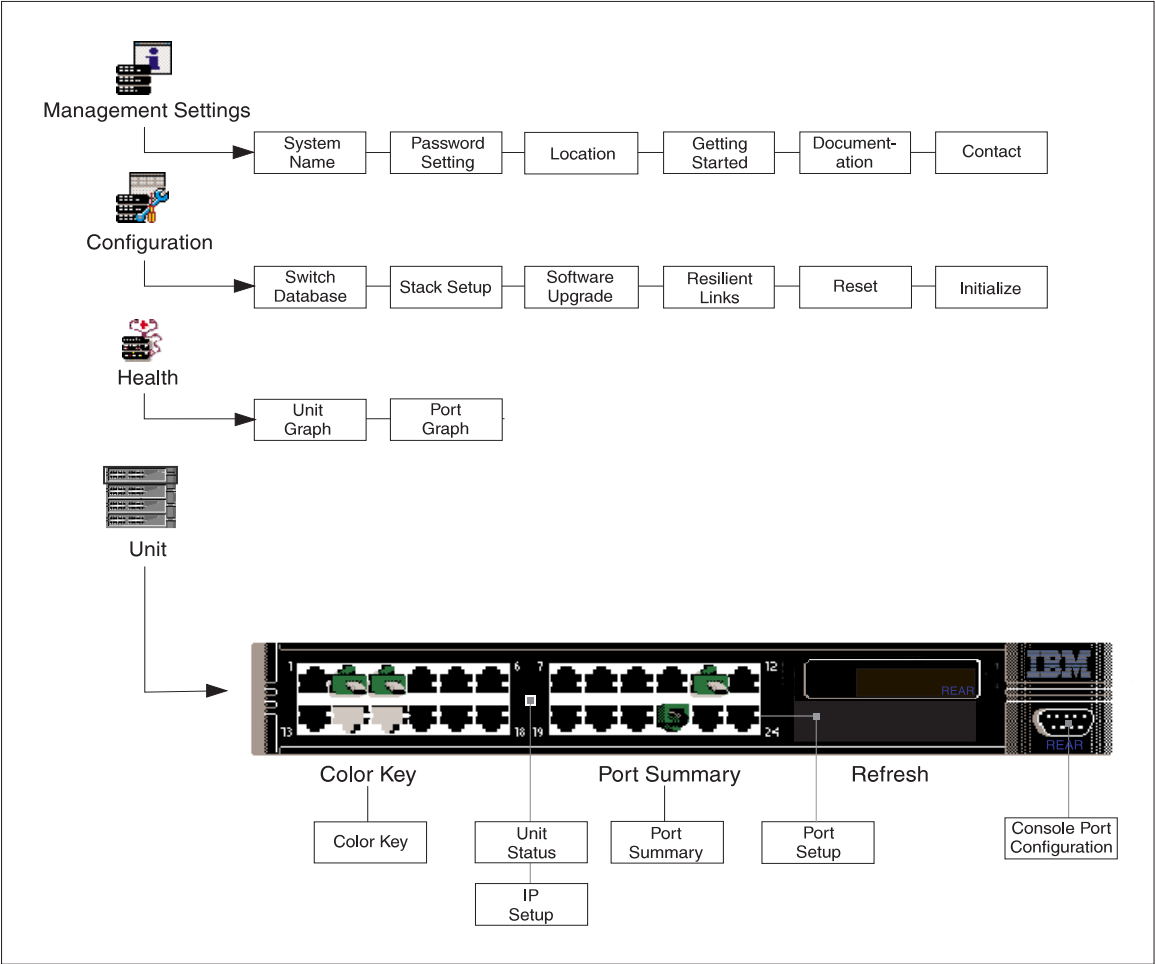


Figure 4-4 Web interface map

## Configuring the Current Switch

You can configure the current Switch and the ports on that Switch using the Unit Pages. These pages allow you to:

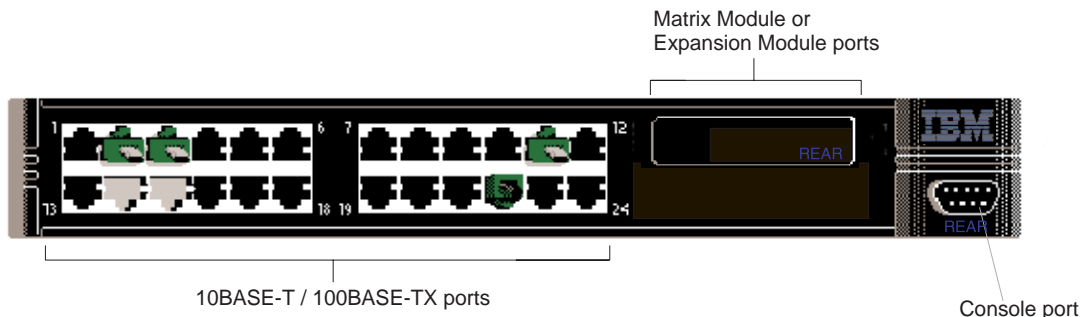
- View the status of the ports on the Switch
- View the general administration details of the Switch
- Set up IP information for the Switch
- Configure individual ports on the Switch
- Configure the console port of the Switch

## Viewing the Status of the Ports

You can view the status of ports on the Switch using the Switch Graphic page.

To access the page:

- Click the *Unit* icon on the side-bar. The Switch Graphic page is displayed as shown in Figure 4-5, containing a graphic of the Switch. Note that this page is always displayed above the other Unit pages.



**Figure 4-5** The Switch graphic

## Viewing the Color Codes Used by the Switch Graphic

The Switch graphic indicates the status of a port using color-coding:

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



You can view the color-coding information using the Color Key page. To access the page, click the *Color Key* hotlink under the Switch graphic.

### Viewing the Speed and Duplex Mode of Ports

You can view the speed and Duplex Mode of ports in the Switch graphic using the Port Summary page.

To access the page:

- Click the *Summary* hotlink under the Switch graphic. The Port Summary page is displayed as shown in Figure 4-6.

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

**Figure 4-6** The Port Summary page



*If you have an Expansion Module fitted to your Switch, the Expansion Module port numbers follow on sequentially from the number of fixed ports.*

### 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; for more information, see “Solving Problems That Occur When Using the Web Interface” on page 8-2.

## Viewing the Administration Details of the Switch

You can view general administration details about the Switch using the Unit Status page.

To access the page:

- Click the *Unit* icon on the side-bar. The Unit Status page is displayed as shown in Figure 4-7.

Unit Status			
<b>System Name:</b>	Floor 1, Accounts	<b>Location:</b>	
<b>Contact:</b>		<b>Unit Description:</b>	Switch
<b>Hardware Version:</b>	1.00	<b>MAC Address:</b>	08:00:4e:35:8c:4d
<b>Software Version:</b>	1.00	<b>Boot PROM Version:</b>	1.0
<b>Unit UpTime:</b>	16 Hrs 30 Mins 1 Secs		<a href="#">IP Setup</a>

**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. For information about assigning a new name for the Switch, see “Specifying a Descriptive Name for the Stack” on page 4-21.

### Location

Displays the physical location of the Switch. For information about assigning a new location for the Switch, see “Specifying the Physical Location of the Stack” on page 4-23.

### Contact

Displays the details of a person to contact about the Switch. For information about assigning new contact details, see “Specifying a Contact for the Stack” on page 4-25.

### Unit Description

Displays the product name of the Switch.

### Hardware Version

Displays the version number of the Switch hardware.

### MAC Address

Displays the MAC (Ethernet) address assigned to the Switch.

**Software Version**

Displays the version number of the management software currently installed on the Switch. For information about how to upgrade the management software, see “Upgrading the Management Software of the Stack” on page 4-35.

**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.

**Setting Up IP  
Information for the  
Switch**

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

To access the page:

- 1 Click the *Unit* icon on the side-bar. The Unit Status page is displayed.
- 2 Click the *IP Setup* hotlink on the Unit Status page. The IP Setup page is displayed as shown in Figure 4-8.

The screenshot shows the 'IP Setup' configuration page. It has a dark header with the text 'IP Setup'. Below the header, there are several sections:

- A prompt: "Enter a unique IP address for the device." followed by the label "IP Address :" and a text input field containing "191.100.100.100".
- A prompt: "Enter a suitable subnet mask." followed by the label "Subnet Mask :" and a text input field containing "255.255.0.0".
- A prompt: "If a default router exists on your network, type in its IP address below." followed by the label "Default Router :" and a text input field containing "191.100.100.100".
- A label "BOOTP :" followed by two radio buttons: "Off" (which is selected) and "On".

At the bottom right of the form area, there is an "Apply" button.

**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. For more information about IP addresses, see “Managing the Stack Over the Network” on page 3-7.



*If you change the IP address of the Switch, you can no longer access the web interface unless you enter the new IP address in the Location field of your browser.*

### **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**

If your network contains one or more routers, this field allows you to enter the IP address of the default router. For more information about IP addresses, see “Managing the Stack Over the Network” on page 3-7.

### **BOOTP On / Off**

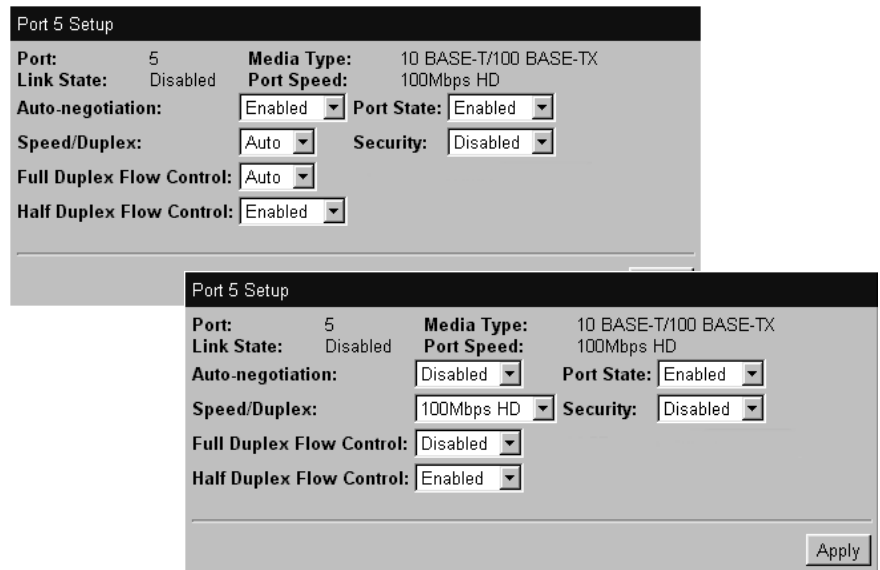
If you have a BOOTP server on your network, these radio buttons allow you to specify whether the server allocates IP information for the Switch automatically.

## **Configuring a Port on the Switch**

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

To access the page:

- 1 Click the *Unit* icon on the side-bar.
- 2 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 elements:

### Port

Displays the number of the selected port.

### Link State *Enabled / Disabled*

Displays the state of the link connected to the port.

### Media Type

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

### Port Speed

Displays the current speed and Duplex Mode of the port. *FC* indicates that flow control is enabled.

### Auto-negotiation *Enabled / Disabled*

Allows you to specify whether auto-negotiation is enabled for the port:

- If auto-negotiation is enabled, the speed and Duplex Mode of the link is automatically detected, and the speed and Duplex Mode of the port is set accordingly.
- If auto-negotiation is disabled, the speed and Duplex Mode of the port is set using the Speed/Duplex drop-down listbox.



*Fiber ports are not auto-negotiating. If the port is a fiber Expansion Module port, 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 F12/F24 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 disabled, or if the device at the other end of the link does not support auto-negotiation, this field allows you to specify the speed and Duplex Mode of the port (*HD* indicates half duplex, *FD* indicates full duplex). If auto-negotiation is enabled, the field displays *Auto* and you cannot change the speed and Duplex Mode of the port manually.



*Expansion Module ports have a fixed speed. If the port is an Expansion Module port, you can only specify the Duplex Mode of the port.*

**Full Duplex Flow Control** *Enabled / Disabled / Auto*

If auto-negotiation is disabled, this field allows you to enable or disable the IEEE 802.3x flow control that can be used when the port is operating in full duplex. If auto-negotiation is enabled, the field displays *Auto*, and you cannot change the flow control setting for the port manually. Flow control prevents any packet loss that may occur on congested ports.



*For IEEE 802.3x flow control to operate correctly, it must be enabled at both ends of the link.*

**Half Duplex Flow Control** *Enabled / Disabled*

Allows you to enable or disable the Intelligent Flow Management flow control that can be used when the port is operating in half duplex. Flow control prevents any packet loss that may occur on congested ports.



*The Half Duplex Flow Control field should be disabled if the port is connected to multiple devices using a repeater.*

**Port State** *Enabled / Disabled*

Allows you enable or disable the port (that is, turn the port on or off).

**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.

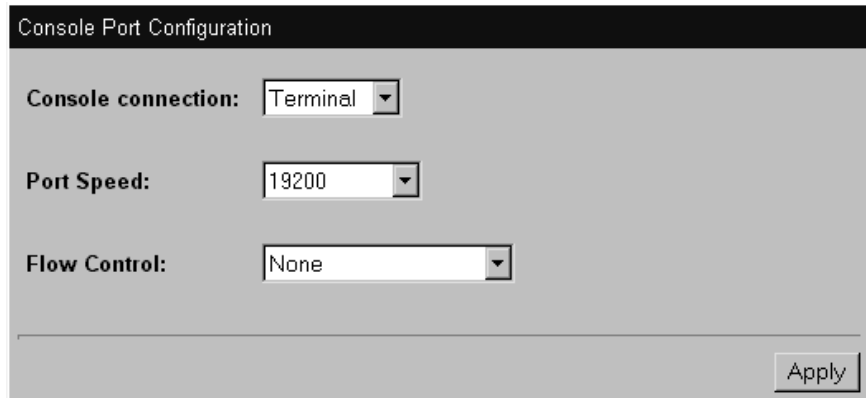
Once the first address is learned, no other endstation is allowed to access the network through the port. If an endstation with a different address attempts to transmit packets through the port, the port is automatically disabled until it is enabled using the Port State field.

### **Configuring the Console Port of the Switch**

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 Configuration 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 serial line flow control option suitable for your terminal or modem. See the documentation accompanying your terminal or modem if you are unsure of the correct setting.



---

## Changing the Management Settings for the Stack

You can change the management settings for the stack using the Management Settings Pages. These pages allow you to:

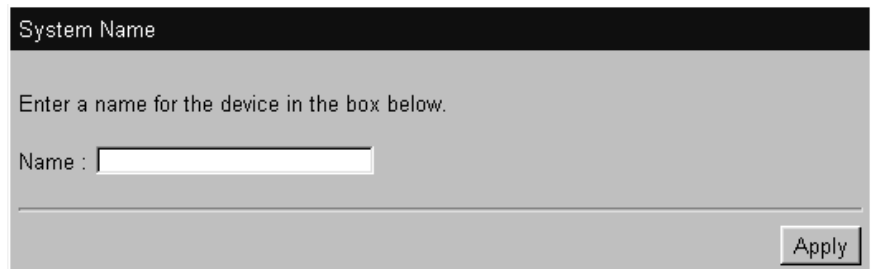
- Specify a descriptive name for the stack.
- Change your password.
- Specify the physical location of the stack.
- Access the Getting Started pages for the stack.
- Specify the location of the online help and documentation for the stack.
- Specify the details of a person to contact about the stack.

### Specifying a Descriptive Name for the Stack

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

To access the page:

- 1 Click the *Management Settings* icon on the side-bar.
- 2 Click the *System Name* hotlink. The System Name page is displayed as shown in in Figure 4-11.



System Name

Enter a name for the device in the box below.

Name :

Apply

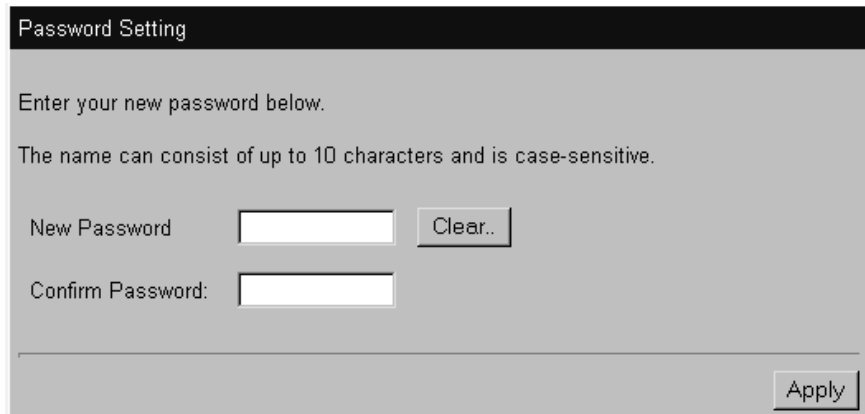
**Figure 4-11** The System Name page

The Name field allows you to enter a descriptive name for the stack. The name can be up to 20 characters long.

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

To access the page:

- 1 Click the *Management Settings* icon on the side-bar.
- 2 Click the *Password Setting* hotlink. The Password Setting page is displayed as shown in Figure 4-12.



Password Setting

Enter your new password below.

The name can consist of up to 10 characters and is case-sensitive.

New Password  Clear..

Confirm Password:

Apply

**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 up to 10 characters long.

**Confirm Password**

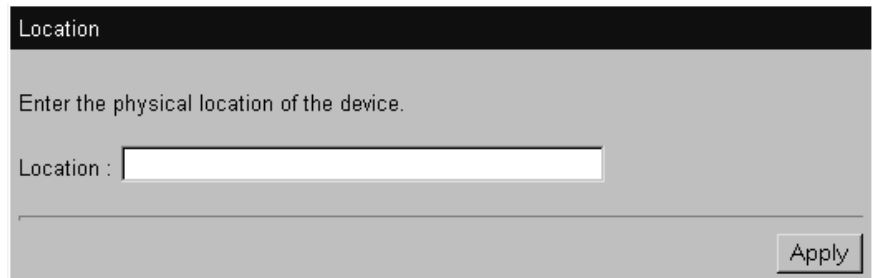
Allows you to re-enter the new password. The password does not change unless you enter it in this field.

### Specifying the Physical Location of the Stack

You can specify the physical location of the stack using the Location page.

To access the page:

- 1 Click the *Management Settings* icon on the side-bar.
- 2 Click the *Location* hotlink. The Location page is displayed as shown in Figure 4-13.



The screenshot shows a web interface for setting the physical location of a device. At the top, there is a dark header with the word "Location" in white. Below the header, the main content area is light gray. It contains the instruction "Enter the physical location of the device." followed by a label "Location :" and a white text input field. At the bottom right of the page, there is a button labeled "Apply".

**Figure 4-13** The Location page

### Accessing the Getting Started Pages

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

To access the Getting Started pages:

- 1 Click the *Management Settings* icon on the side-bar.
- 2 Click the *Getting Started* hotlink. The first Getting Started page, Getting Started - Introduction, is displayed.

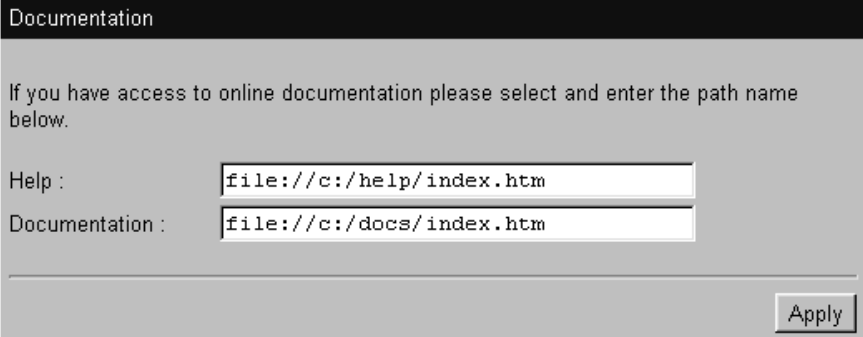
For information about using the Getting Started pages, see "About The Getting Started Pages" on page 4-4.

### Specifying the Location of the Online Help and Documentation

You can specify the location of the online help and documentation for the stack using the Documentation page.

To access the page:

- 1 Click the *Management Settings* icon on the side-bar.
- 2 Click the *Documentation* hotlink. The Documentation page is displayed as shown in Figure 4-14.



The screenshot shows a web interface titled "Documentation". Below the title, there is a text prompt: "If you have access to online documentation please select and enter the path name below." There are two input fields: "Help :" with the value "file://c:/help/index.htm" and "Documentation :" with the value "file://c:/docs/index.htm". An "Apply" button is located at the bottom right of the form.

**Figure 4-14** The Documentation page

The Documentation page contains the following elements:

#### Help

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

#### Documentation

Allows you to specify the URL or file path of the online documentation for Model E12/E24 and Model F12/F24 units in the stack. If the files are installed on your management workstation, on the CD-ROM, or on a network server, you must begin the file path with **file://**. If the files are stored on a Web server, you must begin the URL with **http://**. If you do not know where the online documentation is stored, see "Installing Online Help and Documentation" on page 3-4.

**Specifying a Contact for the Stack**

You can specify the details of a person to contact about the stack using the Contact page.

To access the Contact page:

- 1 Click the *Management Settings* icon on the side-bar.
- 2 Click the *Contact* hotlink. The Contact page is displayed as shown in Figure 4-15.



The screenshot shows a web interface for the 'Contact' page. At the top, there is a black header bar with the word 'Contact' in white. Below the header, the background is a light gray. The text 'Enter a contact name for the device.' is displayed in a dark gray font. Underneath this text, the label 'Contact :' is followed by a white rectangular input field with a thin black border. At the bottom right of the form area, there is a button with the text 'Apply' inside it.

**Figure 4-15** The Contact page

## Configuring the Stack

You can configure the stack using the Configuration pages. These pages allow you to:

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

## Configuring the Switch Database of the Stack

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

To access the page:

- 1 Click the *Configuration* icon on the side-bar.
- 2 Click the *Switch Database* hotlink. The Switch Database page is displayed as shown in Figure 4-16.

Switch Database			
Port Selection Filter			
Port 1			
Enter MAC Address			
000000000000			
Select Action Type			
Display All			
Apply			

Display Database Entries			
Unit	Port	Mac Address	Status
		Age Time = 1800 secs	
1	1	00:20:af08:40:01	Learned
1	1	00:20:af12:17:26	Learned
1	1	00:20:af12:17:7e	Learned
1	1	00:c0:4fc7:4e:55	Learned
1	1	00:c0:4fc7:4e:7a	Learned
1	1	00:c0:4fc7:5e:cc	Learned
1	1	00:c0:4fc7:68:6e	Learned
1	1	08:00:02:17:25:a6	Learned
1	1	08:00:4e:0b:9e:46	Learned
1	1	08:00:4e:35:8c:4d	Learned
		Total = 10 Perm = 0	

**Figure 4-16** The Switch Database page

### What is the Switch Database?

The Switch Database is used by the stack to determine if a packet should be 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 (Ethernet) address information from each endstation that sends packets to the stack.
- The port in the stack that receives packets from that endstation.

The number of addresses that the database can hold depends on the number of Switch units in the stack. Each Model F12/F24 provides support for 12,000 addresses, and each Model E12/E24 provides support for 6,000 addresses.

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-down.
- *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 of the Switch Database page displays the Switch Database entries for the stack:

- **Unit 1 / 2 / 3 / 4**  
Displays the Switch unit in the stack that contains the port for the entry.
- **Port**  
Displays the port for the entry.

- **MAC Address**

Displays the MAC (Ethernet) address for the entry.

- **Status** *Learned / Permanent*

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 the *Apply* button.

To display the entire list of entries:

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

### **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 From the *Port Selection Filter* drop-down listbox, select a port for the entry.
- 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 the *Apply* button.



*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 the *Apply* button.



### 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 the *Apply* button.



*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 the Apply button.*

### Configuring the Operating Modes of the Stack

You can configure the operating modes of the stack using the Advanced Stack Setup page.

To access the page:

- 1 Click the *Configuration* icon on the side-bar.
- 2 Click the *Stack Setup* hotlink. The Advanced Stack Setup page is displayed as shown in Figure 4-17.

Advanced Stack Setup

Forwarding Mode: Intelligent

Spanning Tree: Disabled

Broadcast Storm Control: Disabled

Apply

**Figure 4-17** 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 40µs but without checking time, error packets are propagated onto the network.
- *Fragment Free* — A minimum of 512 bits of the received packet is buffered before 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 ensures that only good packets are forwarded to their destination. The forwarding delay for packets in this mode varies between 64µs and 1.2ms, depending on the length of the packet. In this mode the latency is 7µs (measured as the time between receiving the last bit of the frame and transmitting the first bit).
- *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.



*The Model F12/F24 only supports the Store-and-Forward Forwarding Mode. If the stack is set to another Forwarding Mode, the Model F12/F24 uses the Store-and-Forward Forwarding Mode.*

**Spanning Tree** *Enabled / Disabled*

Allows you to specify whether the stack uses the Spanning Tree Protocol (STP). STP allows your network to be more fault tolerant; for more information, see “Spanning Tree Protocol” on page 6-1.

**Broadcast 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

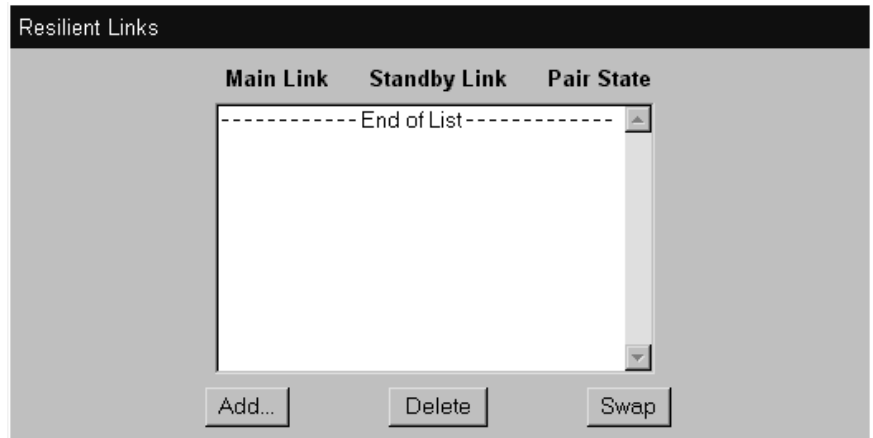
broadcast traffic on the port is blocked until the broadcast traffic returns to 20%.

### 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:

- 1 Click the *Configuration* icon on the side-bar.
- 2 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:
  - Neither of the ports are secure ports (have Security enabled).
  - 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 / ...*  
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 / ...*  
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*  
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

The Resilient Links page allows you to create a resilient link pair. To do this:

- 1 Click the *Add...* button. The first Add Resilient Links page is displayed.
- 2 Select the Switch units that are to contain the main port and standby port of the resilient link pair.
- 3 Click the *Next...* button.
- 4 From the *Main Links* box, select the main port of the resilient link pair.
- 5 Click the *Next...* button.
- 6 From the *Standby Links* box, select the standby port of the resilient link pair.
- 7 Click the *Next...* button. The Resilient Links page is displayed showing the new resilient link pair.

### Deleting a Resilient Link Pair

The Resilient Links page allows you to delete a resilient link pair. To do this:

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

### Swapping the Main and Standby Ports of a Resilient Link Pair

The Resilient Links page allows you to swap the main and standby ports of a resilient link pair. To do this:

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

### Resetting All the Units in the Stack

You can reset all the Switch units in the stack using the Reset page.

To access the page:

- 1 Click the *Configuration* icon on the side-bar.
- 2 Click the *Reset* hotlink. The Reset page is displayed.

To reset the stack, select *Yes* and then click *Apply*.

### What Happens During a Reset?

Resetting the Switch units in the stack simulates a power-off/on cycle. 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.*



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

### Initializing All the Units in the Stack

You can initialize all the Switch units in the stack using the Initialize page.

To access the page:

- 1 Click the *Configuration* icon on the side-bar.
- 2 Click the *Initialize* hotlink. The Initialize page is displayed.

To initialize the stack, select *Yes* and then click *Apply*.

### What Happens During an Initialization?

Initializing the Switch units in the stack returns them to their default (factory) settings. You may want to do this if the stack has previously been used in a different part of your network, and its settings are incorrect for 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.*



**ATTENTION:** *When initializing the stack, note that 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 the Management Software of the Stack

You can upgrade the management software of the Switch units in the stack using the Software Upgrade page.

To access the page:

- 1 Click the *Configuration* icon on the side-bar.
- 2 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, see the documentation that accompanies it.
- 2 Enter the name of the software upgrade file in the *Filename* field. The filename format is:

`nwsxx_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 the *Apply* button. 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 Switch units in the stack are reset.



**ATTENTION:** During the upgrade, do not power-down or reset any Switch units in the stack.

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

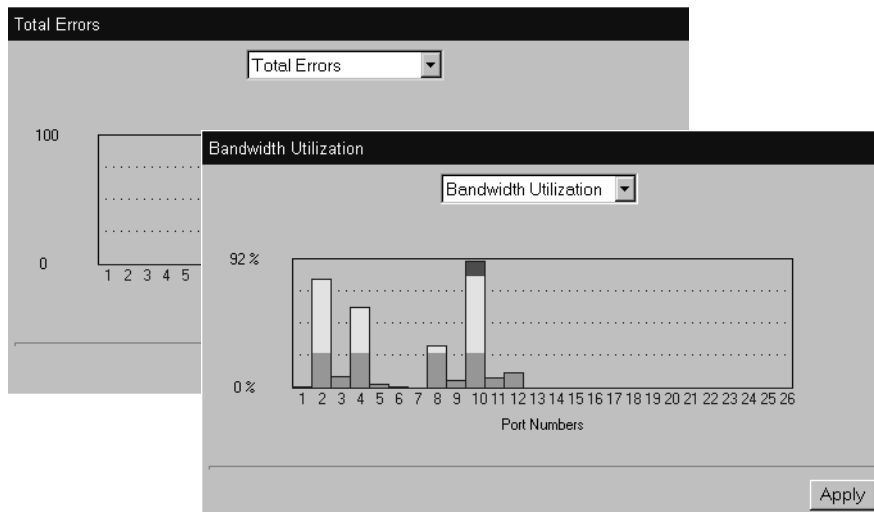
## Displaying Unit Statistics

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

To access the page:

- 1 Click the *Health* icon on the side-bar.
- 2 Click the *Unit Graph* hotlink. The Unit Graph page is displayed.

The graphs that can be displayed by the Unit Graph page are shown in Figure 4-20.



**Figure 4-20** The graphs displayed by the Unit Graph page

You can choose to display graphs for *Bandwidth Utilization* or *Total Errors*.



To display the Bandwidth Utilization graph:

- 1 From the drop-down listbox, choose *Bandwidth Utilization*.
- 2 Click *Apply*.

To display the Total Errors graph:

- 1 From the drop-down listbox, choose *Total Errors*.
- 2 Click *Apply*.



*If you click a port on the Bandwidth Utilization or Total Errors graph, the graph for that port is displayed.*

### Interpreting the Statistics

- The Utilization graph scales automatically to display the percentage of bandwidth used on all ports of 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 26–85% (yellow bar on the graph) indicates that the ports are dealing with a normal traffic load.
  - A bandwidth utilization of 86–100% (red bar on the graph) indicates that the ports are dealing with a heavy traffic load. This could be caused by a fault in your network, or an inadequate network configuration.
- The Total Errors graph scales automatically to display the total number of packets with errors that have been seen on the ports of the Switch over the last 30 seconds.

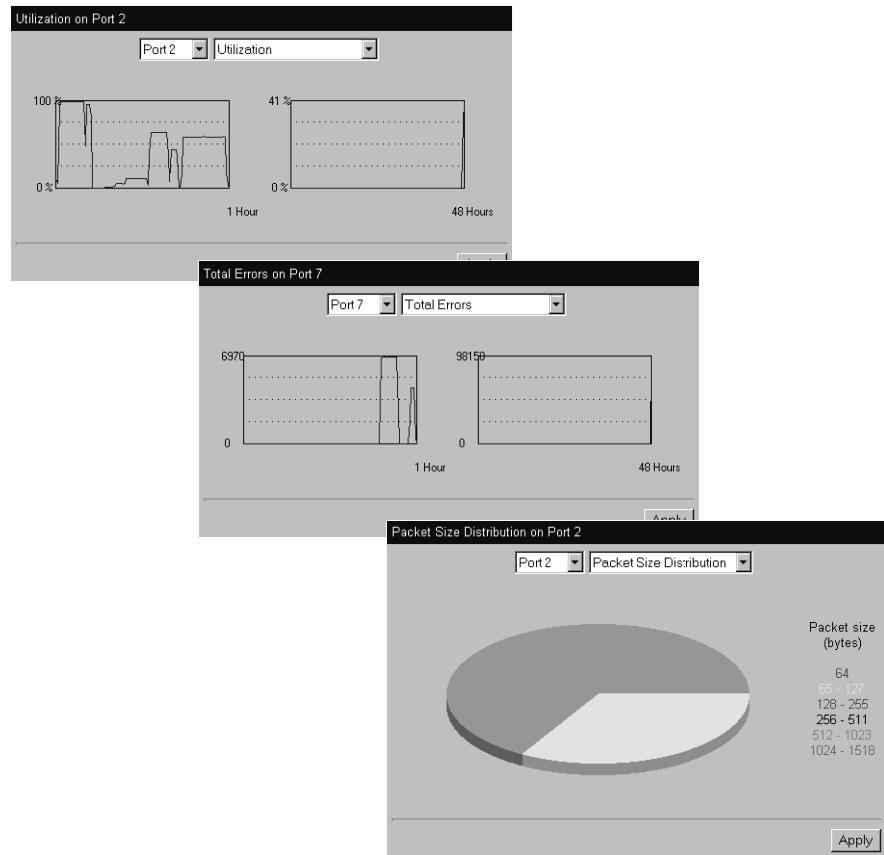
### Displaying Port Statistics

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

To access the page:

- 1 Click the *Health* icon on the side-bar.
- 2 Click the *Port Graph* hotlink. The Port Graph page is displayed.

The graphs that can be displayed by the Port Graph page are shown in Figure 4-21.



**Figure 4-21** The graphs displayed by the Port Graph page

You can choose to display graphs for *Utilization*, *Total Errors* or *Packet Size distribution*:

To display the Utilization graph:

- 1 From the first drop-down listbox, choose a port.
- 2 From the second drop-down listbox, choose *Utilization*.
- 3 Click *Apply*.

To display the Total Errors graph:

- 1 From the first drop-down listbox, choose a port.
- 2 From the second drop-down listbox, choose *Total Errors*.
- 3 Click *Apply*.

To display the Packet Size Distribution graph:

- 1 From the first drop-down listbox, choose a port.
- 2 From the second drop-down listbox, choose *Packet Size Distribution*.
- 3 Click *Apply*.

### **Interpreting the Statistics**

- The Utilization graph scales automatically to display the percentage of bandwidth used on the port over the last hour and last 48 hours:
  - A bandwidth utilization of 0–25% indicates that the port is dealing with a light traffic load.
  - A bandwidth utilization of 26–85% indicates that the port is dealing with a normal traffic load.
  - A bandwidth utilization of 86–100% indicates that the port is dealing with a heavy traffic load. This could be caused by a fault in your network, or an inadequate network configuration.
- The Total Errors graph scales automatically to display the total number of packets with errors that have been seen on the port over the last hour and last 48 hours.
- The Packet Size Distribution graph displays the proportion of packets of certain sizes seen by the port over the last 30 seconds.



# 5

## WORKING WITH THE COMMAND LINE INTERFACE

This chapter describes how to access and use the command line interface. It covers the following topics:

- Accessing the Interface
- About the Interface Menus
- A Quick Guide to the Commands
- Viewing and Changing Information About Ports in the Stack
- Viewing and Changing IP-related Information
- Viewing and Changing Information About the Stack



*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.*

---

## Accessing the Interface

To access the command line interface, take the following steps:

- 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 “Solving Problems That Occur When 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 as described in “About the 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 “Changing Your Password” on page 5-15.

**Exiting the Interface**

You can exit the command line interface at any time; to do this, enter the command **logout** from the top level of the command line interface. If there is a period of inactivity lasting longer than 30 minutes, you exit from the command line interface automatically. After the exit, the first key that you press returns you to the login sequence.

**How Many Users Can Access the Interface?**

The command line interface can be accessed by several users at the same time:

- If the stack contains multiple Switch units, the command line interface can be accessed through each console port in the stack at the same time.
- If the stack is being managed using Telnet, the command line interface can be accessed by an unlimited number of users at the same time.

**About the Interface Menus**

Once you access the command line interface, the Top-level menu is displayed as shown in Figure 5-1.

```
Menu options: ----- IBM 8271 Nways LAN Ethernet Model F24 -----
ethernet      - Administer Ethernet ports
ip            - Administer IP
logout        - Logout of the Command Line Interface
system        - Administer system-level functions

Type ? for help.
----- Floor 1, Accounts -----
```

```
Select menu option :
```

**Figure 5-1** Top-level menu

The command line interface is made up of two areas:

- *The Menu Area* — Contains the current menu of commands. The menu can contain commands to configure the stack or commands to display other menus in the command line interface. Each command is accompanied by a brief description of its purpose.
- *The Command Area* — Contains a `Select menu option` prompt where you can enter the commands displayed in the menu area.

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

- **Ethernet Menu**

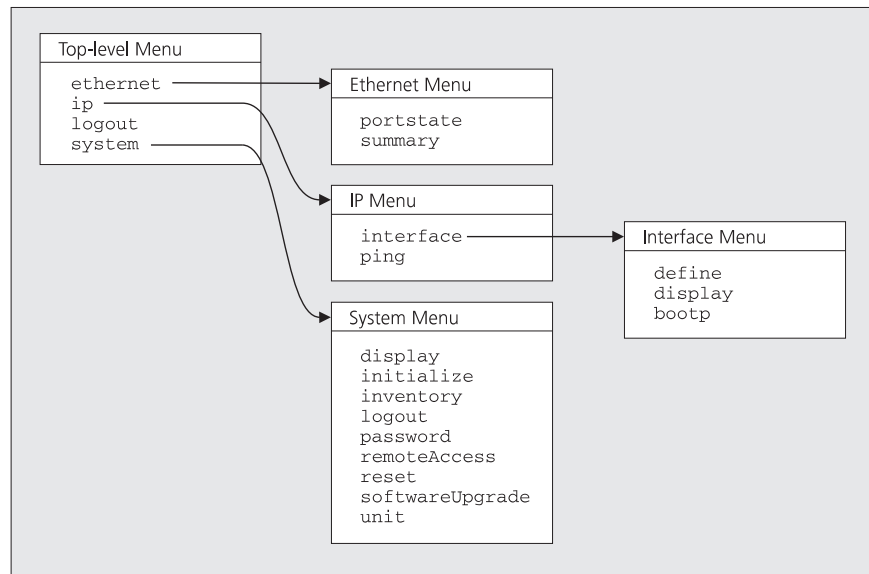
This menu contains commands that allow you to enable or disable the ports in the stack, and view status information about them.

- **IP Menu**

This menu contains commands that allow you to view and change IP-related information for the stack and PING other devices in your network.

- **System Menu**

This menu contains commands that allow you to view and configure information about the Switch units in the stack or the stack as a whole.



**Figure 5-2** Command line interface menu structure

### Entering Commands

The command area of the command line interface contains a `Select menu option` prompt that allows you to enter the commands in the menu area:

- **To enter a simple command:**

At the prompt, enter the name of the command.



- **To enter multiple commands:**

At the prompt, enter each command in succession. For example, to display the system menu and then reset the Switch units in the stack, enter:

```
Select menu option: system reset
```

- **To enter commands that require values:**

Append the values to the name of the command. For example, to display the system menu and then change the password for your user, enter:

```
Select menu option: system password <password>
```

If you do not specify values for a command that requires them, you are prompted to enter the values. At each prompt, the default value is displayed in brackets.

- **To enter abbreviated commands**

At the prompt, enter enough characters to uniquely identify the commands. For example, to display the system menu and then change the password for your user, enter:

```
Select menu option: sy pa <password>
```

## Displaying Menus

There are several ways to display the menus in the command line interface menu structure:

- **To display sub-menus:**

At the Select menu option prompt, enter the name of the menu or menus.

- **To display parent menus:**

At the Select menu option prompt, enter **q**.

- **To display the Top-level menu:**

Press the [Esc] key.

## Obtaining Help

You can access the command line interface help system at any time by entering **?** at the Select menu option prompt.

## A Quick Guide to the Commands

Table 5-1 describes the commands that are available in the command line interface.

**Table 5-1** Command line interface commands

Command	What does it do?
<code>logout</code>	Exits the current user from the command line interface.
<code>(ethernet) portstate</code>	Enables and disables Ethernet ports on the current Switch unit in the stack.
<code>(ethernet) summary</code>	Displays information about the ports on the current Switch unit in the stack.
<code>(ip/interface) bootp</code>	Enables and disables BOOTP for the current Switch in the stack.
<code>(ip/interface) define</code>	Specifies the IP information for the current Switch in the stack.
<code>(ip/interface) display</code>	Displays the IP information for the current Switch in the stack.
<code>(ip) ping</code>	Allows you to PING other devices on your network.
<code>(system) display</code>	Displays configuration information for the current Switch unit in the stack.
<code>(system) initialise</code>	Initialises the Switch units in the stack.
<code>(system) inventory</code>	Displays a list of the units in the stack.
<code>(system) logout</code>	Returns the focus of the command line interface to the previous Switch unit in the stack.
<code>(system) password</code>	Specifies the password for the current user.
<code>(system) remoteAccess</code>	Enables and disables all forms of remote access to the stack.
<code>(system) reset</code>	Resets the Switch units in the stack.
<code>(system) softwareUpgrade</code>	Allows you to upgrade the management software of the Switch units in the stack.
<code>(system) unit</code>	Moves the focus of the command line interface from one Switch unit in the stack to another.

## Viewing and Changing Information About Ports in the Stack

You can view and change information about the ports on the current Switch unit in the stack using the commands on the Ethernet menu. These commands allow you to:

- Enable and disable Ethernet ports on the Switch
- View information about the status of Ethernet ports on the Switch



*To view and change information about the ports on another Switch unit in the stack, you need to select that unit using the `unit` command. For more information, see "Moving the Focus of the Command Line Interface" on page 5-12.*

## Enabling and Disabling Ports

You can enable and disable Ethernet ports on the Switch using the `portstate` command on the Ethernet menu.



*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 following prompt is displayed:

```
Select Ethernet port(s) (1-24|all):
```



*For the Model F12/F24, ports 1 to 24 are the 10BASE-T/100BASE-TX ports. Any additional ports provided through an Expansion Module are numbered 25 and onwards.*

- 2 Enter the number of the port to be enabled or disabled.

The following prompt is displayed:

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

- 3 Enter **disabled** or **enabled**.

### Viewing Port Status Information

You can view information about the status of Ethernet ports on the Switch using the `summary` command on the Ethernet menu.

To view the port status information:

- 1 At the Top-level menu, enter:

```
ethernet summary
```

The following prompt is displayed:

```
Select Ethernet port (1-24|all):
```



*For the Model F12/F24, ports 1 to 24 are the 10BASE-T/100BASE-TX ports. Any additional ports provided through an Expansion Module are numbered 25 and onwards.*

- 2 Enter the number of a port, or enter `all` for all the ports.

The port status information for the port(s) is displayed.

An example of the port status information is shown below:

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

The statistics that are displayed are gathered in the time interval since the last reset, initialization or power-off/on cycle.

### Viewing and Changing IP-related Information

You can view and change IP-related information for the current Switch unit in the stack using the commands on the IP menu. These commands allow you to:

- Specify the IP and SLIP information for the Switch
- Display the IP information for the Switch
- Specify whether the Switch uses BOOTP
- PING other devices on your network



*To view and change IP-related information for another Switch unit in the stack, you need to select that unit using the `unit` command. For more information, see "Moving the Focus of the Command Line Interface" on page 5-12.*

## Specifying IP and SLIP Information

You can specify IP and SLIP information for the current Switch unit in the stack using the `define` command on the Interface menu, which is accessed from the IP menu.

To specify the IP and SLIP information:

- 1 At the Top-level menu, enter:

```
ip interface define
```

The following prompt is displayed, allowing you to enter an IP address for the Switch:

```
Enter IP address [0.0.0.0]:
```



*For more information about IP addresses, see “IP Addresses” on page 3-8.*

- 2 Enter a valid IP address.

The following prompt is displayed, allowing you to enter a subnet mask for the Switch:

```
Enter subnet mask [255.255.0.0]:
```



*For more information about subnet masks, see “Subnets and Using a Subnet Mask” on page 3-8.*

- 3 Enter a subnet mask, if required.

The following prompt is displayed, allowing you to enter the IP address of the default router in your network:

```
Enter default gateway [0.0.0.0]:
```

- 4 If your network contains a router, enter the IP address.

The following prompt is displayed:

```
Enter SLIP address [0.0.0.0]:
```

If you want to manage the stack using the web interface through the console port of the Switch, you need to set up Serial Line Interface Protocol (SLIP) information for the Switch. A SLIP address is similar to an IP address, but it is used for serial line connections to console ports. We recommend that you use the address 192.168.101.1. *For more information, see “Using the Serial Web Utility” on page B-1.*

- 5 Enter a SLIP address, if required.

The following prompt is displayed:

```
Enter SLIP subnet mask [255.255.0.0]:
```

A SLIP subnet mask is similar to an IP subnet mask, but, like the SLIP address, it is used for serial line connections to console ports.

- 6 Enter a SLIP subnet mask, if required.



*If you change the IP address of the Switch, you can no longer access the command line interface unless you specify that your terminal or terminal emulator is to use the new IP address.*

### Displaying IP and SLIP Information

You can display IP and SLIP information for the current Switch unit in the stack using the `display` command on the Interface menu, which is accessed from the IP menu.



*For more information about IP and SLIP, see “Managing the Stack Over the Network” on page 3-7.*

To display the IP and SLIP information:

- At the Top-level menu, enter:

```
ip interface display
```

The IP and SLIP information for the Switch is displayed.

An example of the IP and SLIP information is shown below:

```
IP address           191.128.40.120
Subnet mask:         255.255.0.0
Default gateway:     191.128.40.120
SLIP address:        192.168.101.1
SLIP subnet mask    255.255.0.0
```

### Specifying Whether the Switch Uses BOOTP

If you have a BOOTP server on your network, you can use that server to allocate IP information for the Switch units in the stack automatically.

You can specify whether the Switch uses BOOTP by using the `bootp` command on the Interface menu, which is accessed from the IP menu.

To specify that the Switch uses BOOTP:

- 1 At the Top-level menu, enter:

```
ip interface bootp
```

The following prompt is displayed:

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

- 2 Enter **enabled** to specify that the Switch uses BOOTP, or **disabled** to specify that it does not.

### **Pinging Other Devices On Your Network**

The PING feature allows you to send out a PING request to test whether devices on your network are accessible and functioning correctly. This feature is useful for testing that the stack is installed and set up correctly, and that your network connections are working.

You can PING other devices on your network using the `ping` command on the IP menu.

To PING a device:

- 1 At the top-level menu, enter:

```
ip ping
```

The following prompt is displayed:

```
Enter destination IP address:
```

- 2 Enter the IP address of the device that you want to PING.

The stack sends a single PING request to the specified device and a message similar to the following is displayed:

```
Starting ping, resolution of displayed time is 10 milli-sec  
response from 191.128.40.121: 3 router hops. time = 10ms
```

If the device is accessible and functioning correctly, a message similar to the following is displayed:

```
191.128.40.121 is alive
```

If the device is not accessible, or is not functioning correctly, a message similar to the following is displayed:

```
No answer from 191.128.40.121
```

## Viewing and Changing Information About the Stack

You can view and change information about the Switch units in the stack or the stack as a whole using the commands on the System menu. These commands allow you to:

- Move the focus of the command line interface from one Switch unit in the stack to another
- Display configuration information about the current Switch unit in the stack
- Display summary information about the Switch units in the stack
- Change the password for the current user
- Enable and disable all forms of remote access to the stack
- Reset the Switch units in the stack
- Initialise the Switch units in the stack
- Upgrade the management software of the Switch units in the stack

## Moving the Focus of the Command Line Interface

Many commands in the command line interface perform their actions on a single Switch unit in the stack — the current Switch. You can move the focus of the command line interface from one unit in the stack to another using the `unit` command on the System menu.

To move the focus:

- 1 At the top level menu, enter:

```
system unit
```

The following prompt is displayed, allowing you to enter a unit number:

```
Select unit [1]:
```



*You can have up to four Switch units in a stack:*

- *If the stack contains one unit, that unit is unit 1*
- *If the stack contains two units connected using a Matrix Cable, the first unit to be powered-up is unit 1 and the other unit is unit 2.*
- *If the stack contains a number of units connected using a Matrix Module, the unit containing the Module is unit 1 and the other unit numbers are defined by the port connections on the Module.*

- 2 Enter the number of the unit to be managed.



## Returning the Focus to the Previous Switch Unit

You can return the focus of the command line interface to the previous Switch unit in the stack using the `logout` command on the System menu.

## Displaying Configuration Information About the Current Switch

You can display configuration information about the current Switch unit in the stack using the `display` command on the System menu. This information may be useful for your technical support representative if you have a problem.

To display the information:

- From the top-level menu, enter:

```
system display
```

The configuration information is displayed.

An example of the information is shown below:

```
IBM 8271 Nways Ethernet Switch Model F24
Unit Name: Development
Location: Wiring closet, Floor 2
Contact: Edward Monk
Time since reset: 2 days, 3 hours, 10 minutes
Operational Version: 1.00      Boot Version: 1.00
Hardware Version: 1.00
Serial Number: 2103332
```

The configuration information contains the following read-only fields:

### Unit Name

Displays the descriptive name, or system name, for the unit. For information about assigning a new name, see “Specifying a Descriptive Name for the Stack” on page 4-21.

### Location

Displays the physical location of the unit. For information about assigning a new location, see “Specifying the Physical Location of the Stack” on page 4-23.

### Contact

Displays the details of a person to contact in the event of an emergency. For information about assigning new contact details, see “Specifying a Contact for the Stack” on page 4-25.

**Time Since Reset**

Displays the time that has elapsed since the unit was last reset, initialised or powered-up.

**Operational Version**

Displays the version number of the management software currently installed on the unit. For information about how to upgrade the management software, see “Upgrading the Management Software of the Stack” on page 5-18.

**Boot Version**

Displays the version of Boot PROM software installed on the unit.

**Hardware Version**

Displays the version number of the unit hardware.

**Serial Number**

Displays the serial number of the unit.

### Displaying Summary Information About the Switch Units in the Stack

You can display summary information about the Switch units in the stack using the `inventory` command on the System menu.

To display the information:

- From the top-level menu, enter:

```
system inventory
```

The summary information is displayed.

An example of the summary information is shown below:

<b>Position</b>	<b>Description</b>	<b>Name</b>	<b>State</b>
1	Switch Model E12	Accounts	Operational
2	Switch Model E24	Development	Operational
3	Switch Model F12	Accounts	Loading
4	Switch Model F24	Accounts	Operational

The summary information contains the following read-only fields:

**Position**

This field displays the number of the unit in the stack.



You can have up to four Switch units in a stack:

- If the stack contains one unit, that unit is unit 1
- If the stack contains two units connected using a Matrix Cable, the first unit to be powered-up is unit 1 and the other unit is unit 2.
- If the stack contains a number of units connected using a Matrix Module, the unit containing the Module is unit 1 and the other unit numbers are defined by the port connections on the Module.

### Description

The field displays the product name of the unit.

### Name

This field displays the descriptive name, or system name, for the unit. For information about assigning a new name, see “Specifying a Descriptive Name for the Stack” on page 4-21.

### State

This field displays the current operating state of the unit:

- *Operational* — The unit is operating normally.
- *Loading* — A process taking place on the unit, for example a software upgrade.

## Changing Your Password

You can change the password for the current user using the `password` command on the System menu.

To change the password:

- 1 At the top-level menu, enter:

```
system password
```

The following prompt appears, allowing you to enter the existing password:

```
old password
```

- 2 Enter the existing password.

The following prompt is displayed, allowing you to enter a new password for the current user:

```
Enter new password
```

- 3 Enter the new password.

The following prompt is displayed, allowing you to re-enter the new password as conformation:

```
Retype password:
```

A message is displayed informing you that the password has been successfully changed.

### Enabling and Disabling Remote Access to the Stack

As a basic security measure, you can enable or disable remote access to the management software of the stack:

- When remote access is enabled, you can access the management software using all management methods.
- When remote access is disabled:
  - Users cannot access the stack over the network using the command line interface
  - Users cannot access the stack over the network using the web interface
  - Users cannot access the Switch using an SNMP Network Manager
  - Users can only access the command line interface or web interface using a direct connection the console port of a Switch unit in the stack.

You can enable or disable remote access to the management software of the stack using the `remoteAccess` command on the System menu.

To enable or disable remote access:

- 1 At the top-level menu, enter:

```
system remoteAccess
```

- 2 The following prompt is displayed:

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

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

## Resetting the Switch Units in the Stack

You can reset the Switch units in the stack using the `reset` command on the System menu.

To reset the units:

- 1 At the top-level menu, enter:

```
system reset
```

The following prompt is displayed:

```
Are you sure you want to reset the system (y/n) [y]:
```

- 2 Enter **y** if you wish to proceed, or **n** if you want to stop the reset.

### What Happens During a Reset?

Resetting the Switch units in the stack simulates a power-off/on cycle. 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 command line interface cannot communicate with the stack.*

## Initializing the Switch Units in the Stack

You can initialise the Switch units in the stack using the `initialise` command on the System menu.

To initialise the units:

- 1 At the top-level menu, enter:

```
system initialise
```

The following prompt is displayed:

```
Do you wish to continue (y/n) [y]:
```

- 2 Enter **y** if you wish to proceed, or **n** if you want to stop the initialization.

### What Happens During an Initialization?

Initializing the Switch units in the stack returns them to their default (factory) settings. You may want to do this if the stack has previously been used in a different part of your network, and its settings are incorrect for 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.



**ATTENTION:** When initializing the stack, note that 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 initialise. While the stack is initializing, the command line interface cannot communicate with the stack.

### Upgrading the Management Software of the Stack

You can upgrade the management software of the Switch units in the stack using the `softwareUpgrade` command on the System menu.

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, see the documentation that accompanies it.

- 2 From the Top-level menu, enter:

```
system softwareUpgrade
```

The following prompt is displayed:

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

- 3 Enter the IP address of the TFTP server that holds the software upgrade file. The file must be stored somewhere that is accessible to the TFTP load request. Contact your system administrator if you are unsure where to place the image file.

The following prompt is displayed:

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

- 4 Enter the name of the software upgrade file. The filename format is:

nwsxx\_yy.bin

where xx\_yy is the version of management software.

During the upgrade, the Power/Self Test LED flashes green and the command line interface is locked. The upgrade takes about 5 minutes; when the upgrade is complete, the message `Installation Complete` is displayed and the Switch units in the stack are reset.



**ATTENTION:** *During the upgrade, do not power-down or reset any Switch units in the stack.*







# ADVANCED NETWORKING FEATURES

Chapter 6 Spanning Tree Protocol

Chapter 7 RMON



# 6

## SPANNING TREE PROTOCOL

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

This chapter explains more about STP and the STP features supported by the stack. It covers the following topics:

- What is STP?
- How STP Works
- Enabling STP on a Stack



*STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP more effectively, the stack will be defined as a bridge.*

## What is STP?

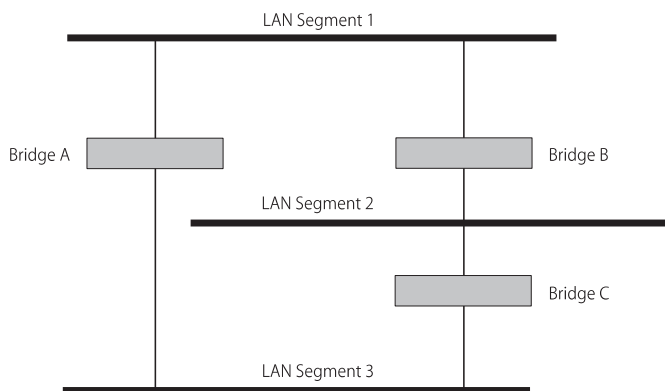
STP is a bridge-based system for providing fault tolerance on networks. It allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational
- Redundant paths are enabled if the main paths fail

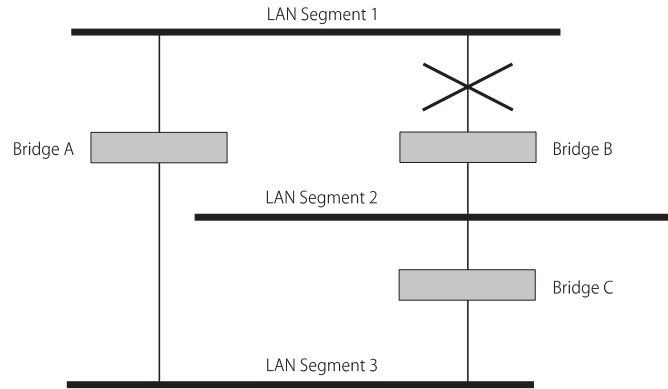
As an example, Figure 6-1 shows a network containing three LAN segments separated by three bridges. With this configuration, each segment can communicate with the others using two paths. This configuration creates loops which cause the network to overload; however, STP allows you to have this configuration 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.

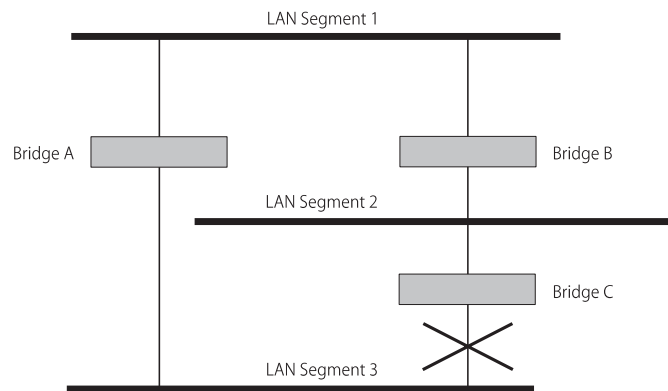
If the link through Bridge C fails, as shown in Figure 6-3, the STP system reconfigures the network so that traffic from segment 2 flows through Bridge B.



**Figure 6-1** A network configuration that creates loops



**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:

- 1 Each network segment has one Designated Bridge Port. All traffic destined to pass in the direction of or through the Root Bridge flows through this port. The Designated Bridge Port is the port which has the lowest Root Path Cost for the segment.

The Root Path Cost consists of the path cost of the Root Port of the bridge, plus the path costs across all the Root Ports back to the Root Bridge. Table 6-1 shows the default path costs for the stack.

**Table 6-1** Default path costs

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

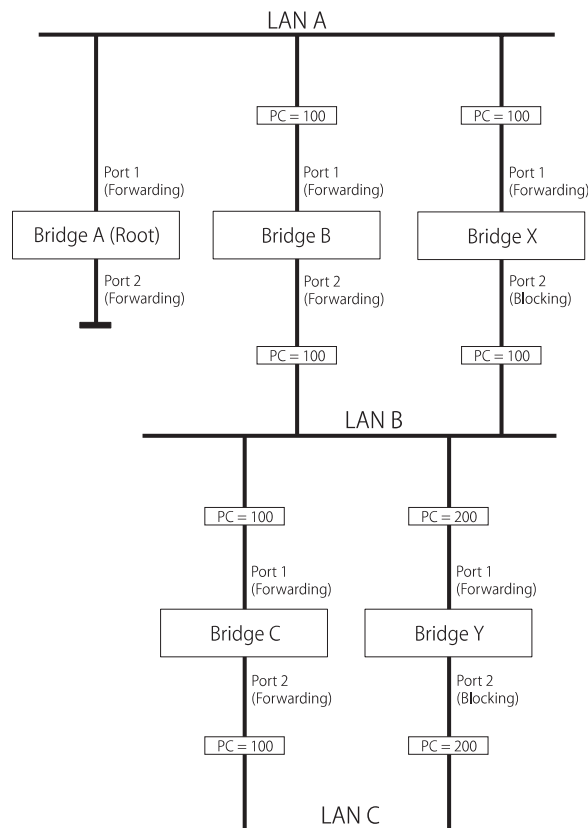
- After all the bridges on the network have determined the configuration of their ports, each bridge only forwards traffic between the Root Port and the ports that are the Designated Bridge Ports for each network segment. All other ports are *blocked*, which means that they are prevented from forwarding 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).



**Figure 6-4** Port costs in a network

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 has a cost of 200, the route through Bridge Y and B has a cost of 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 bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. The bridge then initiates a reconfiguration of the network topology.

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

## STP Configurations

Figure 6-5 shows two possible STP configurations using IBM 8271 Nways units:

### ■ 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 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.

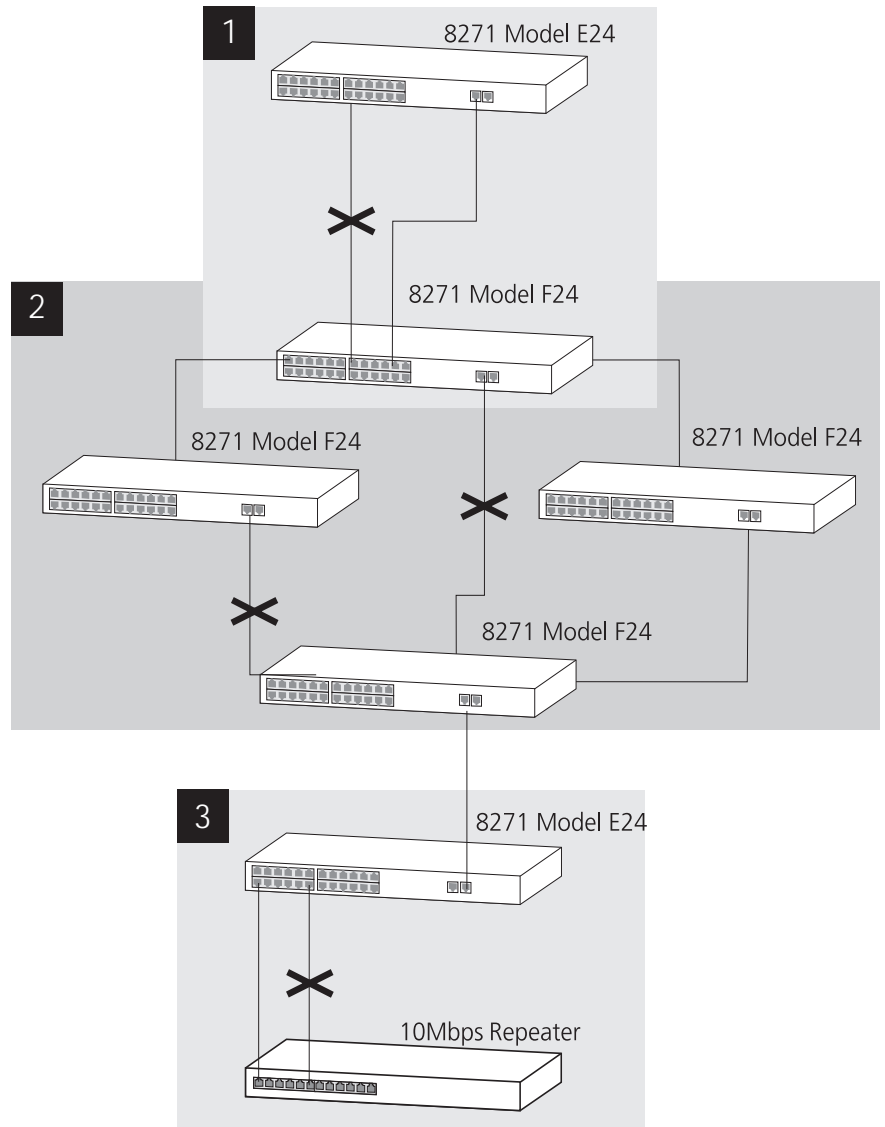
### ■ Configuration 2 — Redundancy through Meshed Backbone

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

## Enabling STP on a Stack

To enable STP on a stack:

- 1 From the web interface, click the *Configuration* icon on the side-bar. The Stack Setup page is displayed.
- 2 From the *Spanning Tree* drop-down listbox, select Enabled.



*You cannot enable STP if you have set up resilient links on any of the stack ports.*

# 7

## RMON

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

This chapter explains more about the RMON concept and the RMON features supported by the stack. It covers the following topics:

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



*You can only use the RMON features of the stack if you have an RMON management application, or using a MIB browser.*

## What is RMON?

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

A typical RMON setup consists of two components:

- **The RMON probe** — An intelligent, remotely-controlled device or software agent that continually collects statistics about a LAN segment, 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

The Filter group provides a mechanism to instruct the RMON probe to capture packets that match a specific criterion or condition. The group is not supported in this release of software.

### Capture

The Capture group allows you to create capture buffers on the probe that can be requested and uploaded to the management workstation for decoding and presentation. The group is not supported in this release of software.

### 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 stack 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 Stack**

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 stack. This allows RMON to be widely deployed around the network without costing more than traditional network management.

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

For example, statistics can be related to individual ports and the stack 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 stack means all ports can have security features enabled.

**RMON Features of  
the Stack**

Table 7-1 details the RMON support provided by the stack.

**Table 7-1** RMON support supplied by the stack

<b>RMON Group</b>	<b>Support supplied by the stack</b>
<b>Statistics</b>	A new or initialized stack has one Statistics session per port.
<b>History</b>	A new or initialized stack has two History sessions per port. These sessions provide the data for the unit and port graphs of the web interface: <ul style="list-style-type: none"> <li>■ 30 second intervals, 10 historical samples stored</li> <li>■ 30 minute intervals, 10 historical samples stored</li> </ul>
<b>Alarms</b>	Although up to 200 alarms can be defined for the stack, a new or initialized stack has two alarms defined for each port: <ul style="list-style-type: none"> <li>■ Broadcast bandwidth used</li> <li>■ Percentage of errors over one minute</li> </ul> <p>You can modify these alarms using an RMON management application, but you cannot create or delete them.</p> <p>For more information about the alarms setup on the stack, see "About Alarm Actions" on page 7-7 and "About Default Alarm Settings" on page 7-8.</p>
<b>Hosts</b>	Although Hosts is supported by the stack, there are no Hosts sessions defined on a new or initialized stack.
<b>Hosts Top N</b>	Although Hosts Top N is supported by the stack, there are no Hosts Top N sessions defined on a new or initialized stack.
<b>Matrix</b>	Although Matrix is supported by the stack, there are no Matrix sessions defined on a new or initialized stack.
<b>Filter</b>	The Filter group is not presently supported by the stack.
<b>Capture</b>	The Capture group is not presently supported by the stack.
<b>Events</b>	A new or initialized stack has events defined for use with the default alarm system, see "About Default Alarm Settings" on page 7-8 for more information.

When using the RMON features of the stack, 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 stack 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 stack. The forwarding performance of the stack 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.

## About Alarm Actions

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

**Table 7-2** Alarm Events

<b>Event</b>	<b>Action</b>
<b>No action</b>	
<b>Notify only</b>	Send Trap.
<b>Notify and filter port</b>	Send Trap. Block broadcast and multicast traffic on the port. Recovers with the <i>unfilter port</i> event.
<b>Notify and disable port</b>	Send Trap. Turn port off.
<b>Notify and enable port</b>	Send Trap. Turn port on.
<b>Disable port</b>	Turn port off.
<b>Enable port</b>	Turn port on.
<b>Notify and switch resilient port</b>	Send Trap. If port is the main port of a resilient link pair then move to standby.
<b>Notify and unfilter port</b>	Send Trap. Stop blocking broadcast and multicast traffic on the port.
<b>Set Forwarding Mode to Store and Forward</b>	
<b>Set Forwarding Mode to Fast Forward</b>	
<b>System started</b>	
<b>Software Upgrade report</b>	

### About Default Alarm Settings

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

- Broadcast bandwidth used
- Percentage of errors over one minute

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

**Table 7-3** Values for the default alarms

Statistic	High Threshold	Low Threshold Recovery	Period
Broadcast bandwidth used	Value: 20% Action: Notify and filter	Value: 10% Action: Notify and unfilter	20 secs
Percentage of errors over one minute	Value: 20 errors per second Action: Set Forwarding Mode to Store and Forward	Value: 1 error per second Action: Set Forwarding Mode to Fast Forward	60 secs

### About the Audit Log

The stack 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

Chapter 8 Problem Solving



# 8

## PROBLEM SOLVING

This chapter contains a list of known problems and suggested solutions. It covers the following topics:

- Solving Problems Indicated by LEDs
- Solving Problems That Occur When Using the Web Interface
- Solving Problems That Occur When Using the Command Line Interface
- Solving Problems That Occur When Using an SNMP Network Manager
- Solving Problems With the Serial Web Utility
- Solving Problems With the Management Software Upgrade Utility
- Solving Other Problems

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

---

## Solving Problems Indicated by LEDs

**A Power LED does not light.** Check that the power cable is firmly connected to the relevant Switch unit and to the supply outlet. If the connection is secure and there is still no power, you may have a faulty power cord.

**On powering-up, a Power/Self Test LED lights yellow.** The relevant Switch unit has failed its Power On Self Test (POST) because of an internal problem. Contact your supplier for advice.

**An Expansion Module Port Status LED flashes yellow.** An unrecognized Expansion Module or Matrix Module is installed into the relevant Switch unit. You may need to remove the Module, or upgrade the management agent software used by the stack to a version that recognizes the Module (see “Upgrading the Management Software of the Stack” on page 4-35 or page 5-18). Contact your supplier for further advice.

**A link is connected and yet the Status LED for the port 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 that is MDIX-only

---

## Solving Problems That Occur When Using the Web Interface

**The Web browser cannot access the stack.** Check that:

- The IP information for the stack is correctly configured. See “Setting Up IP Information for the Switch” on page 4-15 or “Specifying IP and SLIP Information” on page 5-9 for more information.
- If you are managing the stack over the network, remote access to the management software of the stack is enabled. For more information, see “Enabling and Disabling Remote Access to the Stack” on page 5-16.

**The Web browser cannot access the stack over a serial link from a management station running Windows 95.** You must access the stack using the Serial Interface Utility (SLIP Driver) available on the CD-ROM supplied with the Switch; see “Using the Serial Web Utility” on page B-1.

**The Web browser can no longer access the stack over the network.** Check that:

- Remote access to the management software of the stack has not been disabled. For more information, see “Enabling and Disabling Remote Access to the Stack” on page 5-16.
- The port through which you are trying to access the stack has not been disabled. For more information, see “Viewing the Status of the Ports” on page 4-12 or If it is enabled, check the connections and network cabling for the port.

If there is still a problem, try accessing the stack through a different port. If you can now access the stack, a problem may have occurred with the original port. Contact your supplier for further advice.

**Some of the web interface is not displayed in the Web browser after downloading.** This is probably due to large amounts of traffic on the network. Either reload the web interface page, or click in the part of the interface that has not displayed and select the reload frame option in your Web browser.

**The web interface takes time 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 limit the number of users with access.

**"URL not found" messages are displayed when the Help or Documentation icons are clicked.** The web interface cannot access the online help or online documentation files. For more information, see “Installing Online Help and Documentation” on page 3-4.

**"URL not found" messages are displayed when the Library or Support icons are clicked.** Your management workstation 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 a small 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*.
- 3 The *Preferences* dialog box appears.
- 4 Check the *Every Time* checkbox.
- 5 Click *OK*.

To do this for Microsoft Internet Explorer Version 3.0:

- 1 Start Microsoft Internet Explorer.
- 2 From the *View* menu, select *Options*.
- 3 The *Options* dialog box appears.
- 4 Select the *Advanced* tab, and in the *Advanced* property sheet click *Settings*.
- 5 Check the *Every visit to the page* checkbox.
- 6 Click *OK*.

**You forget your password while logged out of the web interface and cannot log in.** Ask another user with Security access level to log in and initialize the stack. This returns the Switch units in the stack to their default (factory) settings, including any password information.

In the case where no-one knows a password for a user with 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 that is not possible, separate each Switch from the stack and use the Management Software Upgrade Utility to upgrade it through the console port. For more information about the Management Software Upgrade Utility, see "Using the Upgrade Utility" on page C-1.



---

## Solving Problems That Occur When Using the Command Line Interface

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

- Your terminal or terminal emulator is correctly configured to operate as a generic (TTY) terminal, or a VT100 terminal.
- You have performed the command line interface wake-up procedure by pressing [Return] a few times.
- The settings on your terminal or terminal emulator are correct:
  - 8 data bits
  - no parity
  - 1 stop bit

The auto-configuration feature of each Switch in the stack only works with line speeds from 1200 to 19200 baud.

- Remote access to the management software of the stack is enabled if you are managing the stack over the network. For more information, see “Enabling and Disabling Remote Access to the Stack” on page 5-16.

If the login sequence still does not display, reset the stack. For more information, see “Resetting All the Units in the Stack” on page 4-33 or page 5-17. If this does not work, initialize the stack. For more information, see “Initializing All the Units in the Stack” on page 4-34 or page 5-17.

**The terminal or terminal emulator can no longer access the device over the network.** Check that:

- Remote access to the management software of the stack has not been disabled. For more information, see “Enabling and Disabling Remote Access to the Stack” on page 5-16.
- The port through which you are trying to access the stack has not been disabled. For more information, see “Viewing the Status of the Ports” on page 4-12 or If it is enabled, check the connections and network cabling for the port.

If there is still a problem, try accessing the stack through a different port. If you can now access the stack, a problem may have occurred with the original port. Contact your supplier for further advice.

**You forget your password and cannot log in.** Ask another user with Security access level to log in and initialize the stack. This returns the Switch units in the stack to their default (factory) settings, including any password information.

In the case where no-one knows a password for a user with Security access level, contact your supplier.

**A management software upgrade has failed, and you can no longer manage the stack using the command line interface.** Try accessing the web interface and upgrading the stack again. If that is not possible, separate each Switch from the stack and use the Management Software Upgrade Utility to upgrade it through the console port. For more information about the Management Software Upgrade Utility, see “Using the Upgrade Utility” on page C-1.

---

### Solving Problems That Occur When Using an SNMP Network Manager

**The SNMP Network Manager cannot access the stack.** Check that:

- The IP information for the stack is correctly configured. See “Setting Up IP Information for the Switch” on page 4-15 or “Specifying IP and SLIP Information” on page 5-9 for more information.
- The stack was reset after the IP information was defined.
- The IP information for the stack is correctly recorded by the Network Manager. For more information, see the documentation supplied with your Network Manager.
- Remote access to the management software of the stack is enabled. For more information, see “Enabling and Disabling Remote Access to the Stack” on page 5-16.

**Traps are not received by the SNMP Network Manager.** Check that the IP information of the SNMP Network Manager is correctly recorded by the stack.

**The SNMP Network Manager can no longer access the stack.**

Check that:

- Remote access to the management software of the stack has not been disabled. For more information, see “Enabling and Disabling Remote Access to the Stack” on page 5-16.
- The port through which you are trying to access the stack has not been disabled. For more information, see “Viewing the Status of the Ports” on page 4-12 or If it is enabled, check the connections and network cabling for the port.

If there is still a problem, try accessing the stack through a different port. If you can now access the stack, a problem may have occurred with the original port. Contact your supplier for further advice.

---

**Solving Problems  
With the Serial  
Web Utility****You cannot connect to the web interface of the Switch.**

Check that:

- The Switch is powered-up.
- You are using a proper null modem cable. Pin-outs are detailed in [“Pin-outs”](#) on page D-1.
- The flow control and line speed (baud rate) settings are the same on the Switch and on the management workstation:
- You have not changed the line speed setting of the management workstation after the Switch has connected (the Switch only configures its line speed the first time it connects).
- You have selected the correct serial port on your management workstation.

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

---

## Solving Problems With the Management Software Upgrade Utility

**An error occurs when the utility attempts to connect through the serial port of the PC.** 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 occurs when the utility attempts to communicate with the Switch.** There could be a number of reasons for this:

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

Retry the command ensuring that you follow all the steps.

**An error occurs when the utility attempts 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 properties of the file using Explorer (in Windows 95) or File Manager (in other versions of Windows).

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

**An error occurs when the utility attempts to transfer the file.**

There could be a number of reasons for this:

- The null modem cable has become disconnected from the Switch 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 is being specified and transferred to the Switch. Check the filenames and start again.

---

**Solving Other Problems**

**You have added the stack to an already busy network, and response times and traffic levels have increased.** You may have added a group of users to one of the stack ports via a repeater, and not disabled half duplex flow control for the port. Disable half duplex flow control for all ports that are operating in half duplex and are connected to multiple devices using a repeater. Disabling half duplex flow control is described in "Configuring a Port on the Switch" on page 4-16.

**You have enabled auto-negotiation for a 10BASE-T/100BASE-TX port, and you are seeing a large number of late events on the port.** The port connected to the stack is not auto-negotiating and is operating in full duplex:

- If you want the link to operate in full duplex, set the port on the stack to operate in full duplex. For more information, see "Configuring a Port on the Switch" on page 4-16.
- If you want the link to operate in half duplex, set the port on the other end of the link to operate in half duplex. For more information, see the documentation supplied with the remote device.



# V

## APPENDICES AND INDEX

- Appendix A Safety Information
- Appendix B Using the Serial Web Utility
- Appendix C Management Software Upgrade Utility
- Appendix D Pin-outs
- Appendix E Switch Technical Specifications
- Appendix F Technical Support and Service
- Appendix G Notices, Trademarks, and Warranties
- Glossary
- 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)
<b>U.S.A. and Canada</b>		
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)
<b>Latin America</b>		
Argentina Columbia	Paraguay Uruguay	6952291 (F/C 6862)
Chile		14F0069 (F/C 6858)

---

(continued)

\* 125V/10A

<b>Country</b>		<b>Part Number (Feature Code)</b>	
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		
<hr/>			
<b>Europe, Middle East, and Africa</b>			
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)

<b>Country</b>		<b>Part Number (Feature Code)</b>
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)
<b>Asia Pacific</b>		
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 Ofcom 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 por pessoal especializado.



**Fare!** Installation og afmontering af enheden skal udføres afuddannet personale.



**Gevaar:** Installatie en verwijdering van de eenheid moet uitsluitend worden uitgevoerd door getraind personeel.



**Verra:** Yksikön saavat asentaa ja irrottaa vain tähän koulutetut henkilöt.



**Pericolo:** L'installazione e la rimozione dell'unità devono essere eseguite esclusivamente da personale specializzato.



**Fare:** Det er bare kvalifisert personale som kan installere og ta ut enheten.



**Perigo:** A instalação e a remoção da unidade devem ser efectuadas apenas por pessoal qualificado.



**Peligro:** La instalación y extracción de la unidad debe efectuarse únicamente por personal cualificado.



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



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.



Neodstrajajte deskni modul, ako je priključeno napajanje.



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 nærheten av enheten, og er tilgjengelig. Du kan bare frakoble enheten ved å trekke ut apparatledningen fra enheten.



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



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



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



请将主插座安装在设备的附近, 以便使用. 您可从设备上移去电器。



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



Je nezbytné, aby si ova zasuvka byla instalována blízko za izení a byla přístupná. Za izení můžete odpojit pouze vytažením napájecího kabelu ze za izení.



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



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



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



주요 소켓 콘센트는 반드시 가까이에 설치되어서 접근하기 쉬워야 합니다. 연결 장치를 제거해야만 장치를 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 dôležité, aby sieťová zásuvka bola nainštalovaná v blízkosti zariadenia a bola prístupná. Zariadenie môžete vypnúť vytiahnutím sieťovej šnúry zo zariadenia.



Zelo pomembno je, da je glavna vtičnica blizu naprave in da je dostopna. Napravo je možno izkjučiti 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, главният 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 o equipamento ao qual ela está conectada também funcionar sob a condição SELV.



**Fare!** Denne enhed fungerer ved svagstrøm i henhold til betingelserne i 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 Low Voltage) -suojajännitepiirejä. Yksikkö täyttää standardissa kuvatut ehdot vain, jos laite, johonyksikkö liitetään, käyttää SELV-piirejä.



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



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



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



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



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

om utrustning till vilken enheten ansluts också arbetar med skyddsklenspänning.



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



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



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



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



Ez az egység biztonsági feszültségű (SELV) áramköri feltételek alatt üzemel, az IEC 950 (MSZ EN 60950) szabványnak megfelelően. Ezek a feltételek csak akkor maradnak fenn, ha a kapcsolódó berendezés szintén biztonsági feszültségű (SELV) 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 SELV 하에서 작동할 수 있는 경우에만 조건이 유지보수됩니다.



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



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



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



Naprava deluje pod pogoji SELV zaščite (Zaščita z Varnostno Malo Napetostjo) v skladu 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 Steckverbindingssicherung 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 strømforsyningsledningene er afmonteret, før du åbner dækslet til IEC-stikkets sikring eller enhedens dæksel.



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



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



**Fare:** Pass på at nettkabelen er frakoblet før du åpner 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.



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



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



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



I E C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 vticu 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 une alimentation redondante (RPS) recommandée.



**Gefahr:** Diese Buchsen sind nur für den Einsatz mit einer empfohlenen redundanten Stromversorgung (RPS) vorgesehen.



**Gevaar:** Deze stekkerdozen zijn ontworpen om alleen te worden gebruikt met een extra voedingseenheid.



**Perigo:** Esses soquetes foram projetados para serem utilizados apenas com uma Fonte de Alimentação Redundante recomendada.



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



**Gevaar:** Deze aansluitingen mogen alleen met een aanbevolen reservevoeding worden gebruikt.



**Vaara:** Näihin 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 utilizadas apenas com uma Redundant Power Supply (Fonte de Alimentação de Reserva) recomendada.



**Peligro:** Estos zócalos han sido diseñados para ser utilizados sólo con un fuente de alimentación redundante recomendada.



**Fara:** De här uttagen är konstruerade för att endast användas tillsammans med det rekommenderade redundanta kraftsystemet.



**危険 :**

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.



**Nebezpe í :**

Tyto zásuvky jsou navrženy pouze pro používání s doporu eným 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.



**Nezbezpečnosť:**

Tieto zásuvky sú určene iba na použitie s odporúčaným zdrojom náhradného napájania (UPS).



**Nevarnost !**

Te vtičnice so namenjene samo za uporabo s priporočenim redundantnim napajalnikom.



**危険：**

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 ungeschirmten Datenkabeln mit abgeschirmten oder ungeschirmten Klinkensteckern verbunden werden.



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



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



**Fare!** RJ45-portene er afskærmede RJ45-datasokler. De kan ikke bruges 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 afgeschermdde als niet-afgeschermdde datakabels metafgeschermdde of niet-afgeschermdde 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



taisojaamattomia 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 connettori per dati RJ45. A queste porte possono essere collegati sia cavi schermati che non schermati dotati di connettori schermati o non schermati.



**Fare:** RJ45-portene er skjermede RJ45-datauttak, og kan ikke brukes som telefonuttak. Du må bare koble RJ45-datakontakter til disse uttakene. Du kan koble enten skjermede eller ikke-skjermede datakabler med skjermede 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 intermédio de fichas blindadas ou não.



**Peligro:** Los puertos RJ45 son zócalos de datos RJ45 protegidos. No se pueden utilizar como zócalos telefónicos. Conecte sólo los conectores de datos RJ45 a estos zócalos. A estos zócalos de datos pueden conectarse tanto cables de datos protegidos como no protegidos con conectores protegidos o no protegidos.



**Fara:** RJ45-portarna är skärmade RJ45 datauttag och kan inte användas som telefonuttag. Anslut endast RJ45 datakontakter till dessa uttag. Antingen skärmade eller oskärmade datakabler 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 RJ45 data utičnice, koji se ne mogu koristiti kao telefonske utičnice. Priključite samo RJ45 data konektore na te utičnice. Oklopljeni ili neoklopljeni kablovi za prijenos podataka



**Nebezpečí :**

Porty RJ45 jsou stíněné 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, telefonáljzatnak nem használhatók. Ezekbe a foglalatokba csak RJ45 típusú adat csatlakozókat dugaszoljunk.

Ezekbe a foglalatokba akár árnyékoltt, akár árnyékolatlan adat kábelek csatlakoztathatók, árnyékoltt 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 케이블들 다 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.

**Nebezpečnostvo:**

RJ45 porty sú tienené RJ45 dátové zásuvky. Nemôžu sa používať ako telefónne zásuvky. Zapoj iba RJ45 - dátové konektory do týchto zásuviek.

Iba tienené a netienené dátové káble s tiených alebo netienených konektorov môžu byť zapojené do týchto dátových zásuviek.

**Неварност !**

Prikjučki RJ45 so oklopljene podatkovne vtičnice. Ne uporabljajte jih kot telefonske vtičnice. Vanje lahko prikjučujete samo podatkovne vtiče tipa RJ45.

Na podatkovne vtičnice lahko prikjučujete bodisi oklopljene ali neoklopljene kable z oklopljenimi ali neoklopljenimi 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 цекови.



**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.



**危險:**

电源线必須具有可用于該國家的認可。



**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:**

Verkkoliitântäjohton 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.



**Nebezpečnostwo:**

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.



**Atenție:**

Ansamblul cordonului de alimentare trebuie certificat pentru țara de utilizare.



**Опасно:**

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



**Nebezpečnostvo**

Napájecí kábel musí být schválený krajinou, v ktorej bude použitý.



**Nevarnost:**

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



**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 workstation running Microsoft Windows 95 and you want to access the web interface through the console port of a Switch, 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 for you using the Serial Line Interface Protocol (SLIP).

If you have any problems accessing the Web interface using the Serial Web Utility, see "Solving Problems With the Serial Web Utility" on page 8-7.

---

### Installing the Serial Web Utility

The Serial Web Utility can be installed on to a management workstation that already has management applications installed on it.

By default, the Serial Web Utility is installed in the following directory:

```
C:\Program Files\IBM\IBM Serial Web
```

This can be changed during the installation if required.

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 is requested.



*If the setup program cannot find specific files on your management workstation, it asks you to insert your 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 a COM port. This is the serial port on your management workstation that you want to use when connecting to the console port of the Switch.

If you click *Advanced*, the Advanced Configuration Parameters dialog box is displayed, showing all the settings that the Serial Web Utility uses when it is running. 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**

Displays the SLIP address that is to be allocated to the management workstation. The default address is 192.168.101.2.

**Device URL**

Displays the URL that the Serial Web Utility uses to access the Switch, which includes the SLIP address for the Switch. 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 serial line flow control that the management workstation uses.

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

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

Allows you to specify the line speed (baud rate) that the management workstation uses.



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 workstation. Click *Finish* to close the dialog box.
- 7 You are asked if you want to restart Windows so that it can use the new settings you have configured. You must restart Windows before running the Serial Web Utility.

When you return to your Windows desktop, the Serial Web Utility shortcut ('Serial Web Management') created by the installation program is displayed. The utility also has its own program group called Serial Web under the default program group specified during the install. This 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 running.
- 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 SLIP address for the Switch. 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 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 password panel of the Web interface is displayed. You are now ready to manage the Switch or stack; see “Working With the Web Interface” on page 4-1.

# C

## MANAGEMENT SOFTWARE UPGRADE UTILITY

The CD-ROM supplied with the Switch includes a management software upgrade utility. This utility can be used to upgrade the management software of the Switch if a previous software upgrade has failed, and you are unable to communicate with the Switch using the web interface. You can find the utility in the following directory:

Agent/Update/



*Only use this utility if a previous software upgrade has failed. At all other times you should use the web interface or command line interface to upgrade your Switch.*

If you have any problems using the management software upgrade utility, see "Solving Problems With the Management Software Upgrade Utility" on page 8-8.

---

### 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 30 minutes.*

To upgrade the management software of a Switch:

- 1 Connect the serial (COM) port of your PC to the console port of the Switch using a null modem cable.
- 2 Insert the CD-ROM into your CD-ROM drive.
- 3 If you are using Windows 3.1, close it down so that you are at the MS-DOS prompt. If you are using Windows 95, open an MS-DOS window.
- 4 At the MS-DOS prompt, change your directory to the root directory of your CD-ROM drive.

- 5 Enter the upgrade command:

```
update nwsxx_yy.bin
```

Where xx\_yy is the version of management software. The version of management software on the CD-ROM is the one that is originally installed on the Switch. Display the contents of the CD-ROM to see the filename for this 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:

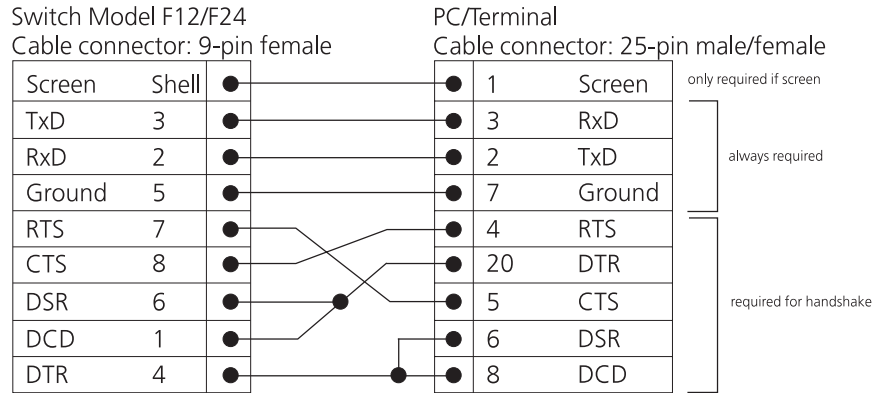
```
update -c 1 nwsxx_yy.bin
```

- 6 Power-down the Switch.
- 7 At your PC, press [Return].
- 8 Power-up the Switch immediately (within 5 seconds).  
The utility transfers the management software to the Switch.
- 9 Repeat all of the steps for any other Switches that need upgrading.

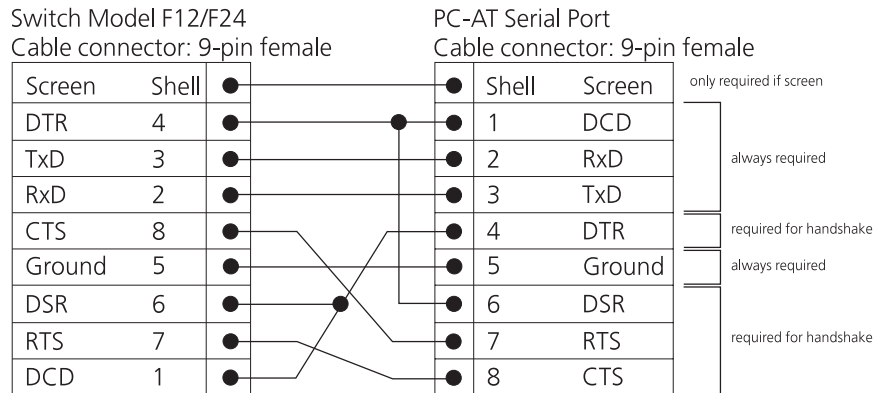
# D

## PIN-OUTS

### Null Modem Cable 9-pin to RS-232 25-pin



### PC-AT Serial Cable 9-pin to 9-pin



**Modem Cable**

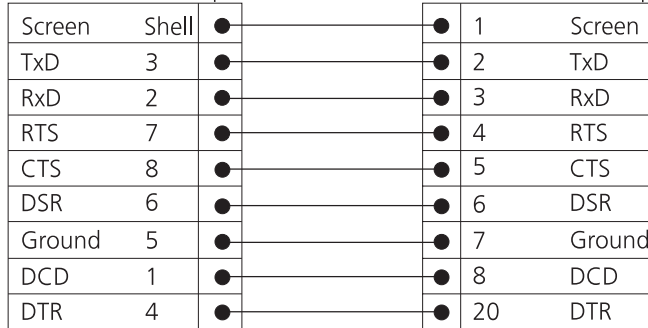
9-pin to RS-232 25-pin

Switch Model F12/F24

Cable connector: 9-pin female

RS-232 Modem Port

Cable connector: 25-pin male



**RJ45 Pin Assignments**

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

**Table D-1** Pin assignments

Pin Number	Signal	Function
<i>Ports configured as MDI</i>		
1	TxDat +	Transmit data
2	TxDat -	Transmit data
3	RxDat +	Receive Data
4	Not assigned	
5	Not assigned	
6	RxDat -	Receive data
7	Not assigned	
8	Not assigned	

**Table D-1** Pin assignments

<b>Pin Number</b>	<b>Signal</b>	<b>Function</b>
<i>Ports configured as MDIX</i>		
1	RxDta +	Receive Data
2	RxData –	Receive Data
3	TxDData +	Transmit data
4	Not assigned	
5	Not assigned	
6	TxDData –	Transmit data
7	Not assigned	
8	Not assigned	





# E

## SWITCH TECHNICAL SPECIFICATIONS

---

<b>Physical Dimensions</b>	Height: 76mm (3.0 in.) x Width: 483mm (19.0 in.) x Depth 300mm (12.0 in.) Weight: 4kg (8.8lbs)
<hr/>	
<b>Environmental Requirements</b>	
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)
<hr/>	
<b>Safety</b>	
Agency Certifications	UL 1950, EN60950, CSA 22.2 No. 950,
<hr/>	
<b>EMC</b>	
Emissions	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. The use of unshielded cables (category 3 or 5 for 10BASE-T ports or category 5 for 100BASE-TX ports) complies with the class A requirements.
Immunity	EN50082-1
<hr/>	
<b>Heat Dissipation</b>	200 watts maximum (628 BTU/hour maximum)
<hr/>	
<b>Power Supply</b>	
AC Line Frequency	50/60Hz
Input Voltage Options	90 – 240 VAC
Current Rating	3amps (maximum)

---

(continued)

---

**Standards Supported**

SNMP

- SNMP protocol (RFC 1157)
- MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Repeater MIB (RFC 1516)
- VLAN MIB (RFC 1573)
- RMON MIB (RFC 1271)
- BOOTP (RFC 951)

Terminal Emulation

- Telnet (RFC 854)

Protocols Used for Administration

- UDP (RFC 768)
  - IP (RFC 791)
  - ICMP (RFC 792)
  - TCP (RFC 793)
  - 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](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 Model F12 and F24**

**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.

Zulassungsbescheinigung laut dem Deutschen 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.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Corporation. Deutschland Informationssysteme GmbH, 70547 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Gerät erfüllt die Schutzanforderungen nach EN.50082-1 und EN 55022 Klasse 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 Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.“

EN 50082-1 Hinweis:

“Wird dieses Geräte in eine Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu veröbern.

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen 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）の基準に基づきクラス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 전자파 적합증을 받은 기기입니다. X미지 또는 사무지는 이 점을  
주의하시기 바라며, 만약 잘못 구입하셨을 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 conformité  
aux normes du  
ministère des  
Communications du  
Canada**

Cet appareil numérique de la classe A est conforme 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.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richtlinie 89/336)

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

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Corporation. Deutschland Informationssysteme GmbH, 70547 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2:

Das Gerät erfüllt die Schutzanforderungen nach EN.50082-1 und EN 55022 Klasse A.

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

“Warnung: dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.“

EN 50082-1 Hinweis:

“Wird dieses Geräte in eine Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu verößern.

Anmerkung:

Um die Einhaltung des EMVG sicherzustellen 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）の基準に基づきクラス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 전자파 적합증을 받은 기기입니다. X미지 또는 사용하지는 이 점을  
주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.





# GLOSSARY

<b>10BASE-T</b>	The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.
<b>100BASE-FX</b>	100 Mbps Ethernet implementation over fiber.
<b>100BASE-TX</b>	100 Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.
<b>ageing</b>	The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.
<b>auto-negotiation</b>	A feature on a port that allows it to advertise its capabilities for speed, duplex and flow control. When connected to a port that also supports auto-negotiation, the link can automatically configure itself to the optimum setup.
<b>backbone</b>	The part of a network used as the primary path for transporting traffic between network segments.
<b>bandwidth</b>	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.
<b>baud rate</b>	The switching speed of a line. Also known as <i>line speed</i> .
<b>BOOTP</b>	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.
<b>bridge</b>	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.
<b>broadcast</b>	A message sent to all destination devices on the network.
<b>broadcast storm</b>	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** Carrier-sense Multiple Access with Collision Detect. 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 packet toward its destination by an internetworking device.
- full duplex** A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.
- half duplex** A system that allows packets to be transmitted and received, but not at the same 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.
- IPX** Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.
- IP address** Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated

with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

- LAN** Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.
- latency** The delay between the time a device receives a packet and the time the packet 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. Part of the SuperStack II product range, provides a backup source of power when connected to the Switch.

- server farm** A cluster of servers in a centralized location serving a large user population.
- SLIP** Serial Line Internet Protocol. A protocol which allows IP to run over a serial line connection.
- 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.
- stack** A group of network devices that are integrated to form a single logical device.
- 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 which filters, forwards and floods packets based on the packet'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

---

## Symbols

? command 5-5

---

## Numerics

10BASE-T/100BASE-TX ports 1-4

---

## A

access levels of default users 3-9  
 Advanced Stack Setup page 4-29  
 agent software upgrade utility C-1  
 agent software, upgrading 4-35, 5-18, C-1  
 alarm events 7-7  
 alarm settings, default 7-8  
 Alarms (RMON group) 7-3, 7-6  
 Apply button 4-10  
 audit log 7-8  
 auto-negotiating ports 1-4  
 Auto-negotiation listbox (Port Setup page) 4-17

---

## B

banner of the web interface 4-6  
 Boot PROM Version field (Unit Status page) 4-15  
 Boot Version field (display command) 5-14  
 bootp command 5-10  
 BOOTP radio buttons (IP Setup page) 4-16  
 BOOTP server, using 4-4, 5-10  
 BPDUs. *See* Bridge Protocol Data Units  
 Bridge Identifier 6-4  
 Bridge Protocol Data Units 6-4  
 Broadcast Storm Control listbox (Advanced Stack Setup page) 4-30  
 browsers required for the web interface 3-5  
 browsers, configuring 8-3

---

## C

cable  
   choosing the correct 2-9  
   Matrix 1-7  
   maximum length 1-4, 1-15  
   pin-outs D-1  
 Capture (RMON group) 7-4, 7-6  
 CD-ROM 3-4

Color Key page 4-13  
 color-coding of ports, viewing 4-12  
 command area of the command line interface 5-3  
 command line interface  
   accessing 5-2  
   Ethernet Menu 5-4  
   exiting 5-3  
   IP Menu 5-4  
   map 5-4  
   menu description 5-3  
   moving the focus of 5-12  
   number of simultaneous users 5-3  
   solving problems 8-5  
   System Menu 5-4  
   Top-level menu 5-3  
 command line interface management 1-9, 3-2  
 commands, entering 5-4  
 Configuration icon 4-8  
 Configuration pages, accessing 4-8  
 Configuration pages, overview 4-9  
 Confirm Password field (Password Setting page) 4-22  
 Console connection listbox (Console Port Configuration page) 4-20  
 console port 1-6  
   configuring 4-19  
   settings 3-6  
 Console Port Configuration page 4-19  
 contact details, specifying 4-25  
 Contact field (display command) 5-13  
 Contact field (Unit Status page) 4-14  
 Contact page 4-25  
 conventions  
   notice icons, About This Guide 8  
   text, About This Guide 8  
 cross-over configuration 1-4, 2-9

---

## D

default  
   passwords 3-9  
   settings 1-10  
 Default Router field (IP Setup page) 4-16  
 default users 3-9  
 define command 5-9  
 Description field (inventory command) 5-15  
 descriptive names  
   specifying 4-21  
 descriptive names, specifying 4-4  
 Designated Bridge Port 6-4  
 display command 5-10, 5-13  
 Documentation field (Documentation page) 4-24  
 Documentation icon 4-7  
 Documentation page 4-24  
 documentation, online. *See* online documentation  
 download utility C-1  
 Duplex Mode 1-7

Duplex Mode of the ports, viewing 4-13

---

## E

electronic emission notices G-5, G-8  
 Enter MAC Address field (Switch Database page) 4-28  
 Ethernet Menu 5-4  
 Events (RMON group) 7-4, 7-6  
 Expansion Module slot 1-6  
 External Link icons 4-7

---

## F

factory defaults 1-10  
 Fast Ethernet configuration rules 1-14  
 Filter (RMON group) 7-3, 7-6  
 flow control 1-7  
 Flow Control listbox (Console Port Configuration page) 4-20  
 Forwarding Mode listbox (Advanced Stack Setup page) 4-30  
 FTP, support site F-1  
 full duplex 1-7  
 full duplex configuration rules 1-15  
 Full Duplex Flow Control listbox (Port Setup page) 4-18, 4-19

---

## G

Getting Started pages 4-4  
 accessing 4-23

---

## H

hardware features 1-2  
 Hardware Version field (display command) 5-14  
 Hardware Version field (Unit Status page) 4-14  
 Health icon 4-8  
 Health pages, accessing 4-8  
 Health pages, overview 4-10  
 Hello BPDUs 6-6  
 Hello Time 6-4  
 Help field (Documentation page) 4-24  
 Help icon 4-7  
 help. See online help  
 History (RMON group) 7-2, 7-6  
 Hosts (RMON group) 7-3, 7-6  
 Hosts Top N (RMON group) 7-3, 7-6

---

## I

IBM World Wide Web site, accessing 4-7  
 icons  
 Configuration 4-8  
 Documentation 4-7  
 External Link 4-7  
 Health 4-8

Help 4-7  
 Library 4-7  
 Management 4-8  
 Management Settings 4-8  
 side-bar 4-8  
 Support 4-7  
 Unit 4-8

## Index 1

initialize command 5-17  
 Initialize page 4-34  
 initializing the stack 4-34, 5-17  
 installing the Switch 2-1  
 prerequisites 2-2  
 inventory command 5-14  
 IP Address field (IP Setup page) 4-16  
 IP addresses  
 entering 4-2  
 format 3-8  
 obtaining 3-8  
 IP information  
 setting up for the stack 3-4, 3-7, 4-4  
 setting up for the Switch 4-15, 5-9  
 IP Menu 5-4  
 IP Setup page 4-15

---

## L

LEDs 1-4  
 solving problems indicated by 8-2  
 Library icon 4-7  
 Light Emitting Diodes. See LEDs  
 Link State field (Port Setup page) 4-17  
 Location field (display command) 5-13  
 Location field (Unit Status page) 4-14  
 location of the stack, specifying 4-23  
 Location page 4-23  
 logging in as a default user 3-9  
 logout command 5-3

---

## M

MAC Address column (Switch Database page) 4-28  
 MAC Address field (Unit Status page) 4-14  
 Main Link column (Resilient Links page) 4-32  
 Management Icons 4-8  
 management of the stack 1-9  
 benefits 3-2  
 command line interface 1-9, 3-2  
 methods 3-2  
 setting up 3-1  
 SNMP 1-9, 3-2  
 web interface 1-9, 3-2, 4-1  
 management settings for the stack, changing 4-21  
 Management Settings icon 4-8  
 Management Settings pages, accessing 4-8  
 Management Settings pages, overview 4-9

Management Software Upgrade Utility C-1  
 management software, upgrading 4-35, 5-18, C-1  
 Managment Software Upgrade Utility  
   solving problems 8-8  
 map of the command line interface 5-4  
 map of the web interface 4-11  
 Matrix (RMON group) 7-3, 7-6  
 Matrix Cable 1-7  
 Matrix Module 1-7  
 Matrix Module slot 1-6  
 matrix port 1-7  
 Max Age 6-6  
 MDI configuration 2-9  
 MDIX configuration 1-4, 2-9  
 Media Type field (Port Setup page) 4-17  
 menu area of the command line interface 5-3  
 menus, displaying 5-5

---

## N

Name field (inventory command) 5-15  
 Name field (System Name page) 4-21  
 network configuration examples 1-11  
 New Password field (Password Setting page) 4-22

---

## O

online documentation 3-4  
   specifying the location 4-5, 4-24  
 online documentation, accessing 4-7  
 online help 3-4  
   specifying the location 4-5, 4-24  
 online help, accessing 4-7, 5-5  
 operating modes of the stack, configuring 4-29  
 Operational Version field (display command) 5-14

---

## P

packet forwarding 4-30  
 page area of the web interface 4-6, 4-8  
   making changes in 4-10  
   navigating 4-10  
 Pair State column (Resilient Links page) 4-32  
 password command 5-15  
 password dialog 4-2  
 Password Setting page 4-22  
 passwords  
   changing 4-22, 5-15  
   default 3-9  
   entering 4-2, 4-5  
   of default users 3-9  
 path costs, default 6-4  
 pin assignments  
   modem cable D-2  
   null modem cable D-1  
   RJ45 D-2

  serial cable D-1  
 ping command 5-11  
 pin-outs D-1  
 Port column (Switch Database page) 4-27  
 Port field (Port Setup page) 4-17  
 Port Graph page 4-37  
 Port Selection Filter listbox (Switch Database page) 4-28  
 Port Setup page 4-16  
 Port Speed field (Port Setup page) 4-17  
 Port Speed listbox (Console Port Configuration page) 4-20  
 Port State listbox (Port Setup page) 4-19  
 port statistics  
   displaying 4-37  
   interpreting 4-39  
 Port Summary page 4-13  
 ports  
   10BASE-T/100BASE-TX 1-4  
   auto-negotiating 1-4  
   color-coding 4-12  
   configuring 4-16, 5-7  
   console 1-6  
     settings 3-6  
   matrix 1-7  
   viewing the status of 4-12, 5-8  
 portstate command 5-7  
 Position field (inventory command) 5-14  
 power socket 1-6  
 powering-up a Switch 2-8  
 problem solving 8-1  
 problems  
   command line interface 8-5  
   Management Software Upgrade Utility 8-8  
   Serial Web Utility 8-7  
   SNMP management 8-6  
   web interface 8-2

---

## R

rack mounting a Switch 2-3  
 rear view 1-6  
 Redundant Power System. See RPS  
 refreshing the Switch graphic 4-13  
 related documentation, About This Guide 9  
 remote access  
   enabling and disabling 5-16  
 Remote Monitoring. See RMON  
 remoteAccess command 5-16  
 reset command 5-17  
 Reset page 4-33  
 resetting the stack 4-33, 5-17  
 resilient link pairs  
   creating 4-33  
   deleting 4-33  
   displaying 4-32

- swapping the main and standby ports 4-33
- resilient links 1-8
  - description 4-31
  - setting up 4-31
- Resilient Links page 4-31
- RMON
  - alarm events 7-7
  - benefits 7-4
  - default alarm settings 7-8
  - features supported 7-6
  - groups 7-2
  - groups supported 7-6
  - probe 7-2
- Root Bridge 6-4
- Root Path Cost 6-4
- RPS 1-6
  - connecting 2-8
  - socket 1-6

---

## S

- safety information
  - English 5
  - notice ii
- security 1-8
- Security listbox (Port Setup page) 4-19
- segment, maximum length 1-4, 1-15
- Select Action Type listbox (Switch Database page) 4-28
- Select menu option prompt 5-3
- Serial Line Interface Protocol. *See* SLIP
- Serial Number field (display command) 5-14
- serial port. *See* console port
- Serial Web Utility B-1
  - solving problems 8-7
- service, technical F-1
- side-bar icons 4-8
- side-bar of the web interface 4-6
- Simple Network Management Protocol. *See* SNMP
- SLIP addresses
  - default 5-9
  - entering 5-9
- SNMP management 1-9, 3-2
  - solving problems 8-6
- socket
  - power 1-6
  - RPS 1-6
- software features
  - explanation 1-7
  - summary 1-2
- Software Upgrade page 4-35
- Software Version field (Unit Status page) 4-15
- software, upgrading 4-35, 5-18, C-1
- softwareUpgrade command 5-18
- Spanning Tree listbox (Advanced Stack Setup page) 4-30
- Spanning Tree Protocol. *See* STP
- specifications, system E-1
- speed of the ports, viewing 4-13
- Speed/Duplex listbox (Port Setup page) 4-18
- stack, configuring 4-26, 5-12
- standards supported E-2
- Standby Link column (Resilient Links page) 4-32
- State field (inventory command) 5-15
- Statistics (RMON group) 7-2, 7-6
- statistics, viewing for the current Switch 4-36
- Status column (Switch Database page) 4-28
- STP 1-9
  - Bridge Identifier 6-4
  - Bridge Protocol Data Units 6-4
    - configurations 6-6
    - default path costs 6-4
    - description 6-2
    - Designated Bridge Port 6-4
    - enabling and disabling 6-8
    - Hello BPDUs 6-6
    - Hello Time 6-4
    - Max Age 6-6
    - Root Bridge 6-4
    - Root Path Cost 6-4
  - straight-through configuration 2-9
  - subnet mask 3-8
  - Subnet Mask field (IP Setup page) 4-16
  - subnets 3-8
    - using 3-8
  - sub-networks. *See* subnets
  - summary command 5-8
  - Support icon 4-7
  - support, technical F-1
  - Switch 1-6
    - 10BASE-T/100BASE-TX ports 1-4
    - console port 1-6
    - dimensions E-1
    - function 1-2
    - hardware features 1-2
    - installation 2-1, 2-2
    - management. *See* management of the stack
    - power socket 1-6
    - powering-up 2-8
    - rack mounting 2-3
    - RPS socket 1-6
    - size E-1
    - software features
      - explanation 1-7
      - summary 1-2
    - standards supported E-2
    - unit information label 1-6
    - viewing the administration details 4-14
    - wall mounting 2-4
    - weight E-1
  - Switch Database
    - configuring 4-26



- deleting entries from 4-29
- description 4-27
- displaying 4-27
- inserting permanent entries into 4-28
- Switch Database page 4-26
- Switch Graphic page 4-12
- Switch graphic, refreshing 4-13
- System Menu 5-4
- System Name field (Unit Status page) 4-14
- System Name page 4-21
- system specifications E-1

---

## T

- Technical support and service F-1
- Time Since Reset field (display command) 5-14
- Top-level menu 5-3
- topology rules for Fast Ethernet 1-14
- topology rules with full duplex 1-15
- trouble-shooting 8-1

---

## U

- Unit column (Switch Database page) 4-27
- unit command 5-12
- Unit Description field (Unit Status page) 4-14
- Unit Graph page 4-36
- Unit icon 4-8
- unit information label 1-6
- Unit Name field (display command) 5-13
- Unit pages, accessing 4-8
- Unit pages, overview 4-8
- unit statistics
  - displaying 4-36
  - interpreting 4-37
- Unit Status page 4-14
- Unit Uptime field (Unit Status page) 4-15
- upgrade utility C-1
- upgrading the management software of the
  - stack 4-35, 5-18
- user name
  - entering 4-2
- user name and password dialog 4-2

---

## V

- Voice support F-1

---

## W

- wall mounting a Switch 2-4
- Web browsers required for the web interface 3-5
- Web browsers, configuring 8-3
- web interface
  - accessing 4-2
  - Advanced Stack Setup page 4-29

- Apply button 4-10
- banner 4-6
- banner icons 4-7
- Color Key page 4-13
- Configuration pages, overview 4-9
- Console Port Configuration page 4-19
- Contact page 4-25
- description 4-6
- Documentation page 4-24
- exiting 4-3
- External Link icons 4-7
- Getting Started pages 4-4
- Health pages, overview 4-10
- Initialize page 4-34
- IP Setup page 4-15
- Location page 4-23
- Management Settings pages, overview 4-9
- map 4-11
- online documentation 3-4
- online help 3-4
- page area 4-6, 4-8
  - making changes in 4-10
- page area, navigating 4-10
- Password Setting page 4-22
- Port Graph page 4-37
- Port Setup page 4-16
- Port Summary page 4-13
- required browsers 3-5
- Reset page 4-33
- Resilient Links page 4-31
- side-bar 4-6
- Software Upgrade page 4-35
- solving problems 8-2
- Switch Database page 4-26
- Switch Graphic page 4-12
- System Name page 4-21
- Unit Graph page 4-36
- Unit pages, overview 4-8
- Unit Status page 4-14
- web interface management 1-9, 3-2, 4-1
- World Wide Web (WWW)
  - IBM Networking home page F-1

