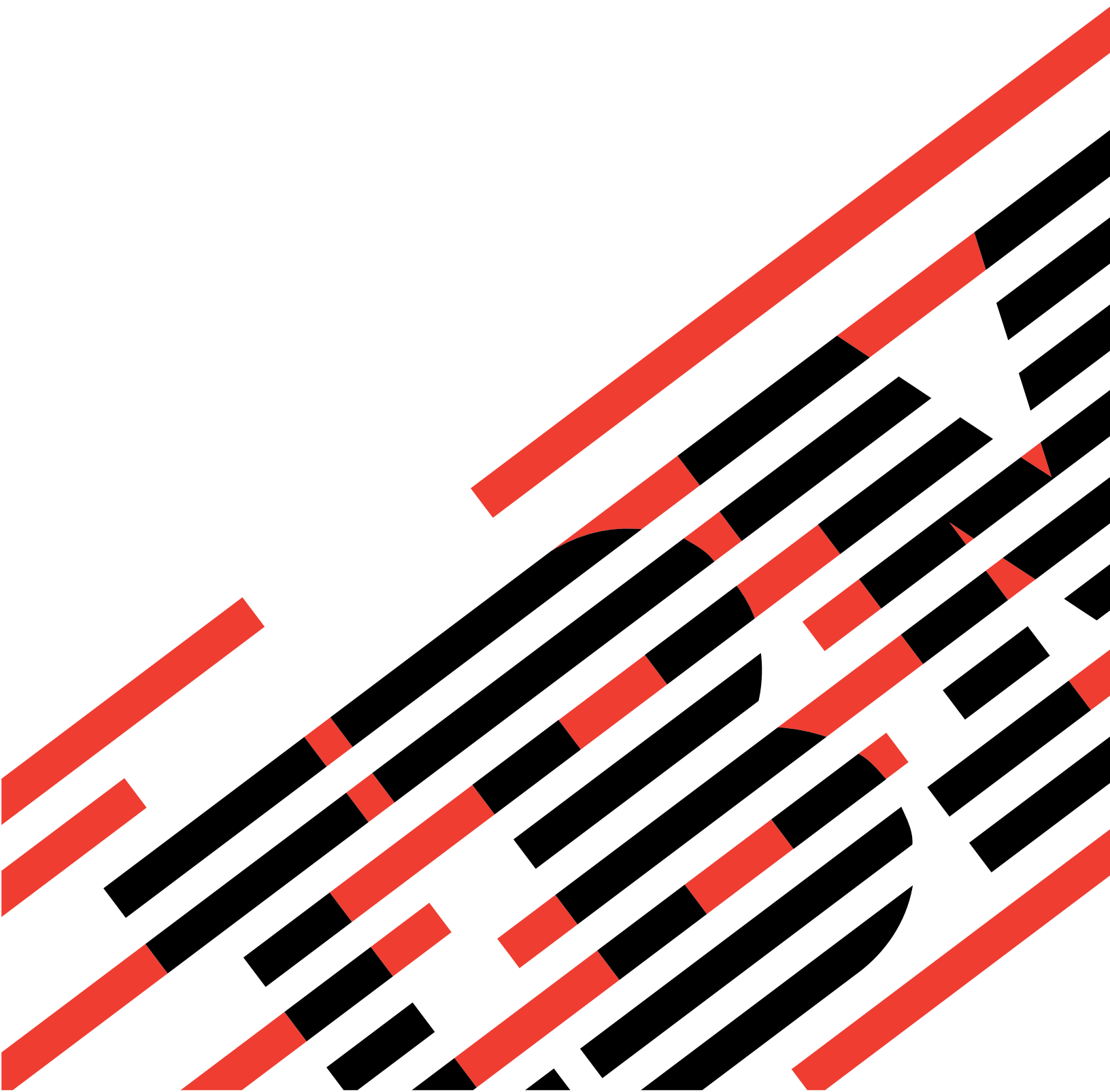




IBM BladeCenter 4-Port Gb Ethernet Switch Module
Installation and User's Guide





@server

IBM BladeCenter 4-Port Gb Ethernet Switch Module
Installation and User's Guide

Note:

Before using this information and the product it supports, read the general information in Appendix F, "Warranty information" on page 143 and Appendix G, "Notices" on page 155.

First Edition (November 2002)

© Copyright International Business Machines Corporation 2002. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Safety	ix
Chapter 1. Introducing the IBM BladeCenter 4-Port Gb Ethernet Switch	
Module	1
Related publications	2
Notices and statements used in this book	4
Major components of the BladeCenter 4-Port Gb Ethernet Switch Module.	4
Specifications and features	5
Standards and topology	6
Chapter 2. Installing and removing a switch module	7
Ethernet interface requirements	7
Installation guidelines	8
System reliability considerations	8
Handling static-sensitive devices	9
Installing a switch module	9
Removing a switch module	12
Chapter 3. Information panel LEDs and external ports	15
Information panel	15
LEDs	15
Chapter 4. Switch management and operating concepts	17
Ethernet switch subsystem overview	17
BladeCenter chassis configuration and operation	17
Switch management and control	18
IP addresses and SNMP community names	19
Traps	20
MIBs	21
SNMP	22
Authentication	22
Packet forwarding	23
Spanning Tree Protocol.	23
VLANs	24
Notes about VLANs on IBM BladeCenter 4-port Gb Ethernet switch module	24
IEEE 802.1Q VLANs.	24
802.1Q VLAN packet forwarding	25
802.1Q VLAN tags	26
Port VLAN ID	27
Tagging and untagging	28
Ingress filtering	29
VLANs	29
DHCP	29
Chapter 5. Web-Based network management	31
Introduction	31
Remotely managing the Ethernet switch module	31
Getting started	32
Configuration	34
Switch Information	35
IP Setup	36
Port Setting	38
Configure Ports.	38

Display Ports	38
Switch Settings	39
Telnet Settings	40
VLANs	40
Edit 802.1Q VLANs	40
802.1Q VLANs Entry Settings -- Add	41
802.1Q VLANs Entry Settings -- Edit	42
Port VLAN ID (PVID).	42
Port Priority	43
Port Ingress Filter	44
Port GVRP Settings	45
Multicasting	45
IGMP Snooping	45
IEEE 802.1q Multicast Setting	46
Mirroring	47
Spanning Tree	48
Configure Spanning Tree	48
STP Port Settings	49
Class of Service	50
Link Aggregation	52
Distribution Method	53
Port Trunking	54
Setup IEEE 802.3ad Link Aggregation	55
Forwarding	56
Remote Management Setup	57
Management Station IP Settings	58
SNMP Community Settings	58
Setting up trap receivers	58
Setting up user accounts	59
Assigning Root, User+, and User privileges	61
Network Monitoring	62
Statistics	62
Port Utilization	62
Port Error Packets	62
Port Packet Analysis	64
Address Table	65
Applications	66
GVRP	66
LACP Aggregator	66
IGMP Snooping	67
Switch History	67
Maintenance	68
Using TFTP Server	68
Download Configuration File	68
Upgrade Firmware	69
Upload Configuration File	70
Save Log	70
Using the Browser	71
Upgrade Firmware/Configuration File	71
Download Configuration/Log Files	72
Saving changes	72
Restoring the default configuration parameters	73
Restarting the switch.	73
Chapter 6. Configuring the switch module through the Telnet interface	75
Remotely managing the Ethernet switch module	75

Connecting to the switch module	76
Telnet usage conventions	76
First-time connection to the Ethernet switch module	76
Setting up user accounts	78
Assigning Root, User+, and User privileges	79
Saving changes	80
Restoring default configuration values	81
Logging onto the switch module	82
Viewing current user accounts	82
Updating a user account	82
Deleting a user account	83
Basic Setup	84
Switch Information	84
IP Setup	84
Remote Management Setup	86
Switch Settings	88
Telnet Settings	88
Configure Ports	89
Utilities	89
Upgrade Firmware from TFTP Server	90
Download Configuration File from TFTP Server	90
Upload Configuration File to TFTP Server	91
Save Log to TFTP Server	91
Ping Test	92
Network Monitoring	92
Port Utilization	93
Port Error Packets	93
Port Packet Analysis	94
Browse MAC Address Table	94
GVRP	95
IGMP Snooping	95
LACP Aggregator	96
Switch History	96
Restarting the switch module	97
Logging out	98
Advanced Setup	99
Spanning Tree	99
STP Port Settings	100
Forwarding	101
Class of Service	101
Class of Service Configuration	102
802.1p Priority Mapping	102
Diffserv Mapping	103
Mirroring	103
Multicasting	104
IGMP Snooping	105
Setup IEEE 802.1q Multicast Settings	106
VLANs	107
VLAN Menu	107
Edit 802.1Q VLANs	107
Configure 802.1Q Port Settings	109
Link Aggregation	110
Port Trunking	112
IEEE 802.3ad Link Aggregation	112
Appendix A. RJ-45 pin specifications	115

Appendix B. Run-time switching software default settings	117
Appendix C. Cable lengths	119
Appendix D. Understanding and troubleshooting the Spanning Tree Protocol	121
STP operation levels	121
Bridge protocol data units	122
Creating a stable topology	122
STP port states	122
Setting user-changeable STP parameters	124
Illustration of STP	125
Blocking state	127
Listening state	128
Learning state	129
Forwarding state	130
Disabled state	132
Troubleshooting STP	133
Spanning Tree Protocol Failure	133
Full/half duplex mismatch	133
Unidirectional link	134
Packet corruption	135
Resource errors	135
Identifying a data loop	136
Avoiding network problems	136
Appendix E. Getting help and technical assistance	141
Before you call	141
Using the documentation	141
Getting help and information from the World Wide Web	141
Software service and support	142
Hardware service and support	142
Appendix F. Warranty information	143
Warranty period	143
Problem determination	143
Running diagnostics	143
Checking software	143
Warranty service and support	144
International Warranty Service	144
Purchasing additional services	145
IBM Statement of Limited Warranty Z125-4753-06 8/2000	146
Part 1 - General Terms	146
Part 2 - Country-unique Terms	148
Appendix G. Notices	155
Edition notice	155
Trademarks	156
Important notes	156
Electronic emission notices	157
Federal Communications Commission (FCC) statement	157
Industry Canada Class A emission compliance statement	158
Australia and New Zealand Class A statement	158
United Kingdom telecommunications safety requirement	158
European Union EMC Directive conformance statement	158
Taiwanese Class A warning statement	158

Japanese Voluntary Control Council for Interference (VCCI) statement	159
Index	161

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الأمنية

Antes de instalar este produto, leia as Informações de Segurança.

在安装本产品之前，请仔细阅读 **Safety Information** (安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Læs sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.

Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informações sobre Segurança.

Перед установкой продукта прочтите инструкции по технике безопасности.

Pred inštaláciou tohto zariadenia si pečítajte Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

Statement 1:



DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	To Disconnect:
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 2:



CAUTION:

When replacing the lithium battery, use only IBM Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

Statement 3:



CAUTION:

When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.



DANGER

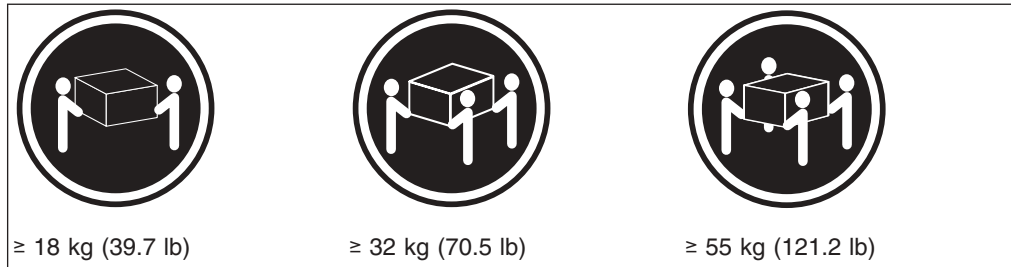
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following.

Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.



Class 1 Laser Product
Laser Klasse 1
Laser Klass 1
Luokan 1 Laserlaite
Appareil À Laser de Classe 1

Statement 4:

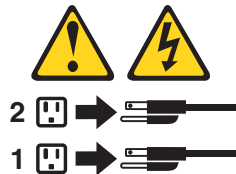


CAUTION:
Use safe practices when lifting.

Statement 5:



CAUTION:
The power control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.



Statement 6:



CAUTION:

If you install a strain-relief bracket option over the end of the power cord that is connected to the device, you must connect the other end of the power cord to an easily accessible power source.

Statement 8:



CAUTION:

Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Statement 13:



DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device for electrical specifications.

Statement 14:



CAUTION:

Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the following label is attached.



Chapter 1. Introducing the IBM BladeCenter 4-Port Gb Ethernet Switch Module

Thank you for purchasing an IBM® BladeCenter™ 4-Port Gb Ethernet Switch Module. This *Installation and User's Guide* contains information about:

- Setting up and installing your switch module
- Configuring your switch module

For installation details, see Chapter 2, "Installing and removing a switch module" on page 7. For additional information, see the instructions in your BladeCenter publications.

Your IBM BladeCenter 4-Port Gb Ethernet Switch Module is one of up to four Ethernet switch modules that can be installed in the IBM @server BladeCenter Type 8677, also known as the BladeCenter unit. This high-performance BladeCenter 4-Port Gb Ethernet Switch Module is ideally suited for networking environments that require superior microprocessor performance, efficient memory management, flexibility, and reliable data storage.

Performance, reliability, and expansion capabilities were key considerations in the design of your BladeCenter 4-Port Gb Ethernet Switch Module. These design features make it possible for you to customize the system hardware to meet your needs today, while providing flexible expansion capabilities for the future.

If you have access to the World Wide Web, you can obtain up-to-date information about your BladeCenter 4-Port Gb Ethernet Switch Module model and other IBM server products at <http://www.ibm.com/eserver/xseries/>.

The product name, machine type and serial number are located on the identification label on the side of the BladeCenter 4-Port Gb Ethernet Switch Module. You will need this information when you register your BladeCenter 4-Port Gb Ethernet Switch Module with IBM. The media access control (MAC) address also is located on the identification label. See "Major components of the BladeCenter 4-Port Gb Ethernet Switch Module" on page 4 for an illustration that shows the location of the identification label.

Note: The MAC address is also located on a separate label on the information panel under the external Ethernet port connectors.

Record your product information in this table.	
Product name	IBM BladeCenter 4-Port Gb Ethernet Switch Module
Type	_____
Model number	_____
Serial number	_____
Media access control (MAC) address	_____

Verify that the shipping carton contains an IBM BladeCenter 4-Port Gb Ethernet Switch Module. If the Ethernet switch module is missing or damaged, contact your local reseller for replacement. Otherwise, return the Ethernet switch module to its static-protective package.

Note: The illustrations in this document might differ slightly from your hardware.

Related publications

This *Installation and User's Guide* contains detailed setup and installation instructions for the IBM BladeCenter 4-Port Gb Ethernet Switch Module. This publication also provides general information about your Ethernet switch module, including information about features, how to configure your BladeCenter 4-Port Gb Ethernet Switch Module, and how to get help.

In addition to this *Installation and User's Guide*, the following related documentation is provided with your BladeCenter 4-Port Gb Ethernet Switch Module:

- *BladeCenter 4-Port Gb Ethernet Switch Module Installation Guide*
This printed publication contains setup and installation instructions for the IBM BladeCenter 4-Port Gb Ethernet Switch Module. This publication also provides general information about your Ethernet switch module, including information about getting started, first-time connection to the Ethernet switch module, and how to configure your Ethernet switch module.
- *Rack Installation Instructions*
This publication contains the instructions to install your BladeCenter unit in a rack.
- *Safety Information Book*
This multilingual publication is provided in Portable Document Format (PDF) on the *IBM BladeCenter Documentation CD*. It contains translated versions of the caution and danger statements that appear in the documentation for your server. Each caution and danger statement has an assigned number, which you can use to locate the corresponding statement in your native language.
- *@server BladeCenter Type 8677 Installation and User's Guide*
This publication is provided in PDF on the *IBM BladeCenter Documentation CD*. It provides general information about your BladeCenter unit, including:
 - Information about features
 - How to set up, cable, and start your BladeCenter unit
 - How to install options in your BladeCenter unit
 - How to configure your BladeCenter unit

- How to perform basic troubleshooting of your BladeCenter unit
- How to get help
- *BladeCenter HS20 Type 8678 Installation and User's Guide*

This publication is provided in PDF on the *IBM BladeCenter Documentation CD*. It provides general information about your blade server, including:

 - Information about features
 - How to set up and start your blade server
 - How to install options in your blade server
 - How to configure your blade server
 - How to install an operating system on your blade server
 - How to perform basic troubleshooting of your blade server
 - How to get help
- *Hardware Maintenance Manual and Troubleshooting Guides*

The BladeCenter unit and the BladeCenter HS20 Type 8678 product each come with a customized *Hardware Maintenance Manual and Troubleshooting Guide*. These publications are provided in PDF on the *IBM BladeCenter Documentation CD*. They contain information to help you solve the problem yourself or to provide helpful information to a service technician.

Depending on your blade server model, additional publications might be included on the *IBM BladeCenter Documentation CD*.

In addition to reviewing the publications in this library, be sure to review the *IBM BladeCenter Planning and Installation Guide* located at <http://www.pc.ibm.com/eserver/bladecenter> on the World Wide Web for information to help you prepare for system installation and configuration.

Notices and statements used in this book

The caution and danger statements that appear in this book are also in the multilingual *Safety Information Book*, which is on the *IBM BladeCenter Documentation CD*. Each statement is numbered for reference to the corresponding statement in the *Safety Information Book*.

The following notices and statements are used in this book:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.
- **Danger:** These statements indicate situations that can be potentially lethal or extremely hazardous to you. A danger statement is placed just before the description of a potentially lethal or extremely hazardous procedure step or situation.

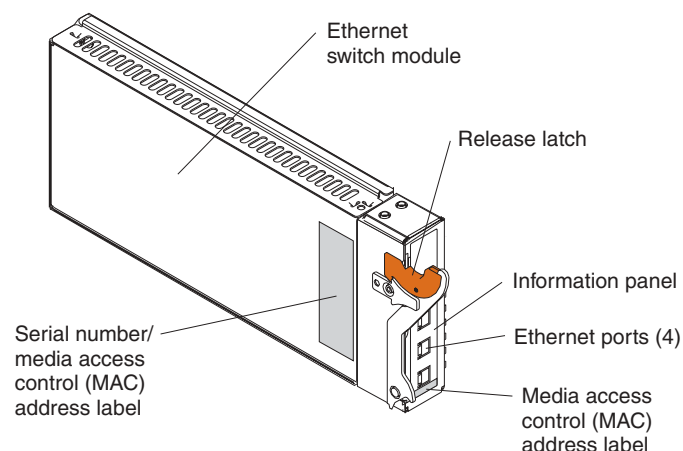
Major components of the BladeCenter 4-Port Gb Ethernet Switch Module

The orange color on components and labels on your Ethernet switch module and BladeCenter unit identifies hot-swap or hot-plug components. You can install or remove these components while the system is running, provided that your system is configured to support this function.

The blue color on components and labels indicates touch points where a component can be gripped, a latch moved, and so on.

The following illustration shows the major components of your Ethernet switch module.

Note: The illustrations in this document might differ slightly from your hardware.



For more information about the components of the information panel, see Chapter 3, “Information panel LEDs and external ports” on page 15. For more information about the MAC address, see “IP addresses and SNMP community names” on page 19.

Specifications and features

This section provides a summary of the specifications and features for your IBM BladeCenter 4-Port Gb Ethernet Switch Module.

The IBM BladeCenter 4-Port Gb Ethernet Switch Module features include:

- Ports
 - Four external 1000BASE-T ports for making 10/100/1000 Mbps connections to a backbone, end stations, and servers
 - Fourteen internal full-duplex gigabit ports, one connected to each of the BladeCenter blade servers
 - Two internal full-duplex 10/100 Mbps ports connected to the management module
- Performance features
 - Transmission method: Store-and-forward
 - Random-access memory (RAM) buffer: 8 MB
 - Packet filtering/forwarding rate:
 - Full-wire speed for all connections. 148800 packets per second (pps) per port (for 100 Mbps)
 - 1488100 pps per port (for 1000 Mbps)
 - Media access control (MAC) address learning: Automatic update. Supports 28 K MAC address
 - Priority queues: Four priority queues per port
 - Forwarding table age time: Maximum age: 17 to 2100 seconds. Default is 300 seconds.
 - 802.1D Spanning Tree support. Can be disabled on the entire switch or on a per-port basis
 - 802.1Q Tagged virtual local area network (VLAN) support, including Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)
 - Support for 256 VLANs in total, including 128 static VLANs
 - Internet group management protocol (IGMP) snooping support per VLAN
 - Link aggregation with 802.3ad support on four external ports for up to two static trunk groups or two link aggregation control protocol (LACP) 802.3ad link aggregation groups
- Management
 - Spanning Tree Algorithm (STA) protocol for creation of alternative backup paths and prevention of network loops
 - Simple network management protocol (SNMP) version 1
 - Fully configurable either in-band or out-of-band control through SNMP based software
 - Flash memory for software upgrades. This can be done through trivial file transfer protocol (TFTP) or hypertext transfer protocol (HTTP) Web interface.
 - Built-in SNMP management:
 - Bridge management information base (MIB) (RFC 1493)

- MIB-II (RFC 1213)
- 802.1P/Q MIB (RFC 2674)
- Interface MIB (RFC 2233)
- Mini-RMON MIB (RFC 1757) - four groups. The remote monitoring (RMON) specification defines the counters for the receive functions only. However, the switch provides counters for both receive and transmit functions.
- Supports Web-based management
- TFTP support
- Bootstrap protocol (BOOTP) support
- Dynamic host configuration protocol (DHCP) client support
- Password enabled
- Telnet remote control console
- Network cables:
 - 10BASE-T:
 - UTP Category 3, 4, 5 (100 meters maximum)
 - 100-ohm STP (100 meters maximum)
 - 100BASE-TX:
 - UTP Category 5 (100 meters maximum)
 - EIA/TIA-568 100-ohm STP (100 meters maximum)
 - 1000BASE-T:
 - UTP Category 5e (100 meters maximum)
 - UTP Category 5 (100 meters maximum)
 - EIA/TIA-568B 100-ohm STP (100 meters maximum)

Standards and topology

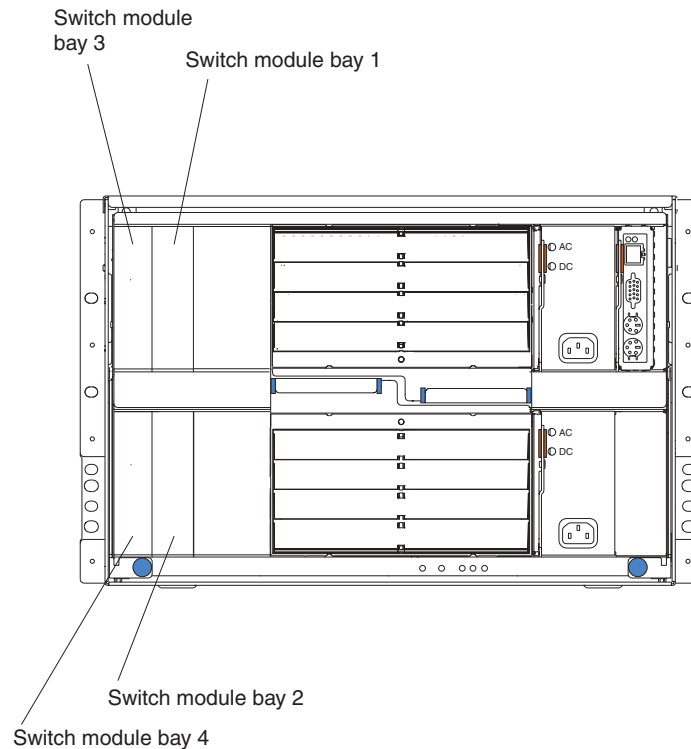
The following standards apply to the Ethernet switch module:

- IEEE 802.3 10BASE-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- IEEE 802.3z Gigabit Ethernet
- IEEE 802.1Q Tagged VLAN
- IEEE 802.1P Tagged Packets
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3x Full-duplex Flow Control
- ANSI/IEEE 802.3 NWay auto-negotiation

The following topology applies to the Ethernet switch module: Star

Chapter 2. Installing and removing a switch module

The following illustration shows the switch-module bay locations.



Attention: To maintain proper system cooling, each module bay must contain either a module or a filler module; each blade bay must contain either a blade or a filler blade.

Ethernet interface requirements

Your BladeCenter unit supports a minimum of one hot-swap Ethernet switch module in switch-module bay 1. This switch module is a fully functional four-connector Ethernet switch that provides a network connection to Ethernet Link 1 in all the blade servers in the BladeCenter unit. To provide a network connection for Ethernet Link 2 in each blade server, install an Ethernet switch module in switch-module bay 2.

If you install an interface option on any blade server, you must install a hot-swap switch module of the same interface type in switch-module bay 3 to obtain connection 1 for the interface option. To provide connection 2 for the interface option, install a switch module of that interface type in switch-module bay 4. The switch modules in bays 3 and 4 provide connections to all the interface options in the BladeCenter unit.

Important: The switch modules in switch-module bays 3 and 4 and all blade server interface options in the BladeCenter unit must use the same interface type. For example: if you install an Ethernet interface option on a blade server, the switch modules that you install in switch-module bays 3 and 4 must be Ethernet, and all other interface options in the BladeCenter unit must also be Ethernet interface options.

The following table summarizes the application for each switch module.

Bay	Switch-module function
1	Connection 1 (Ethernet Link 1) for all blade servers in the BladeCenter unit
2	Connection 2 (Ethernet Link 2) for all blade servers in the BladeCenter unit
3	Connection 3 (from all blade server interface options in the BladeCenter unit)
4	Connection 4 (from all blade server interface options in the BladeCenter unit)

For additional information, see the *BladeCenter Type 8677 Installation and User's Guide* on the *IBM BladeCenter Documentation CD*.

Installation guidelines

Before you begin to install the Ethernet switch module in your BladeCenter unit, read the following information:

- Become familiar with the safety and handling guidelines specified under “Safety” on page ix and “Handling static-sensitive devices” on page 9, and read the safety statements in BladeCenter unit option publications.
- The orange color on components and labels in your BladeCenter unit identifies hot-swap or hot-plug components. You can install or remove hot-swap modules while the BladeCenter unit is running. For complete details about installing or removing a hot-swap or hot-plug component, see the detailed information in this chapter.
- The blue color on components and labels identifies touch points where you can grip a component, move a latch, and so on.
- You do not need to turn off the BladeCenter unit to install or replace any of the hot-swap modules on the rear of the BladeCenter unit.
- For a list of supported options for your BladeCenter unit, go to <http://www.ibm.com/pc/us/compat/> on the World Wide Web.

System reliability considerations

Attention: To help ensure proper cooling and system reliability, make sure that:

- Each of the module bays on the rear of the BladeCenter unit has either a module or filler module installed.
- A removed hot-swap module is replaced with an identical module or filler module within 1 minute of removal.
- Cables for the optional modules are routed according to the illustrations and instructions in this document.

Handling static-sensitive devices

Attention: Static electricity can damage electronic devices and your system. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

To reduce the possibility of electrostatic discharge, observe the following precautions:

- Limit your movement. Movement can cause static electricity to build up around you.
- Handle the device carefully, holding it by its edges or its frame.
- Do not touch solder joints, pins, or exposed printed circuitry.
- Do not leave the device where others can handle and possibly damage the device.
- While the device is still in its static-protective package, touch it to an unpainted metal part of the BladeCenter chassis for at least two seconds. (This drains static electricity from the package and from your body.)
- Remove the device from its package and install it directly into your BladeCenter unit without setting it down. If it is necessary to set the device down, place it in its static-protective package. Do not place the device on your BladeCenter chassis or on a metal table.
- Take additional care when handling devices during cold weather because heating reduces indoor humidity and increases static electricity.

Installing a switch module

Statement 8:



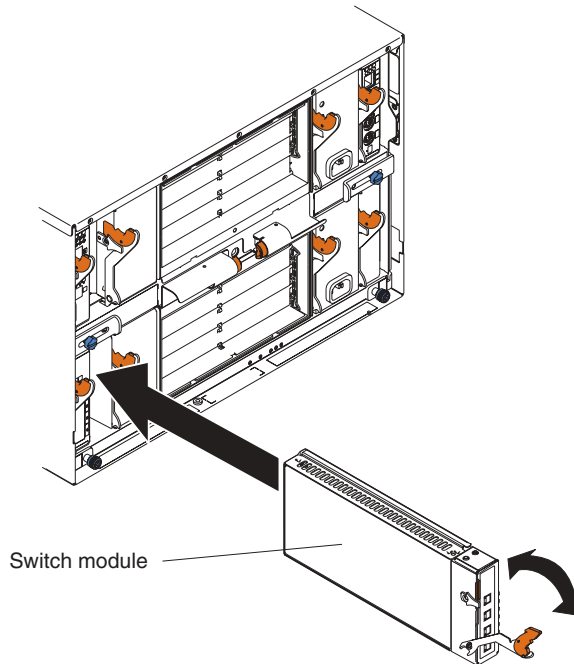
CAUTION:

Never remove the cover on a power supply or any part that has the following label attached.



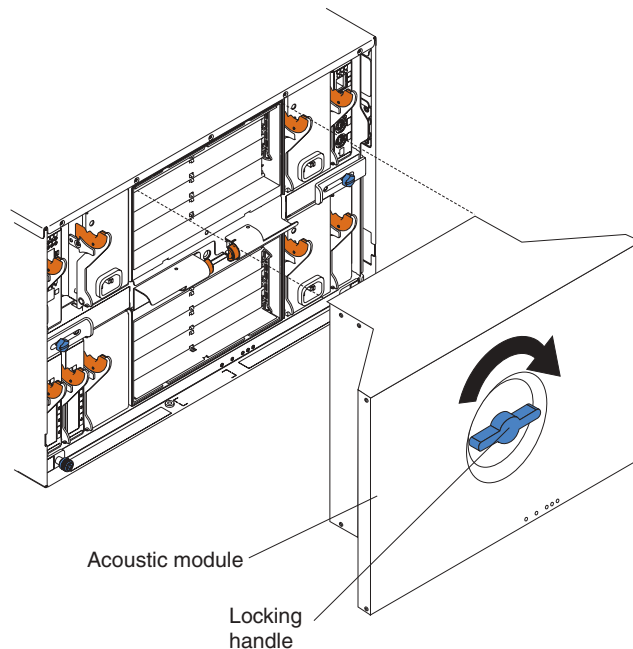
Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

The following illustration shows how to install a switch module in the rear of the BladeCenter unit.



Complete the following steps to install a switch module.

1. Review the information in “Safety” on page ix and “Installation guidelines” on page 8 through “Handling static-sensitive devices” on page 9.
2. Remove the acoustic attenuation module, if installed, from the rear of the BladeCenter unit.



3. Select a switch-module bay in which to install the switch module.
4. Select a switch-module bay in which to install the switch module, in accordance with the instructions in “Ethernet interface requirements” on page 7.

5. Remove the filler module from the selected bay. Store the filler module for future use.
6. If you have not already done so, touch the static-protective package that contains the switch module to an unpainted metal part of the BladeCenter unit for at least two seconds.
7. Remove the switch module from its static-protective package.
8. Ensure that the release latch on the switch module is in the open position (perpendicular to the module).
9. Slide the switch module into the appropriate switch-module bay until it stops.
10. Push the release latch on the front of the switch module to the closed position.
11. Make sure that the LEDs on the switch module indicate that it is operating properly. Verify that:
 - The dc power LED and the ac power LED on each power module are lit.
 - The OK LED on each management module is lit.
 - The OK LED on each switch module is lit.
12. If you have other switch modules to install, do so now; otherwise, go to step 13.
13. Attach any cables required by the switch module. For the location of the connectors on the BladeCenter unit, see *@server BladeCenter Type 8677 Installation and User's Guide* on the *IBM BladeCenter Documentation CD*.
14. Replace the acoustic attenuation module, if you removed it in step 2 on page 10.

Removing a switch module

Statement 8:



CAUTION:

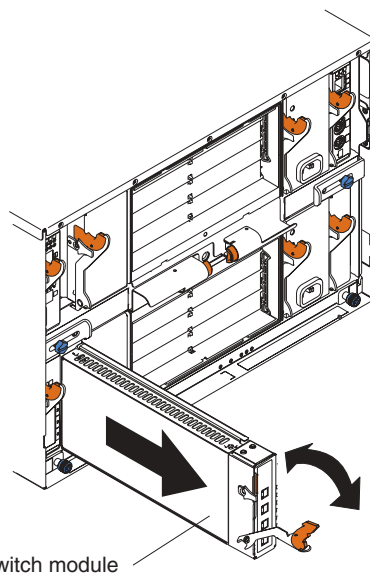
Never remove the cover on a power supply or any part that has the following label attached.



Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Complete the following steps to remove a switch module.

1. Remove the acoustic attenuation module, if installed, from the rear of the BladeCenter unit (see step 2 on page 10 for location).
2. Select an appropriate switch-module bay from which to remove a switch module, in accordance with the instructions in “Ethernet interface requirements” on page 7.
3. Unplug any cables from the selected switch module.
4. Pull the release latch toward the bottom of the switch module as shown in the illustration. The module moves out of the bay about 0.64 cm (0.25 inch).



5. Slide the switch module out of the bay and set it aside.
6. Place either another switch module or a filler module in the bay within 1 minute.

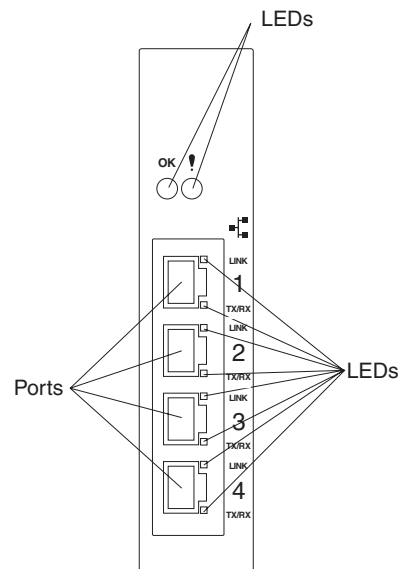
7. If you placed another switch module in the bay, reconnect any cables that you unplugged in step 3.
8. Replace the acoustic attenuation module option, if you removed it in step 1.

Chapter 3. Information panel LEDs and external ports

This chapter describes the information panel and LEDs (also known as indicators) on the IBM BladeCenter 4-Port Gb Ethernet Switch Module. This chapter also identifies the external ports on the information panel.

Information panel

The information panel of the switch module consists of LEDs and four external 1000BASE-T ports, as shown in the following illustration.

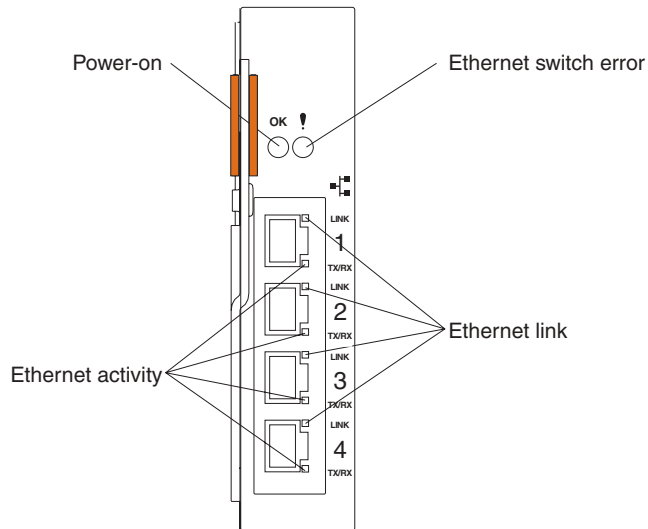


The switch module contains:

- Comprehensive LEDs display the status of the switch module and the network (see “LEDs”).
- Fourteen internal ports, one connected to each of the processor blades.
- Two internal full-duplex 10/100 Mbps ports connected to the management module.
- Four external 1000BASE-T Ethernet ports for 10/100/1000 Mbps connections to external Ethernet devices, such as backbones, end stations, and servers. These ports are identified as Ext1, Ext2, Ext3, and Ext4 in the switch configuration menus and are labeled 1 through 4 (from top to bottom) on the switch module, as shown in the preceding illustration.

LEDs

The LEDs on the information panel of the switch module include OK, !, Ethernet link, and Ethernet activity. The following illustration shows the LEDs on the switch module. A description of each LED follows the illustration.



Notes:

1. The illustrations in this document might differ slightly from your hardware.
2. An amber LED illuminates when a system error or event has occurred. To identify the error or event, check the LEDs on the information panel of the switch module.

OK (power-on): This green LED is located above the four external 10/100/1000 Mbps ports on the information panel. When this LED is on, it indicates that the switch module has passed the power-on self-test (POST) and is operational.

! (Ethernet switch error): This amber LED is located next to the OK (power-on) LED on the information panel. This LED indicates that the switch module has a fault. If the switch module fails the POST, this fault LED will be lit.

Ethernet link: This green link status LED is located at the top of each external 10/100/1000 Mbps port. When this LED is lit on a port, it indicates that there is a connection (or link) to a device on that port.

Ethernet activity: This green activity LED is located at the bottom of each external 10/100/1000 Mbps port. When this LED blinks on a port, it indicates that data is being received or transmitted (that is, activity is occurring) on that port. The blink frequency is proportional to the amount of traffic on that port.

Chapter 4. Switch management and operating concepts

This chapter discusses many of the concepts and features used to manage the switch and the concepts necessary to understand how the switch functions. In addition, this chapter explains many important points regarding these features.

Configuring the switch to implement these concepts and use its many features is discussed in detail in the following chapters.

Ethernet switch subsystem overview

This section provides information that you should be familiar with when managing and configuring the internal switch modules. If you are familiar with Layer 2 Ethernet switches, you will recognize the industry-standard parameters and terminology that are used in this document. However, it is important that you also understand the BladeCenter operating environment with regard to the internal switches.

The Ethernet switch modules are hot-swappable subsystems that provide Ethernet switching capabilities within a BladeCenter chassis. The primary purpose of the switch module is to provide Ethernet interconnectivity among the processor blades, management modules, and the external network infrastructure.

Two independent switch modules provide redundancy in the base system configuration. Each of the 14 server blades within a BladeCenter chassis has a dedicated, 1000 Mbps (1 Gbps) full-duplex link to each of the two switch modules. Ports 1 through 14 on the switch module correspond to server blades 1 through 14, respectively (numbered left to right when viewed from the front of the chassis). Each switch module has four external 10/100/1000 Mbps Ethernet ports for connection to the external network infrastructure. These ports are identified as Ext1, Ext2, Ext3, and Ext4 in the switch configuration menus and are labeled 1 through 4 (from top to bottom) on the switch module (see Chapter 3, "Information panel LEDs and external ports" on page 15 for an illustration).

Depending on the application, the external Ethernet interfaces can be configured to meet a variety of requirements for bandwidth or function.

The BladeCenter Ethernet switch modules have been preconfigured with default parameter settings that can be used with most typical installations. All switch modules will need a few basic parameter settings initially, such as an Internet protocol (IP) address for management and control, security access and control parameters, and basic setup of the external ports for link aggregation.

BladeCenter chassis configuration and operation

The BladeCenter Ethernet switch module is an integral subsystem within the overall BladeCenter system. For additional BladeCenter system level information, see the applicable *BladeCenter Installation and User's Guide* publications on the *IBM BladeCenter Documentation* CD. The BladeCenter chassis includes a management module (MM) as the central element for overall chassis management and control. The switch module includes a 100-Mbps internal Ethernet port that can only be accessed by the management module. To prevent inadvertent changes, this management port is "hidden" and does not appear in the port configuration and status screens. The factory default settings will *only* permit management and control access to the switch module through the 10/100 Mbps Ethernet port on the

management module. You can use the four external 10/100/1000 Mbps Ethernet ports on the switch module for management and control of the switch by selecting this mode as an option through the management module configuration utility program (see the applicable *BladeCenter Installation and User's Guide* publications on the *IBM BladeCenter Documentation CD* for more information).

Switch management and control

This document describes the user interfaces, screens, parameters, and other information that you need for remote management and control of your BladeCenter 4-Port Gb Ethernet Switch Module. Complete the following initial configuration steps:

1. Connect the Ethernet port of the management module to a 10/100 Mbps network (with access to a management station) or directly to a management station.
2. Initially configure the management module with the appropriate IP addresses for network access (see the applicable *BladeCenter Installation and User's Guide* publications on the *IBM BladeCenter Documentation CD* for more information).
3. Assign an initial IP address to the switch module through the management module. You can assign this IP address through one of the following methods:
 - Automatically through a DHCP server
 - Automatically through the IBM Director Configuration Wizard
 - Manually through the BladeCenter configuration utility program

Once a transmission control protocol/Internet protocol (TCP/IP) communication path has been established with the switch module through the MM Ethernet port, you can perform a series of management and control tasks. These tasks are in the following categories:

- Configuration
 - Modify switch parameter settings
- Remote Management Setup
- Network Monitoring
 - Automatically receive error alerts (traps)
 - View/reset port traffic statistics
 - Monitor data traffic on selected output ports, and so on
- Maintenance
 - Update the switch software
 - Query history log
 - Restore factory default settings, and so on

The switch module supports two primary management and control user interfaces. A built-in Web browser interface is the primary interface that will be invoked through the IBM Director Configuration Wizard (see Chapter 5, “Web-Based network management” on page 31 for detailed information). The Web browser interface can also be invoked from the BladeCenter MM management and configuration utility program, along with the telnet interface that provides a series of menu windows (see Chapter 6, “Configuring the switch module through the Telnet interface” on page 75 for detailed information). Both interfaces provide access to the same switch information and control parameters.

In addition, you can access an extensive set of both standard and private MIB objects through SNMP protocols.

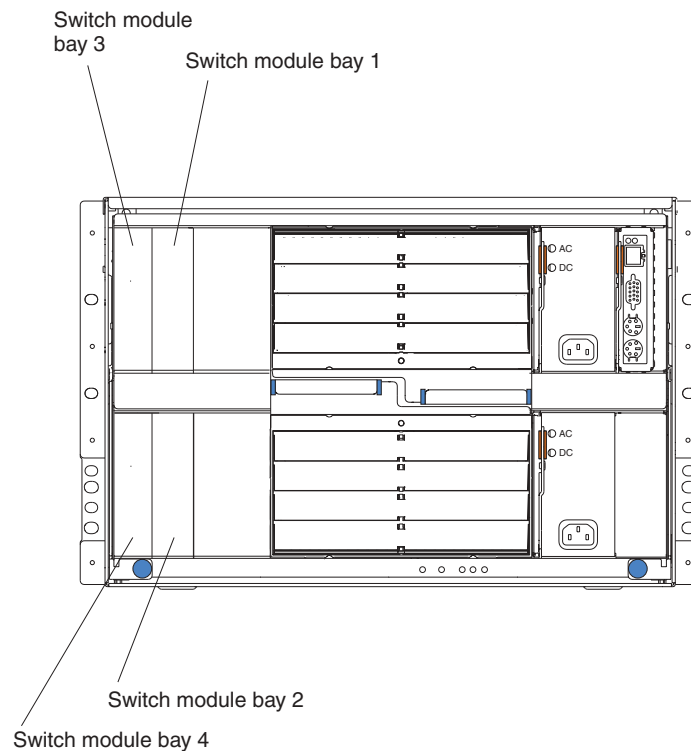
IP addresses and SNMP community names

Each switch must be assigned its own Internet protocol (IP) address, which is used for communication with an SNMP network manager or other transmission control protocol/Internet protocol (TCP/IP) applications (for example, BOOTP or TFTP). The switch default IP address is 192.168.70.1xx, where xx depends on the number of the bay into which you have installed the switch module, as shown in Table 1.

Table 1. Default IP addresses based on switch-module bay numbers

Bay number	Default IP address
Bay 1	192.168.70.127
Bay 2	192.168.70.128
Bay 3	192.168.70.129
Bay 4	192.168.70.130

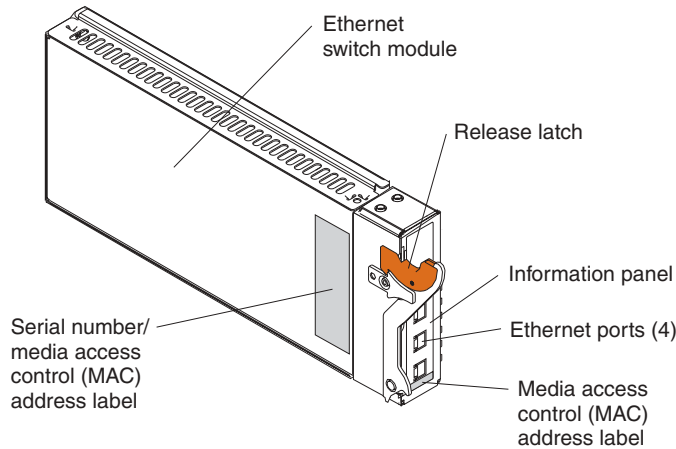
The following illustration shows the switch-module bay locations.



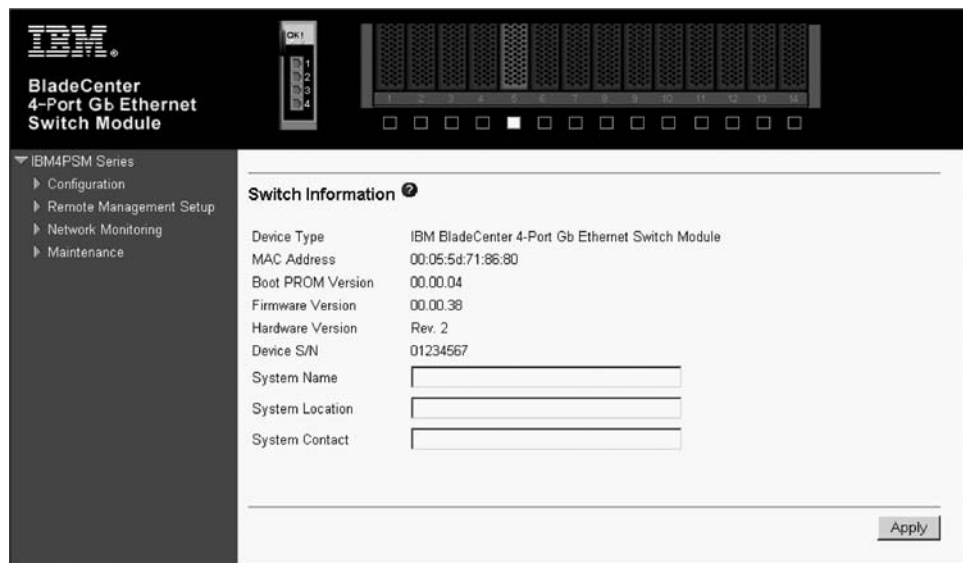
You can change the default switch IP address to meet the specification of your networking address scheme.

The switch also has a unique, factory-assigned media access control (MAC) address. The switch MAC address is located on one side of the switch module, on the same label as the serial number, as shown in the following illustration.

Note: The MAC address is also located on a separate label on the information panel under the external Ethernet port connectors.



The switch MAC address can also be found under the **Switch Information** menu item, as shown in the following illustration.



In addition, you can also set an IP address for a gateway router. This becomes necessary when the network management station is located on a different IP network from the switch, making it necessary for management packets to go through a router to reach the network manager, and vice versa.

For security, you can set a list of IP addresses of the network managers that are permitted to manage the switch. You can also change the default SNMP community strings in the switch and set the access rights of these community strings.

Traps

Traps are messages that alert you of events that occur on the switch. The events can be as serious as a restart (for example, someone accidentally turned off the switch) or less serious, such as a port-status change. The switch generates traps and sends them to the network manager (trap recipient).

Trap recipients are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap recipients will receive

traps sent from the switch; they must immediately take certain actions to avoid future failure or breakdown of the network.

You can also specify which network managers can receive traps from the switch by entering a list of the IP addresses of authorized network managers. You can enter up to four trap recipient IP addresses, and four corresponding SNMP community strings.

SNMP community strings function like passwords in that the community string entered for a given IP address must be used in the management station software, or a trap will be sent.

The following are trap types that the switch can send to a trap recipient:

Cold start

This trap indicates that the switch has been turned on and initialized such that software settings are reconfigured and hardware systems are restarted. A cold start is different from a factory reset in that configuration settings saved to nonvolatile random-access memory (NVRAM) used to reconfigure the switch.

Warm start

This trap indicates that the switch module has been restarted; however, the power-on self-test (POST) is skipped.

Authentication failure

This trap indicates that someone has tried to log on to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.

New root

This trap indicates that the switch has become the new root of the Spanning Tree. The trap is sent by the switch soon after its election as the new root. This implies that upon expiration of the topology change timer, the new root trap is sent out immediately after the switch is elected as the new root.

Topology change (Spanning Tree Protocol (STP))

This trap indicates that one or more of the configured ports changes from the learning state to the forwarding state, or from the forwarding state to the blocking state. The trap is not sent if a new root trap is sent for the same change.

Link up

This trap indicates that the link of a port has changed from link down to link up.

Link down

This trap indicates that the link of a port has changed from link up to link down.

MIBs

Management and counter information are stored in the switch in the management information base (MIB). The switch uses the standard MIB-II management information base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II module, the switch also supports its own proprietary enterprise MIB as an extended management information base. These MIBs can also be retrieved by

specifying the object identifier (OID) of the MIB as the network manager. MIB values can be either read-only or read-write.

Read-only MIB variables can be either constants that are programmed into the switch or variables that change while the switch is in operation. Examples of read-only constants are the number of ports and type of ports. Examples of read-only variables are the statistics counters, such as the number of errors that have occurred, or how much data (in kilobytes) has been received and forwarded through a port.

Read-write MIBs are variables usually related to user-customized configurations. Examples of these are the switch IP address, STA parameters, and port status.

If you use a third-party vendor's SNMP software to manage the switch, a diskette listing the switch propriety enterprise MIBs can be obtained by request. If your software provides functions to browse or modify MIBs, you can also get the MIB values and change them (if the attributes of the MIBs permit the write operation). However, this process can become complicated, because you must know the MIB OIDs and retrieve them one by one.

SNMP

The Simple Network Management Protocol (SNMP) is an open system interconnection (OSI) layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package such as IBM NetView or Hewlett-Packard OpenView. SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol
- Collecting information about the status and current configuration of network devices
- Modifying the configuration of network devices

The switch has a software program, called an *agent*, that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the user datagram protocol/Internet protocol (UDP/IP) to exchange packets.

Authentication

The authentication protocol ensures that both the router SNMP agent and the remote user SNMP application program discard packets from unauthorized users. Authentication is accomplished through using community strings, which function like passwords. The remote user SNMP application and the router SNMP must use the same community string. SNMP community strings of up to 20 characters can be entered under the Remote Management Setup menu.

Packet forwarding

The switch uses a forwarding table to store the information that it collects. The switch programs the mapping from the destination MAC address to the destination port number into its forwarding table. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only. For example, if port 1 receives a packet destined for a station on port 2, the switch transmits that packet through port 2 only and transmits nothing through the other ports. This process is referred to as learning the network topology.

The aging time affects the learning process of the switch. Dynamic forwarding table entries, which consist of the source and destination MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time.

The aging time can be from 17.2 to 2200 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out of date or no longer exist. This might cause the switch to make incorrect packet-forwarding decisions.

If the aging time is too short, however, many entries might be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table. In this case, the switch will broadcast the packet to all ports, thus negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

Spanning Tree Protocol

The Institute of Electrical and Electronics Engineers (IEEE) 802.1D Spanning Tree Protocol (STP) enables the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol enables the duplicate links to be used in the event of a failure of the primary link. When the STP is configured and enabled, primary links are established, and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically, without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the STP and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the spanning tree is incorrectly configured. Read the following information before making any changes from the default values.

The switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree
- Reconfigures the spanning tree without operator intervention

Improper configuration of the switch module external ports or improper cabling of the external ports to another switch device can create duplicate links that might cause network loops. Consult your network administrator for details about the configuration requirements for your system.

For additional information about the STP, see Appendix D, “Understanding and troubleshooting the Spanning Tree Protocol” on page 121.

VLANs

A virtual local area network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of blade servers into an autonomous user group that appears as a group within one or more chassis. VLANs also logically segment the blade servers into different broadcast domains so that packets are forwarded only between blade servers and the four external ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains.

Notes about VLANs on IBM BladeCenter 4-port Gb Ethernet switch module

No matter what basis is used to uniquely identify blade servers and assign these nodes VLAN membership, packets *cannot* cross VLANs without a network device performing a routing function between the VLANs.

The switch supports only IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The switch default is to assign all blade servers and the four external ports to a single 802.1Q VLAN named DEFAULT_VLAN.

The DEFAULT_VLAN has a VLAN ID (VID) of 1.

The Ethernet switch module can be configured to enable a wide variety of VLAN configurations among the various external ports.

IEEE 802.1Q VLANs

The following terms are relevant to VLANs and important with respect to understanding how VLANs function:

Tagging

The act of putting 802.1Q VLAN information into the header of a packet.

Untagging

The act of stripping 802.1Q VLAN information out of the packet header.

Ingress port

A port on a switch where packets are flowing into the switch and where VLAN decisions must be made.

Egress port

A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and where tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the IBM BladeCenter 4-Port Gb Ethernet Switch Module. 802.1Q VLANs require tagging, which enables them to span the entire network (provided that all switches on the network are IEEE 802.1Q-compliant).

VLANs enable a network to be segmented to reduce the size of broadcast domains. All packets entering a VLAN will be forwarded only to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN. This includes broadcast, multicast, and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will deliver packets only between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs enables VLANs to work with legacy switches that do not recognize VLAN tags in packet headers. The tagging feature enables VLANs to span multiple 802.1Q-compliant switches through a single physical connection and enables spanning tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN of which the receiving port is a member.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering
- Assumes the presence of a single global spanning tree
- Uses an explicit tagging scheme with one-level tagging

802.1Q VLAN packet forwarding

The switch makes packet-forwarding decisions based on the following types of rules:

Ingress rules

Rules relevant to the classification of received frames belonging to a VLAN.

Forwarding rules between ports

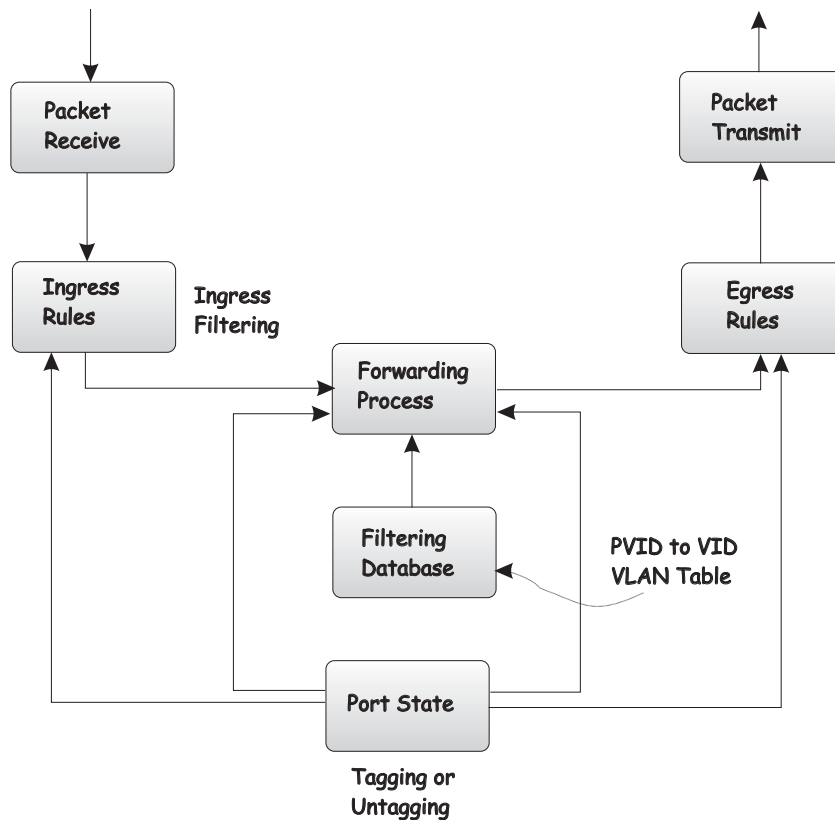
The switch decides whether to filter or forward the packet.

Egress rules

The switch determines whether the packet must be sent tagged or untagged.

The following illustration shows the 802.1Q VLAN packet-forwarding decision-making process of the switch. For more information about packet forwarding, see “Packet forwarding” on page 23. For more information about port VLAN IDs (PVIDs), see “Port VLAN ID” on page 27. For more information about tagging and untagging, see “Tagging and untagging” on page 28. For more information about port states, see “STP port states” on page 122.

802.1Q Packet Forwarding



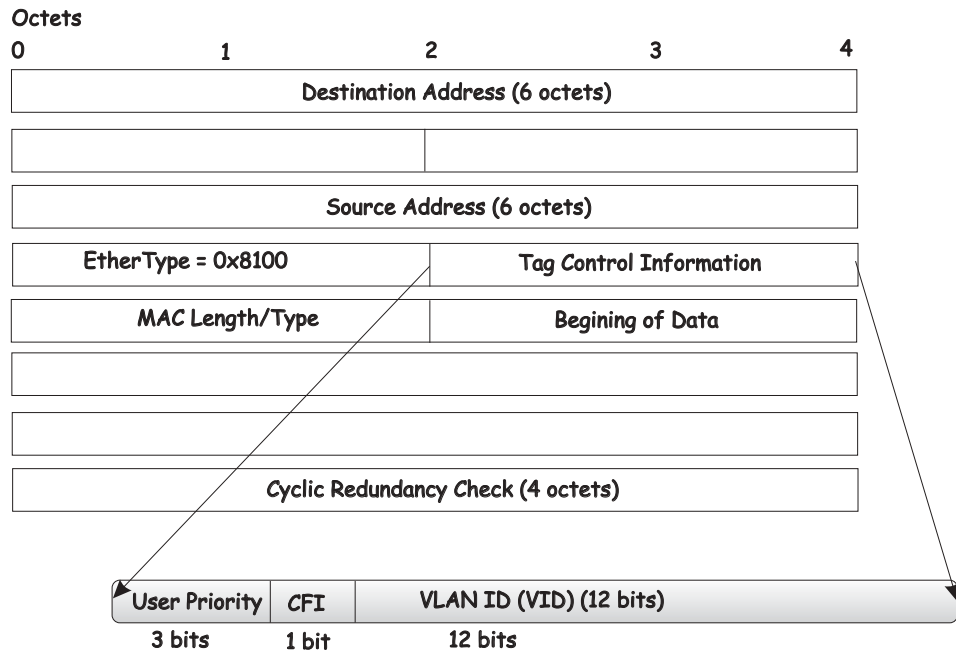
802.1Q VLAN tags

The following illustration shows the 802.1Q VLAN tag. Four additional octets are inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the **EtherType** field. When a packet **EtherType** field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following 2 octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI)¹ and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header, increasing the length of the entire packet by 4 octets. All of the information that was originally contained in the packet is retained.

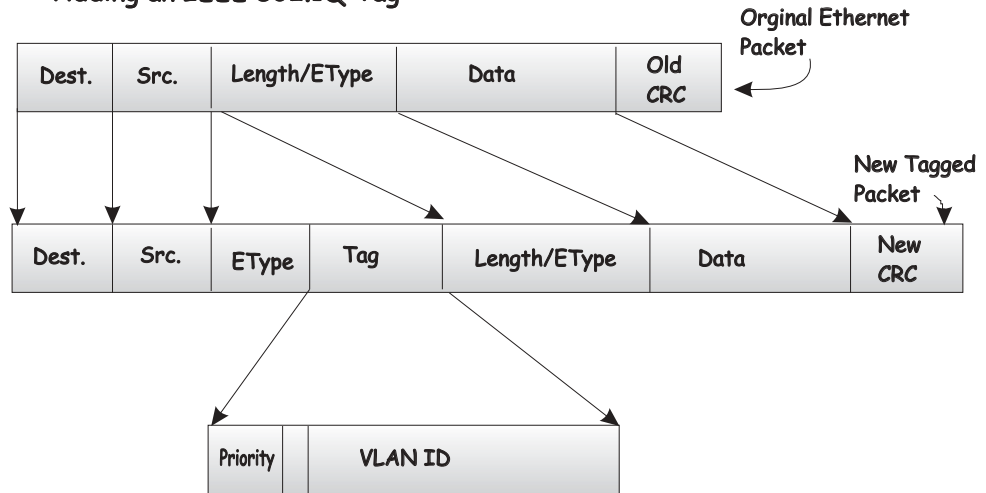
1. CFI is used for encapsulating Token Ring packets so that they can be carried across Ethernet backbones.

IEEE 802.1Q Tag



The **EtherType** and **VLAN ID** are inserted after the MAC source address, but before the original **EtherType/Length** or **Logical Link Control**. Because the packet is now 1 bit longer than it was originally, the cyclic redundancy check (CRC) must be recalculated.

Adding an IEEE 802.1Q Tag



Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This enables 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Before the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port PVID and then be forwarded to the port that corresponded to the packet destination address (found in the switch forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet.

Within the switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID of 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, where VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions; the VID is.

Tag-aware switches must keep a table to relate PVIDs within the switch to VIDs on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network might be tag-unaware, a decision must be made at each port on a tag-aware device before a packet is transmitted, whether or not to tag the packet. If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority, and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet does not have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the switch). Untagging is used to send packets from an 802.1Q-compliant network device to a noncompliant network device.

Ingress filtering

A port on a switch where packets are flowing into the switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the switch will examine the VLAN information in the packet header (if present) and decide whether to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine whether the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the switch then determines whether the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded, and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines whether the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded, and the destination port transmits it on its attached network segment.

This process is referred to as *ingress filtering* and is used to conserve bandwidth within the switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

VLANs

The switch initially configures one VLAN (VID = 1), known as the DEFAULT_VLAN. The factory default setting assigns all ports on the switch to the DEFAULT_VLAN. As new VLANs are configured, their respective member ports are removed from the DEFAULT_VLAN. In addition, the VID value of 4095 is reserved for internal use.

Packets cannot cross VLANs. If a member of one VLAN is to connect to another VLAN, the link must be through an external router.

All VLANs must be configured before the IP interface is set up. An IP addressing scheme must then be established, and implemented when the IP interface is set up on the switch.

Notes:

1. If no VLANs are configured on the switch, all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.
2. An IP interface consists of two parts: a subnet mask and a network address. You will need to use this information when you configure the IP interface of the switch.

DHCP

The Dynamic Host Configuration Protocol (DHCP) can reduce the administrative burden of assigning and maintaining IP address information. DHCP provides reliable and simple TCP/IP network configuration, ensures that address conflicts do not occur, and helps to conserve the use of IP addresses through the centralized management of address allocation.

Dynamic address allocation enables a client to be assigned an IP address from a pool of free addresses. Each address is assigned with a lease and a lease expiration period. The client must renew the lease to continue using the assigned address. Dynamically assigned addresses can be returned to the free address pool if the computer is not being used, if it is moved to another subnet, or if its lease expires. Usually, network policy ensures that the same IP address is assigned to a client each time and that addresses returned to the free address pool are reassigned.

When the address lease expires, the DHCP client enters the renewing state. The client sends a request message to the DHCP server that provided the address. The DHCP server sends an acknowledgement that contains the new lease and configuration parameters. The client then updates its configuration values and returns to the bound state.

When the DHCP client is in the renewing state, it must release its address immediately in the rare event that the DHCP server sends a negative acknowledgment. The DHCP server sends this message to inform a client that it has incorrect configuration information, forcing it to release its current address and acquire new information.

If the DHCP client cannot successfully renew its lease, the client enters a rebinding state. The client then sends a request message to all DHCP servers in its range, attempting to renew its lease. Any DHCP server that can extend the lease sends an acknowledgment containing the extended lease and updated configuration information. If the lease expires or if a DHCP server responds with a negative acknowledgment, the client must release its current configuration and then return to the initializing state.

If the DHCP client uses more than one network adapter to connect to multiple networks, this protocol is followed for each adapter that you want to configure for TCP/IP. Multi-homed systems are selectively configured for any combination of system interfaces.

When a DHCP-enabled computer is restarted, it sends a message to the DHCP server with its current configuration information. The DHCP server either confirms this configuration or sends a negative reply so that the client must begin the initializing state again. System startup might, therefore, result in a new IP address for a client computer, but neither the user nor the network administrator has to take any action in the configuration process.

Before loading TCP/IP with an address acquired from the DHCP server, DHCP clients check for an IP address conflict by sending an Address Resolution Protocol (ARP) request containing the address. If a conflict is found, TCP/IP does not start, and the user receives an error message. The conflicting address should be removed from the list of active leases, or it should be excluded until the conflict is identified and resolved.

Chapter 5. Web-Based network management

This chapter describes how to use the Web-based network management module to access and configure the internal switching software.

Important: Before you configure your Ethernet switch module, be sure that the management modules in your BladeCenter unit are properly configured. In addition, to access and manage your Ethernet switch module from an external environment, you might need to enable certain features, such as the external ports and external management over all ports. See the applicable *BladeCenter Installation and User's Guide* publications on the *IBM BladeCenter Documentation* CD for more information.

In addition to reviewing the publications in this library, be sure to review the *IBM BladeCenter Planning and Installation Guide* located at <http://www.pc.ibm.com/eserver/bladecenter> on the World Wide Web for information to help you prepare for system installation and configuration.

Introduction

The switch module offers an embedded hypertext markup language (HTML), Web-based interface that enables you to manage the switch through a standard browser, such as Opera, Netscape Navigator/Communicator, or Microsoft® Internet Explorer. The Web browser acts as an access tool and can communicate directly with the switch using the HTTP protocol. Your browser window might vary with the window illustrations in this guide.

Note: This Web-based management module does not accept Chinese language input (or other double-byte character-set languages).

The Web-based management module and the Telnet program are different ways to access the same internal switching software and configure it. Thus, all the settings that you encounter in Web-based management are the same as those found in the Telnet program. If your system application requires that you use the Telnet program, see Chapter 6, "Configuring the switch module through the Telnet interface" on page 75 for additional information.

Remotely managing the Ethernet switch module

The Ethernet switch module supports two remote-access modes for management through Ethernet connections. You can select the mode that is best suited for your BladeCenter environment. The Ethernet switch module has an internal Ethernet path to the management module and the four external Ethernet ports on the switch module.

- The default mode uses the internal path to the management module only. In this mode, the remote-access link to the management console must be attached to the 10/100 Mbps Ethernet port on the management module. With this mode, the IP addresses and SNMP parameters of the Ethernet switch modules can be automatically assigned by the IBM Director BladeCenter Deployment Wizard or, you must manually assign them through the BladeCenter Management and Configuration Program. This mode enables the system administrator to provide a secure LAN for management of the BladeCenter subsystems separately from the data network.

Important: With this mode, the Ethernet switch module does not respond to remote-management commands through the four external Ethernet ports on the switch module.

See the applicable *BladeCenter Installation and User's Guide* on the *IBM BladeCenter Documentation* CD for additional instructions for configuring the Ethernet switch module for this mode of operation.

- The system administrator can select to enable remote management of the Ethernet switch module through the four external Ethernet ports on the switch module, instead of or in addition to access through the management module. This mode can only be enabled through the management module configuration interface. Once this mode is enabled, the external Ethernet ports will support both management traffic and BladeCenter application data traffic. Also, the Ethernet switch module can transmit DHCP and BOOTP request frames through the external Ethernet ports.

This mode enables the Ethernet switch module IP addresses to reside on a different subnet than the management modules. This is useful when the Ethernet switch modules are to be managed and controlled as part of the overall network infrastructure, while maintaining secure management of other BladeCenter subsystems through the management module. However, management access to the Ethernet switch-module link will be lost if the Ethernet switch module IP address is not on the same subnet as the management module. This chapter contains additional instructions for configuring the Ethernet switch module for this mode of operation.

The two previously described modes are only applicable to the Ethernet switch module. The management module can only be remotely accessed through the 10/100 Mbps Ethernet port on the management module.

Getting started

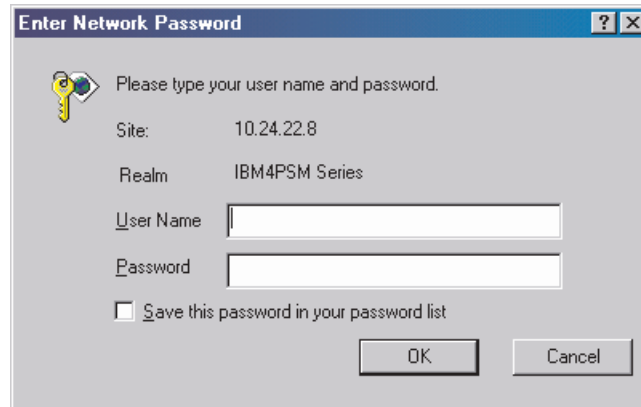
The first step in getting started with using Web-based management for your switch is to install a browser. A Web browser is a program that enables a person to read hypertext, for example, Opera, Netscape Navigator, or Microsoft Internet Explorer. Follow the installation instructions for the browser.

The second and last step is to configure the IP interface of the switch. To do this, use the IBM Director Configuration and Deployment Wizard or the BladeCenter Configuration Management program (see the applicable *BladeCenter Installation and User's Guide* publications on the *IBM BladeCenter Documentation* CD for more information).

Note: An IP interface consists of two parts: a subnet mask and a network address. You will need to use this information when you configure the IP interface of the switch.

You are now ready to begin managing your switch by simply running the browser installed on your computer and pointing it to the IP address that you have defined for the device. The URL in the address bar should have the following format and contain information similar to: `http://123.123.123.123`, where the numbers *123* represent the IP address of the switch.

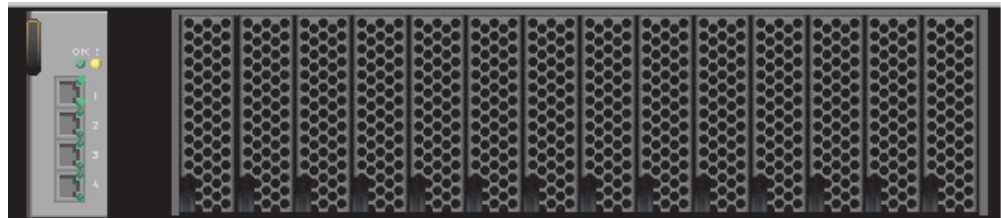
Depending on which browser you are using, a dialog box similar to the following will open:



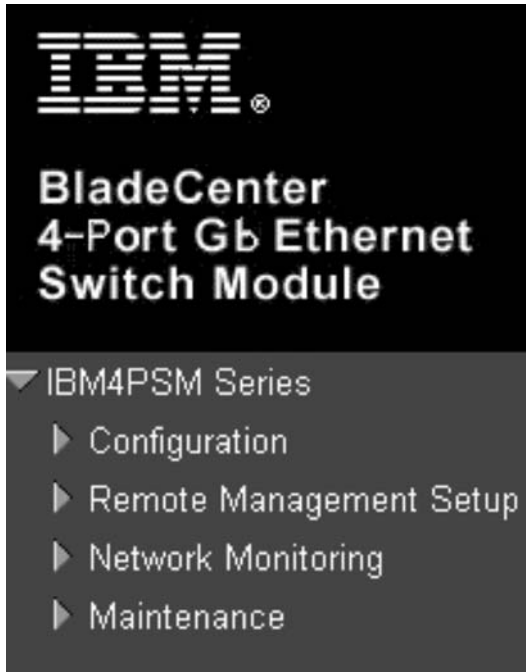
Enter USERID for the **User Name** and PASSWORD for the **Password** (where the sixth alphanumeric character is the number zero, not the letter O) and click **OK**. This opens the main page in the management module.

Note: Capital letters are required, as these fields are both case-sensitive. To increase system security, change the password after you log onto the system for the first time and, be sure to store the new password in a safe location.

The top panel shows a real-time information-panel display of the switch module:



The panel on the left side contains the main menu. The featured items include: **Configuration, Remote Management Setup, Network Monitoring, and Maintenance.**

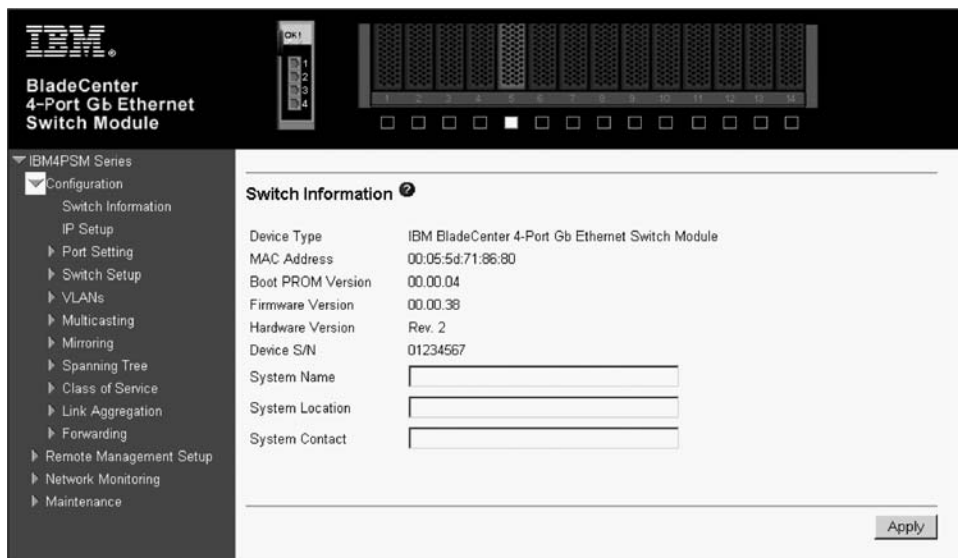


These are the major categories for switch module management. If the sub-menus for each main category do not appear, click the small square hyperlink to the left of the folder icon.

The Web-based switch module management features are described in the following sections in this chapter.

Configuration

The Configuration menu includes: **Switch Information, IP Setup, Port Setting, Switch Setup, VLANs, Multicasting, Mirroring, Spanning Tree, Class of Service, Link Aggregation, and Forwarding**, as well as secondary windows.



Switch Information

When you select **Switch Information** from the Configuration menu, a window similar to the following opens:

Device Type	IBM BladeCenter 4-Port Gb Ethernet Switch Module
MAC Address	00:05:5d:71:86:80
Boot PROM Version	00.00.04
Firmware Version	00.00.38
Hardware Version	Rev. 2
Device S/N	01234567
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

Apply

To establish the basic switch settings, enter a name for the switch in the **System Name** field, the physical location of the switch in the **System Location** field, and the name of the contact person responsible for the switch in the **System Contact** field. Then, click **Apply**.

The data fields on the Switch Information window are described as follows:

Device Type

A description of the switch type.

MAC Address

The Ethernet address for the device.

Boot PROM Version

Version number for the firmware startup code.

Firmware Version

Version number of the firmware code installed on the switch. This can be updated by using the Update Firmware window in the **Reset and Update** section of the Switch Information window.

Hardware Version

Version number of the hardware installed on the switch.

System Name

A user-assigned name for the switch.

System Location

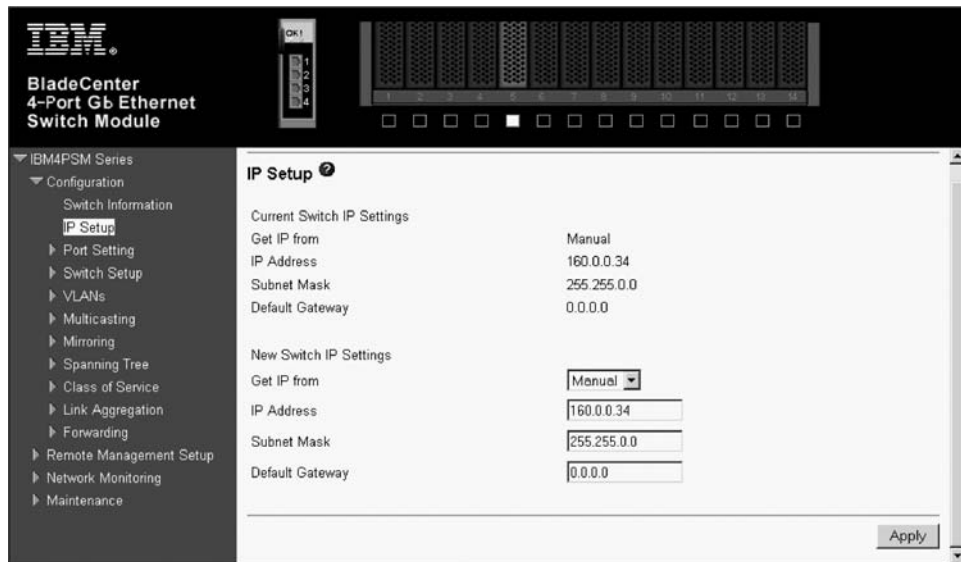
A user-assigned description for the physical location of the switch.

System Contact

The name of the person to contact regarding any problems or questions with respect to the switch. You might also want to include a phone number or extension.

IP Setup

When you select **IP Setup** from the **Configuration** menu, a window similar to the following opens:



This window is used to determine whether the switch should get its IP Address settings from the user (Manual), a BOOTP server, or a DHCP server. If you are not using either BOOTP or DHCP, enter the **IP Address**, **Subnet Mask**, and **Default Gateway** of the switch. If you enable BOOTP, you do not need to configure any IP parameters because a BOOTP server automatically assigns IP configuration parameters to the switch. If you enable DHCP, a Dynamic Host Configuration Protocol request will be sent when the switch is turned on. Once you have selected a setting under **Get IP From**, click **Apply** to activate the new settings.

Note: BOOTP and DHCP are only supported through the four external Ethernet ports on the switch module. To use BOOTP and DHCP, you must first enable these ports for remote-management access through the BladeCenter management and configuration program. For a detailed description of this program, see the *@server BladeCenter Type 8677 Installation and User's Guide* on the *IBM BladeCenter Documentation CD*.

The switch default IP address is 192.168.70.1xx, where xx depends on the number of the bay into which you have installed the switch module, as shown in Table 2.

Table 2. Default IP addresses based on switch-module bay numbers (IP Setup window of Web-based Configuration menu)

Bay number	Default IP address
Bay 1	192.168.70.127
Bay 2	192.168.70.128
Bay 3	192.168.70.129
Bay 4	192.168.70.130

The data fields on the IP Setup window are described as follows:

Get IP From

There are three choices for how the switch receives its IP Address settings: **Manual**, **BOOTP**, and **DHCP**.

Manual

You can enter an IP address, a subnet mask, and a default gateway for the switch. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields that require entries under this option are as follows:

IP Address

The host address for the device on the TCP/IP network.

Subnet Mask

The address mask that controls subnetting on your TCP/IP network. This address mask is a bitmask that determines the extent of the subnet that the switch module is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but you can also use custom subnet masks.

Note: For switch communication with a remote management station, such as the IBM Director server, through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

Default Gateway

The IP address that determines where packets with a destination address outside the current subnet should be sent. The IP address of the device is usually the address of a router or a host acting as an IP gateway to handle connections to other subnets or other TCP/IP networks. If your network is not part of an intranet, or you do not want the device to be accessible outside your local network, you can enter a value of **0.0.0.0** in this field.

BOOTP

The switch module will send out a BOOTP broadcast request when it is turned on. The BOOTP protocol enables IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the switch module will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

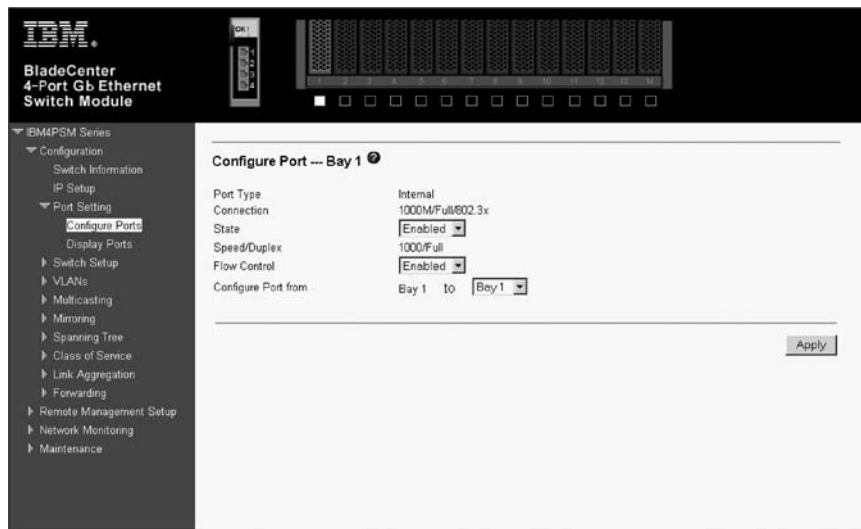
DHCP The switch module will send out a DHCP broadcast request when it is turned on. The DHCP protocol enables IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.

Port Setting

When you select **Port Setting** from the Configuration menu, you can then select either **Configure Ports** or **Display Ports** from the Port Setting menu. These menu choices are described in the following sections.

Configure Ports

When you select **Port Setting** from the Configuration menu and **Configure Ports** from the Port Setting menu, a window similar to the following opens:



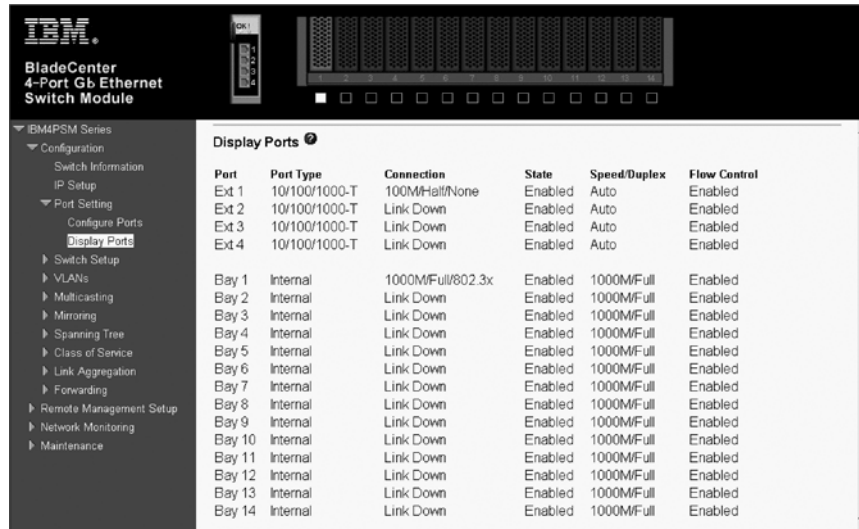
Select the port that you want to configure by using the drop-down menus in the **Configure Port from and to** fields. Follow these steps:

1. Enable or disable the port. If you select **Disabled** in the **State** field, devices connected to that port cannot use the switch, and the switch purges their addresses from its address table after the MAC address aging time elapses.
2. Configure the **Speed/Duplex** setting for the four external 10/100/1000 Mbps ports. Select **Auto** to enable the port to select the best transmission speed, duplex mode, and flow control settings based on the capabilities of the device at the other end. The other selections enable you to force the port to operate in the specified manner. Select **1000M/Full** for port operation at 1000 Mbps and full duplex. Select **100M/Full** for port operation at 100 Mbps and full duplex. Select **100M/Half** for port operation at 100 Mbps and half duplex. Select **10M/Full** for port operation at 10 Mbps and full duplex. Select **10M/Half** for port operation at 10 Mbps and half duplex. The 14 internal ports are **1000M/Full** only.
3. Configure the **Flow Control** setting for the port. Selecting **Enabled** in full-duplex mode will implement IEEE 802.3x flow control. Select **Disabled** for no flow control. Also, if the port is set for **Auto (NWay)** in the **Speed/Duplex** field and flow control is enabled, flow control (whether full- or half-duplex) will only be implemented if the other device can auto-negotiate flow control.
4. Click **Apply** to make your changes effective.

To view the configuration settings for the ports on the switch module, see “Display Ports”.

Display Ports

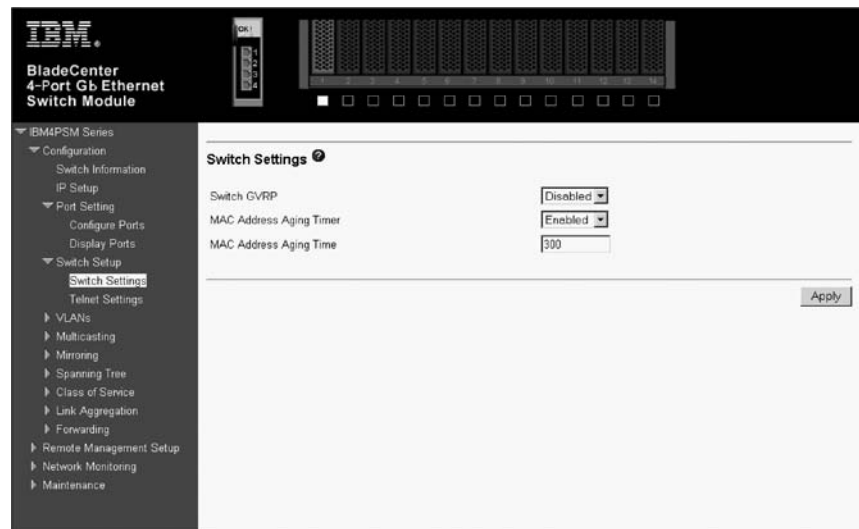
When you select **Port Setting** from the Configuration menu and **Display Ports** from the Port Setting menu, a window similar to the following opens:



This window displays the applicable configuration information for all the internal and external ports on the switch module, based on the configuration settings that you selected or accepted in “Configure Ports” on page 38. Ports are not selectable on this window and, the information on this window is not changeable. To change the configuration settings for the ports on the switch module, see “Configure Ports” on page 38.

Switch Settings

When you select **Switch Setup** from the Configuration menu and **Switch Settings** from the Switch Setup menu, a window similar to the following opens:



The user-changeable parameters on this window are as follows:

Switch GVRP <Disabled>

Group VLAN Registration Protocol is a protocol that enables members to dynamically join VLANs. This is used to enable or disable GVRP on the switch module.

MAC Address Aging Timer <Enabled>

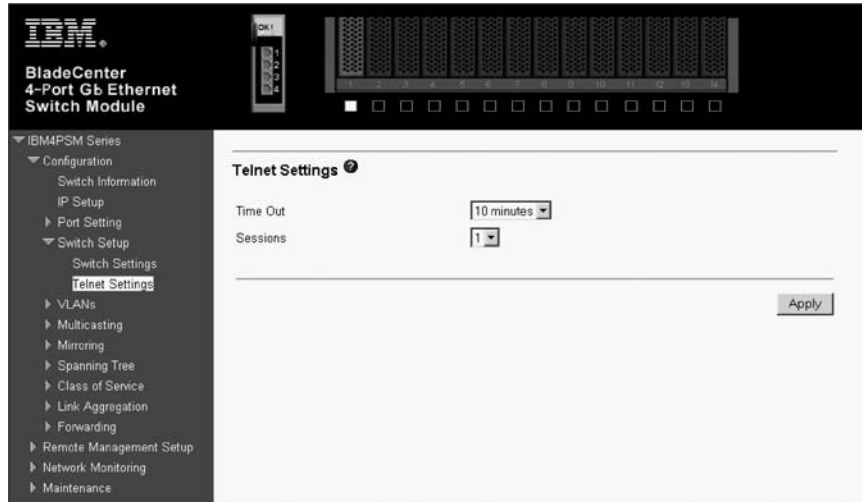
This field specifies whether the aging timer is on or off.

Telnet Settings

Complete the following steps to display the Telnet Settings window:

1. Select **Switch Setup** from the Configuration menu (see “Configuration” on page 34).
2. Select **Telnet Settings** from the Switch Setup menu.

A window similar to the following opens:



The user-changeable parameters on this window are as follows:

Time Out <10 mins>

This sets the time that the Telnet interface can be idle before the switch automatically logs-out the user. The options are: **2 mins, 5 mins, 10 mins, 15 mins, and Never.**

Sessions [1]

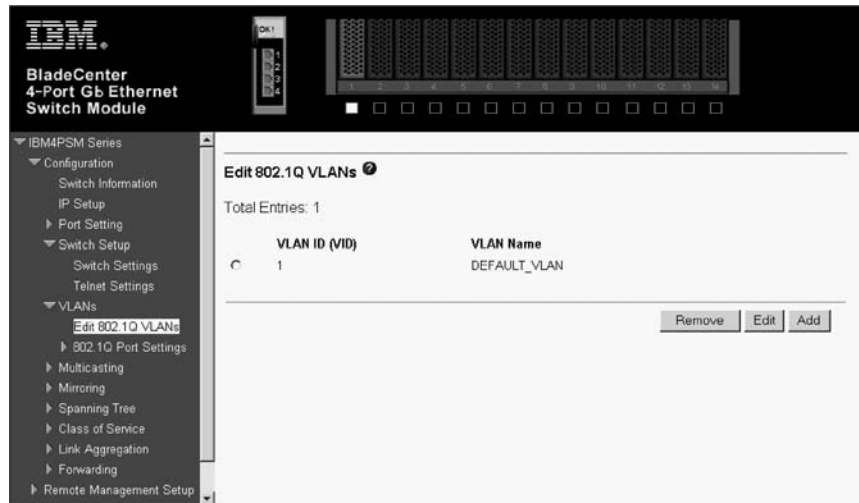
This sets the maximum number of available Telnet sessions.

VLANs

This section includes **Edit 802.1Q VLANs** and **802.1Q Port Settings**.

Edit 802.1Q VLANs

To create, modify, or remove an 802.1Q VLAN, select **VLANs** from the Configuration menu (see “Configuration” on page 34) and **Edit 802.1Q VLANs** from the VLANs menu. A window similar to the following opens:



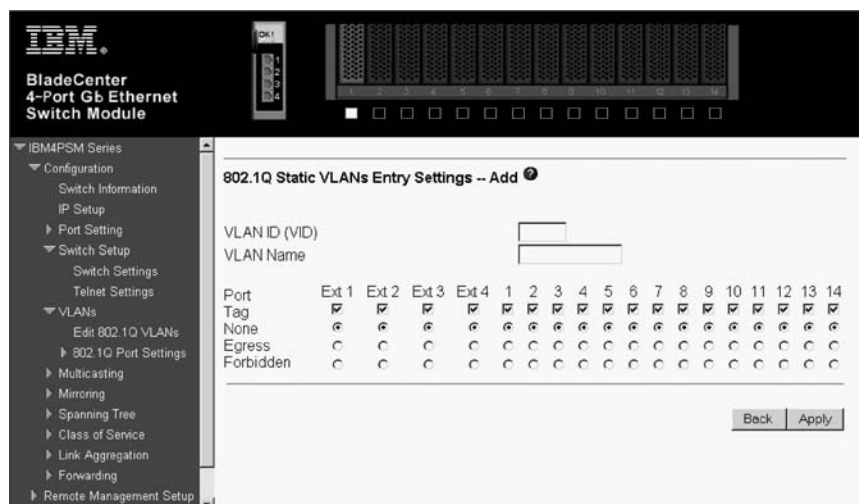
You can delete, add, and remove entries through this window. To delete an entry, click the circle next to the appropriate entry; then, click **Remove**. To add an entry, click **Add** and follow the instructions in “802.1Q VLANs Entry Settings -- Add”. To modify an existing entry, click **Edit** and follow the instructions in “802.1Q VLANs Entry Settings -- Edit” on page 42.

802.1Q VLANs Entry Settings -- Add

Complete the following steps to display the 802.1Q VLANs Entry Settings -- Add window:

1. Select **VLANs** from the Configuration menu (see “Configuration” on page 34).
2. Select **Edit 802.1Q VLANs** from the VLANs menu.
3. Click **Add** on the Edit 802.1Q VLANs window.

A window similar to the following opens:



To add an entry, enter the appropriate information in the preceding window. Click **Apply** to make the changes effective.

To configure an 802.1Q static VLAN entry, select the desired VLAN ID number in the first field and then enter a VLAN name in the second field. Next, either check the **Tag** option, or leave it unchecked if you do not want a member port to be a Tagging port. In the last two rows, check **None** if you do not want a port to belong

to the VLAN. Otherwise, check **Egress** to statically set a port to belong to a VLAN, or **Forbidden** to prevent a port from being a member of the VLAN. Click **Apply** to make the changes effective.

802.1Q VLANs Entry Settings -- Edit

Complete the following steps to display the 802.1Q VLANs Entry Settings -- Edit window:

1. Select **VLANs** from the Configuration menu (see “Configuration” on page 34).
2. Select **Edit 802.1Q VLANs** from the VLANs menu.
3. Click **Edit** on the Edit 802.1Q VLANs window.

The 802.1Q VLANs Entry Settings -- Edit window opens.

To modify an entry, complete the appropriate information on the window, and then click **Apply**.

The information on this window is described as follows:

VLAN ID (VID)

The VLAN ID of the VLAN that is being created.

VLAN Name

The name of the VLAN that is being created.

Tag Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.

None Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.

Egress

Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.

Forbidden

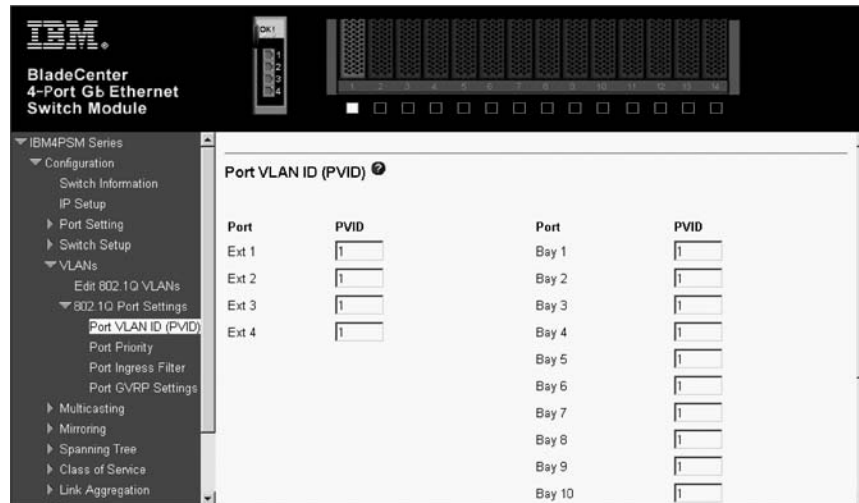
Specifies the port that is not permitted to be a member of the VLAN.

Port VLAN ID (PVID)

Complete the following steps to display the Port VLAN ID (PVID) window:

1. Select **VLANs** from the Configuration menu (see “Configuration” on page 34).
2. Select **802.1Q Port Settings** from the VLANs menu.
3. Select **Port VLAN ID (PVID)** from the 802.1Q Port Settings window.

A window similar to the following opens:



This window enables you to assign a Port VLAN ID (PVID) number to an individual port. Click **Apply** to make your changes effective.

The information on this window is described as follows:

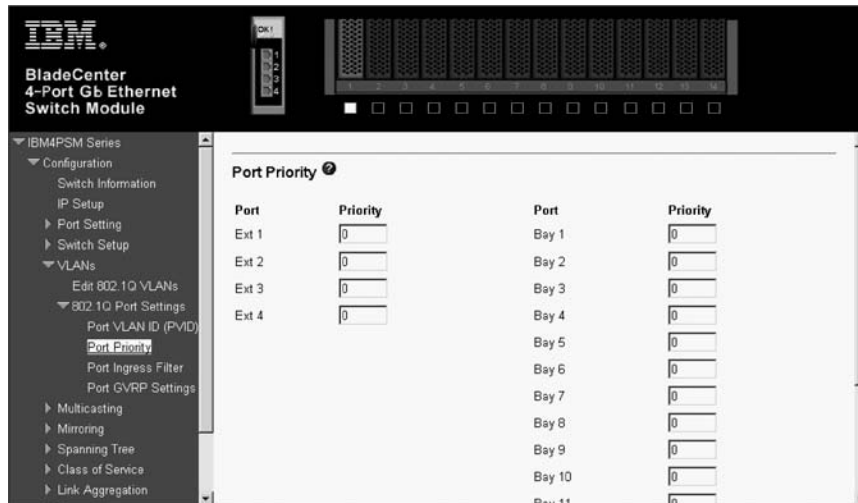
PVID The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port and, Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.

Port Priority

Complete the following steps to display the Port Priority window:

1. Select **VLANs** from the Configuration menu (see “Configuration” on page 34).
2. Select **802.1Q Port Settings** from the VLANs menu.
3. Select **Port Priority** from the 802.1Q Port Settings window.

A window similar to the following opens:



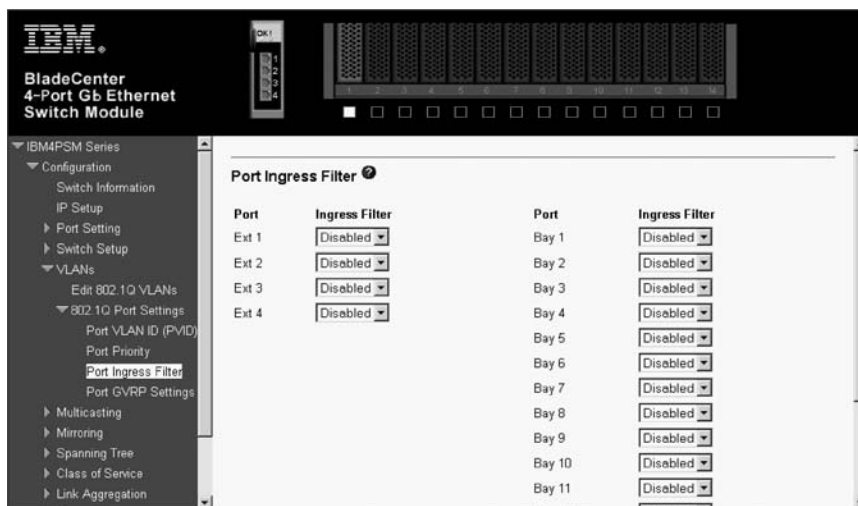
This window enables you to set a default priority for packets that have not already been assigned a priority value. After entering a **Priority** value, click **Apply** to make your changes effective.

Port Ingress Filter

Complete the following steps to display the Port Ingress Filter window:

1. Select **VLANs** from the Configuration menu (see “Configuration” on page 34).
2. Select **802.1Q Port Settings** from the VLANs menu.
3. Select **Port Ingress Filter** from the 802.1Q Port Settings window.

A window similar to the following opens:



To set an Ingress Filter, select the desired port and then use the drop-down menu to enable it. Click **Apply** to make your change effective.

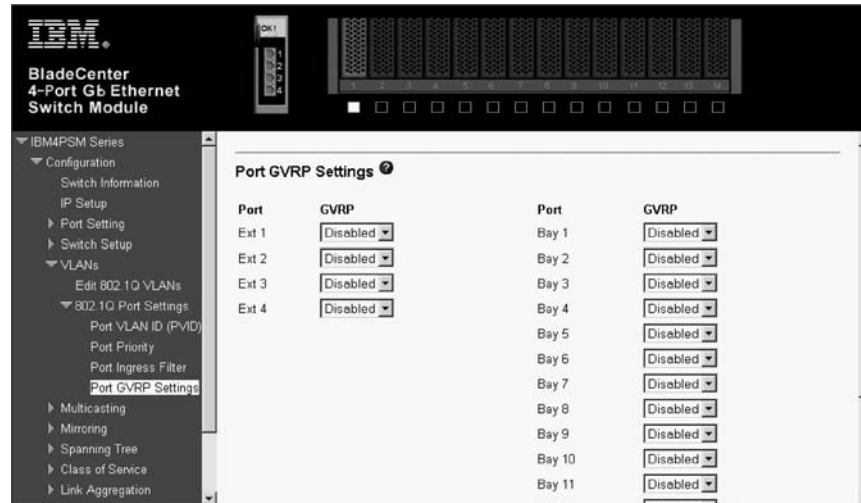
An Ingress Filter enables the port to compare the VID tag of an incoming packet with the both the VIDs and PVIDs of VLANs assigned to the port. If the VID tag of an incoming port is different from either the VID or PVID assigned to the port, the port filters (drops) the packet.

Port GVRP Settings

Complete the following steps to display the Port GVRP Settings window:

1. Select **VLANs** from the Configuration menu (see “Configuration” on page 34).
2. Select **802.1Q Port Settings** from the VLANs menu.
3. Select **Port GVRP Settings** from the 802.1Q Port Settings window.

A window similar to the following opens:



GARP VLAN Registration Protocol (GVRP) is a Generic Attribute Registration Protocol (GARP) application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports.

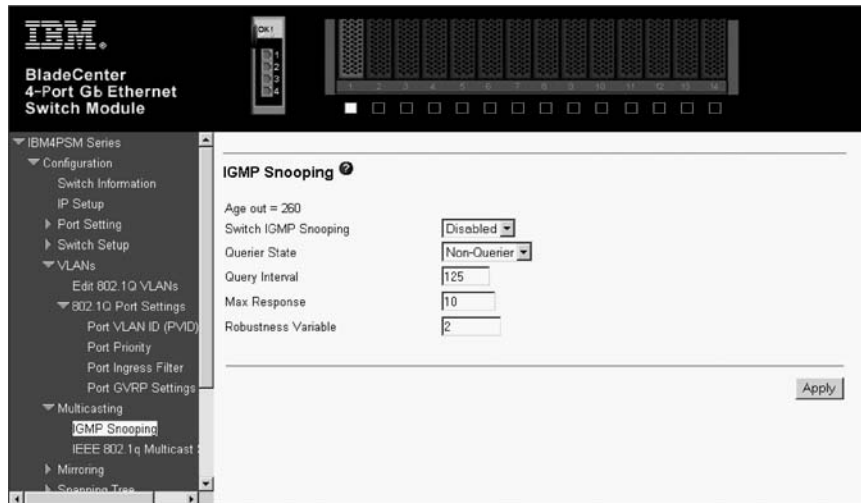
Once you enable the desired port, click **Apply** to make your changes effective.

Multicasting

Multicasting is described in the following sections.

IGMP Snooping

To access the IGMP Snooping window, select **IGMP Snooping** from the Multicasting menu. IGMP Snooping can be globally enabled or disabled from the IGMP Snooping window.



To configure IGMP Snooping, change the **Switch IGMP Snooping** drop-down menu to **Enabled**. Adjust the Querier State field to the appropriate choice among **Non-Querier**, **V1-Querier**, and **V2-Querier** to determine the version of IGMP that is used in your network. You can enter a value between 1 and 255 for the **Robustness Variable** (default is 2). You can set the **Query Interval** between 1 and 65500 seconds (default is 125 seconds). This sets the time between IGMP queries. The **Max Responses** enables a setting between 1 and 25 seconds (default is 10) and specifies the maximum available amount of time before sending a response report. The **Age Out** timer is fixed at 260 seconds. Click **Apply** to make the settings effective.

The user-changeable parameters are as follows:

Switch IGMP Snooping: <Disabled>

This drop-down menu can be used to enable or disable IGMP Snooping, globally, on the switch.

Querier State: <Non-Querier>

This drop-down menu can be set to **Non-Querier**, **V1-Querier**, or **V2-Querier**. This is used to specify the IGMP version (1 or 2) that will be used by the IGMP interface when making queries.

Robustness Variable: [2]

A tuning variable for sub-networks that are expected to lose a large number of packets. You can enter a value between 1 and 255, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.

Query Interval: [125]

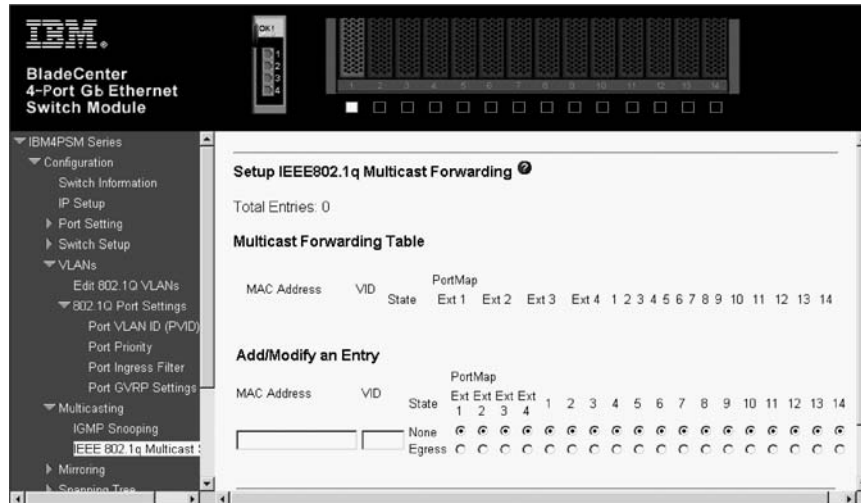
Specifies the length of time between sending IGMP queries. You can enter a value between 1 and 65500 seconds, with a default of 125 seconds.

Max Responses: [10]

Sets the maximum available amount of time before sending an IGMP response report. You can enter a value between 1 and 25 seconds, with a default of 10 seconds.

IEEE 802.1q Multicast Setting

To edit the IEEE 802.1q multicast settings, highlight **IEEE 802.1q Multicast Setting** on the Multicasting menu to access the following window:



To add a new entry to the multicast forwarding table, enter the MAC address of the multicast source in the **Multicast MAC Address** field and enter the VLAN ID number of the VLAN that will be receiving the multicast packets in the **VID** field. Then, select the member ports. Each port can be an Egress or a non-member of the multicast group, on a per-VLAN basis. An **Egress** member specifies the port as being a static member of the multicast group. Egress member ports are ports that will be transmitting traffic for the multicast group. A **Non-Member** specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically. Click **Apply** to make the changes current. Select **Save Changes** to enter the changes into NVRAM (see “Saving changes” on page 72).

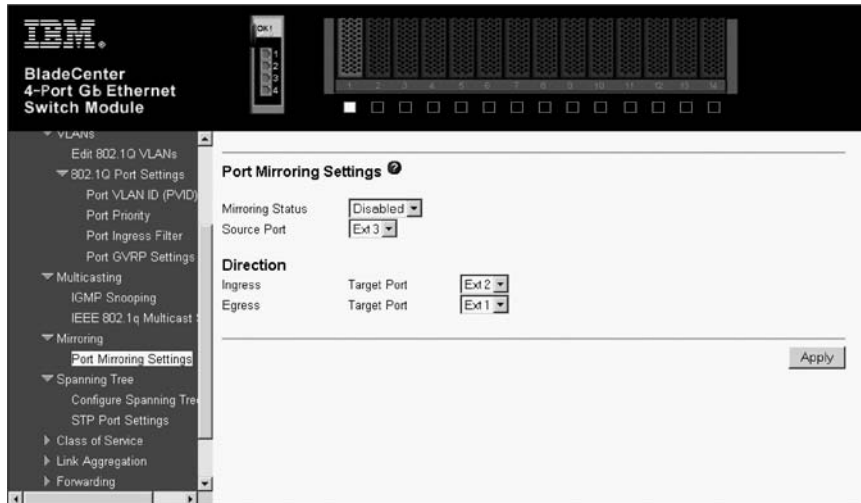
Mirroring

The switch module enables you to copy frames that were transmitted and received on a source port and to redirect the copies to another target port. The source port can be one of the four 10/100/1000 Mbps external ports, while the target port is where you will connect a monitoring/troubleshooting device, such as a sniffer or an RMON probe and, it must be one of the four 10/100/1000 Mbps external ports.

You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets that pass through the first port. This is useful for network monitoring and troubleshooting purposes.

The default setting for port mirroring is **Disabled**.

The Port Mirroring Settings window contains the following information:



To configure a mirror port, enter the port from where you want to copy frames in the **Source Port** field, and the Ingress and/or Egress port in the appropriate **Target Port** field(s). The source port must be one of the four external ports (Ext1, Ext2, Ext3, or Ext4). The target port must be one of the four external ports (Ext1, Ext2, Ext3, or Ext4). Finally, use the Mirroring Status drop-down menu to enable the feature. The default value for **Mirroring Status** is **Disabled**. Click **Apply** to make your changes effective.

Notes:

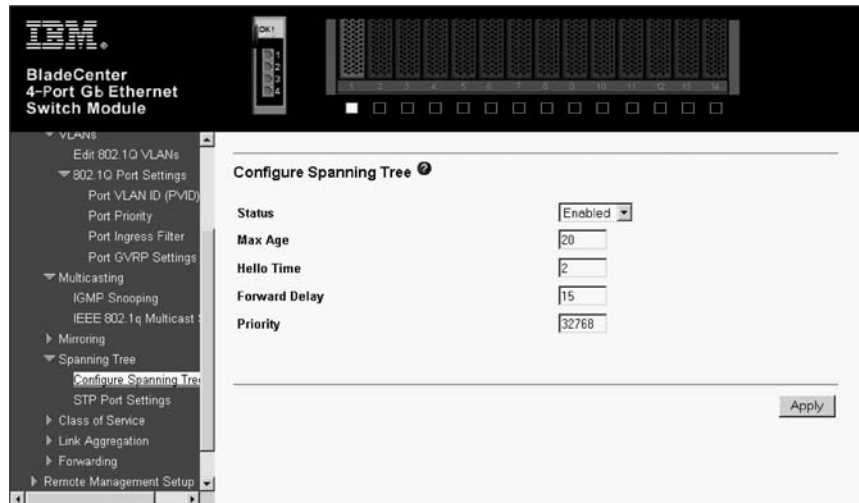
1. Do not mirror a faster port or higher traffic ports onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port from which you are copying frames should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port cannot be a member of a trunk group.
2. Port mirroring is not possible if you use the same egress and ingress target port.

Spanning Tree

This section includes two windows, **Configure Spanning Tree** and **STP Port Settings**.

Configure Spanning Tree

The switch supports 801.2d STP, which enables you to create alternative paths (with multiple switches or other types of bridges) in your network. See “Spanning Tree Protocol” on page 23 for a detailed explanation.



Click **Apply** after making changes to the preceding window.

The parameters that you can change are:

Status

This drop-down menu enables you to enable the STP setting.

Max Age: [6 .. 40] <20>

The maximum age can be set from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the root bridge, your switch will start sending its own BPDU to all other switches for permission to become the root bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the root bridge.

Hello Time: (1 .. 10 Sec) <2>

The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge. If you set a Hello Time for your switch, and it is not the root bridge, the set Hello Time will be used if and when your switch becomes the root bridge.

Note: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Forward Delay: (4 .. 30 Sec) <15>

The Forward Delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

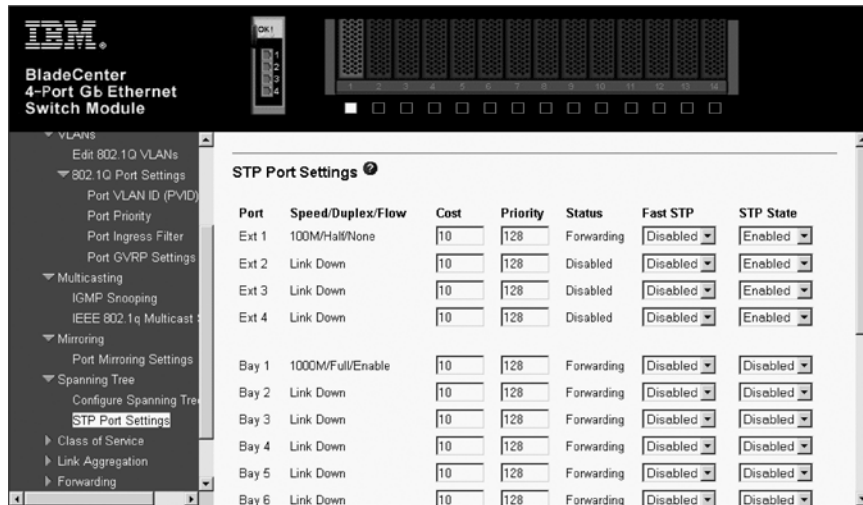
Priority: (0 .. 65535 Sec) <32768>

A bridge priority can be from 0 to 65535. Zero is equal to the highest bridge priority.

STP Port Settings

In addition to setting Spanning Tree parameters for use on the switch level, the switch module enables for the configuration of STP on individual ports.

To define individual ports, highlight **STP Port Settings** on the Configure Spanning Tree menu and press Enter.



To configure STP functions for individual ports, enter the desired information in the fields on this window (see the following descriptions for assistance) and then click **Apply**.

The information on this window is described as follows:

View Ports

Enter the range of ports to be configured and displayed.

Cost [10]

A port cost can be set between 1 and 65535. The lower the cost, the greater the probability that the port will be chosen as the designated port (chosen to forward packets).

Priority [128]

A port priority can be set from 0 to 255. The lower the priority, the greater the probability that the port will be chosen as the root port.

Fast STP <Disabled>

Use the drop-down menu to switch between **Enabled** and **Disabled**. When the STP is turned on, a change from link-down to link-up will trigger the STP. The STP will set the port to the listening state. After the forward delay, the STP will set the port to the learning state. After another forward delay, the STP will set the port to the forwarding state. If the forward delay is 15 seconds, the port will take 30 seconds to forward packets. However, when Fast STP is **Enabled** on a port, the port will only take 15 seconds from link-up to the time that it starts forwarding packets. This is because enabling the Fast STP option will skip the learning state, jumping directly to the forwarding state from the listening state.

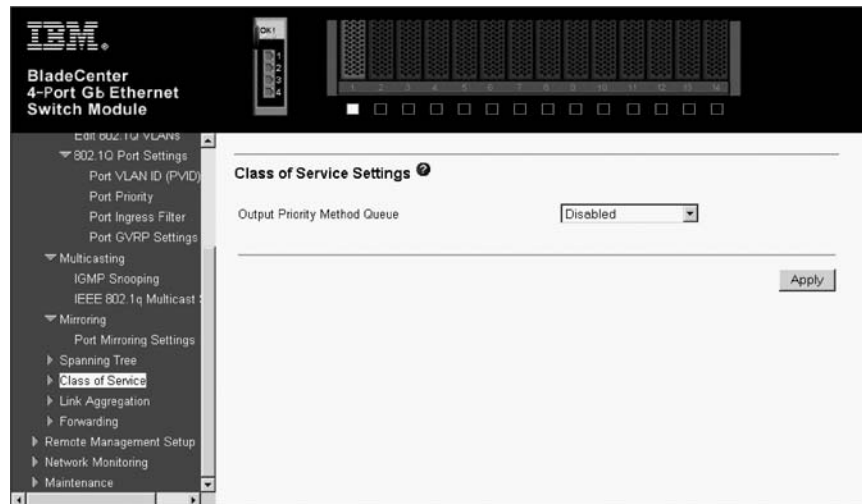
STP State <Enabled>

The STP state for a selected port can either be **Enabled** or **Disabled**.

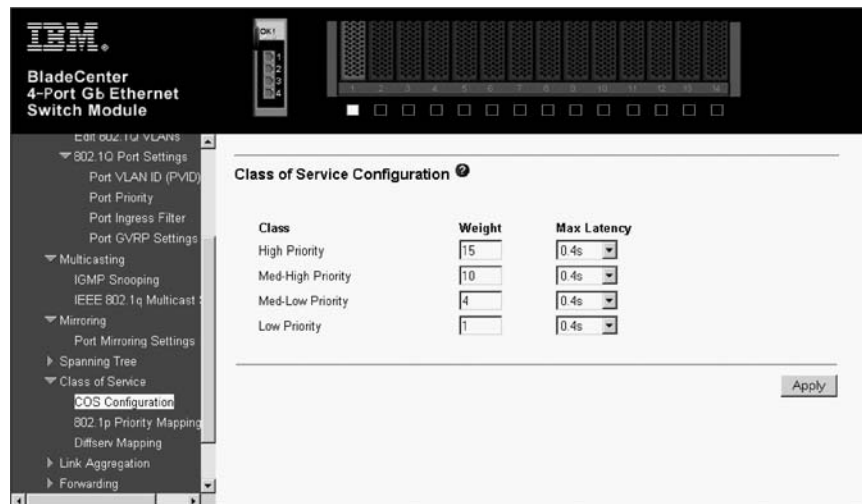
Class of Service

The switch module supports 802.1p priority queuing; four priority queues are supported per port. The switch module provides user-programmable mapping (four Priority Queue assignments: High, Med-High, Med-Low, Low) for the eight 802.1p priority classes (0 to 7). For the priority queue feature to take effect, users must first enable the Output Priority Queue Method on the Class of Service following window. Otherwise, only the round-robin method can be used to schedule the packets in four different priority queues.

When Output Priority Queue Method is enabled, the weight and latency specified in the Class of Service Configuration window will take effect. Note that the weight can only be a value between 1 and 15. A higher priority queue always has a larger weight than a lower priority queue.

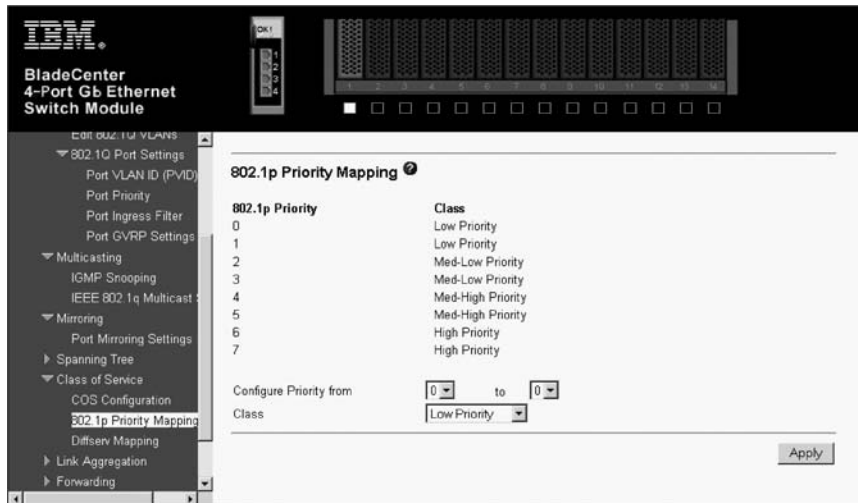


To enable priority queuing on the switch module, select **Weighted Round Robin** on the drop-down menu on the preceding window and click **APPLY**.



The switch module supports 802.1p priority queuing; four priority queues are supported per port. The switch module provides user-programmable mapping (four Priority Queue assignments: High, Med-High, Med-Low, Low) for the eight 802.1p priority classes (0 to 7). For the priority queue feature to take effect, users must first enable the Output Priority Queue Method on the Class of Service window. Otherwise, only the round-robin method can be used to schedule the packets in four different priority queues.

When Output Priority Queue Method is enabled, the weight and latency specified in the Class of Service Configuration preceding window will take effect. Note that the weight can only be a value between 1 and 15. A higher priority queue always has a larger weight than a lower priority queue.



This window enables you to configure traffic class priority by specifying the class value, from **Low Priority** to **High Priority**, of the switch eight levels of priority. Click **Apply** to make your changes effective.



This window enables you to set the following features:

To set up DiffServ Mapping, select **Enabled** in the first drop-down menu on the preceding window, enter a beginning and ending Code Point (0 to 63) in the second field, and select the desired Class in the next field (**Low Priority**, **Med-L Priority**, **Med-H Priority**, or **High Priority**). When you are finished, click **Apply** to make your changes effective.

Link Aggregation

The switch module supports Link Aggregation, or port trunking. Port trunks (aggregated ports) can be used to increase the bandwidth of a network connection or to ensure fault recovery.

You can configure up to two trunk connections (combining two to four ports into one fat pipe) between any two BladeCenter switches or other Layer 2 switches. However, before making any physical connections between devices, use the Link Aggregation menus to specify the ports that will belong to the trunking group on both switches.

When using a port trunk, note that:

- The ports used in a trunk must all be of the same speed (100 Mbps or 1000 Mbps) and operate in full-duplex mode only.
- The ports that can be assigned to the same trunk have certain other restrictions, as described in this section.
- Each port can only be assigned to one trunk group, whether a static or dynamic group.
- The ports at both ends of a connection must be configured as trunk ports.
- All of the ports in a trunk have to be treated as a whole when moved from/to, added, or deleted from a VLAN.
- The Spanning Tree Protocol (STP) will treat all the ports in a trunk as a whole.
- Enable the trunk before connecting any cable between the switches to avoid creating a data loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a data loop.

Trunking can be set as a static port/group using the Port Trunking window or as a dynamic port/group using the IEEE 802.3ad Link Aggregation windows. When trunking is enabled, a blue border will be placed around the ports on the Web device panel display.

Distribution Method

Link aggregation, or port trunking, enables several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single-link bandwidth.

Port trunking is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

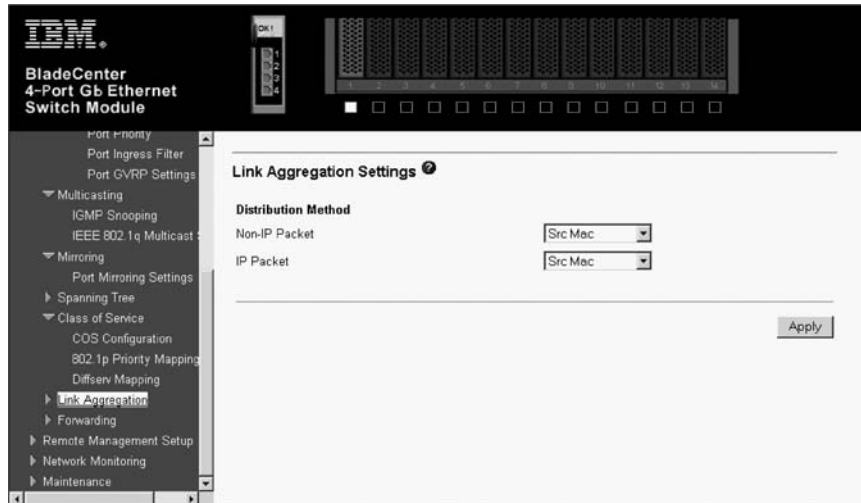
The switch module offers link aggregation on four external ports for up to two static trunk groups or two LACP 802.3ad link aggregation groups. The trunked ports can be non-continuous (that is, have non-sequential port numbers). All of the ports in the group must be members of the same VLAN. In addition, the trunked ports must all have the same speed and be configured as full duplex.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the port trunking group. This port is called the Master Port of the group, and all configuration options, including the VLAN configuration, that can be applied to the Master Port are applied to the entire port trunking group.

Load balancing is automatically applied to the ports in the trunked group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The STP will treat a port trunking group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the port trunking group. If two redundant port trunking groups are configured on the switch, STP will block one entire group, in the same way STP will block a single port that has a redundant link.

Use the **Distribution Method** window to set the distribution method for both IP packets and non-IP packets and then click **Apply** to make your changes effective.



The information on the preceding window includes:

Distribution Method

The switch module permits different load sharing methods when ports are trunked together. In some environments, a different method can improve balancing the packet traffic between trunked ports. Generally, you should select the method that can best differentiate packets that go through your trunked ports. If you do not know which method will be the best for your environment, use the trial-and-error approach, checking the network monitoring windows to see which method will yield the best results in terms of efficiency. The selected method is used as a hashing function to determine which packets will go to which port.

Non-IP Packet <Src Mac>

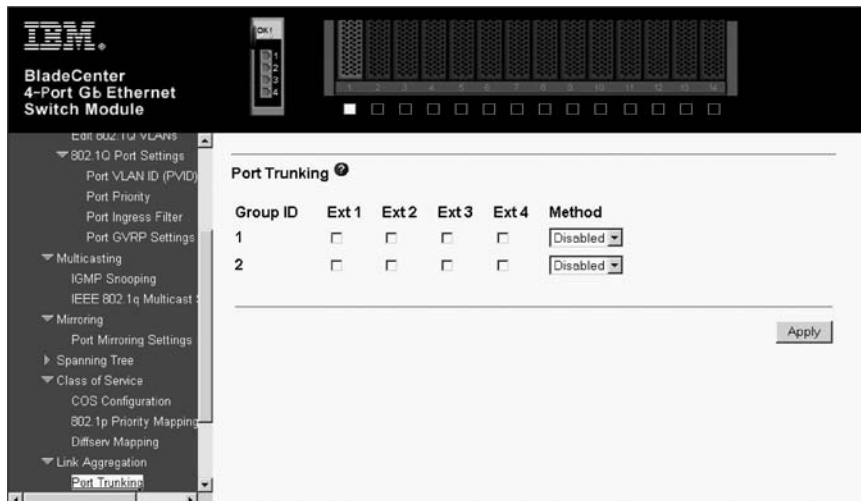
For non-IP packets, the available methods are: **Src Mac**, **Dest Mac**, or **Src & Dest Mac**.

IP Packet <Src Mac>

For IP packets, the available methods are: **Src Mac**, **Dest Mac**, **Src & Dest Mac**, **Src IP**, **Dest IP**, or **Src & Dest IP**.

Port Trunking

The Port Trunking window contains the following information:



The switch module offers link aggregation on four external ports for up to two static trunk groups or two LACP 802.3ad link aggregation groups. The trunked ports can be non-continuous (that is, have non-sequential port numbers). All of the ports in the group must be members of the same VLAN. In addition, the trunked ports must all have the same speed and be configured as full duplex.

To create or modify a trunk group, check the ports that will comprise the port trunk, and change the **Method** field to **Enabled**. Click **Apply** to activate your settings.

The user-changeable parameters on this window are as follows:

Group ID

The ID number of the trunk group

Port Checks the number of ports that will be members of the trunk group

Method

Enables or disables the trunk group

Setup IEEE 802.3ad Link Aggregation

Use the IEEE 802.3ad Link Aggregation window to set up dynamic port trunking.



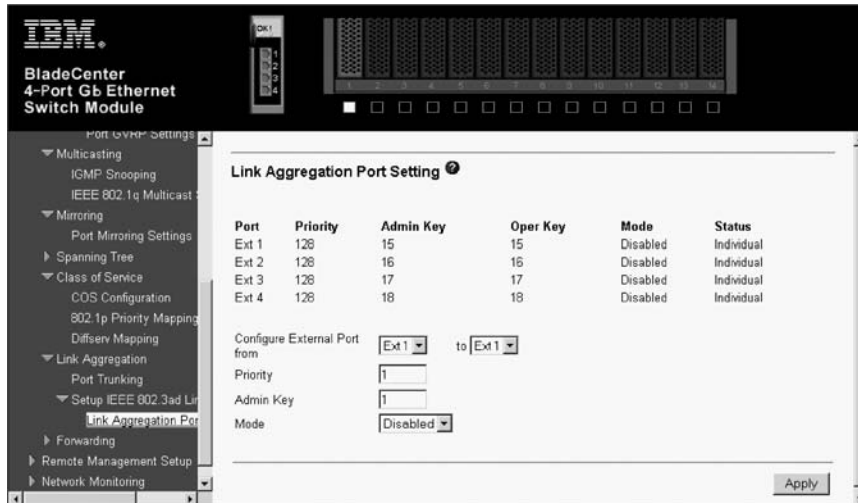
The user-changeable parameters on this window are as follows:

LACP This parameter enables Link Aggregation to be **Enabled** or **Disabled**. Disabling LACP when it is not in use can eliminate some traffic on the network. Enabling Link Aggregation creates an active LACP switch module.

System Priority

An admin ID can be assigned to the switch module to differentiate other LACP switches running on the network.

This window enables you to set up dynamic port trunking on individual ports.



Select the range of ports to be configured in the first field, assign a Priority in the second field, enter the Admin Key in the next field, and select **Enabled** in the **Mode** field to enable this feature. After you click **APPLY**, the new port settings will be displayed in the table in the lower portion of the preceding window.

The information on the preceding window includes:

Configure External Port From

Enter the ports that will form the external port trunking group in this field.

Priority [1]

Lower port priority means a higher priority over other enabled link aggregation ports in the group.

Admin Key [1]

This is the administrative key to control the way that links are aggregated. In order to aggregate ports together, the ports must have an equal Admin Key.

Mode <Enabled>

A port or ports can be enabled to permit them to join or create a link aggregation group.

Oper Key

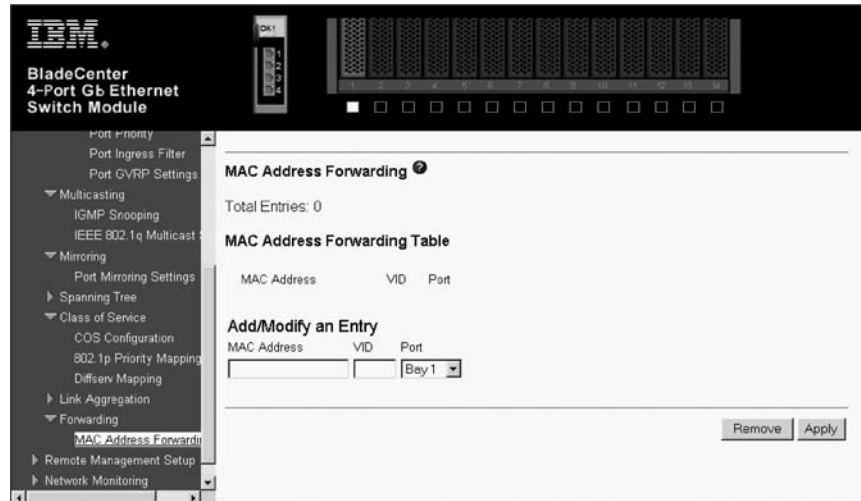
This displays the operational key used by the port to communicate with other LACP switches.

Status

This displays the current status of a link aggregation port.

Forwarding

The MAC Address Forwarding window enables you to set up static packet forwarding on the switch.



The information on the window is described as follows:

MAC Address

The MAC address from which packets will be statically filtered.

VID The VLAN ID number of the VLAN to which the MAC address belongs.

Type Select the filter type, **Permanent** or **DeleteOnReset**.

Port Map

You can designate the port on which the MAC address resides.

Remote Management Setup

This section includes: **Management Station IP Settings**, **SNMP Community Settings**, **Setup Trap Receivers**, **Setup User Accounts**, and **Serial Port Settings**, as well secondary windows.

The following information pertains to the windows illustrated in “Management Station IP Settings” on page 58, “SNMP Community Settings” on page 58, and “Setting up trap receivers” on page 58.

Note: Some of the described data fields only appear on some of these windows.

- A trap receiving station is a device that constantly runs a network management application to receive and store traps. You can enter up to four entries.
- The information on these windows is described as follows:

IP Address

The IP address of the trap receiving station. If necessary, consult your system network administrator to obtain this IP address.

Community String

A user-defined SNMP community name. This community string will be included on SNMP packets sent to and from the switch. Any station that is not a member of this community will not receive the packet.

Rights

Enables each community to be separately set to either **Read** (read-only), meaning that the community member can only view switch settings or **R/W** (read/write), which enables the member to change settings in the switch.

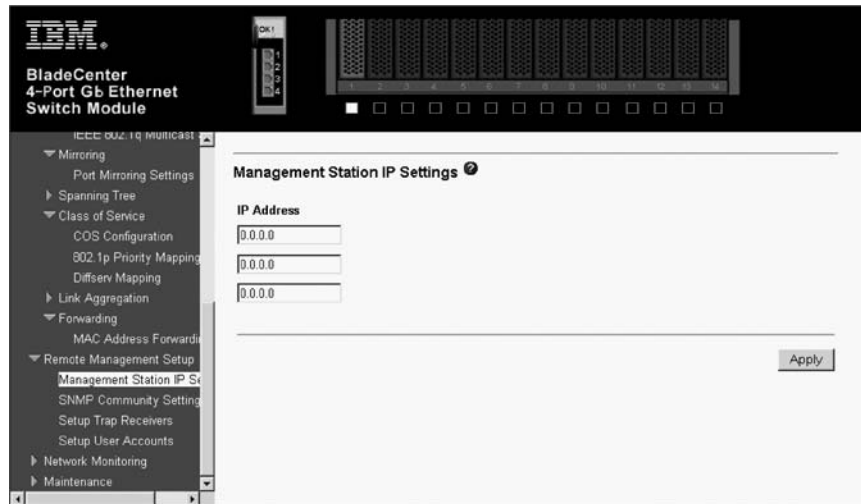
Status

Option to set the trap receiving station to **Enabled** or **Disabled**.

- Click **Apply** to make the settings effective.

Management Station IP Settings

The Management Station IP Settings window contains the following information:



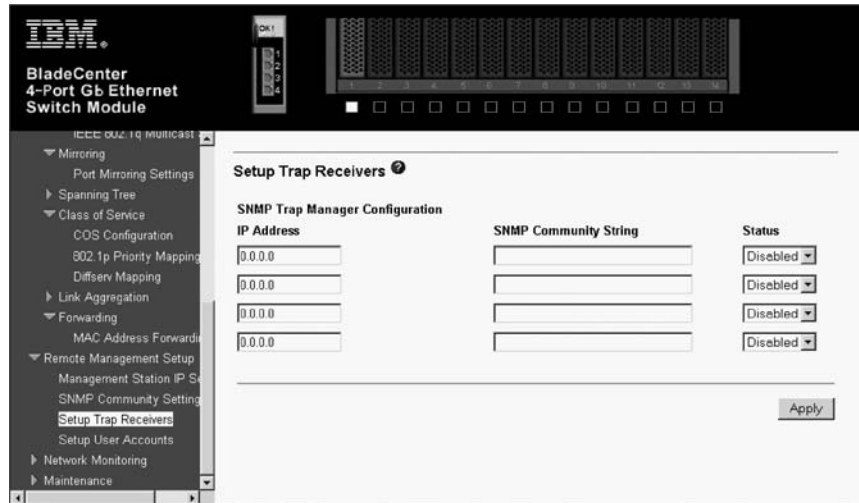
SNMP Community Settings

The SNMP Community Settings window contains the following information:



Setting up trap receivers

The Setup Trap Receivers window contains the following information:

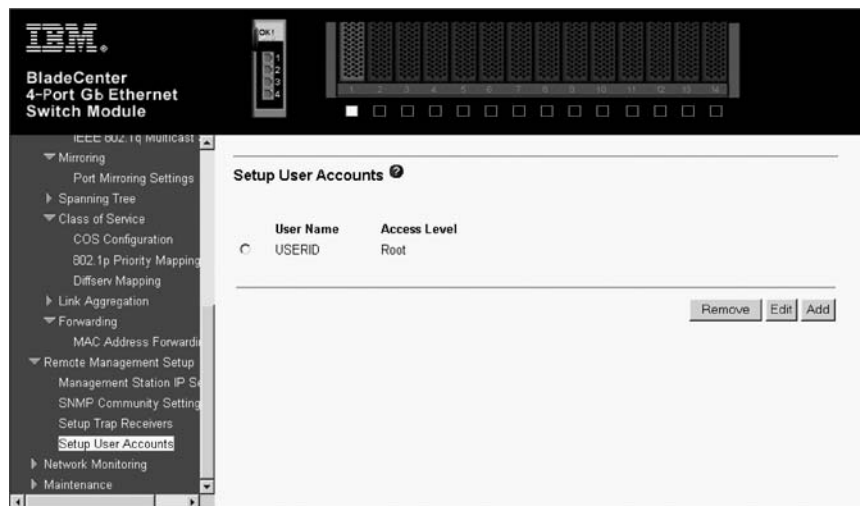


For a detailed list of the trap types that are used for this switch, see “Traps” on page 20.

Setting up user accounts

The switch module enables you to set up and manage user accounts in the following three windows.

The Setup User Accounts window contains the following information:



The information on this window is described as follows:

User Name

Displays all current users for the switch.

Access Level

Displays the current access level assigned to each corresponding user. There are three access levels: **<User>**, **<User+>**, and **<Root>**. A **<Root>** user has full read/write access, while a **<User>** has read-only access. A **<User+>** has the same privileges as a **<User>**, but with the added ability to restart the switch. See “Assigning Root, User+, and User privileges” on page 61 for complete details about access levels.

New Select this hyperlink to add a new user to the table.

You can delete, add, and remove entries through this window. To delete an entry, click the circle next to the appropriate entry; then, click **Remove**. To add an entry, click **Add** and follow the instructions in this section. To modify an existing entry, click **Edit** and follow the instructions in this section.

The following information pertains to the Setup User Account - Add window and the Setup User Account - Edit window that are illustrated in this section.

- To add a user account, fill in the appropriate information in the **User Name**, **New Password**, and **Confirm New Password** fields. Then, select the desired access level, **<Root>**, **<User>**, or **<User+>**, in the **Access Level** control and click **Apply**.
- The information on these windows is described as follows:

User Name

Enter a user name in this field.

New Password

Enter the desired new password in this field.

Confirm New Password

Enter the new password a second time.

Access Level

Displays the current access level assigned to each corresponding user. There are three access levels: **<User>**, **<User+>**, and **<Root>**. A **<Root>** user has full read/write access, while a **<User>** has read only access. A **<User+>** has the same privileges as a **<User>**, but with the added ability to restart the switch.





Assigning Root, User+, and User privileges

There are three levels of user privileges: Root, User+, and User. Some menu selections that are available to users with Root privileges might not be available to those with User+ and User privileges.

Note: User privileges are also known as normal user privileges.

The following table summarizes the Root, User+, and User privileges:

Table 3. Root, User+, and User privileges

Switch configuration	Privilege		
	Root	User+	User
Management			
Configuration	Yes	Read only	Read only
Network monitoring	Yes	Read only	Read only
Community strings and trap stations	Yes	Read only	Read only
Update firmware and configuration files	Yes	No	No
System utilities	Yes	Ping only	Ping only
Factory reset	Yes	No	No
Reboot switch	Yes	Yes	No
User accounts management			
Add/update/delete user accounts	Yes	No	No
View user accounts	Yes	No	No

After establishing a user account with Root-level privileges, press Esc. Then, highlight **Save Changes** and press Enter (see “Saving changes” on page 72). The switch will save any changes to its NVRAM and restart. Log on with the new user name and password as described in “Getting started” on page 32. You are now ready to continue configuring the switch.

Network Monitoring

This section is divided into three main areas: Statistics, Address Table, and Applications. In addition, this section contains secondary windows.

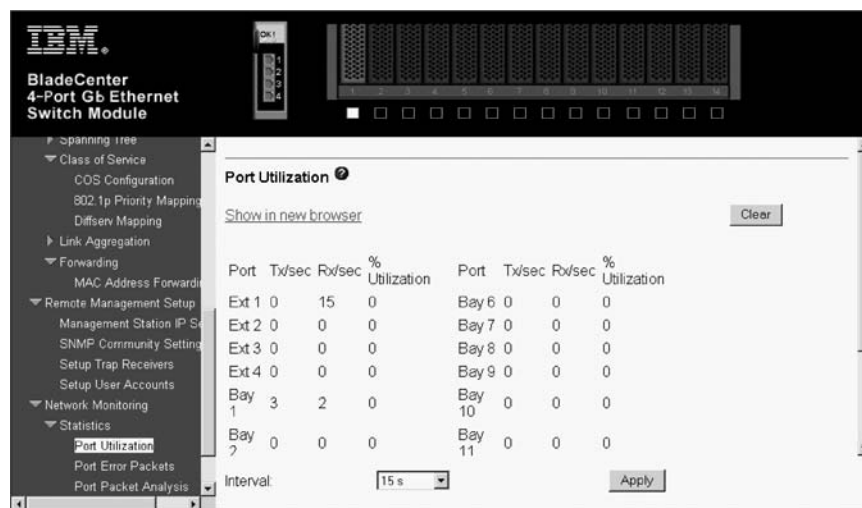
Statistics

This section contains descriptions and illustrations of the following windows:

- **Port Utilization**
- **Port Error Packets**
- **Port Packet Analysis**

Port Utilization

The switch module can display the utilization percentage of a specified port in the following window.



The information on this window is described as follows:

Tx/sec

The rate at which the given port is transmitting packets, in packets per second.

Rx/sec

The rate at which the given port is receiving packets, in packets per second.

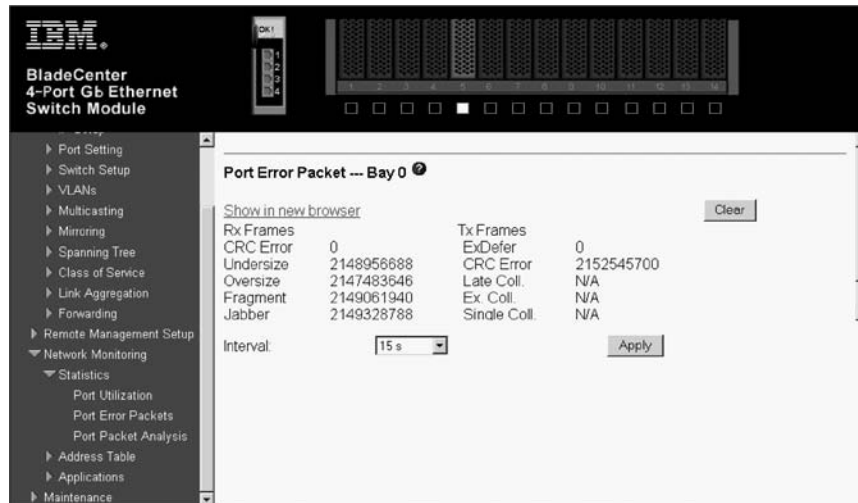
% Utilization

The percentage utilization of the available bandwidth of the given port.

Port Error Packets

The Web Manager enables various packet statistics to be viewed as either a line graph or a table.

The Port Error Packet window contains the following information:



Rx Frames

Received packets.

CRC Error

For 10 Mbps ports, the counter records CRC errors; that is, frame-check sequence (FCS) errors or alignment errors. For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).

Undersize

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

Oversize

The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well-formed.

Fragments

The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.

Jabber

The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.

Drop Pkts

The total number of events in which packets were dropped due to a lack of resources.

Tx Frames

Transmitted packets.

ExDefer

The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.

Late Coll.

Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Ex. Coll.

Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.

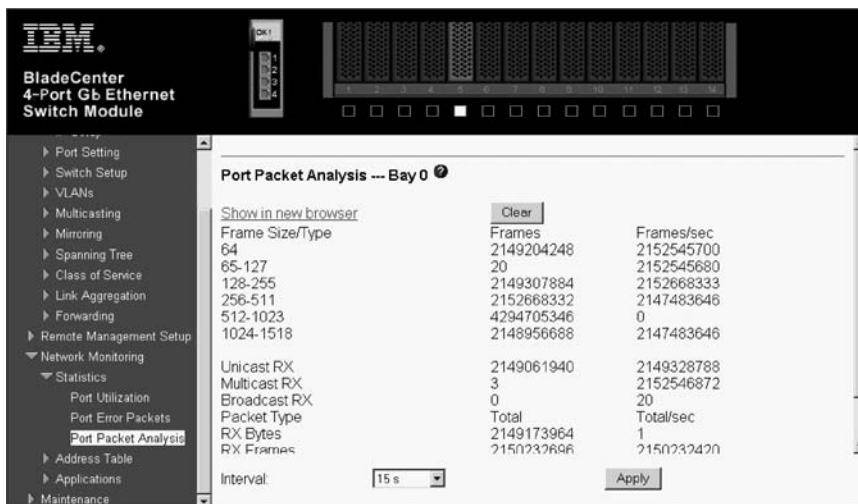
Single Coll.

Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.

Coll. An estimate of the total number of collisions on this network segment.

Port Packet Analysis

The Port Packet Analysis window contains the following information:



The information on this window is described as follows:

Frames

The number of packets (or frames) received or transmitted by the switch with the size, in octets, given by the column on the right.

Frames/sec

The number of packets (or frames) transmitted or received, per second, by the switch.

Unicast RX

Displays the number of unicast packets received by the switch in total number (**Frames**) and the rate (**Frames/sec**).

Multicast RX

Displays the number of multicast packets received by the switch in total number (**Frames**) and the rate (**Frames/sec**).

Broadcast RX

Displays the number of broadcast packets received by the switch in total number (**Frames**) and the rate (**Frames/sec**).

RX Bytes

Displays the number of bytes (octets) received by the switch in total number (**Total**), and rate (**Total/sec**).

RX Frames

Displays the number of packets (frames) received by the switch in total number (**Total**), and rate (**Total/sec**).

TX Bytes

Displays the number of bytes (octets) transmitted by the switch in total number (**Total**), and rate (**Total/sec**).

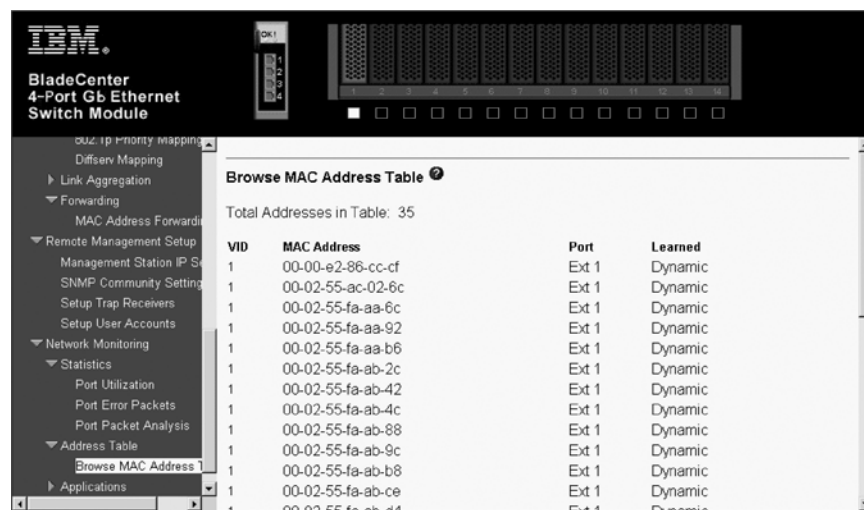
TX Frames

Displays the number of packets (frames) transmitted by the switch in total number (**Total**), and rate (**Total/sec**).

Address Table

This section contains a description and illustration of the **Browse MAC Address Table** window.

The Web manager enables the switch MAC address table (sometimes referred to as a forwarding table) to be viewed:



The information on this window is described as follows:

Search by VLAN ID

Enables the forwarding table to be browsed by VLAN ID (VID).

Search by MAC Address

Enables the forwarding table to be browsed by MAC Address.

Search by Port

Enables the forwarding table to be browsed by port number.

Jump Enables the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.

Find Click the icon to find the data entry.

Clear All

Clears all forwarding table entries.

Clear By Port

Clears the forwarding table entries that have the entered port number.

VID The VLAN ID of the VLAN of which the port is a member.

MAC Address

The MAC address that you entered into the address table.

Port The port to which the MAC address corresponds.

Learned

How the switch discovered the MAC address. The possible entries are **Dynamic**, **Self**, and **Static**.

Next Click this button to view the next page of the address table.

Applications

This section contains descriptions and illustrations of the following windows:

- **GVRP**
- **LACP Aggregator**
- **IGMP Snooping**
- **Switch History**

GVRP

The read-only GVRP Status window contains the following information:

The screenshot shows the GVRP Status window. On the left is a navigation menu with categories like Remote management, Setup, Network Monitoring, Statistics, Address Table, Applications, and Maintenance. The 'Applications' section is expanded to show 'GVRP'. The main content area displays the following information:

IEEE 802.1Q VLAN ID	Status	Creation time since switch power up
1	Permanent	01:27:51

Below this table are two sections: 'Egress Ports' and 'Untagged Ports'. Each section has a grid of checkboxes for ports Ext 1 through Ext 4 and 1 through 14. All checkboxes in both sections are checked.

At the bottom, it says 'Number of IEEE 802.1Q VLAN: 2' and has a 'Previous' button.

LACP Aggregator

The Link Aggregation Control Protocol aggregator displays the status of dynamic LACP trunked ports from the group point of view.

The screenshot shows the LACP Aggregator window. The navigation menu on the left is expanded to 'Applications' > 'LACP Aggregator'. The main content area displays a table with the following information:

Index	Operation Key	Ext 1.4				Status	Failure Event
		1	2	3	4		
0	15	-	-	-	-	Individual	No Error
1	16	-	-	-	-	Individual	No Error
2	17	-	-	-	-	Individual	No Error
3	18	-	-	-	-	Individual	No Error

The information on this read-only window is described as follows:

Index The LACP Aggregator ID number.

Operation Key

Displays the operational key used by the aggregator to communicate with other aggregators.

Member Port

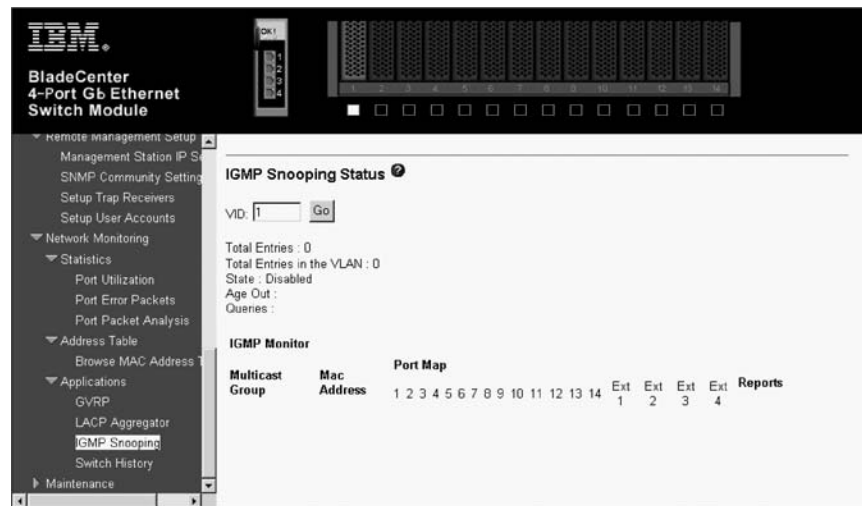
Displays the port member status in the aggregator group.

Status

Displays the status of each aggregator. When there is only one port member in the aggregator, the aggregator acts as a normal individual port (by default, each LACP-enabled port is assigned to their own aggregator group). Otherwise, it will start to aggregate when there is more than one port that wants to join the aggregator group.

IGMP Snooping

The switch IGMP snooping table can be browsed by using the Web manager. The table is displayed by VLAN ID (VID).



The information on this window is described as follows:

VID VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.

Search

Click this button to display the IGMP Snooping Table for the current VID.

Multicast Group

The IP address of a multicast group learned by IGMP snooping.

MAC Address

The corresponding MAC address learned by IGMP snooping.

Port Map

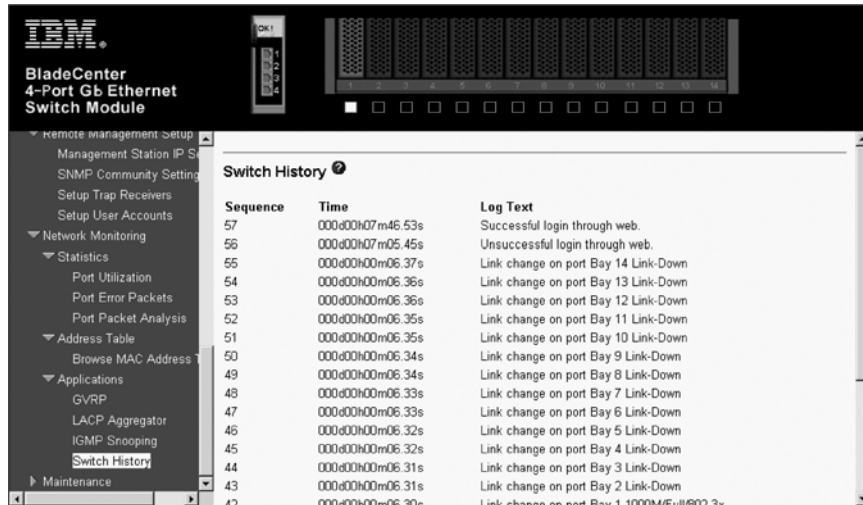
Displays the ports that have forwarded multicast packets.

Reports

The number of IGMP reports for the listed source.

Switch History

The Web Manager enables the switch history log, as compiled by the switch management agent, to be viewed.



The switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected through a Telnet interface. Clicking **Next** at the bottom of the window will enable you to display all the switch trap logs.

The information on this window is described as follows:

Sequence

A counter incremented whenever an entry to the switch history log is made. The table displays the last entry (highest sequence number) first.

Time Displays the time in days, hours, and minutes since the switch was last restarted.

Log Text

Displays text describing the event that triggered the history log entry.

Maintenance

This section includes **Using TFTP Server (Download Configuration File, Upgrade Firmware, Upload Configuration File, and Save Log)**, **Using Browser (Upgrade Firmware/Configuration File and Download Configuration/Log Files)**, **Save Changes, Factory Reset, and Restart System.**

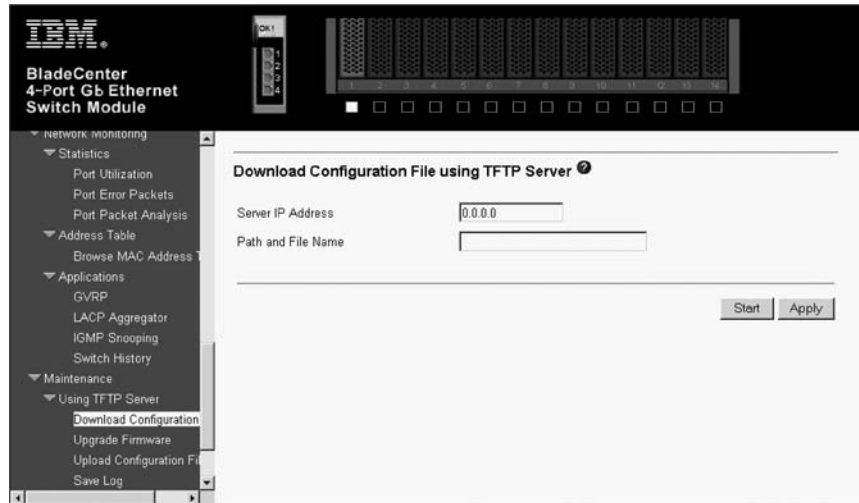
Using TFTP Server

Trivial File Transfer Protocol (TFTP) services enable the switch firmware code to be upgraded by downloading a new firmware code file from a TFTP server to the switch. A configuration file can also be loaded into the switch, and switch settings can be saved to a TFTP server. In addition, the switch history log can be uploaded from the switch to a TFTP server.

Note: TFTP server software must be running on the management station for the TFTP services listed here to work.

Download Configuration File

The Download Configuration File from TFTP Server window contains the following information:



Enter the IP address of the TFTP server in the **Server IP Address** field and the complete path and file name of the firmware code file for the switch. Click **Apply** to enter the server IP address into the switch RAM (select **Save Changes** to enter the address into the switch NVRAM). Click **Start** to initiate the file transfer.

The information on this window is described as follows:

Server IP Address

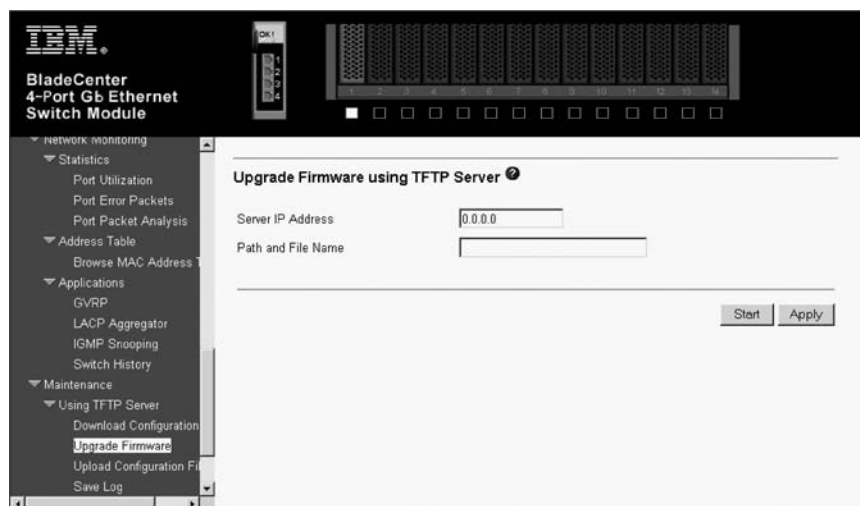
The IP address of the TFTP server.

Path and File Name

The full file name (including path) of the new firmware code file on the TFTP server.

Upgrade Firmware

A configuration file can be downloaded from a TFTP server to the switch. This file is then used by the switch to configure itself.



Enter the IP address of the TFTP server in the **Server IP Address** field and the complete path and file name of the firmware code file for the switch. Click **Apply** to enter the server IP address into the switch RAM (select **Save Changes** to enter the address into the switch NVRAM). Click **Start** to initiate the file transfer.

The information on this window is described as follows:

Server IP Address

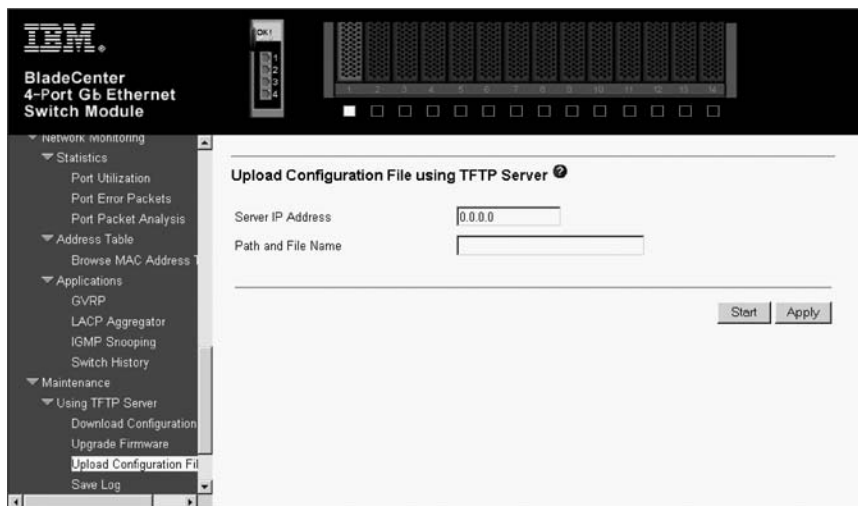
The IP address of the TFTP server.

Path and File Name

The full file name (including path) of the new firmware code file on the TFTP server.

Upload Configuration File

The switch module current settings can be uploaded to a TFTP Server by the switch module management agent.



Enter the IP address of the TFTP server in the **Server IP Address** field and the complete path and file name of the firmware code file for the switch. Click **Apply** to enter the server IP address into the switch RAM (select **Save Changes** to enter the address into the switch NVRAM). Click **Start** to initiate the file transfer.

Note: If you do not save configurations to NVRAM, the configurations that you are uploading to a TFTP server will not be saved correctly.

The information on this window is described as follows:

Server IP Address

The IP address of the TFTP server.

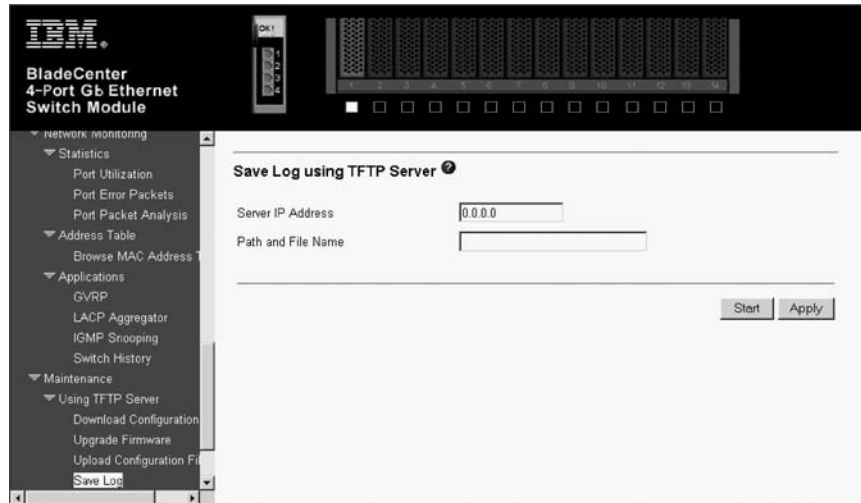
Path and File Name

The full file name (including path) of the new firmware code file on the TFTP server.

Save Log

The switch module management agent can upload its history log file to a TFTP server.

Note: An empty history file on the TFTP server must exist on the server before the switch can upload its history file.



Enter the IP address of the TFTP server in the **Server IP Address** field and the complete path and file name of the firmware code file for the switch. Click **Apply** to enter the server IP address into the switch RAM (select **Save Changes** to enter the address into the switch NVRAM). Click **Start** to initiate the file transfer.

The information on this window is described as follows:

Server IP Address

The IP address of the TFTP server.

Path and File Name

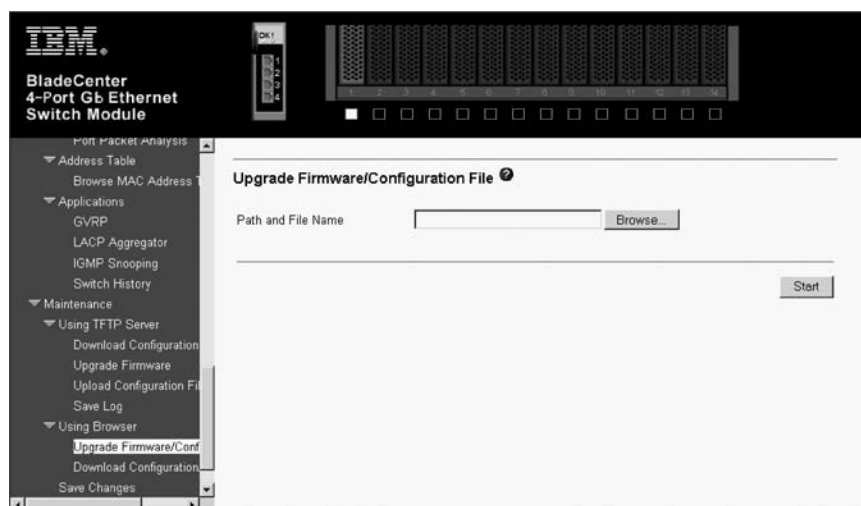
The full file name (including path) of the new firmware code file on the TFTP server.

Using the Browser

This section contains information about the Upgrade Firmware/Configuration File and Download Configuration/Log Files windows.

Upgrade Firmware/Configuration File

The Upgrade Firmware/Configuration File window contains the following information:

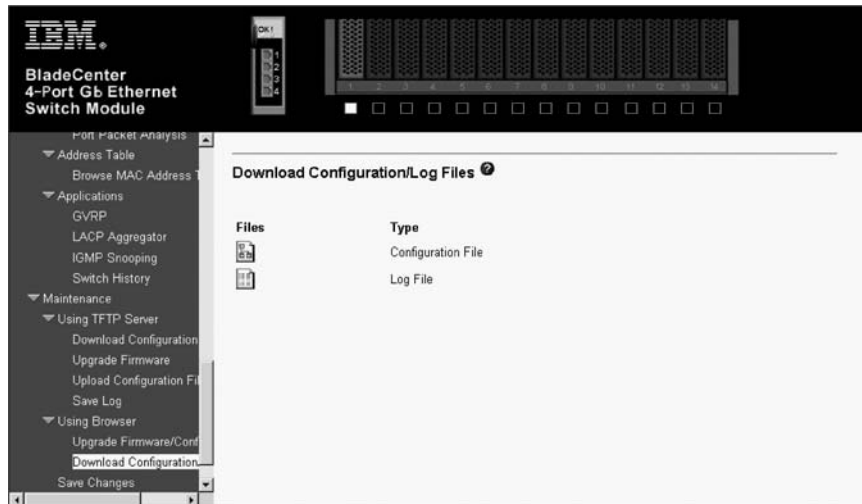


Enter the **Path** and **File Name** of the desired file or use the Browse button to access recently used entries. Click **Start** to begin.

Download Configuration/Log Files

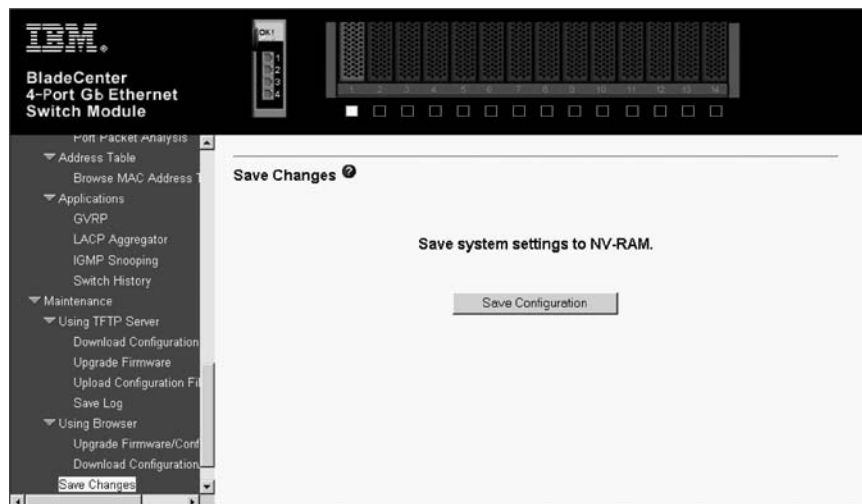
To download a switch configuration file from the browser, highlight **Configuration File** on the Download Configuration/Log Files menu and press Enter. To download a switch log file from the browser, highlight **Log File** on the Download Configuration/Log Files menu and press Enter.

The Download Configuration/Log Files window contains the following information:



Saving changes

The Save Changes window contains the following information:

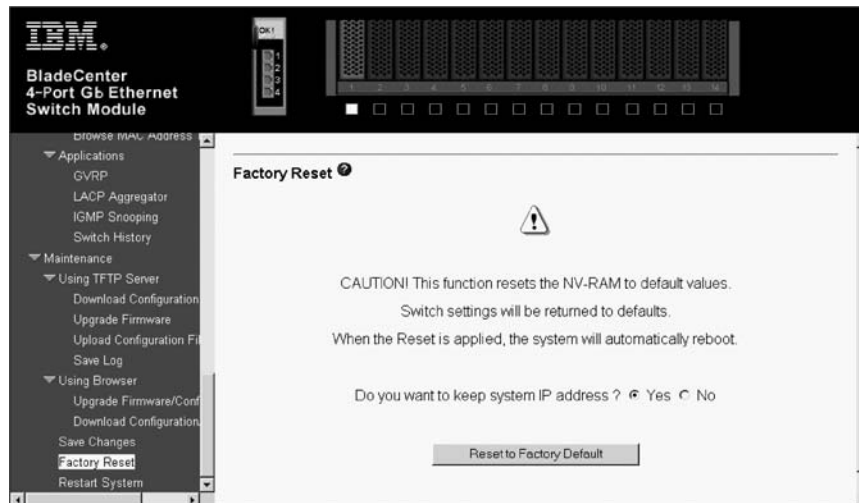


To save all the changes that you made to the switch flash memory in the current session, click the **Save Configuration** button.

When the switch configuration settings have been saved to NVRAM, they become the default settings for the switch. These settings will be used every time that the switch module is restarted.

Restoring the default configuration parameters

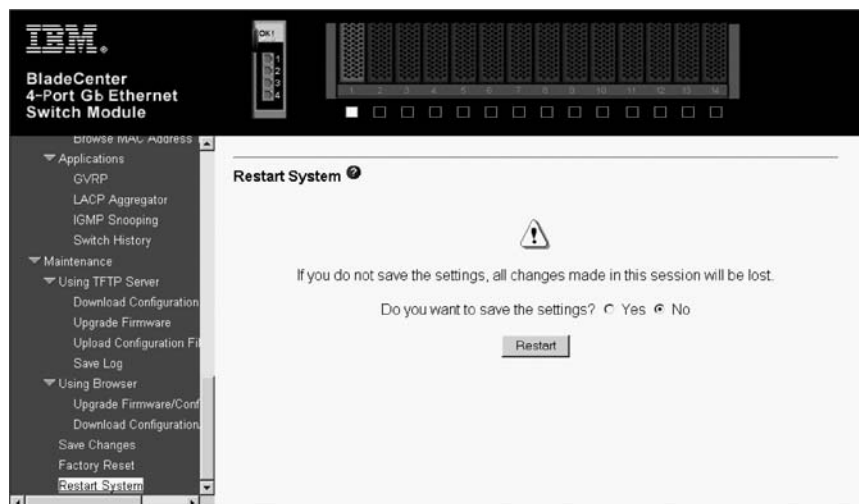
The Factory Reset window contains the following information:



A remote reset returns the device to the initial parameters that were set at the factory. Click **Reset to Factory Default** to reset the switch module.

Restarting the switch

The Restart System window contains the following information:



To perform a restart of the switch, which resets the system, click the **Restart** button.

Chapter 6. Configuring the switch module through the Telnet interface

Your switch module supports a management interface that you can use to set up and control your device over the network using the TCP/IP Telnet protocol. You can use this facility to perform many basic network management functions. In addition, you can use the Telnet interface to configure the switch module for management using an SNMP-based network management system. This chapter describes how to use the Telnet interface to access the switch module, change its settings, and monitor its operation.

Important: Before you configure your Ethernet switch module, be sure that the management modules in your BladeCenter unit are properly configured. In addition, to access and manage your Ethernet switch module from an external environment, you might need to enable certain features, such as the external ports and external management over all ports. See the applicable *BladeCenter Installation and User's Guide* publications on the *IBM BladeCenter Documentation CD* for more information.

In addition to reviewing the publications in this library, be sure to review the *IBM BladeCenter Planning and Installation Guide* located at <http://www.pc.ibm.com/eserver/bladecenter> on the World Wide Web for information to help you prepare for system installation and configuration.

Remotely managing the Ethernet switch module

The Ethernet switch module supports two remote-access modes for management through Ethernet connections. You can select the mode that is best suited for your BladeCenter environment. The Ethernet switch module has an internal Ethernet path to the management module and the four external Ethernet ports on the switch module.

- The default mode uses the internal path to the management module only. In this mode, the remote-access link to the management console must be attached to the 10/100 Mbps Ethernet port on the management module. With this mode, the IP addresses and SNMP parameters of the Ethernet switch modules can be automatically assigned by the IBM Director BladeCenter Deployment Wizard or, you must manually assign them through the BladeCenter Management and Configuration Program. This mode enables the system administrator to provide a secure LAN for management of the BladeCenter subsystems separately from the data network.

Important: With this mode, the Ethernet switch module does not respond to remote-management commands through the four external Ethernet ports on the switch module.

See the applicable *BladeCenter Installation and User's Guide* on the *IBM BladeCenter Documentation CD* for additional instructions for configuring the Ethernet switch module for this mode of operation.

- The system administrator can select to enable remote management of the Ethernet switch module through the four external Ethernet ports on the switch module, instead of or in addition to access through the management module. This mode can only be enabled through the management module configuration interface. Once this mode is enabled, the external Ethernet ports will support

both management traffic and BladeCenter application data traffic. Also, the Ethernet switch module can transmit DHCP and BOOTP request frames through the external Ethernet ports.

This mode enables the Ethernet switch module IP addresses to reside on a different subnet than the management modules. This is useful when the Ethernet switch modules are to be managed and controlled as part of the overall network infrastructure, while maintaining secure management of other BladeCenter subsystems through the management module. However, management access to the Ethernet switch-module link will be lost if the Ethernet switch module IP address is not on the same subnet as the management module. This chapter contains additional instructions for configuring the Ethernet switch module for this mode of operation.

The two previously described modes are only applicable to the Ethernet switch module. The management module can only be remotely accessed through the 10/100 Mbps Ethernet port on the management module.

Connecting to the switch module

When you know the IP address for your switch module and provided that you have an existing network connection, you can use the Telnet program (in VT-100 compatible terminal mode) to access and control the switch module. If you need to obtain the IP address for your switch module or establish a network connection, consult your system or network administrator. Be sure to use the correct IP address in the required command, as specified in “First-time connection to the Ethernet switch module”.

Telnet usage conventions

The Telnet interface uses the following conventions:

- Items in <angle brackets> can be toggled among several choices using the Spacebar.
- Items in [square brackets] can be changed by typing a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.
- The Up and Down Arrow keys, the Left and Right Arrow keys, the Tab key, and the Backspace key can be used to move between selected items.
- Items in UPPERCASE are commands. Moving the selection to a command (such as **APPLY**) and pressing Enter will issue that command.

Important: The command **APPLY** makes changes to the switch configuration for the current session only. If you want your changes to be permanent, select **Save Changes** in the main menu. Selecting **Save Changes** enters the current switch configuration, including all changes, into NVRAM and then restarts the switch module.

First-time connection to the Ethernet switch module

The switch module supports user-based security that you can use to prevent unauthorized users from accessing the switch module or changing its settings. This section tells how to log on to the switch module.

Note: The passwords used to access the switch module are case-sensitive; therefore, an uppercase *S* is not the same as a lowercase *s*.

Complete the following steps to connect to the switch module through the Telnet interface:

1. Display a window that contains a DOS prompt command line; for example, **C:\>**.
2. Type the following command on the DOS prompt command line and press Enter: **telnet x**
where **x** is the IP address for your switch module

When you first connect to the switch module, the first login window (shown in the following illustration) opens.

Note: Press Ctrl+R to refresh the window. This command can be used at any time to force the program in the switch module to refresh the current window.

```
IBM BladeCenter 4-Port Gb Ethernet Switch Module Console

Username: [          ]
Password: [          ]

Copyright(C) 2000, 2002 IBM Corporation                DISCONNECT
-----
Function: Enter case-sensitive username.
Message:
CTRL+R = Refresh
```

Note: The initial user name in the **Username** field is USERID, and the initial password in the **Password** field is PASSWORD (where the sixth alphanumeric character is the number zero). Remember that both the **Username** and **Password** fields are case-sensitive. To increase system security, change the password after you log onto the system for the first time and, be sure to store the new password in a safe location.

Press Enter in both the **Username** and **Password** fields. The main menu is displayed, as shown in the following illustration:

```
IBM BladeCenter 4-Port Gb Ethernet Switch Module - Main Menu
-----
Basic Setup
Switch Information
IP Setup
Remote Management Setup
Switch Settings
Configure Ports
Setup User Accounts
Utilities
Network Monitoring
Save Changes
Reboot
Logout

Advanced Setup
Spanning Tree
Forwarding
Class Of Service
Mirroring
Multicasting
VLANs
Link Aggregation

-----
Function: Setup and browse switch information.
Message:
For Help, press F1
```

Note: The first user automatically gets Root privileges (see “Assigning Root, User+, and User privileges” on page 79). Create at least one Root-level user for the switch module, as described in “Setting up user accounts”.

Setting up user accounts

Only a user with Root privileges can add new user accounts or make changes to existing user accounts. Before you can update a user account, you must also enter the password for that user account. If you are updating or deleting an existing user account, see “Updating a user account” on page 82 or “Deleting a user account” on page 83 for complete details.

To create a new user account, highlight **Setup User Accounts** in the main menu and press Enter:

```

IBM BladeCenter 4-Port Gb Ethernet Switch Module - Main Menu
-----
Basic Setup                               Advanced Setup
Switch Information                       Spanning Tree
IP Setup                                  Forwarding
Remote Management Setup                  Class Of Service
Switch Settings                           Mirroring
Configure Ports                           Multicasting
Setup User Accounts                       VLANs
Utilities                                  Link Aggregation
Network Monitoring
Save Changes
Reboot
Logout

-----
Function: Setup user account and password.
Message:
For Help, press F1
  
```

The Setup User Accounts window opens, as shown in the following illustration.

```

Setup User Accounts
-----
Current Accounts:      User Name      Access Level
                       USERID        Root

Action                 <Add >
Username               [          ]
Old Password           [          ]
New Password           [          ]
Confirm New Password  [          ]
Access Level           <Root >

APPLY

-----
Function: Select action - Add, Delete, or Update.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
  
```


Complete the following steps to create a new user account:

1. Toggle the **Action** field to **<Add>** using the Spacebar. This will enable the addition of a new user. The other options are:

<Delete>

Deletes a user entry.

<Update>

Makes changes to an existing user entry.

2. Enter the new user's name in the **Username** field, assign an initial password in the **New Password** field, and then confirm the new password in the **Confirm New Password** field. Determine whether the new user should have root, user+, or user privileges (see "Assigning Root, User+, and User privileges" for descriptions of these privileges). The Spacebar toggles among these three options in the **Access Level** field.
3. Highlight **APPLY** and press Enter to make the user addition effective.
4. Press Esc to return to the previous window or Ctrl+T to go to the root window.
A listing of all user accounts and access levels is displayed below the user setup menu. This list is updated when **APPLY** is processed.

Important: The command **APPLY** makes changes to the switch configuration for the current session only. If you want your changes to be permanent, select **Save Changes** in the main menu. Selecting **Save Changes** enters the current switch configuration, including all changes, into NVRAM, and then restarts the switch module.

Assigning Root, User+, and User privileges

There are three levels of user privileges: Root, User+, and User. Some menu selections that are available to users with Root privileges might not be available to those with User+ and User privileges.

Note: User privileges are also known as normal user privileges.

The following table summarizes the Root, User+, and User privileges.

Table 4. Root, User+, and User privileges

Switch configuration	Privilege		
	Root	User+	User
Management			
Configuration	Yes	Read only	Read only
Network monitoring	Yes	Read only	Read only
Community strings and trap stations	Yes	Read only	Read only
Update firmware and configuration files	Yes	No	No
System utilities	Yes	Ping only	Ping only
Factory reset	Yes	No	No
Reboot switch	Yes	Yes	No
User accounts management			
Add/update/delete user accounts	Yes	No	No
View user accounts	Yes	No	No

After establishing a user account with Root-level privileges, press Esc. Then, highlight **Save Changes** and press Enter (see “Saving changes”). The switch will save any changes to its NVRAM and restart. Log on with the new user name and password as described in “Logging onto the switch module” on page 82. You are now ready to continue configuring the switch.

Saving changes

The switch module has two levels of memory: normal random-access memory (RAM) and NVRAM. To make configuration changes effective, highlight **APPLY** and press Enter. When this is done, the settings will be immediately applied to the switching software in RAM and will immediately take effect.

However, some settings require you to restart the switch before they will take effect. Restarting the switch erases all settings in RAM and reloads the stored settings from the NVRAM. Thus, it is necessary to save all setting changes to NVRAM before restarting the switch.

To keep any configuration changes permanently, highlight **Save Changes** in the main menu and press Enter.

```
IBM BladeCenter 4-Port Gb Ethernet Switch Module - Main Menu
-----
Basic Setup                               Advanced Setup
Switch Information                         Spanning Tree
IP Setup                                   Forwarding
Remote Management Setup                   Class Of Service
Switch Settings                           Mirroring
Configure Ports                           Multicasting
Setup User Accounts                       VLANs
Utilities                                  Link Aggregation
Network Monitoring
Save Changes
Reboot
Logout

-----
Function: Save changes.
Message:
For Help, press F1
```

To verify that your new settings have been saved to NVRAM, the following window opens.

```
Save all settings to NVRAM... done.
Press any key to continue..._
```

When the switch configuration settings have been saved to NVRAM, they become the default settings for the switch. These settings will be used every time that the switch module is restarted.

Restoring default configuration values

The only way to change the configuration stored in NVRAM is to save a new configuration using **Save Changes**, or to process a **Load Factory Default Configuration** function from the Reboot menu. This will clear all settings and restore them to their initial values listed in Appendix B, “Run-time switching software default settings” on page 117. These are the configuration settings that were entered at the factory.

```
IBM BladeCenter 4-Port Gb Ethernet Switch Module - Main Menu
-----
Basic Setup
Switch Information
IP Setup
Remote Management Setup
Switch Settings
Configure Ports
Setup User Accounts
Utilities
Network Monitoring
Save Changes
Reboot
Logout

Advanced Setup
Spanning Tree
Forwarding
Class Of Service
Mirroring
Multicasting
VLANs
Link Aggregation

-----
Function: Reboot Configuration.
Message:
For Help, press F1
```

Highlight **Reboot** in the main menu and press Enter.

```
Reboot
-----
Reboot
Save Configuration & Reboot
Reboot & Load Factory Default Configuration
Reboot & Load Factory Default Configuration Except IP Address

-----
Function: Reboot the system.
Message:
CTRL+I = Main Menu          Esc = Prev. Screen          CTRL+R = Refresh
```

Highlight the applicable choice and press Enter to reset the switch NVRAM to the factory default settings (or just restart the switch module). Loading the factory default configuration will erase any user accounts (and all other configuration settings) that you might have entered and return the switch module to its original state at the time of purchase. The **Load Factory Default Configuration Except IP Address** option is used when the IP address of the switch module needs to be preserved.

Logging onto the switch module

To log in after you have created a registered user, complete the following steps from the login window (see “First-time connection to the Ethernet switch module” on page 76 for additional information):

1. Type your user name in the **Username** field and press Enter.
2. Type your password in the **Password** field and press Enter.

The main menu window opens based on your access level or privilege.

Viewing current user accounts

Access to the switch is controlled through using an authorized user name and password. The switch supports a maximum of eight user accounts. The interface does not permit deletion of the currently logged-in user, to prevent accidentally deleting all the users with Root privileges.

Only a user with Root privileges can delete users.

To view the current user accounts, highlight **Setup User Accounts** in the main menu and press Enter. You can read the current user accounts from the Setup User Accounts window.

Updating a user account

Only a user with Root privileges can add new user accounts or make changes to existing user accounts. Before you can update a user account, you must also enter the password for that user account. If you are adding a new user account, see “Setting up user accounts” on page 78 for complete details.

Complete the following steps to update a user account:

1. Select **Setup User Accounts** in the main menu. The following Setup User Accounts window opens:

```

Setup User Accounts
-----
Current Accounts:   User Name      Access Level
                   USERID         Root

Action             <Add >
Username           [                ]
Old Password       [                ]
New Password       [                ]
Confirm New Password [          ]
Access Level       <Root >
                                           APPLY
-----
Function: Select action - Add, Delete, or Update.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

2. Toggle the **Action** field by using the Spacebar to select **Update**.
3. Type in the user's name in the **Username** field for the user account that you want to change; then, press Enter. Type in the old password in the **Old Password** field for that user account; then, press Enter.
4. You can now modify the password or the privilege level for this user account.
 - To change the password, type in the **New Password** that you have chosen, and press Enter. Type in the same new password in the **Confirm New Password** field to verify that you have not mistyped it.
 - To change the privilege level, toggle the **Access Level** field until the appropriate level is displayed - **Root**, **User+**, or **User**.
5. Highlight **APPLY** and press Enter to make the change effective.
6. You must enter the configuration changes into the NVRAM through the **Save Changes** choice on the main menu if you want the configuration to be used after a switch restart.

Deleting a user account

Only a user with Root privileges can delete user accounts. Before you can delete a user account, you must also enter the password for that user account.

Complete the following steps to delete a user account and password:

1. Select **Setup User Accounts** in the main menu. The following Setup User Accounts window opens.

```

Setup User Accounts
-----
Current Accounts:   User Name      Access Level
                   USERID         Root

Action             <Add >
Username           [                ]
Old Password       [                ]
New Password       [                ]
Confirm New Password [          ]
Access Level       <Root >
                                           APPLY
-----
Function: Select action - Add, Delete, or Update.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

2. Toggle the **Action** field to **Delete**.
3. Enter the applicable information in the **Username** and **Old Password** fields for the account that you want to delete.

4. Highlight **APPLY** and press Enter to make the deletion of the selected user effective.
5. You must enter the configuration changes into the NVRAM through the **Save Changes** choice on the main menu if you want the configuration to be used after a switch module restart.

Basic Setup

The main menu is divided into two sections, **Basic Setup** and **Advanced Setup**. The **Basic Setup** menus are organized into 12 main categories: **Switch Information** (see “Switch Information”), **IP Setup** (see “IP Setup”), **Remote Management Setup** (see “Remote Management Setup” on page 86), **Switch Settings** (see “Switch Settings” on page 88), **Configure Ports** (see “Configure Ports” on page 89), **Setup User Accounts** (see “Setting up user accounts” on page 78), **Utilities** (see “Utilities” on page 89), **Network Monitoring** (see “Network Monitoring” on page 92), **Save Changes** (see “Saving changes” on page 80), **Reboot** (see “Restarting the switch module” on page 97), and **Logout** (see “Logging out” on page 98).

Switch Information

Highlight **Switch Information** on the main menu and press Enter. The following window opens:

```

Switch Information
-----
Device Type       : Ethernet Switch Module
MAC Address      : 00-05-5D-71-86-80
Boot PROM Version: 00.00.04
Firmware Version : 00.00.38
Hardware Version : Rev. 2
Device S/N       : 01234567

System Name      [ _____ ]
System Location  [ _____ ]
System Contact   [ _____ ]

APPLY

Function: Sets a name for identification purposes.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

The Switch Information window shows the type of switch module and its MAC address (assigned by the factory and unchangeable). In addition, the boot PROM and firmware version numbers are shown. This information is helpful to keep track of PROM and firmware code updates and to obtain the switch module MAC address for entry into another network device address table, if necessary.

You can also enter the name of the system, its location, and the name and telephone number of the system administrator. In this case, the system administrator is the person who is responsible for the maintenance of the network system on which this switch module is installed.

IP Setup

Some settings must be entered to enable the switch module to be managed from an SNMP-based Network Management System such as SNMP version 1 or to be able to access the switch module using the Telnet protocol.

Select the **IP Setup** window to specify how the switch module will be assigned an IP address to enable it to be identified on the network.

The switch default IP address is 192.168.70.1xx, where xx depends on the number of the bay into which you have installed the switch module, as shown in Table 5.

Table 5. Default IP addresses based on switch-module bay numbers (IP Setup window of Telnet Basic Setup menu)

Bay number	Default IP address
Bay 1	192.168.70.127
Bay 2	192.168.70.128
Bay 3	192.168.70.129
Bay 4	192.168.70.130

To set up the switch module for remote management, highlight **IP Setup** in the main menu and press Enter. The following window opens.

```

IP Setup
-----
Current Switch IP Settings
Get IP From      :Manual
IP Address       :160.0.0.34
Subnet Mask      :255.255.0.0
Default Gateway  :0.0.0.0

New Switch IP Settings
Get IP From      <Manual>
IP Address       [160.0.0.34]  |
Subnet Mask      [255.255.0.0]  |
Default Gateway  [0.0.0.0]     |

APPLY      SAVE/APPLY
-----
Function: Get IP from Manual, BOOTP or DHCP.
Message:
CTRL+T = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
  
```

The switch module must have an IP address assigned to it so that a network management system (that is, Telnet) client can find it on the network.

The fields listed under the **Current Switch IP Settings** heading are those currently being used by the switch module. The fields listed under the **New Switch IP Settings** heading are those that will be used after the switch module has been restarted. Toggle the **Get IP From** field using the Spacebar to select from **Manual**, **BOOTP**, or **DCHP**. This selects how the switch module will be assigned an IP address on the next restart (or startup).

Note: BOOTP and DHCP are only supported through the four external Ethernet ports on the switch module. To use BOOTP and DHCP, you must first enable these ports for remote-management access through the BladeCenter management and configuration program. For a detailed description of this program, see the *@server BladeCenter Type 8677 Installation and User's Guide* on the *IBM BladeCenter Documentation CD*.

The **Get IP From** options are:

BOOTP

The switch module will send out a BOOTP broadcast request when it is turned on. The BOOTP protocol enables IP addresses, network masks, and

default gateways to be assigned by a central BOOTP server. If this option is selected, the switch module will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

DCHP The switch module will send out a DCHP broadcast request when it is turned on. The DCHP protocol enables IP addresses, network masks, and default gateways to be assigned by a DCHP server. If this option is set, the switch will first look for a DCHP server to provide it with this information before using the default or previously entered settings.

Manual

This option enables the entry of an IP address, subnet mask, and a default gateway for the switch. These entries should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the network administrator. The fields that require entries under this option are as follows:

Subnet Mask

A bitmask that determines the extent of the subnet that the switch module is on. It should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a class A network, 255.255.0.0 for a class B network, and 255.255.255.0 for a class C network, but custom subnet masks are permitted.

Note: For switch communication with a remote management station, such as the IBM Director server, through the management module external Ethernet port, the switch module internal network interface and the management module internal and external interfaces must be on the same subnet.

Default Gateway

An IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or if you do not want the device to be accessible outside your local network, you can enter a value of **0.0.0.0** in this field.

Remote Management Setup

The switch sends out SNMP traps to network management stations whenever certain exceptional events occur, such as when the switch is turned on or when a system reset occurs. The switch enables traps to be routed to up to four different network management hosts.

For a detailed list of the trap types that are used for this switch, see “Traps” on page 20.

SNMP (version 1) implements a rudimentary form of security by requiring that each request include a *community name*. A community name is an arbitrary string of characters used as a “password” to control access to the switch. If the switch receives a request with a community name that it does not recognize, it will trigger an authentication trap.

The SNMP enables up to four different community names to be defined. The community name **public** is defined by default; you can change this name and add others. You will need to coordinate these names with the community name settings that you use in your network management system.

When you select **Remote Management Setup** on the main menu, the following window opens.

```

Remote Management Setup
-----
Management Station IP Settings
IP Address [10.0.0.0 ]
IP Address [0.0.0.0 ]
IP Address [0.0.0.0 ]

SNMP Community Settings
Community String      Rights      Status
[public               ] <Read>    <Enabled >
[private              ] <R/W >   <Enabled >
[                     ] <Read>   <Disabled>
[                     ] <Read>   <Disabled>

                                SETUP TRAP RECEIVERS      APPLY
-----
Function: Create a list of IP addresses that can access the switch.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

You can set the following parameters:

IP Address

The IP address of the network management station to receive traps.

Community String

The community string that will be included on SNMP packets sent to and from the switch. Any station that is not a member of this community will not receive the packet.

Rights

Enables each community to be separately set to either **Read** (read-only), meaning that the community member can only view switch settings or **R/W** (read/write), which enables the member to change settings in the switch.

Status

Determines whether this community name entry is **Enabled** or **Disabled**.

To set up trap recipients, highlight **SETUP TRAP RECEIVERS** at the bottom of the Remote Management Setup menu and press Enter.

```

Setup Trap Recipients
-----
SNMP Trap Recipients:
IP Address      SNMP Community String      Status
[               ] [               ] <Disabled>
[               ] [               ] <Disabled>
[               ] [               ] <Disabled>
[               ] [               ] <Disabled>

                                APPLY
-----
Function: Edit SNMP Trap Receivers.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

You can set the following parameters:

IP Address

The IP address of the network management station to receive traps.

SNMP Community String

The community string that will be included on SNMP packets sent to and from the switch. Any station that is not a member of this community will not receive the packet.

Status

Determines whether this community name entry is **Enabled** or **Disabled**.

Highlight **APPLY** and press Enter to make your changes effective.

Switch Settings

Highlight **Switch Settings** in the main menu and press Enter to set GVRP globally, enable the MAC address aging timer, and to set the upper threshold of the storm control.

```
Switch Settings
-----
Switch GVRP                <Disabled>
MAC Address Aging Timer    <Enabled >
MAC Address Aging Time(sec) [300 ]

Telnet Settings
  Telnet Time Out(min)     <10 mins>
  Telnet Sessions(1..4)    [1]

APPLY

Function: Set GVRP status.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

The user-changeable parameters in the switch are as follows:

Switch GVRP <Disabled>

Group VLAN Registration Protocol is a protocol that enables members to dynamically join VLANs. This option is used to enable or disable GVRP on the switch module.

MAC Address Aging Timer <Enabled>

This field specifies whether the aging timer is on or off.

MAC Address Aging Time(sec) [300]

The aging timer of MAC address entries can be set from 10 to 1000000 seconds.

Telnet Settings

The user-changeable parameters in the switch are as follows:

Telnet Time Out (min) <10 mins>

This sets the time that the Telnet interface can be idle before the switch automatically logs out the user. The options are **2 mins**, **5 mins**, **10 mins**, **15 mins**, and **Never**.

Telnet Sessions (1..4) [1]

This sets the maximum number of available Telnet sessions.

Configure Ports

Highlight **Configure Ports** in the main menu and press Enter. The following window opens.

```
Configure Ports
-----
Port   State   Speed/Duplex/Flow  Connection  Port Type
1      Enabled 1000M/Full/Enabled 1000M/Full/802.3x Internal
2      Enabled 1000M/Full/Enabled Link Down    Internal
3      Enabled 1000M/Full/Enabled Link Down    Internal
4      Enabled 1000M/Full/Enabled Link Down    Internal
5      Enabled 1000M/Full/Enabled Link Down    Internal
6      Enabled 1000M/Full/Enabled Link Down    Internal

View Ports      <[unt 1 to 6]>
Configure Port  <[1 ] to [1 ]>
State          <Enabled >
Speed/Duplex   <1000M/Full>
Flow Control    <Enabled >

APPLY

Function: Select the scope of ports for display and configuration.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

Toggle the **View Ports** field, using the Spacebar, to view the configuration of a range of internal or external ports. To configure a specific port, toggle the **Configure Port from [] to []** field until the applicable port number or port range appears. Toggle the **State** field to either enable or disable a port.

Toggle the **Speed/Duplex** field to select the speed and duplex/half-duplex state of the four external ports **Ext1** to **Ext4**. **Auto** means auto-negotiation between 10, 100, and 1000 Mbps devices, in full-duplex or half-duplex mode. The **Auto** setting enables these ports to automatically determine the fastest settings that the device to which the port is connected can handle and then to use those settings. The other options are **100M/Full**, **100M/Half**, **10M/Full**, and **10M/Half**. There is no automatic adjustment of port settings with any option other than **Auto**. **Flow Control** can be enabled or disabled in conjunction with all of the **Speed/Duplex** settings except **10M/Half** and **100M/Half**. In these two cases, back pressure is automatically selected.

The 14 internal ports in the switch module support only **1000M/Full**, and each port can have **Flow Control** enabled or disabled.

Utilities

To access the Switch Utilities menu, highlight **Utilities** on the main menu and press Enter.

```
Switch Utilities
-----
Switch Settings
Server IP Address: 0.0.0.0
Switch IP Address: 160.0.0.34
Subnet Mask       : 255.255.0.0
Gateway Router    : 0.0.0.0

TFTP Services
Upgrade Firmware from TFTP Server
Download Configuration File from TFTP Server
Upload Configuration File to TFTP Server
Save Log to TFTP Server

Others
Ping Test

Function: Upgrade firmware.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

Notes:

1. Trivial file transfer protocol (TFTP) services enable the switch firmware code to be upgraded by transferring a new firmware code file from a TFTP server to the switch. A configuration file can also be loaded into the switch from a TFTP server, switch settings can be saved to the TFTP server, and a history log can be uploaded from the switch to the TFTP server.
2. The TFTP server must be on the same IP subnet as the switch.
3. The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages. Shareware packages also are available through the Internet.

Upgrade Firmware from TFTP Server

To update the switch firmware code, highlight **Upgrade Firmware from TFTP Server** and press Enter.

```
Upgrade Firmware from TFTP Server
-----
Server IP Address [0.0.0.0]
Path\Filename [ ]
                                     START  APPLY
-----
Function: Enter the Server IP address.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

Enter the IP address of the TFTP server in the **Server IP Address** field.

Enter the path and the file name for the firmware code file on the TFTP server.

Highlight **APPLY** and press Enter to record the IP address of the TFTP server. Select **Save Changes** in the main menu to enter the address into NVRAM.

Highlight **START** and press Enter to initiate the file transfer.

Download Configuration File from TFTP Server

To download a switch configuration file from a TFTP server, highlight **Download Configuration File from TFTP Server** on the Switch Utilities menu and press Enter.

```

Download Configuration File from TFTP Server
-----
Server IP Address [1.0.0.0]
Path\Filename [ ]
START APPLY
-----
Function: Enter the Server IP address.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

Enter the IP address of the TFTP server and specify the path and file name of the switch configuration file on the TFTP server.

Highlight **APPLY** and press Enter to record the IP address of the TFTP server. Select **Save Changes** in the main menu to enter the address into NVRAM.

Highlight **START** and press Enter to initiate the file transfer.

Upload Configuration File to TFTP Server

To upload a configuration file to the TFTP server, highlight **Upload Configuration File to TFTP Server** on the Switch Utilities menu and press Enter.

```

IBM BladeCenter 4-Port Gb Ethernet Switch Module - Main Menu
-----
Basic Setup
Switch Information
IP Setup
Remote Management Setup
Switch Settings
Configure Ports
Setup User Accounts
Utilities
Network Monitoring
Save Changes
Reboot
Logout

Advanced Setup
Spanning Tree
Forwarding
Class Of Service
Mirroring
Multicasting
VLANs
Link Aggregation
-----
Function: Configure Current Switch IP Settings.
Message:
For Help, press F1

```

Enter the IP address of the TFTP server and the path and specify the path and file name of the switch configuration file on the TFTP server and press **APPLY**. Highlight **START** and press Enter to initiate the file transfer.

Save Log to TFTP Server

To save a history log on a TFTP server, highlight **Save Log File to TFTP Server** on the Switch Utilities menu and press Enter.



Enter the IP address of the TFTP server and the path and file name for the history log on the TFTP server. Highlight **APPLY** and press Enter to make the changes current. Highlight **START** and press Enter to initiate the file transfer.

Ping Test

To test the connection with another network device, highlight **Ping Test** on the Switch Utilities menu and press Enter.



Enter the IP address of the network device to be pinged and the number of test packets to be sent (three is usually enough). Highlight **START** and press Enter to initiate the Ping test.

Note: The Ethernet switch module will issue Ping Requests through the internal Ethernet link to the management module and optionally, through the external Ethernet ports. When Ping Requests are issued on both of these paths, it is likely that one or more Pings will not reach the intended destination through one of these paths. Through the management module path, the Ethernet switch module can only Ping IP addresses that are on the same IP subnet as the IP addresses of the Ethernet switch module and management module.

Network Monitoring

The switch module provides extensive network monitoring capabilities.

To display the network data compiled by the switch, highlight **Network Monitoring** on the main menu and press Enter.

```

Network Monitoring Menu
-----
Statistics
  Port Utilization
  Port Error Packets
  Port Packet Analysis
Address Table
  Browse MAC Address Table

Applications
  GURP
  IGMP Snooping
  LACP Aggregator
  Switch History

Function: Switch port utilization overview.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

Port Utilization

To view the port utilization of all the ports on the switch, highlight **Port Utilization** on the **Network Monitoring** menu and press Enter.

```

Port Utilization
-----
Port  TX/sec  RX/sec  %Util.  Port  TX/sec  RX/sec  %Util.
EX1   1         16      0        1     1         0        0
EX2   0         0        0        2     0         0        0
EX3   0         0        0        3     0         0        0
EX4   0         0        0        4     0         0        0
      5     0         0        0
      6     0         0        0
      7     0         0        0
      8     0         0        0
      9     0         0        0
     10    0         0        0
     11    0         0        0
     12    0         0        0
     13    0         0        0
     14    0         0        0

Interval <2 sec >

Function: Select the polling interval.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

The **Port Utilization** window shows the number of packets transmitted and received per second and calculates the percentage of the total available bandwidth being used on the port (displayed under **%Util.**). Highlight **CLEAR COUNTER** and press Enter to reset the counters.

Port Error Packets

To view the error statistics for a port, highlight **Port Error Packets** on the **Network Monitoring** menu and press Enter.

```

Port Error Packets
-----
CRC Error      0      RX Frames
Undersize      0
Oversize       0
Fragment       0
Jabber         0
Drop Pkts      0
Port Link Change 1
Ext Link Change 2
Int Link Change 2

ExDefer        0      TX Frames
CRC Error      0
Late Coll.     N/A
Ex. Coll.      N/A
Single Coll.   N/A
Coll.          N/A

Module <Internal Ports>
Port [1]
Interval <2 sec >

CLEAR COUNTER

Function: Select internal ports(1-14) or external ports(1-4) to monitor.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

Enter the module and port number of the port to be viewed. The **Interval** field can be toggled among **2 seconds**, **1 minute**, and **suspend**. This sets the interval at which the error statistics are updated. Highlight **CLEAR COUNTER** and press Enter to reset the counters.

Port Packet Analysis

To view an analysis of the size of packets received or transmitted by a port, highlight **Port Packet Analysis** on the **Network Monitoring** menu and press Enter.

```

Port Packet Analysis
-----
      Frames      Frames/sec      Total      Total/sec
64          3853             1          9223705       71
65-127      1861             0          RX Frames 8094         1
128-255     1774             0          TX Bytes 1113301       95
256-511     128              0          TX Frames 6094           0
512-1023    439              0
1024-1518   6133             0
Unicast RX   8007             1
Multicast RX 4                0
Broadcast RX 83              0

Module <[Internal Ports]>
Port [1 ]
Interval <2 sec >

CLEAR COUNTER

Function: Select internal ports(1-14) or external ports(1-4) to monitor.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

In addition to the size of packets received or transmitted by the selected port, statistics on the number of unicast, multicast, and broadcast packets are displayed. Highlight **CLEAR COUNTER** and press Enter to reset the counters.

Browse MAC Address Table

To set the MAC address aging time and view the MAC address forwarding table, highlight **Browse MAC Address Table** on the **Network Monitoring** menu and press Enter:

```

Browse MAC Address Table
-----
Total Addresses in Table:35

UID  MAC Address  Port  Learned  UID  MAC Address  Port  Learned
1    0000E286CCCF  EX1  Dynamic  1    000255FAB9C  EX1  Dynamic
1    000255AC026C  EX1  Dynamic  1    000255FABBB8  EX1  Dynamic
1    000255FARA6C  EX1  Dynamic  1    000255FARBCE  EX1  Dynamic
1    000255FARA92  EX1  Dynamic  1    000255FABD4  EX1  Dynamic
1    000255FARAB6  EX1  Dynamic  1    000255FARC54  EX1  Dynamic
1    000255FARB2C  EX1  Dynamic  1    000255FARC58  EX1  Dynamic
1    000255FARB40  EX1  Dynamic  1    000255FARD06  EX1  Dynamic
1    000255FARB42  EX1  Dynamic  1    000255FARD50  EX1  Dynamic
1    000255FARB4C  EX1  Dynamic  1    000255FARD5E  EX1  Dynamic
1    000255FARB88  EX1  Dynamic  1    000255FARD60  EX1  Dynamic

Browse By <ALL>
BROWSE      CLEAR ALL

Function: Select Mac address, Port, UID, or ALL to browse.
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page

```

The **Browse By** field can be toggled between **ALL**, **MAC Address**, **Port**, and **VLAN**. This sets a filter to determine which MAC addresses from the forwarding table are displayed. **ALL** specifies no filter.

Note: A very long aging time can result with the out-of-date dynamic entries that might cause incorrect packet filtering or forwarding decisions. A very short aging time might cause entries to be aged out too soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table. In this case, the switch will broadcast the packet to all ports, thus negating many of the benefits of having a switch.

Complete the following steps to search for a particular MAC address:

Toggle the **Browse By** field to **MAC Address**. A **MAC Address** field will appear. Enter the MAC address in the field and press Enter. Highlight **BROWSE** and press Enter to initiate the browsing action. Highlight **CLEAR ALL** and press Enter to reset the table counters.

Complete the following steps to search for a particular port:

Toggle the **Browse By** field to **Port**. The **Module** and **Port** fields will appear. Enter the desired information in the respective fields and press Enter. Highlight **BROWSE** and press Enter to reset the table counters.

Complete the following steps to search for a particular VLAN:

Toggle the **Browse By** field to **VLAN**. A **VLAN** field will appear. Enter the VID in the field and press Enter. Highlight **BROWSE** and press Enter to initiate the browsing action.

GVRP

To view the GVRP table, highlight **GVRP** on the **Network Monitoring** menu and press Enter.

```
GVRP
-----
Number of
IEEE 802.1Q VLAN : 1
IEEE 802.1Q VLAN ID: 1

Egress Ports      : EX1, EX2, EX3, EX4
                   1,  2,  3,  4,  5,  6
                   7,  8,  9, 10, 11, 12, 13, 14

Untagged Ports    : EX1, EX2, EX3, EX4
                   1,  2,  3,  4,  5,  6
                   7,  8,  9, 10, 11, 12, 13, 14

Status            : Permanent
Creation time since
switch power up  : 00:19:48
-----
Function:
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page
```

This read-only window displays Group VLAN Registration Protocol (GVRP) information.

IGMP Snooping

This enables the switch IGMP Snooping table to be viewed. IGMP Snooping enables the switch to read the multicast group IP address and the corresponding MAC address from IGMP packets that pass through the switch. The ports where the IGMP packets were snooped are displayed, indicated by an *M*. The number of IGMP reports that were snooped is also displayed in the **Reports** field.

To view the IGMP Snooping table, highlight **IGMP Snooping** in the **Network Monitoring** menu and press Enter.

```

IGMP Snooping
-----
Total Entries      : 0          VID :          Age Out:
Total Entries in the VLAN: 0      State:          Queries:

Multicast group   MAC address   Reports   Ext Ports   Int Ports
                1 4           1 8       14

VID [0]

APPLY

Function: Enter VID<1-4094>.
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page

```

Enter a VLAN ID number in the first field and select GO to display the IGMP Snooping Status window that you selected.

LACP Aggregator

The Link Aggregation Control Protocol (LACP) aggregator displays the status of dynamic LACP trunked ports from the group point of view.

To view the LACP Aggregator Monitoring window, highlight **LACP Aggregator** in the **Network Monitoring** menu and press Enter.

```

LACP Aggregator Monitoring
-----
index   Operation. Key  EX1--4   Status
0       15             ----    Individual
1       16             ----    Individual
2       17             ----    Individual
3       18             ----    Individual

Function:
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

The information on this read-only window is described as follows:

Index The LACP Aggregator ID number.

Operation Key

Displays the operational key used by the aggregator to communicate with other aggregators.

Member Port

Displays the port member status in the aggregator group.

Status

Displays the status of each aggregator. When there is only one port member in the aggregator, the aggregator acts as a normal individual port (by default, each LACP-enabled port is assigned to its own aggregator group). Otherwise, it will start to aggregate when there is more than one port that wants to join the aggregator group.

Switch History

To view the switch history log, highlight **Switch History** from the **Network Monitoring** menu and press Enter.

```

Switch History
-----
Seq.#  Time                Log Text
-----
57     000d00h03m52.78s    Successful login through telnet.
56     000d00h03m29.04s    Authentication Failure.
55     000d00h00m06.37s    Link change on port Bay 14 Link-Down
54     000d00h00m06.36s    Link change on port Bay 13 Link-Down
53     000d00h00m06.36s    Link change on port Bay 12 Link-Down
52     000d00h00m06.35s    Link change on port Bay 11 Link-Down
51     000d00h00m06.35s    Link change on port Bay 10 Link-Down
50     000d00h00m06.34s    Link change on port Bay 9 Link-Down
49     000d00h00m06.34s    Link change on port Bay 8 Link-Down
48     000d00h00m06.33s    Link change on port Bay 7 Link-Down
47     000d00h00m06.33s    Link change on port Bay 6 Link-Down
46     000d00h00m06.32s    Link change on port Bay 5 Link-Down
-----
Function:
Message:
CTRL+N=Next Page  CTRL+P=Previous Page  B=Begin  E=End  C=Clear  CTRL+R=Refresh

```

Restarting the switch module

The switch module has several reboot (restart) options.

To restart the switch, highlight **Reboot** in the main menu and press Enter.

```

Reboot
-----
Reboot
Save Configuration & Reboot
Reboot & Load Factory Default Configuration
Reboot & Load Factory Default Configuration Except IP Address
-----
Function: Reboot the system.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

The reboot options are as follows:

Reboot

Restarts the switch. Any configuration settings that are not saved through **Save Changes** in the main menu will be lost. The switch configuration will be restored to the last configuration that was saved in NVRAM.

Save Configuration & Reboot

Saves the configuration to NVRAM (identical to using **Save Changes**) and then restarts the switch.

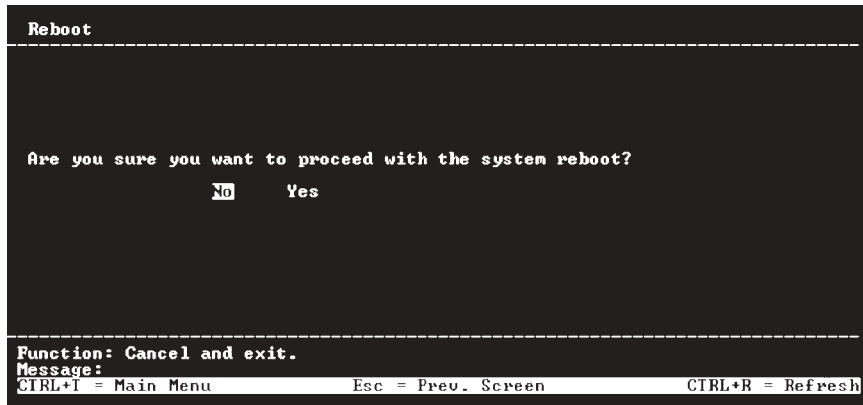
Reboot & Load Factory Default Configuration

Restarts the switch using the default factory configuration. All configuration data will be lost. This is identical to using **Factory Reset** and then **Reboot**.

Reboot & Load Factory Default Configuration Except IP Address

Restarts the switch using the default factory configuration, except the user configured IP address will be retained. All other configuration data will be lost.

A confirmation window will open.



To restart the switch, in the mode entered in the preceding window, highlight **Yes** and press Enter.

Logging out

When you are finished with the current switch-module session, select **Logout** from the main menu. You can select one of two methods for processing the changes that you made during the current switch-module session:

- If you made changes and used the **APPLY** function during the current switch-module session, but did not save your changes on the main menu, the following window will open:



If you do not want to save your changes, select **Yes** to log out without saving your changes. The current switch-module session will close and, the login window will open so that you can start a new switch-module session (see “First-time connection to the Ethernet switch module” on page 76 for additional information).

- If you either saved your changes on the main menu or did not make any changes during the current switch-module session, the Logout window will not open when you select **Logout**. Instead, the current switch-module session will immediately close and, the Login window will open so that you can start a new switch-module session (see “First-time connection to the Ethernet switch module” on page 76 for additional information).

Advanced Setup

The main menu is divided into two sections, **Basic Setup** and **Advanced Setup**. The **Advanced Setup** menus are organized into seven main categories: **Spanning Tree** (see “Spanning Tree”), **Forwarding** (see “Forwarding” on page 101), **Class of Service** (see “Class of Service” on page 101), **Mirroring** (see “Mirroring” on page 103), **Multicasting** (see “Multicasting” on page 104), **VLANs** (see “VLANs” on page 107), and **Link Aggregation** (see “Link Aggregation” on page 110).

Spanning Tree

To globally configure the Spanning Tree Protocol (STP) on the switch, select **Spanning Tree** on the main menu and press Enter. The following window opens:

```
-----
Configure Spanning Tree
-----
Switch Settings
Status      <Enabled>
Max Age     [20]
Hello Time  [2]
Forward Delay [15]
Priority     [32768]
Designated Root Bridge: 00055D718680
Root Priority : 32768
Cost to Root  : 0
Root Port     : 0
Last Topology Change : 1726 secs
Topology Changes Count: 0

-----
STP Port Settings      APPLY
-----
Function: Set spanning tree status.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

The STP operates on two levels. On the switch level, the settings are globally implemented, and on the port level, the settings are implemented on a per user-defined group basis.

Note: The factory default settings should cover the majority of installations. Therefore, it is advisable to keep the default settings as set at the factory unless it is absolutely necessary to change them.

The user-changeable parameters in the switch are as follows:

Status: <Disabled>

Toggle to **Enabled** to implement the Spanning Tree Protocol on the switch.

Max Age: [20]

The maximum age can be set from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the root bridge, your switch will start sending its own BPDU to all other switches for permission to become the root bridge. If your switch has the lowest bridge identifier, it will become the root bridge.

Hello Time: [2]

The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge. If you set a Hello Time for your switch, and it is not the root bridge, the set Hello Time will be used if and when your switch becomes the root bridge.

Note: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Forward Delay: [15]

The Forward Delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

Priority: [32768]

A priority for the switch can be set from 0 to 65535. Zero is equal to the highest priority. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch.

Note: Observe the following formulas when setting the preceding parameters:

- Max. Age $\leq 2 \times$ (Forward Delay - 1 second)
- Max. Age $\geq 2 \times$ (Hello Time + 1 second)

STP Port Settings

In addition to setting Spanning Tree parameters for use on the switch level, the switch module enables the configuration of Spanning Tree Protocol on individual ports.

To define individual ports, highlight **STP Port Settings** on the Configure Spanning Tree menu in “Spanning Tree” on page 99 and press Enter. The following window opens:

STP Port Settings							
Port	Speed/Duplex/Flow	Cost	Priority	Status	Fast STP	STP State	
1	1000M/Full/802.3x	10	128	Forwarding	Disabled	Disabled	
2	Link Down	10	128	Forwarding	Disabled	Disabled	
3	Link Down	10	128	Forwarding	Disabled	Disabled	
4	Link Down	10	128	Forwarding	Disabled	Disabled	
5	Link Down	10	128	Forwarding	Disabled	Disabled	
6	Link Down	10	128	Forwarding	Disabled	Disabled	

View Ports	<[nt 1 to 6]>
Configure Port	[1] to [1]
Port Cost	[10]
Priority	[128]
Fast STP	<Disabled>
STP State	<Disabled>

APPLY

Function: Select the scope of ports for display and configuration.
Message:
CTRL+I = Main Menu Esc = Prev. Screen CTRL+R = Refresh

Toggle the **View Ports** field to the range of ports to be configured. Enter the port number or port range in the **Configure Port from [] to []** field. When the **STP State** is **Enabled**, you can set the spanning tree port cost and priority.

View Ports

Enter the range of ports to be configured and displayed.

Configure Port

Enter the specific ports to be configured, inputting the starting port in the first field and the ending port in the second field.

Port Cost [10]

The spanning tree port cost can be set between 1 and 65535. The lower the cost, the greater the probability that the port will be chosen as the designated port (chosen to forward packets).

Priority [128]

The spanning tree port priority can be set between 0 and 255. The lower the priority, the greater the probability that the port will be chosen as the root port.

Fast STP <Disabled>

Toggle between **Enabled** and **Disabled**. When the STP is turned on, a change from link-down to link-up will trigger the STP. The STP will set the port to the listening state. After the forward delay, the STP will set the port to the learning state. After another forward delay, the STP will set the port to the forwarding state. If the forward delay is 15 seconds, the port will take 30 seconds to forward packets. However, when Fast STP is **Enabled** on a port, the port will only take 15 seconds from link-up to the time that it starts forwarding packets. This is because enabling the Fast STP option will skip the learning state, jumping directly to the forwarding state from the listening state.

STP State <Enabled>

The Spanning Tree Protocol state for a selected port can either be **Enabled** or **Disabled**.

Forwarding

Highlight **Forwarding** on the main menu to access the following MAC Address Forwarding window:

```
MAC Address Forwarding
-----
Total Entries: 0
MAC Address      VID      Port      MAC Address      UID      Port
-----
Action           <Add/Modify>
UID              [ 1 ]
Unicast MAC Address [000000000000]
Module <Internal Ports> Port [ 1 ]
-----
APPLY
Function: Select the action- ADD/MODIFY or DELETE.
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page
```

The **Action** field can be toggled between **Add/Modify** and **Delete** using the Spacebar. Enter the VLAN ID in the **VID** field, the MAC address to be entered in the forwarding table in the **Unicast MAC Address** field, and select either internal or external ports in the **Module** field. Enter the port number in the **Port** field.

Highlight **APPLY** and press Enter to make the changes current. Use **Save Changes** in the main menu to enter the changes into NVRAM.

Class of Service

The switch module enables you to customize class of service settings on the Class of Service menu.

Select **Class of Service** on the main menu and press Enter. The following window opens:

```

Class Of Service
-----
Output Priority Queue Method: <Disabled >

COS Configuration      802.1p Priority Mapping    Diffserv Mapping    APPLY
-----
Function: Select Priority method.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

To enable priority queuing on the switch module, toggle the field on the preceding window from **Disabled** to **Weighted Round Robin** and press **APPLY**.

Class of Service Configuration

Select **COS Configuration** on the Class of Service menu and press Enter to access the Class of Service Configuration window.

The Class of Service Configuration window contains the following information:

```

Class of Service Configuration
-----
Class                Weight      Max. Latency
-----
High Priority        [15]       <0.4 sec>
Med-H Priority       [10]       <0.4 sec>
Med-L Priority       [4 ]       <0.4 sec>
Low Priority         [1 ]       <0.4 sec>

APPLY

Function: Specify the weight(the number of packets).
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

The switch module supports 802.1p priority queuing; four priority queues are supported per port. The switch module provides user-programmable mapping (four Priority Queue assignments: High, Med-High, Med-Low, Low) for the eight 802.1p priority classes (0 to 7). For the priority queue feature to take effect, users must first enable the Output Priority Queue Method on the Class of Service menu. Otherwise, only the round-robin method can be used to schedule the packets in four different priority queues.

When the Output Priority Queue Method is enabled, the weight and latency specified in the preceding Class of Service Configuration window will take effect. Note that the weight can only be a value between 1 and 16. A higher priority queue always has a larger weight than a lower priority queue.

802.1p Priority Mapping

Select **802.1p Priority Setting** on the Class of Service menu and press Enter to access the following window:


```

Setup 802.1p Priority Mapping
-----
802.1p Priority      Class
0                   Low Priority
1                   Low Priority
2                   Med-L Priority
3                   Med-L Priority
4                   Med-H Priority
5                   Med-H Priority
6                   High Priority
7                   High Priority

Configure Priority  [?] to [0]
Class              <Low Priority >

APPLY

Function: Input port number.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

This window enables you to configure traffic class priority by specifying the class value, from **Low Priority** to **High Priority**, of the switch eight levels of priority. Press **APPLY** to make your changes effective.

Diffserv Mapping

The switch module supports DiffServ Mapping (Differential Services RFC 2475) for Ipv4 frames when DiffServ Mapping is enabled on the Setup DiffServ Mapping window. If the frame is not an Ipv4 frame or DiffServ is not enabled, 802.1p is used. The size of the switch module DiffServ table is 64 by 4. This specifies the mapping of 64 DiffServ code points to the four priority queues.

Select **Diffserv Mapping** on the Class of Service menu and press Enter to access the following window:

```

Setup Diffserv Mapping
-----
0:Low  1:Low  2:Low  3:Low  4:Low  5:Low  6:Low  7:Low
8:Low  9:Low  10:Low  11:Low  12:Low  13:Low  14:Low  15:Low
16:Low 17:Low 18:Low 19:Low 20:Low 21:Low 22:Low 23:Low
24:Low 25:Low 26:Low 27:Low 28:Low 29:Low 30:Low 31:Low
32:Low 33:Low 34:Low 35:Low 36:Low 37:Low 38:Low 39:Low
40:Low 41:Low 42:Low 43:Low 44:Low 45:Low 46:Low 47:Low
48:Low 49:Low 50:Low 51:Low 52:Low 53:Low 54:Low 55:Low
56:Low 57:Low 58:Low 59:Low 60:Low 61:Low 62:Low 63:Low

Diffserv Mapping      <Disabled>
Configure Code Point  [0 ] to [0 ]
Class                 <Low Priority >

APPLY

Function: Enable or Disable Diffserv Mapping.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

To set up DiffServ Mapping, toggle DiffServ Mapping to **Enabled**, enter a beginning and ending Code Point (0 to 63) in the second field, and select the desired Class in the next field (**Low Priority**, **Med-L Priority**, **Med-H Priority**, and **High Priority**). When you are finished, highlight **APPLY** and press Enter to make your change effective.

Mirroring

The switch module enables you to copy frames that were transmitted and received on a source port and to redirect the copies to another target port. The source port can be one of the four 10/100/1000 Mbps external ports, while the target port is where you will connect a monitoring/troubleshooting device, such as a sniffer or an RMON probe and, it must be one of the four 10/100/1000 Mbps external ports.

You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets that pass through the first port. This is useful for network monitoring and troubleshooting purposes.

The default setting for port mirroring is **Disabled**.

Select **Mirroring** in the main menu to access the following window:

```
Port Mirroring Settings
-----
Mirroring Status    <Disabled>
Source Port         <Ext3>
Ingress Target Port <Ext2>
Egress Target Port  <Ext1>

APPLY

Function: Enable/Disable mirroring function.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

To configure a mirror port, enter the port from where you want to copy frames in the **Source Port** field, and the Ingress and/or Egress port in the appropriate **Target Port** field(s). The source port must be one of the four external ports (Ext1, Ext2, Ext3, or Ext4). The target port must be one of the four external ports (Ext1, Ext2, Ext3, or Ext4).

Finally, toggle the **Mirroring Status** field to **Enabled**, highlight **APPLY**, and press Enter.

Notes:

1. You should not mirror a faster port or higher traffic ports on to a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port from which you are copying frames should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port cannot be a member of a trunk group.
2. Port mirroring is not possible if you use the same egress and ingress target port.

Multicasting

Select **Multicasting** on the main menu to access the following window:

```

Multicasting Menu
-----
IGMP Snooping
Setup IEEE 802.1q Multicast Settings

-----
Function: Setup IGMP snooping configuration.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

IGMP Snooping

IGMP Snooping can be globally enabled or disabled from the IGMP Snooping window.

To configure IGMP Snooping, highlight **IGMP Snooping** on the Multicasting Menu and press Enter:

```

IGMP Snooping
-----
Switch IGMP Snooping <Disabled>
Querier State <Non-Querier>
Robustness Variable [2 ]
Query Interval [125 ]
Max Response [10]
Age Out :260

APPLY
-----
Function: Set IGMP snooping status.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

To configure IGMP Snooping, complete the following steps:

Toggle the **Switch IGMP Snooping** field to **Enabled**. Toggle the **Querier State** field to the appropriate choice among **Non-Querier**, **V1-Querier**, and **V2-Querier** to determine the version of IGMP that is used in your network. You can enter a value between 1 and 255 for the **Robustness Variable** (default is 2). You can set the **Query Interval** between 1 and 65500 seconds (default is 125 seconds). This sets the time between IGMP queries. The **Max Response** enables a setting between 1 and 25 seconds (default is 10) and specifies the maximum amount of time available before sending a response report. The **Age Out** timer is fixed at 260 seconds.

Highlight **APPLY** and press Enter to make the settings effective.

The user-changeable parameters in the switch are as follows:

Switch IGMP Snooping: <Disabled>

This field can be toggled using the Spacebar between **Disabled** and **Enabled**. This is used to enable or disable IGMP Snooping, globally, on the switch.

Querier State: <Non-Querier>

This field can be toggled among **Non-Querier**, **V1-Querier**, and **V2-Querier**. This is used to specify the IGMP version (1 or 2) that will be used by the IGMP interface when making queries.

Robustness Variable: [2]

A tuning variable to allow for sub-networks that are expected to lose a large number of packets. You can enter a value between 1 and 255, with larger values being specified for sub-networks that are expected to lose larger numbers of packets.

Query Interval: [125]

Enables the entry of a value between 1 and 65500 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.

Max Response: [10]

Sets the maximum amount of time available before sending an IGMP response report. You can enter a value between 1 and 25 seconds, with a default of 10 seconds.

Age Out

The time out function is fixed at 260 seconds.

Setup IEEE 802.1q Multicast Settings

To edit the IEEE 802.1q multicast settings, highlight **Setup IEEE 802.1q Multicast Settings** on the Multicasting Menu to access the following window:

```

Setup IEEE 802.1q Multicast Forwarding
-----
Total Entries: 0
MAC Address  VID  1      8      14  Ext1--4

Action                <Add/Modify>
UID                    [1]
Multicast MAC Address [000000000000]
Port 1 8 14 Ext1--4
<E/-> [-----] [-----]
-----
Function: Select the action- ADD/MODIFY or DELETE.
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page

```

The **Action** field can be toggled between **Add/Modify** and **Delete** using the Spacebar. To add a new entry to the multicast forwarding table, select **Add/Modify** and enter the VLAN ID number of the VLAN that will be receiving the multicast packets in the **VID** field. Enter the MAC address of the multicast source in the **Multicast MAC Address** field, and then enter the member ports. Each port can be Egress or a non-member of the multicast group, on a per-VLAN basis.

To set a port multicast group membership status, highlight the first field of **(E/-)**. Each port multicast group membership can be set individually by highlighting the port entry using the arrow keys, and then toggling between **E** and **-** using the Spacebar.

E (Egress Member)

Specifies the port as being a static member of the multicast group. Egress member ports are ports that will be transmitting traffic for the multicast group.

- (Non-Member)

Specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically.

Highlight **APPLY** and press Enter to make the changes current. Use **Save Changes** in the main menu to enter the changes into NVRAM.

VLANs

The switch reserves one VLAN, VID = 1, called the DEFAULT_VLAN, for internal use. The factory default setting assigns all ports on the switch to the DEFAULT_VLAN. As new VLANs are configured, their respective member ports are removed from the DEFAULT_VLAN. If the DEFAULT_VLAN is reconfigured, all ports are again assigned to it. Ports that are not wanted as part of the DEFAULT_VLAN are removed during the configuration.

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, it must be through a router.

Note: The switch default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLANs are created, the member ports assigned to the new VLAN will be removed from the default VLAN port member list.

VLAN Menu

The first item on the VLAN Menu enables you to add or modify an 802.1Q VLAN, and to edit the VLAN definitions. The second item enables you to configure the port settings for IEEE 802.1Q VLAN support. Highlight **VLANs** in the main menu and press Enter.

```
-----
VLAN Menu
-----
Edit 802.1Q VLANs
Configure 802.1Q Port Settings

-----
Function: Configure IEEE802.1Q VLAN settings.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh
```

Edit 802.1Q VLANs

To create or modify an 802.1Q VLAN, highlight Edit 802.1Q **Edit 802.1Q VLANs** on the VLAN Menu and press Enter:

```

Edit 802.1Q VLANs
-----
Total Entries:1
UID      VLAN Name      1      8      14  Ext1--4
1      DEFAULT_VLAN  EEEEEEEEEEEEEEE EEEE
          UUUUUUUUUUUUUU          UUUU

Action   <Add/Modify>      Port      1      8      14  Ext1--4
UID      [      ]          Member<E/F/-> [-----] [----]
VLAN Name [      ]          Tagging <U/T> [TTTTTTTTTTTTTT] [TTTT]
                                          APPLY

Function: Select the action- ADD/MODIFY or DELETE.
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page

```

To create an 802.1Q VLAN, complete the following steps:

1. Select **Add/Modify** in the **Action** field.
2. Enter a VLAN ID number in the **VID** field and a name for the new VLAN in the **VLAN Name** field.
3. Set the membership and tagging status.
4. Highlight **APPLY** and press Enter to make your changes effective.

To modify an existing 802.1Q VLAN, complete the following steps:

1. Select **Add/Modify** in the **Action** field.
2. Enter a VLAN ID number in the **VID** field and the name for the VLAN in the **VLAN Name** field.
3. Make the required changes to the membership and tagging status.
4. Highlight **APPLY** and press Enter to make your changes effective.

To delete an 802.1Q VLAN, complete the following steps:

1. Select **Delete** in the **Action** field.
2. Enter a VLAN ID number in the **VID** field and the name for the VLAN in the **VLAN Name** field.
3. Highlight **APPLY** and press Enter to make your changes effective.

To set the 802.1Q VLAN membership status of a port, go to the **Membership (E/F/-)** line in the preceding window. Each port 802.1Q VLAN membership can be set individually by highlighting the port entry using the arrow keys, and then toggling among **E**, **F**, and **-** using the Spacebar.

E (Egress Member)

Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.

F (Forbidden Non-Member)

Defines the port as a non-member and also forbids the port from joining a VLAN dynamically.

- (Non-Member)

Specifies the port as not being a member of the VLAN, but the port can become a member of the VLAN dynamically.

Next, determine which of the ports that are members of the new VLAN will be tagged or untagged ports.

To set a port as either a tagged or an untagged port, highlight the first field of **Tagging (U/T)** field. The state of each port can be set by highlighting the port entry using the arrow keys and then toggling between **U** or **T** using the Spacebar.

- U** Specifies the port as an Untagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
- T** Specifies the port as a Tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the Port VLAN Identifier (PVID); see “Configure 802.1Q Port Settings”). When a tagged packet exits the port, the packet header is unchanged.

If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then the port should be set to **U** - Untagged.

If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then the port should be set to **T** - Tagged.

Press **APPLY** to make the changes effective for the current session. To enter the changes into NVRAM, highlight **Save Changes** in the main menu and press Enter.

Configure 802.1Q Port Settings

To configure an 802.1Q VLAN, highlight **Configure 802.1Q Port Settings** on the VLAN Menu and press Enter:

```

Configure 802.1Q Port Settings
-----
Ext Port: 1 2 3 4
PVID : 1 1 1 1
Priority: 0 0 0 0
Ingress : DIS DIS DIS DIS
GURP : DIS DIS DIS DIS

Int Port: 1 2 3 4 5 6 7 8 9 10 11 12 13 14
PVID : 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Priority: 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Ingress : DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS
GURP : DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS DIS

Port <Internal> Priority [1]
Configure Port [1 ] to [1 ] Ingress Filter <Disabled>
PVID [1 ] GURP <Disabled>
APPLY

Function: Select the internal ports or external ports to configure.
Message:
CTRL+I = Main Menu Esc = Prev. Screen CTRL+R = Refresh

```

To assign a port a Port VLAN Identifier (PVID), select the desired module and port(s) in the first two fields, and enter the PVID for the VLAN member ports that you want to configure in the third field.

PVID is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the **Edit 802.1Q VLANs** window shown in “Edit 802.1Q VLANs” on page 107.

To set the priority of a port, select the desired module and port(s) in the first two fields and then enter the desired priority value in the **Priority** field.

To set an Ingress Filter, select the desired module and port(s) in the first two fields and then use the Spacebar to toggle between **Enabled** and **Disabled** in the **Ingress Filter** field.

An Ingress Filter enables the port to compare the VID tag of an incoming packet with the both the VIDs and PVIDs of VLANs assigned to the port. If the VID tag of an incoming port is different from either the VID or PVID assigned to the port, the port filters (drops) the packet.

You can enable a port to dynamically become a member of a VLAN, enable or disable GARP VLAN Registration Protocol (GVRP), where GARP is the Generic Attribute Registration Protocol, on an individual port. To set GVRP, complete the following steps:

1. Enter the module and range of ports to be configured in the first two fields and then toggle the GVRP State to **Enabled**.
2. Press **APPLY** to make your changes effective.

GVRP is a GARP application that provides 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports. GVRP updates dynamic VLAN registration entries and communicates the new VLAN information across the network. This enables, among other things, stations to physically move to other switch ports and keep their same VLAN settings, without having to reconfigure VLAN settings on the switch.

Link Aggregation

The switch module supports Link Aggregation, or port trunking. Port trunks (aggregated ports) can be used to increase the bandwidth of a network connection or to ensure fault recovery.

You can configure up to two trunk connections (combining two to four ports into one fat pipe) between any two BladeCenter switches or other Layer 2 switches. However, before making any physical connections between devices, use the Link Aggregation menus to specify the ports that will belong to the trunking group on both switches.

When using a port trunk, note that:

- The ports used in a trunk must all be of the same speed (100 Mbps or 1000 Mbps) and operate in full-duplex mode only.
- The ports that can be assigned to the same trunk have certain other restrictions, as described in this section.
- Each port can only be assigned to one trunk group, whether a static or dynamic group.
- The ports at both ends of a connection must be configured as trunk ports.
- All of the ports in a trunk have to be treated as a whole when moved from/to, added, or deleted from a VLAN.
- The Spanning Tree Protocol (STP) will treat all the ports in a trunk as a whole.
- Enable the trunk before connecting any cable between the switches to avoid creating a data loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a data loop.

Trunking can be set as a static port/group using the Port Trunking window or as a dynamic port/group using the IEEE 802.3ad Link Aggregation window.

To configure a port trunking group, highlight **Link Aggregation** on the main menu and press Enter.

```
Link Aggregation
-----
Distribution Method
Non-IP Packet <Src Mac >
IP Packet <Src Mac >

Port Trunking IEEE 802.3ad Link Aggregation Apply
-----
Function: Select distribution method for non-ip packet.
Message:
CTRL+I = Main Menu Esc = Prev. Screen CTRL+R = Refresh
```

Link aggregation, or port trunking, enables several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single-link bandwidth.

Port trunking is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The switch module offers link aggregation on four external ports for up to two static trunk groups or two LACP 802.3ad link aggregation groups. The trunked ports can be non-continuous (that is, have non-sequential port numbers). All of the ports in the group must be members of the same VLAN. In addition, the trunked ports must all have the same speed and be configured as full duplex.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the port trunking group. This port is called the Master Port of the group, and all configuration options, including the VLAN configuration, that can be applied to the Master Port are applied to the entire port trunking group.

Load balancing is automatically applied to the ports in the trunked group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The STP will treat a port trunking group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the port trunking group. If two redundant port trunking groups are configured on the switch, STP will block one entire group, in the same way that STP will block a single port that has a redundant link.

Use the Link Aggregation menu to set the distribution method for both IP packets and non-IP packets and then click **APPLY** to make your change effective.

The information on the preceding window includes:

Distribution Method

The switch module permits different load sharing methods when ports are trunked together. In some environments, a different method can improve

balancing the packet traffic between trunked ports. Generally, you should select the method that can best differentiate packets that go through your trunked ports. If you do not know which method will be the best for your environment, use the trial-and-error approach, checking the network monitoring windows to see which method will yield the best results in terms of efficiency. The selected method is used as a hashing function to determine which packets will go to which port.

Non-IP Packet <Src Mac>

For non-IP packets, the available methods are: **Src Mac**, **Dest Mac**, or **Src & Dest Mac**.

IP Packet <Src Mac>

For IP packets, the available methods are: **Src Mac**, **Dest Mac**, **Src & Dest Mac**, **Src IP**, **Dest IP**, or **Src & Dest IP**.

Port Trunking

To set up a static port trunking group, select **Port Trunking** on the Link Aggregation menu:

```

Port Trunking
-----
Group ID  Master  1  4
  1      -      -  -
  2      -      -  -

Group ID      [ ]
External Port  1  4
Member Port   [---]
Method        <Disabled>

APPLY

Function: Enter Trunking Group ID.
Message:
Esc=Previous Screen  CTRL+R=Refresh  CTRL+N=Next Page  CTRL+P=Previous Page
  
```

Enter a Group ID in the first field, use the Spacebar to toggle the **Member Port** field to M for each port that will be part of the trunking group, and select **TRUNK** in the **Method** field to enable this feature. After you click **APPLY**, the new port trunking group will be displayed in the table in the lower portion of the preceding window.

The user-changeable parameters on this window are as follows:

Group ID

The switch module enables up to two port trunk groups to be configured. The group number identifies each of these groups.

Member Port

Toggle between **M** to indicate membership of the port trunking group, or a dash (-) to indicate non-membership.

Method <Disabled>

This field can be toggled between **TRUNK** and **Disabled**. This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.

IEEE 802.3ad Link Aggregation

Use the IEEE 802.3ad Link Aggregation menu to set up dynamic port trunking.

To enable Link Aggregation Control Protocol and set the System Priority, value select **Setup IEEE 802.3ad Link Aggregation** on the Link Aggregation menu:

```

IEEE 802.3ad Link Aggregation
-----
LACP      <Disabled>
System Priority [32768]

Link Aggregation Port Setting      Apply

Function: Enable/Disable LACP
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

The user-changeable parameters on this window are as follows:

LACP This parameter enables Link Aggregation to be **Enabled** or **Disabled**. Disabling LACP when it is not in use can eliminate some traffic on the network. Enabling Link Aggregation creates an active LACP switch module.

System Priority

An admin ID can be assigned to the switch module to differentiate other LACP switches running on the network.

To set up dynamic port trunking on individual ports, select **Link Aggregation Port Setting** on the IEEE 802.3ad Link Aggregation menu:

```

Link Aggregation Port Setting
-----
Port      Priority  Admin. Key  Oper Key  Mode      Status
Ext1      128          15          15        Disabled  Individual
Ext2      128          16          16        Disabled  Individual
Ext3      128          17          17        Disabled  Individual
Ext4      128          18          18        Disabled  Individual

Configure external port [1 ] to [1 ]
Priority                [1 ]
Administrator Key      [1 ]
Mode                    <Enabled >

APPLY

Function: Input port number.
Message:
CTRL+I = Main Menu      Esc = Prev. Screen      CTRL+R = Refresh

```

Select the range of ports to be configured in the first field, assign a Priority in the second field, enter the Admin. Key in the next field, and select **Enabled** in the **Mode** field to enable this feature. After you click **APPLY**, the new port settings will be displayed in the table in the lower portion of the preceding window.

The information on the preceding window includes:

Configure external port [1] to [1]

Enter the ports that will form the external port trunking group in this field.

Priority [1]

Lower port priority means a higher priority over other enabled link aggregation ports in the group.

Administrator Key [1]

This is the administrative key to control the way that links are aggregated. In order to aggregate ports together, the ports must have an equal Administrator Key.

Mode <Enabled>

A port or ports can be enabled to permit them to join or create a link aggregation group.

Oper Key

This displays the operational key used by the port to communicate with other LACP switches.

Status

This displays the current status of a link aggregation port.

Appendix A. RJ-45 pin specifications

When you connect the switch to another switch, a bridge, or a hub, a normal cable is necessary. Review the documentation that comes with these products for matching cable pin assignments.

The following illustration and table show the standard RJ-45 receptacle/connector and their corresponding pin assignments for the switch-to-network adapter connection, and the normal cable for the switch-to-switch/hub/bridge connection.

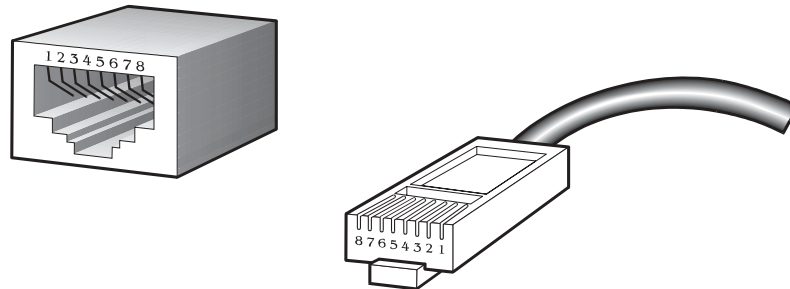


Table 6. Standard Category 3 cable, RJ-45 pin assignment

RJ-45 Connector pin assignment	
Contact (pin number)	Media direct interface signal
1	Tx + (transmit)
2	Tx - (transmit)
3	Rx + (receive)
4	Not used
5	Not used
6	Rx - (receive)
7	Not used
8	Not used

The four external Ethernet ports of this switch module are auto-configuring and do not require straight-through or crossover cables.

Appendix B. Run-time switching software default settings

Table 7 contains the default settings for the run-time switching software variables.

Table 7. Default settings for run-time switching software variables

Variable	Default value
Load mode	Ethernet
Configuration update	Disable
Firmware update	Disable
Out-of-band baud rate	9600
IP address	192.168.70.1xx, where xx depends on the number of the bay into which you have installed the switch module, as shown in Table 1 on page 19
Subnet mask	255.0.0.0
Default gateway	0.0.0.0
BOOTP service	Disable
TFTP server IP address	0.0.0.0
Auto log-out	10 min
User name	None
Password	None
MAC address aging time	300 secs
IGMP snooping	Disable
Switch GVRP	Disable
Telnet status	Enable
Web status	Enable
Device STP	Disable
Port STP	Enable
Port enable	Enable
Scheduling mechanism for COS queues	Strict
Trunk load sharing algorithm	Src address
Bridge max age	20 secs
Bridge hello time	2 secs
Bridge forward delay	15 secs
Bridge priority	32768
Port STP cost	100
Port STP priority	128
NWay	Enable
Flow control	Enable
Community string	"public", "private"
VLAN mode	IEEE 802.1Q
Default port VID	1
Ingress rule checking	Disable

Appendix C. Cable lengths

Use the following table as a guide for the maximum cable lengths:

Table 8. Maximum cable lengths

Standard	Data Transmission Rate	Media type	Maximum distance
1000BASE-T	1000 Mbps	Category 5e UTP cable Category 5 UTP cable	100 meters (328.1 ft)
100BASE-TX	100 Mbps	Category 5 UTP cable	100 meters (328.1 ft)
10BASE-T	10 Mbps	Category 3 UTP cable	100 meters (328.1 ft)

Appendix D. Understanding and troubleshooting the Spanning Tree Protocol

This appendix provide details about how the STP works and describes how to troubleshoot it.

STP operation levels

STP calculates the bridge identifier (ID) for each switch and then sets the root bridge and the designated bridges.

The following table shows the user-configurable STP parameters for the switch level.

Table 9. STP parameters -- switch level

Parameter	Description	Default value
Bridge identifier (Not user-configurable except by setting the priority as described in this table)	A combination of the user-set priority and the switch MAC address. The bridge identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address.	32768 + MAC
Priority	A relative priority for each switch. Lower numbers assign a higher priority and increase the probability of a switch being elected as the root bridge	32768
Hello time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum age timer	Measures the age of a received bridge protocol data unit (BPDU) for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer	20 seconds
Forward delay timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that might return the port to the blocking state	15 seconds

The following table shows the user-configurable STP port parameters for the switch level.

Table 10. STP port parameters -- switch level

Variable	Description	Default value
Port priority	A relative priority for each port. Lower numbers give a higher priority and a greater chance of a given port being elected as the root port.	32768
Port cost	A value used by STP to evaluate paths	19

Bridge protocol data units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using bridge protocol data units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently recognizes as the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which a packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches through BPDUs causes the following results:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a stable topology

If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For example, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

STP port states

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes in which a port that changed directly from a blocking state to a forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to enable the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must go through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists in one of the following five states:

Blocking

The port is blocked from forwarding or receiving packets. For additional information, see “Blocking state” on page 127.

Listening

The port is waiting to receive BPDU packets that might tell the port to go back to the blocking state. For additional information, see “Listening state” on page 128.

Learning

The port is adding addresses to its forwarding database but not yet forwarding packets. For additional information, see “Learning state” on page 129.

Forwarding

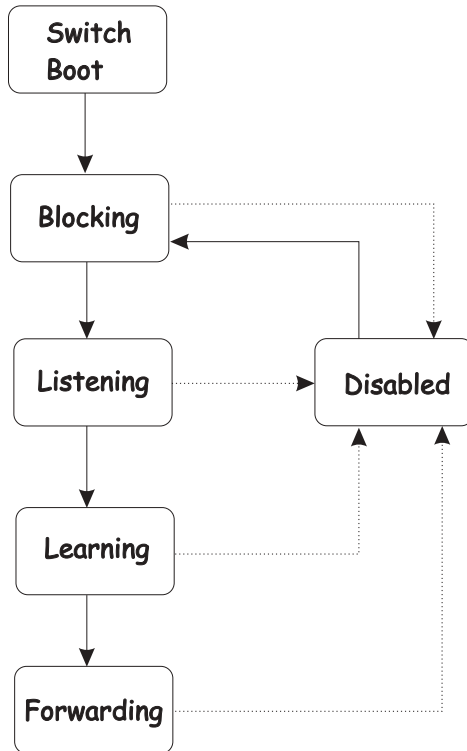
The port is forwarding packets. For additional information, see “Forwarding state” on page 130.

Disabled

The port responds only to network management messages and must return to the blocking state first. For additional information, see “Disabled state” on page 132.

A port changes from one state to another as follows:

- From initialization (switch startup) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking



When you enable STP, every port on every switch in the network goes through the blocking state and then goes through the states of listening and learning at startup. If properly configured, each port stabilizes to the forwarding or blocking state.

No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

Table 11 shows the default spanning-tree configuration.

Table 11. Default STP parameters

Feature	Default Value
Enable state	STP enabled for all ports
Port priority	128
Port cost	19
Bridge priority	32768

Setting user-changeable STP parameters

The factory default settings are compatible with the majority of installations. However, it is advisable to keep the default settings as set at the factory, unless it is absolutely necessary to change them. The user-changeable parameters in the switch are as follows:

Priority

You can set a priority for the switch from 0 to 65535. A value of 0 indicates the highest priority.

Hello Time

The hello time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge. If you set a hello time for your

switch, and it is not the root bridge, the set hello time will be used if and when your switch becomes the root bridge.

Note: The hello time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age

The Max. Age can be from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the root bridge, your switch will start sending its own BPDU to all other switches for permission to become the root bridge. If your switch has the lowest bridge identifier, it will become the root bridge.

Forward Delay

The Forward Delay can be from 4 to 30 seconds. This is the time that any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

Note: Observe the following formulas when setting the previously described parameters:

- $\text{Max. Age} \leq 2 \times (\text{Forward Delay} - 1 \text{ second})$
- $\text{Max. Age} \geq 2 \times (\text{Hello Time} + 1 \text{ second})$

Port Priority

You can set a port priority from 0 to 255. The lower the number, the greater the probability that the port will be chosen as the root port.

Port Cost

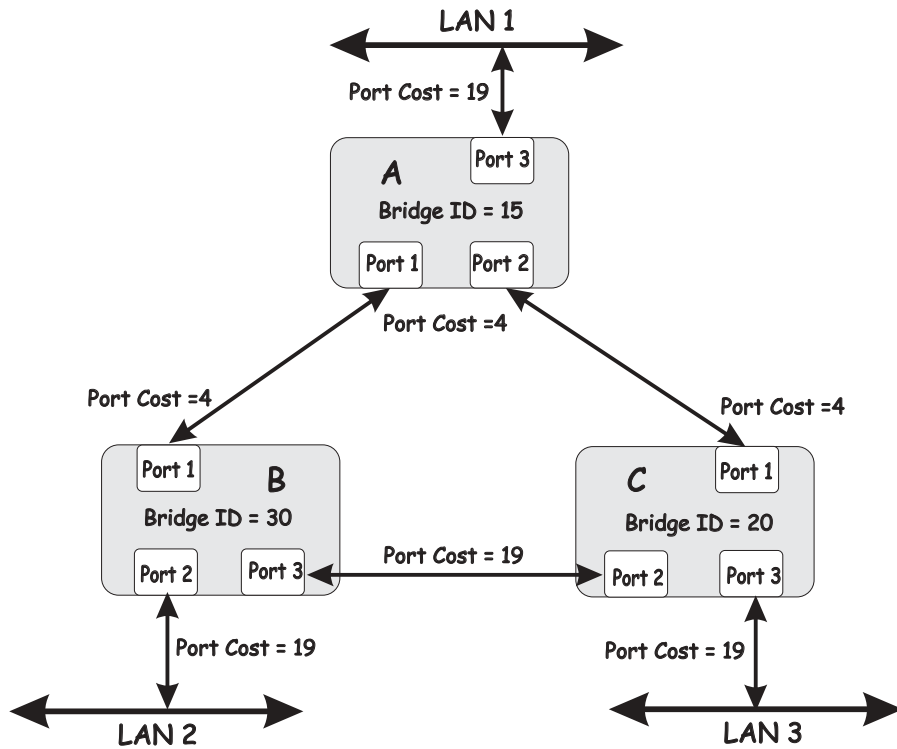
You can set a port cost from 1 to 65535. The lower the number, the greater the probability that the port will be chosen to forward packets.

Illustration of STP

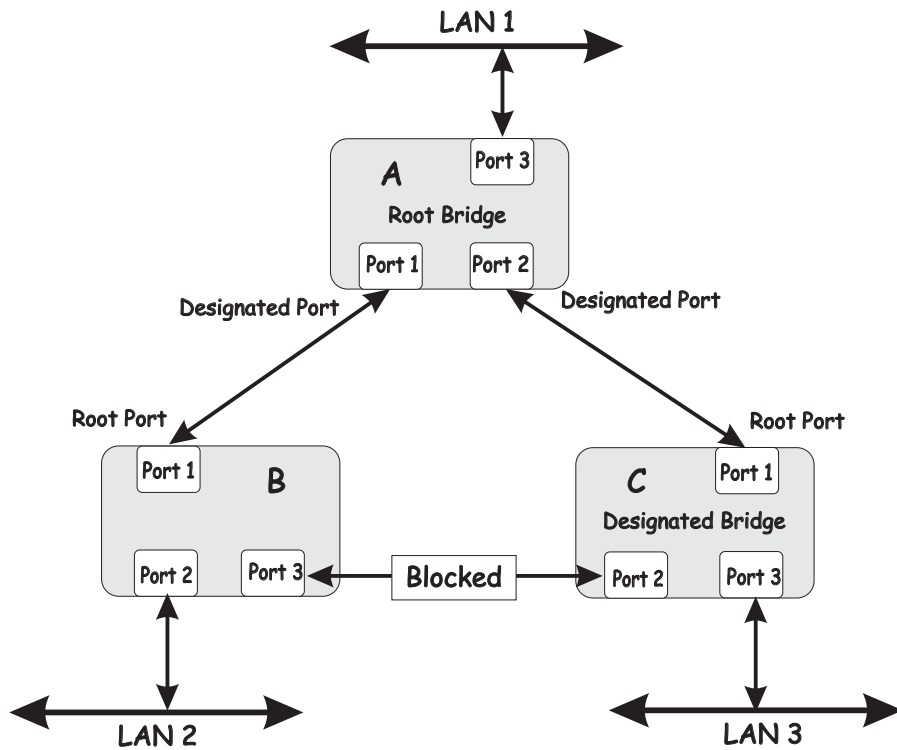
A simple illustration of three bridges (or three switches) connected in a loop is depicted in this section. In this example, you can anticipate some major network problems if the STP assistance is not applied. If bridge A broadcasts a packet to bridge B, bridge B will broadcast it to bridge C, and bridge C will broadcast it to back to bridge A, and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure.

STP can be applied as shown in the following illustration. In this example, STP breaks the loop by blocking the connection between bridges B and C. The decision to block a particular connection is based on the STP calculation of the most current bridge and port settings. If bridge A broadcasts a packet to bridge C, bridge C will drop the packet at port 2, and the broadcast will end there.

Setting up STP using values other than the defaults can be complex. Therefore, keep the default factory settings, and STP will automatically assign root bridges, ports, and block loop connections. However, influencing STP to choose a particular switch as the root bridge using the **Priority** setting, or influencing STP to choose a particular port to block using the **Port Priority** and **Port Cost** settings is relatively straightforward.



Note: In this example, only the default STP values are used.



The switch with the lowest bridge ID (switch A) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C.

Note also that the example network topology is intended to provide redundancy to protect the network against a link or port failure, not a switch failure or removal. For example, a failure of switch A would isolate LAN 1 from connecting to LAN 2 or LAN 3.

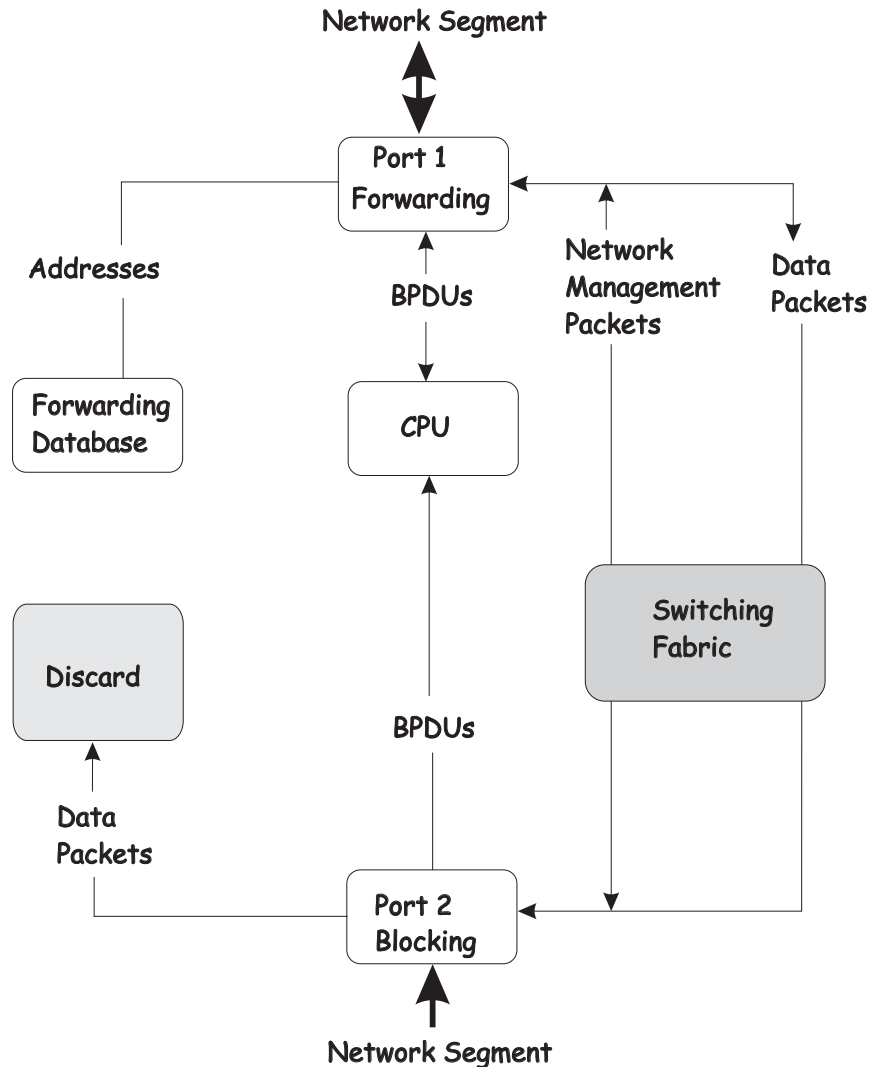
Blocking state

A port in the blocking state does not forward packets. When the switch is started, a BPDU is sent to each port in the switch putting these ports into the blocking state. A switch initially assumes it is the root, and then begins the exchange of BPDUs with other switches. This will determine which switch in the network is the best choice for the root switch. If there is only one switch on the network, no BPDU exchange occurs, the forward delay timer expires, and the ports move to the listening state. All STP enabled ports enter the blocking state following the switch startup.

A port in the blocking state does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database
- Receives BPDUs and directs them to the central processing unit (CPU).
- Does not transmit BPDUs received from the CPU.
- Receives and responds to network management messages.

The following illustration shows the actions that occur when a port is in the blocking state.



Listening state

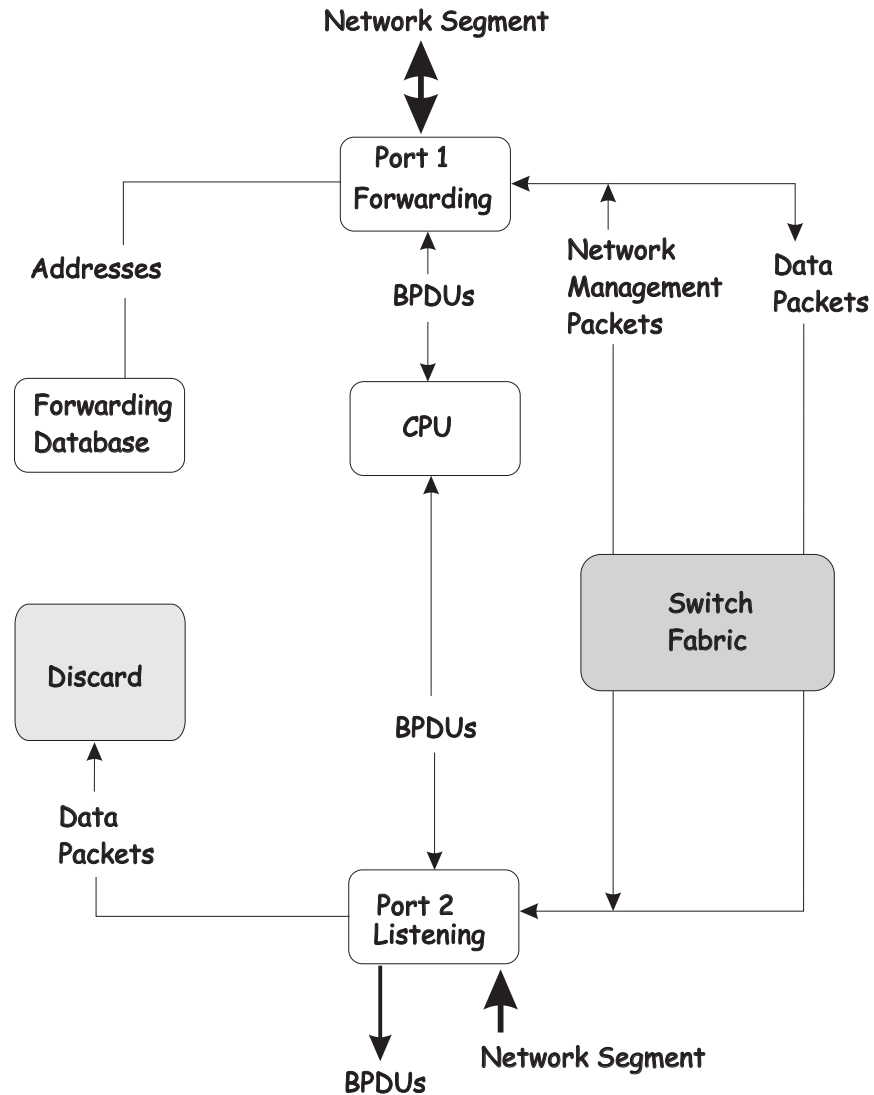
The listening state is the first change for a port from the blocking state. Listening is an opportunity for the switch to receive BPDUs that might tell the switch that the port should not continue to change to the forwarding state, but should return to the blocking state (that is, a different port is a better choice).

There is no address learning or packet forwarding from a port in the listening state.

A port in the listening state does the following:

- Discards frames received from the network segment to which it is attached
- Discards packets sent from another port on the switch for forwarding
- Does not add addresses to its forwarding database
- Receives BPDUs and directs them to the CPU
- Processes BPDUs received from the CPU
- Receives and responds to network management messages

The following illustration shows the actions that occur when a port is in the listening state.



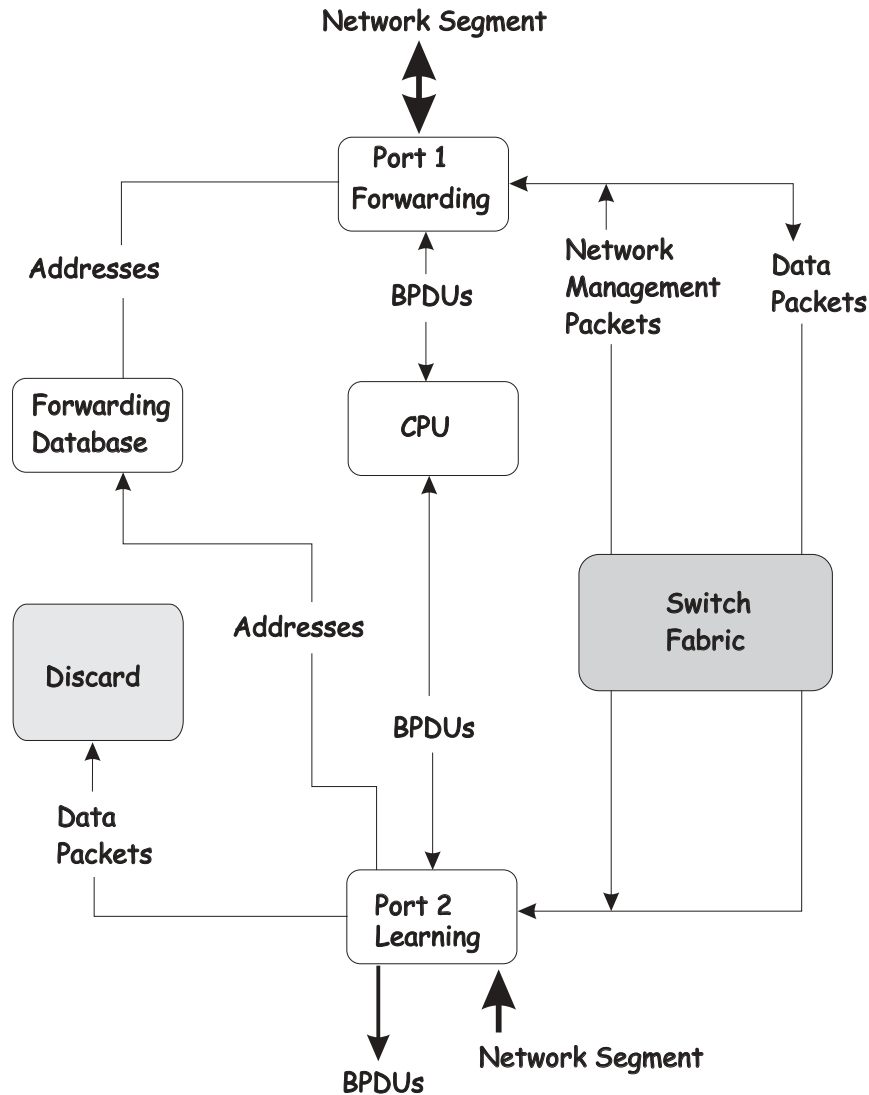
Learning state

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state.

A port in the learning state does the following:

- Discards frames received from the network segment to which it is attached
- Discards packets sent from another port on the switch for forwarding
- Adds addresses to its forwarding database
- Receives BPDUs and directs them to the CPU
- Processes and transmits BPDUs received from the CPU
- Receives and responds to network management messages

The following illustration shows the actions that occur when a port is in the learning state.



Forwarding state

A port in the forwarding state forwards packets. The port enters the forwarding state from the learning state when the forward delay timer expires.

When the spanning-tree algorithm determines that a port should be changed to the forwarding state, the following occurs:

The port is put into the listening state, where it receives bridge protocol data units (BPDUs) and passes them to the switch CPU. BPDUs from the CPU are processed. If no BPDUs are received, this indicates that the port should go to the blocking state:

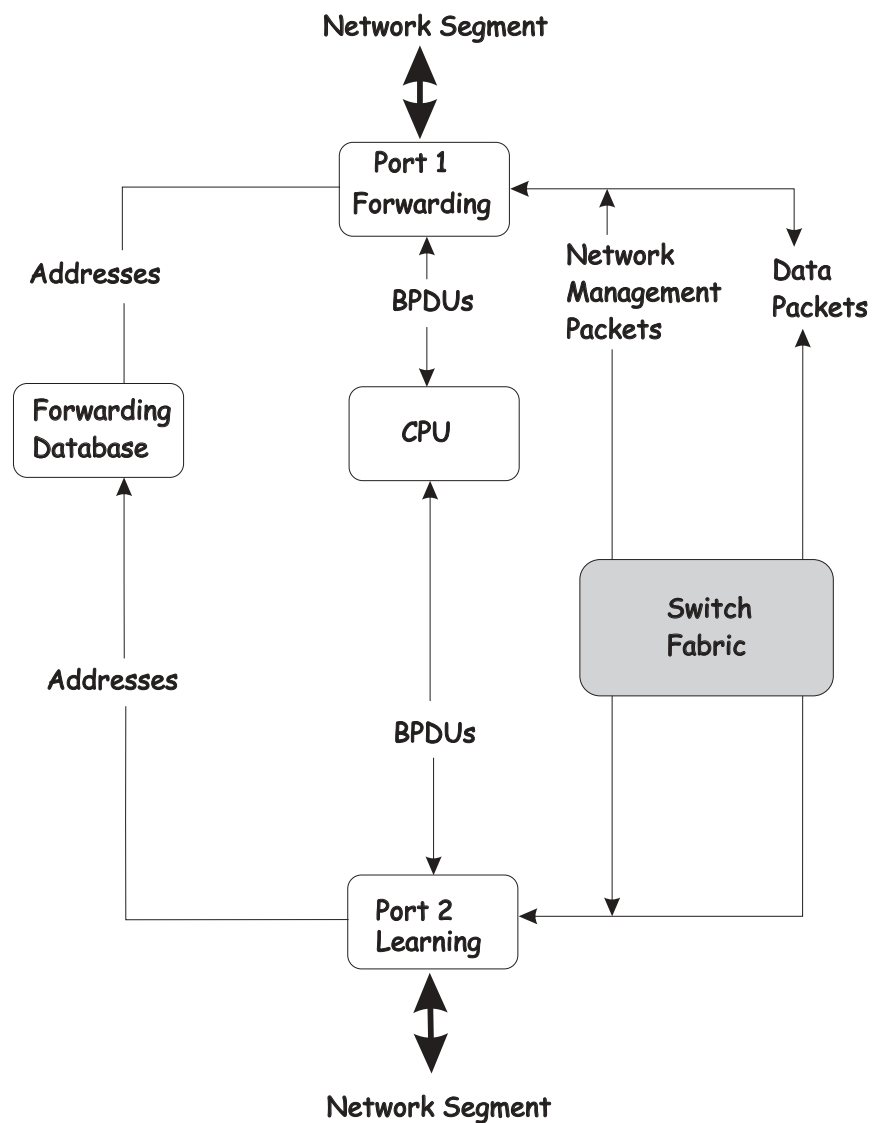
- The port waits for the expiration of the forward delay timer. It then moves to the learning state.
- In the learning state, the port learns station location information from the source address of packets and adds this information to its forwarding database.

- The expiration of the forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, packets are forwarded by the port.

A port in the forwarding state does the following:

- Forwards packets received from the network segment to which it is attached.
- Forwards packets sent from another port on the switch for forwarding.
- Incorporates station location information into its address database.
- Receives BPDUs and directs them to the system CPU.
- Receives and responds to network management messages.

The following illustration shows the actions that occur when a port is in the forwarding state.



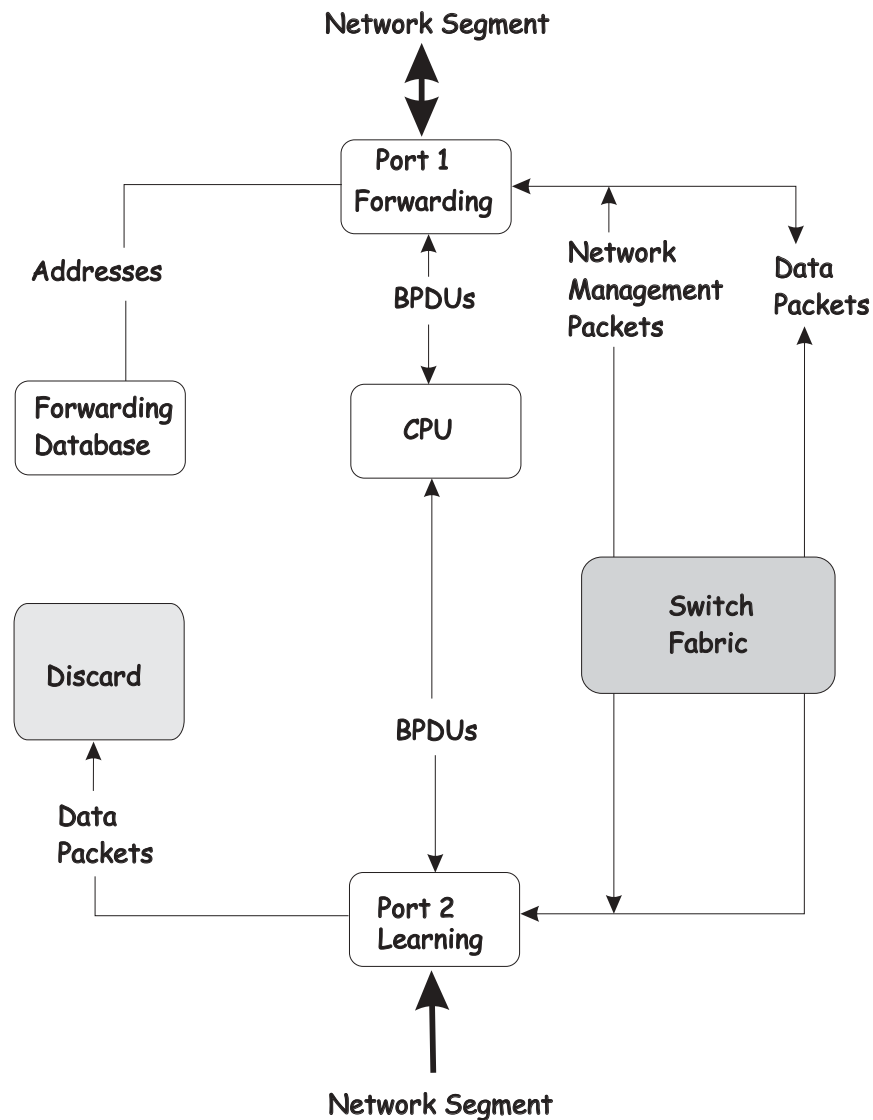
Disabled state

A port in the disabled state does not participate in frame forwarding or STP. A port in the disabled state is virtually non-operational.

A disabled port does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.
- Does not receive BPDUs for transmission from the system CPU.
- Receives and responds to network management messages.

The following illustration shows the actions that occur when a port is in the disabled state.

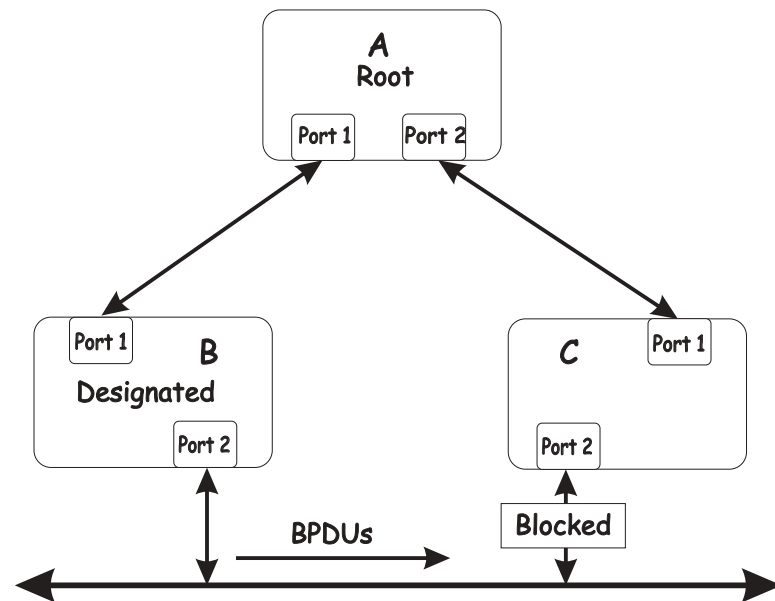


Troubleshooting STP

This section describes how to troubleshoot the STP.

Spanning Tree Protocol Failure

A failure in the STA generally leads to a bridging loop. A bridging loop in an STP environment comes from a port that should be in the blocking state, but is forwarding packets.



In this example, B has been elected as the designated bridge and port 2 on bridge C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between bridges B and C. Bridge B had a better BPDU than bridge C. Bridge B continues sending BPDUs that advertise its superiority over the other bridges on this LAN. If bridge C fails to receive these BPDUs for longer than the Max. Age (default of 20 seconds), it could start to change its port 2 from the blocking state to the forwarding state.

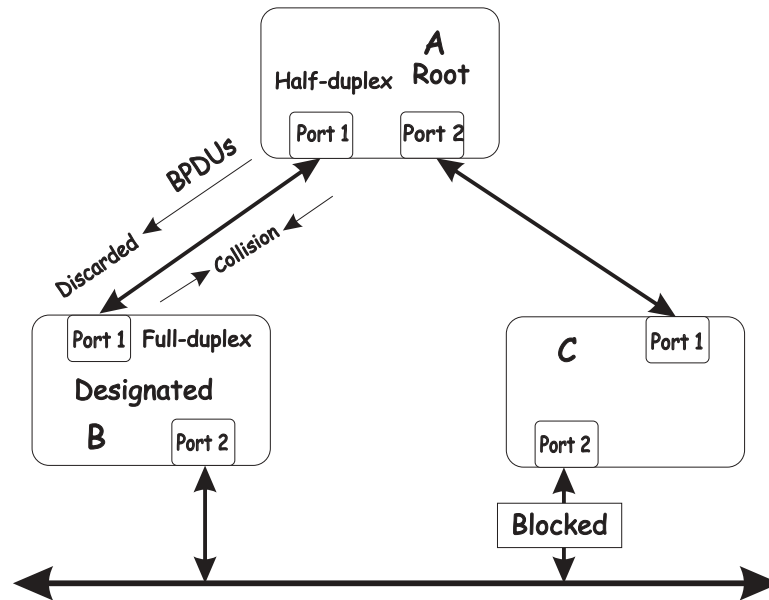
Note: To remain in the blocking state, a port must continue to receive BPDUs that advertise superior paths.

There are several circumstances in which the STA can fail, mostly related to the loss of a large number of BPDUs. These situations will cause a port in the blocking state to change to the forwarding state.

Full/half duplex mismatch

A mismatch in the duplex state of two ports is a very common configuration error for a point-to-point link. If one port is configured as a full duplex, and the other port is left in auto-negotiation mode, the second port will end up in half-duplex because

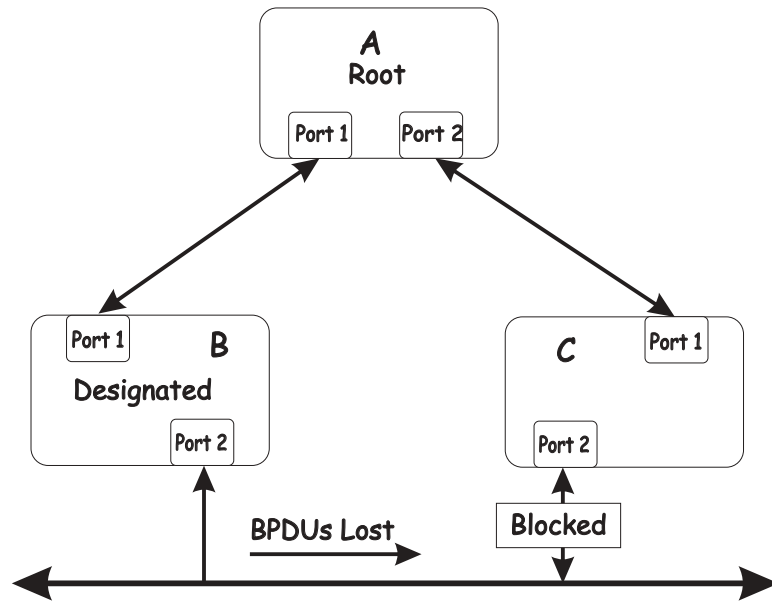
ports configured as half- or full-duplex do not negotiate.



In the preceding example, port 1 on bridge B is configured as a full-duplex port and port 1 on bridge A is either configured as a half-duplex port, or left in auto-negotiation mode. Because port 1 on bridge B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. Bridge B will then start sending packets even if bridge A is using the link. A will then detect collisions and begin to run the flow control algorithm. If there is enough traffic between bridges B and A, all packets (including BPDUs) will be dropped. If the BPDUs sent from bridge A to bridge B are dropped for longer than the Max. Age, bridge B will lose its connection to the root (bridge A) and will unblock its connection to bridge C. This will create a data loop.

Unidirectional link

Unidirectional links can be caused by an undetected failure in one side of a fiber cable, or a problem with a ports transceiver. Any failure that enables a link to remain up while providing one-way communication is very dangerous for STP.



In this example, port 2 on bridge B can receive but not transmit packets. Port 2 on bridge C should be in the blocking state, but since it can no longer receive BPDUs from port 2 on bridge B, it will change to the forwarding state. If the failure exists at boot, STP will not converge and restarting the bridges will have no effect.

Note: In the previous example, restarting the bridges will provide a temporary resolution.

This type of failure is difficult to detect because the Link-state LEDs for Ethernet links rely on the transmit side of the cable to detect a link. If a unidirectional failure on a link is suspected, it is usually required to go to the console or other management software and look at the packets received and transmitted for the port. For example, a unidirectional port will have many packets transmitted but none received, or vice versa.

Packet corruption

Packet corruption can lead to the same type of failure. If a link is experiencing a high rate of physical errors, a large number of consecutive BPDUs can be dropped and a port in the blocking state would change to the forwarding state. The blocking port would have to have the BPDUs dropped for 50 seconds (at the default settings) and a single BPDU would reset the timer. If the Max. Age is set too low, this time is reduced.

Resource errors

The switch performs its switching and routing functions primarily in hardware, using specialized application specific integrated circuits (ASICs). STP is implemented in software and is thus reliant upon the speed of the CPU and other factors to converge. If the CPU is over-utilized, it is possible that BPDUs might not be sent in a timely fashion. STP is generally not very CPU intensive and is given priority over other processes, so this type of error is rare.

It can be seen that very low values for the Max. Age and the Forward Delay can result in an unstable spanning tree. The loss of BPDUs can lead to data loops. The diameter of the network can also cause problems. The default values for STP give a maximum network diameter of about seven. This means that two switches in the

network cannot be more than seven hops apart. Part of this diameter restriction is the BPDU age field. As BPDUs are propagated from the root bridge to the leaves of the spanning tree, each bridge increments the age field. When this field is beyond the maximum age, the packet is discarded. For large diameter networks, STP convergence can be very slow.

Identifying a data loop

Broadcast storms have a very similar effect on the network to data loops, but broadcast storm controls in modern switches have (along with subnetting and other network practices) have been very effective in controlling broadcast storms. The best way to determine if a data loop exists is to capture traffic on a saturated link and check if similar packets are seen multiple times.

Generally, if all the users of a given domain are unable to connect to the network at the same time, a data loop is the cause. In this case, the port-utilization data in the switch Telnet windows will give unusually high values.

The priority for most cases is to restore connectivity as soon as possible. The simplest remedy is to manually disable all of the ports that provide redundant links. Disabling the ports one at a time, and then checking for the restoration of a user's connectivity will identify the link that is causing the problem, if sufficient time is available. Connectivity will be restored immediately after disabling a data loop.

Avoiding network problems

To help your network operate more efficiently, you can avoid or minimize network problems, as described in this section.

- Know where the root is located.

Although the STP can elect a root bridge, a well-designed network has an identifiable root for each VLAN. Careful setup of the STP parameters results in the selection of this best switch as the root for each VLAN. Redundant links can then be built into the network. STP is well-suited to maintaining connectivity in the event of a device failure or removal, but is poorly suited to designing networks.

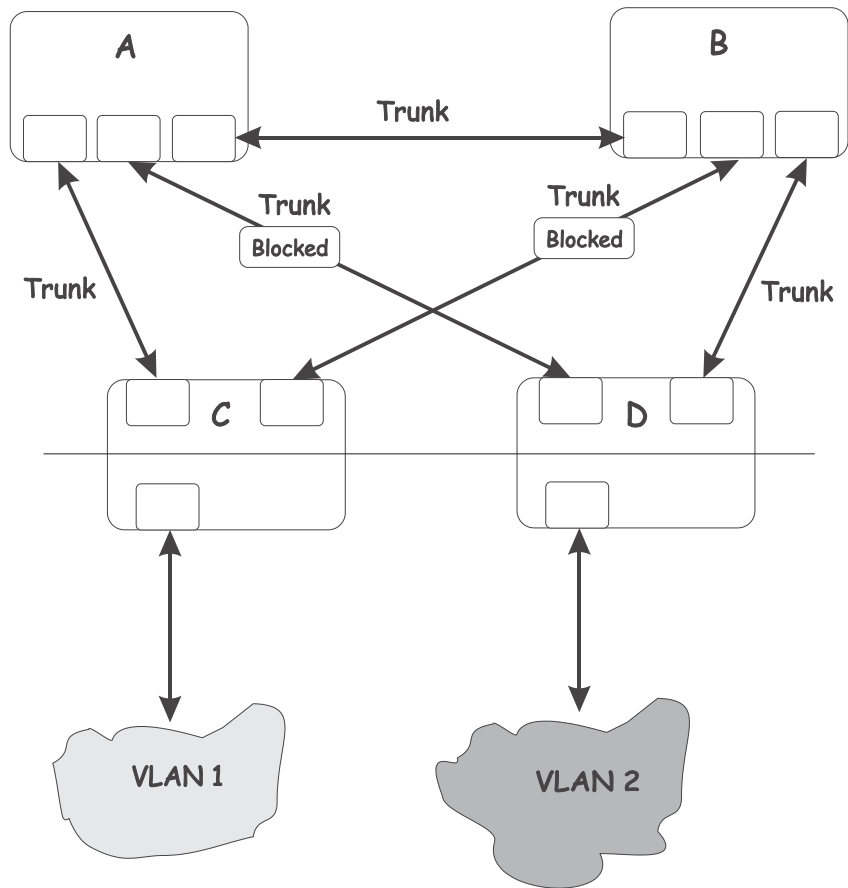
- Know which links are redundant.

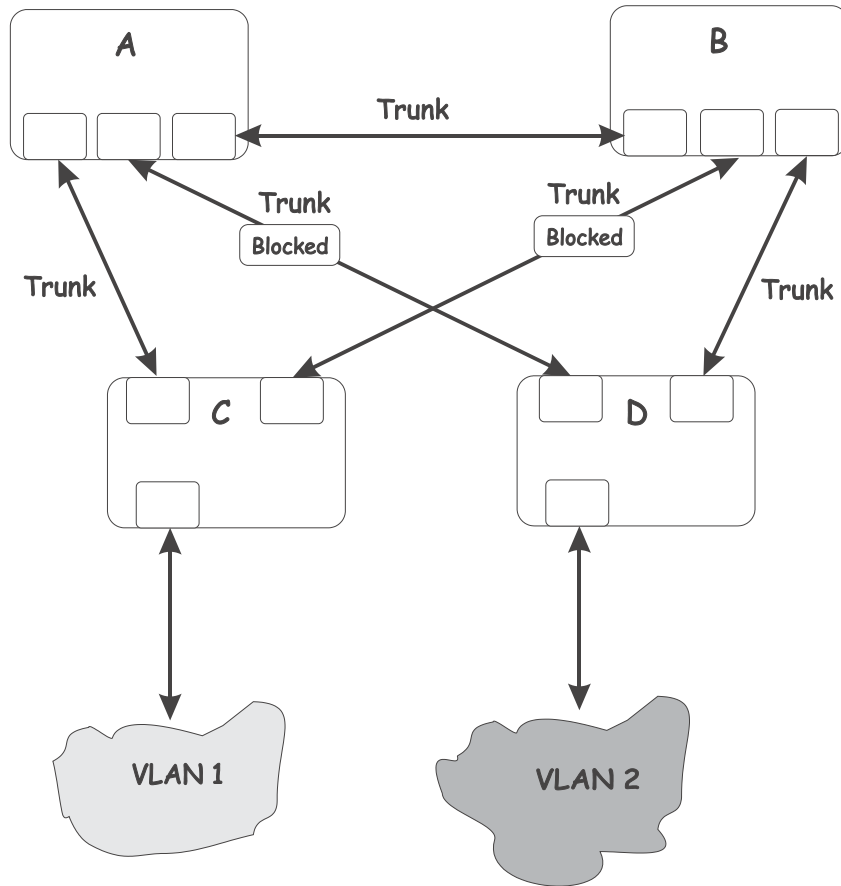
Organize the redundant links and tune the port cost parameter of STP to force those ports into the blocking state.

For each VLAN, know which ports should be blocking in a stable network. A network illustration that shows each physical loop in the network and which ports break which loops is extremely helpful.

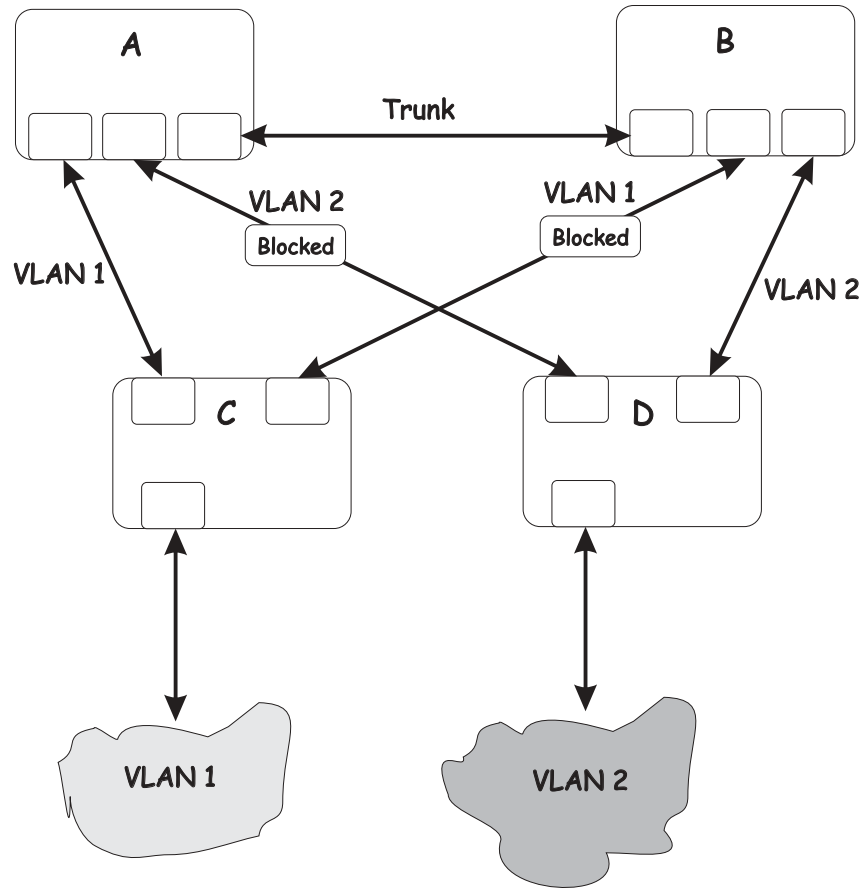
- Minimize the number of ports in the blocking state.

A single blocking port changing to the forwarding state at an inappropriate time can cause a large part of a network to fail. Limiting the number of blocked ports helps to limit the risk of an inappropriate change.





This is a common network design. Through trunks, switches C and D have redundant links to backbone switches A and B. Trunks, by default, carry all the VLAN traffic from VLAN 1 and VLAN 2. Therefore, switch C is not only receiving traffic for VLAN 1, but switch C is also receiving unnecessary broadcast and multicast traffic for VLAN 2. Switch C is also blocking one port for VLAN 2. Thus, there are three redundant paths between switches A and B and two blocked ports per VLAN. This increases the chance of a data loop.



In this example, the VLAN definitions are extended to switches A and B. This gives only a single blocked port per VLAN and enables the removal of all redundant links by removing switch A or B from the network.

Appendix E. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you. This chapter contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your xSeries or IntelliStation® system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system is turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system.
- Go to the IBM Support Web site at <http://www.ibm.com/pc/support/> to check for technical information, hints, tips, and new device drivers.
- Use an IBM discussion forum on the IBM Web site to ask questions.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the publications that are provided with your system and software. The information that comes with your system also describes the diagnostic tests that you can perform. Most xSeries and IntelliStation systems, operating systems, and programs come with information that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the information for the operating system or program.

Using the documentation

Information about your IBM xSeries or IntelliStation system and preinstalled software, if any, is available in the documentation that comes with your system. That documentation includes printed books, online books, README files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to <http://www.ibm.com/pc/support/> and follow the instructions. Also, you can order publications through the IBM Publications Ordering System at <http://www.elink.ibm.com/public/applications/publications/cgibin/pbi.cgi>.

Getting help and information from the World Wide Web

On the World Wide Web, the IBM Web site has up-to-date information about IBM xSeries and IntelliStation products, services, and support. The address for IBM xSeries information is <http://www.ibm.com/eserver/xseries/>. The address for IBM IntelliStation information is <http://www.ibm.com/pc/intellistation/>.

You can find service information for your IBM products, including supported options, at <http://www.ibm.com/pc/support/>. If you click **Profile** from the support page, you can create a customized support page. The support page has many sources of information and ways for you to solve problems, including:

- Diagnosing problems, using the IBM Online Assistant
- Downloading the latest device drivers and updates for your products
- Viewing Frequently Asked Questions (FAQ)
- Viewing hints and tips to help you solve problems
- Participating in IBM discussion forums
- Setting up e-mail notification of technical updates about your products

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with xSeries servers, IntelliStation workstations, and appliances. For information about which products are supported by Support Line in your country or region, go to <http://www.ibm.com/services/sl/products/>.

For more information about Support Line and other IBM services, go to <http://www.ibm.com/services/>, or go to <http://www.ibm.com/planetwide/> for support telephone numbers.

Hardware service and support

You can receive hardware service through IBM Integrated Technology Services or through your IBM reseller, if your reseller is authorized by IBM to provide warranty service. Go to <http://www.ibm.com/planetwide/> for support telephone numbers.

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

Appendix F. Warranty information

This section contains information about your warranty period and the service and support that are provided by your warranty.

Warranty period

The warranty period varies by machine type and country or region.

Contact your place of purchase for warranty service information. Some IBM Machines are eligible for on-site warranty service depending on the country or region where service is performed.

Prior to on-site warranty service, you are required to go through problem determination with an IBM service specialist call center technician.

This paragraph applies only to products with a warranty period of 3 years on parts and 1 year on labor. A warranty period of 3 years on parts and 1 year on labor means that IBM will provide warranty service without charge for:

1. parts and labor during the first year of the warranty period
2. parts only, on an exchange basis, in the second and third years of the warranty period. IBM will charge you for any labor it provides in performance of the repair or replacement.

The IBM Machine Warranties Web site at http://www.ibm.com/servers/support/machine_warranties/ contains a worldwide overview of the IBM Statement of Limited Warranty for IBM Machines, a glossary of terms used in the Statement of Limited Warranty, Frequently Asked Questions (FAQ), and links to Product Support Web pages. The IBM Statement of Limited Warranty is available from this Web site in 29 languages in Portable Document Format (PDF).

Machine - IBM BladeCenter 4-Port Gb Ethernet Switch Module

Country or region	Warranty period	Service delivery method
Worldwide	3 years	On-site

Problem determination

Prior to on-site warranty service, you are required to go through problem determination with an IBM service specialist call center technician. The service specialist will run diagnostic tests on the hardware and check the software.

Running diagnostics

The IBM service specialist will help you determine whether your equipment is functioning as specified. It might be necessary to isolate the failing xSeries, Netfinity®, or IntelliStation system; IBM component; or both from any active production environment to run diagnostics and perform defect-isolation programs. You are responsible for making the system, IBM component, or both available for running diagnostics and defect-isolation programs.

Checking software

The IBM service specialist will help you ensure that the correct BIOS code, firmware, device drivers, and other supporting IBM software are installed and correctly configured. It might be necessary to manually gather information about the

relevant software levels or run IBM-approved utility programs to gather this information. It might be necessary to isolate the failing system from any active production environment to gather this information. You are responsible, with assistance from the service specialist, for gathering this information. The IBM Statement of Limited Warranty does not include on-site assistance with this activity.

Warranty service and support

With the original purchase of an IBM xSeries or IntelliStation system, you have access to extensive service and support. During the IBM Machine warranty period, you may call IBM or your reseller for problem-determination assistance under the terms of the IBM Statement of Limited Warranty.

The following services are available during the warranty period:

- **Problem determination** - Trained personnel are available to assist you with determining if you have a hardware problem and deciding what action is necessary to fix the problem.
- **IBM hardware repair** - If the problem is determined to be caused by IBM hardware under warranty, trained service personnel are available to provide the applicable level of service, either on-site or at an IBM service center as determined by IBM.
- **Engineering Change management** - Occasionally, there might be changes that are required after a product has been shipped from IBM. In those instances, IBM will make Engineering Changes (ECs) available that apply to your hardware.
- **Customer replaceable units (CRUs)** - Some parts of IBM xSeries and IntelliStation systems are designated as customer replaceable units. IBM ships CRUs to you for replacement by you. CRUs include keyboards, monitors, memory, diskette drives, hard disk drives, and mice (this list is not inclusive of all CRUs).

The following items are not covered under warranty service:

- Replacement or use of non-IBM parts. All IBM parts contain a 7-character identification in the format IBM FRU XXXXXXXX.
- Identification of software problem sources.
- Installation of customer replaceable units (CRUs).
- Installation and configuration of BIOS code, firmware, or device drivers that are designated as customer installable.

See the IBM Statement of Limited Warranty for a full explanation of IBM warranty terms. Be sure to retain your proof of purchase to obtain warranty service.

Please have the following information ready when you call:

- The machine type and model of your IBM hardware product (if available)
- Serial numbers of your IBM hardware products
- A description of the problem
- The exact wording of any error messages
- Hardware and software configuration information

International Warranty Service

If you travel with your xSeries or IntelliStation system or relocate it to a country or region where your system is sold and serviced by IBM or IBM resellers authorized

to perform warranty service, International Warranty Service (IWS) is available during the warranty period. Eligible IBM systems are identified by their four-digit machine types.

You can obtain IWS through the service delivery method (such as depot, carry-in, or on-site) provided in the servicing country or region. Service methods and procedures vary by country or region, and some service or parts might not be available in all countries and regions. Service centers in certain countries or regions might not be able to service all models of a particular machine type. In addition, some countries or regions might have fees and restrictions that apply at the time of service.

To determine whether your system is eligible for IWS, go to <http://www.ibm.com/pc/support/> and click **Warranty lookup**.

Purchasing additional services

During and after the warranty period, you can purchase additional services, such as support for IBM and non-IBM hardware, operating systems, and application programs; network setup and configuration; upgraded or extended hardware repair services; and custom installations. Service availability and service name might vary by country or region.

For more information about these services, contact your IBM marketing representative.

IBM Statement of Limited Warranty Z125-4753-06 8/2000

Part 1 - General Terms

This Statement of Limited Warranty includes Part 1 - General Terms and Part 2 - Country-unique Terms. The terms of Part 2 replace or modify those of Part 1. The warranties provided by IBM in this Statement of Limited Warranty apply only to Machines you 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. The term "Machine" does not include any software programs, whether pre-loaded with the Machine, installed subsequently or otherwise. Unless IBM specifies otherwise, the following warranties apply only in the country where you acquire the Machine. Nothing in this Statement of Limited Warranty affects any statutory rights of consumers that cannot be waived or limited by contract. If you have any questions, contact IBM or your reseller.

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 ("Specifications"). The warranty period for a Machine is a specified, fixed period commencing on its Date of Installation. The date on your sales receipt is the Date of Installation unless IBM or your reseller informs you otherwise.

If a Machine does not function as warranted during the warranty period, and IBM or your reseller are unable to either 1) make it do so or 2) replace it with one that is at least functionally equivalent, you may return it to your place of purchase and your money will be refunded.

Extent of Warranty: The warranty does not cover the repair or exchange of a Machine resulting from misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, or failure caused by a product for which IBM is not responsible. The warranty is voided by removal or alteration of Machine or parts identification labels.

THESE WARRANTIES ARE YOUR EXCLUSIVE WARRANTIES AND 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 OR LIMITATION 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.

Items Not Covered by Warranty: IBM does not warrant uninterrupted or error-free operation of a Machine. Any technical or other support provided for a Machine under warranty, such as assistance via telephone with "how-to" questions and those regarding Machine set-up and installation, will be provided **WITHOUT WARRANTIES OF ANY KIND.**

Warranty Service: To obtain warranty service for a Machine, contact IBM or your reseller. If you do not register your Machine with IBM, you may be required to present proof of purchase.

During the warranty period, IBM or your reseller, if approved by IBM to provide warranty service, provides without charge certain types of repair and exchange service to keep Machines in, or restore them to, conformance with their Specifications. IBM or your reseller will inform you of the available types of service for a Machine based on its country of installation. At its discretion, IBM or your reseller will 1) either repair or exchange the failing Machine and 2) provide the service either at your location or a service center. IBM or your reseller will also manage and install selected engineering changes that apply to the Machine.

Some parts of IBM Machines are designated as Customer Replaceable Units (called "CRUs"), e.g., keyboards, memory, or hard disk drives. IBM ships CRUs to you for replacement by you. You must return all defective CRUs to IBM within 30 days of your receipt of the replacement CRU. You are responsible for downloading designated Machine Code and Licensed Internal Code updates from an IBM Internet Web site or from other electronic media, and following the instructions that IBM provides.

When warranty 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. Many features, conversions, or upgrades involve the removal of parts and their return to IBM. A part that replaces a removed part will assume the warranty service status of the removed part.

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

1. ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange;
2. obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
3. where applicable, before service is provided:
 - a. follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provides;
 - b. secure all programs, data, and funds contained in a Machine;
 - c. provide IBM or your reseller with sufficient, free, and safe access to your facilities to permit them to fulfill their obligations; and
 - d. inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Neither IBM nor your reseller is responsible for any of your confidential, proprietary or personal information contained in a Machine which you return to IBM or your reseller for any reason. You should remove all such information from the Machine prior to its return.

Limitation of Liability: Circumstances may arise where, because of a default on IBM's part or other liability, 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), except for any liability that cannot be waived or limited by applicable laws, IBM is liable for no more than

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, up to the charges (if recurring, 12 months' charges apply) for the Machine that is subject of the claim. For purposes of this item, the term "Machine" includes Machine Code and Licensed Internal Code.

This limit also applies to IBM's suppliers and your reseller. It is the maximum for which IBM, its suppliers, and your reseller are collectively responsible.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING: 1) THIRD-PARTY CLAIMS AGAINST YOU FOR 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, LOST PROFITS OR LOST SAVINGS, EVEN IF IBM, ITS SUPPLIERS 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 LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Governing Law: Both you and IBM consent to the application of the laws of the country in which you acquired the Machine to govern, interpret, and enforce all of your and IBM's rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this Agreement, without regard to conflict of law principles.

Part 2 - Country-unique Terms

AMERICAS

BRAZIL

Governing Law: *The following is added after the first sentence:* Any litigation arising from this Agreement will be settled exclusively by the court of Rio de Janeiro.

NORTH AMERICA

Warranty Service: *The following is added to this Section:* To obtain warranty service from IBM in Canada or the United States, call 1-800-IBM-SERV (426-7378).

CANADA

Governing Law: *The following replaces "laws of the country in which you acquired the Machine" in the first sentence:* laws in the Province of Ontario.

UNITED STATES

Governing Law: *The following replaces "laws of the country in which you acquired the Machine" in the first sentence:* laws of the State of New York.

ASIA PACIFIC

AUSTRALIA

The IBM Warranty for Machines: *The following paragraph is added to this Section:* The warranties specified in this Section are in addition to any rights you may have under the Trade Practices Act 1974 or other similar legislation and are only limited to the extent permitted by the applicable legislation.

Limitation of Liability: *The following is added to this Section:* Where IBM is in breach of a condition or warranty implied by the Trade Practices Act 1974 or other similar legislation, IBM's liability is limited to the repair or replacement of the goods or the supply of equivalent goods. Where that condition or warranty relates to right to sell, quiet possession or clear title, or the goods are of a kind ordinarily acquired for personal, domestic or household use or consumption, then none of the limitations in this paragraph apply.

Governing Law: *The following replaces "laws of the country in which you acquired the Machine" in the first sentence:* laws of the State or Territory.

CAMBODIA, LAOS, AND VIETNAM

Governing Law: *The following replaces "laws of the country in which you acquired the Machine" in the first sentence:* laws of the State of New York.

The following is added to this Section: Disputes and differences arising out of or in connection with this Agreement shall be finally settled by arbitration which shall be held in Singapore in accordance with the rules of the International Chamber of Commerce (ICC). The arbitrator or arbitrators designated in conformity with those rules shall have the power to rule on their own competence and on the validity of the Agreement to submit to arbitration. The arbitration award shall be final and binding for the parties without appeal and the arbitral award shall be in writing and set forth the findings of fact and the conclusions of law.

All proceedings shall be conducted, including all documents presented in such proceedings, in the English language. The number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator.

The two arbitrators appointed by the parties shall appoint a third arbitrator before proceeding upon the reference. The third arbitrator shall act as chairman of the proceedings. Vacancies in the post of chairman shall be filled by the president of the ICC. Other vacancies shall be filled by the respective nominating party. Proceedings shall continue from the stage they were at when the vacancy occurred.

If one of the parties refuses or otherwise fails to appoint an arbitrator within 30 days of the date the other party appoints its, the first appointed arbitrator shall be the sole arbitrator, provided that the arbitrator was validly and properly appointed.

The English language version of this Agreement prevails over any other language version.

HONG KONG AND MACAU

Governing Law: *The following replaces "laws of the country in which you acquired the Machine" in the first sentence:* laws of Hong Kong Special Administrative Region.

INDIA

Limitation of Liability: *The following replaces items 1 and 2 of this Section:*

1. liability for bodily injury (including death) or damage to real property and tangible personal property will be limited to that caused by IBM's negligence;
2. as to any other actual damage arising in any situation involving nonperformance by IBM pursuant to, or in any way related to the subject of this Statement of Limited Warranty, IBM's liability will be limited to the charge paid by you for the individual Machine that is the subject of the claim.

JAPAN

Governing Law: *The following sentence is added to this Section:* Any doubts concerning this Agreement will be initially resolved between us in good faith and in accordance with the principle of mutual trust.

NEW ZEALAND

The IBM Warranty for Machines: *The following paragraph is added to this Section:* The warranties specified in this Section are in addition to any rights you may have under the Consumer Guarantees Act 1993 or other legislation which cannot be excluded or limited. The Consumer Guarantees Act 1993 will not apply in respect of any goods which IBM provides, if you require the goods for the purposes of a business as defined in that Act.

Limitation of Liability: *The following is added to this Section:* Where Machines are not acquired for the purposes of a business as defined in the Consumer Guarantees Act 1993, the limitations in this Section are subject to the limitations in that Act.

PEOPLE'S REPUBLIC OF CHINA (PRC)

Governing Law: *The following replaces this Section:* Both you and IBM consent to the application of the laws of the State of New York (except when local law requires otherwise) to govern, interpret, and enforce all your and IBM's rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this Agreement, without regard to conflict of law principles.

Any disputes arising from or in connection with this Agreement will first be resolved by friendly negotiations, failing which either of us has the right to submit the dispute to the China International Economic and Trade Arbitration Commission in Beijing, the PRC, for arbitration in accordance with its arbitration rules in force at the time. The arbitration tribunal will consist of three arbitrators. The language to be used therein will be English and Chinese. An arbitral award will be final and binding on all the parties, and will be enforceable under the Convention on the Recognition and Enforcement of Foreign Arbitral Awards (1958).

The arbitration fee will be borne by the losing party unless otherwise determined by the arbitral award.

During the course of arbitration, this Agreement will continue to be performed except for the part which the parties are disputing and which is undergoing arbitration.

EUROPE, MIDDLE EAST, AFRICA (EMEA)

THE FOLLOWING TERMS APPLY TO ALL EMEA COUNTRIES: The terms of this Statement of Limited Warranty apply to Machines purchased from IBM or an IBM reseller.

Warranty Service: If you purchase an IBM Machine in Austria, Belgium, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland or United Kingdom, you may obtain warranty service for that Machine in any of those countries from either (1) an IBM reseller approved to perform warranty service or (2) from IBM. If you purchase an IBM Personal Computer Machine in Albania, Armenia, Belarus, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Georgia, Hungary, Kazakhstan, Kirghizia, Federal Republic of Yugoslavia, Former Yugoslav Republic of Macedonia (FYROM), Moldova, Poland, Romania, Russia, Slovak Republic, Slovenia, or Ukraine, you may obtain warranty service for that Machine in any of those countries from either (1) an IBM reseller approved to perform warranty service or (2) from IBM.

If you purchase an IBM Machine in a Middle Eastern or African country, you may obtain warranty service for that Machine from the IBM entity within the country of purchase, if that IBM entity provides warranty service in that country, or from an IBM reseller, approved by IBM to perform warranty service on that Machine in that country. Warranty service in Africa is available within 50 kilometers of an IBM authorized service provider. You are responsible for transportation costs for Machines located outside 50 kilometers of an IBM authorized service provider.

Governing Law: The applicable laws that govern, interpret and enforce rights, duties, and obligations of each of us arising from, or relating in any manner to, the subject matter of this Statement, without regard to conflict of laws principles, as well as Country-unique terms and competent court for this Statement are those of the country in which the warranty service is being provided, except that in 1) Albania, Bosnia-Herzegovina, Bulgaria, Croatia, Hungary, Former Yugoslav Republic of Macedonia, Romania, Slovakia, Slovenia, Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan, the laws of Austria apply; 2) Estonia, Latvia, and Lithuania, the laws of Finland apply; 3) Algeria, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Congo, Djibouti, Democratic Republic of Congo, Equatorial Guinea, France, Gabon, Gambia, Guinea, Guinea-Bissau, Ivory Coast, Lebanon, Mali, Mauritania, Morocco, Niger, Senegal, Togo, and Tunisia, this Agreement will be construed and the legal relations between the parties will be determined in accordance with the French laws and all disputes arising out of this Agreement or related to its violation or execution, including summary proceedings, will be settled exclusively by the Commercial Court of Paris; 4) Angola, Bahrain, Botswana, Burundi, Egypt, Eritrea, Ethiopia, Ghana, Jordan, Kenya, Kuwait, Liberia, Malawi, Malta, Mozambique, Nigeria, Oman, Pakistan, Qatar, Rwanda, Sao Tome, Saudi Arabia, Sierra Leone, Somalia, Tanzania, Uganda, United Arab Emirates, United Kingdom, West Bank/Gaza, Yemen, Zambia, and Zimbabwe, this Agreement will be governed by English Law and disputes relating to it will be submitted to the exclusive jurisdiction of the English courts; and 5) in Greece, Israel, Italy, Portugal, and Spain any legal claim arising out of this Statement will be brought before, and finally settled by, the competent court of Athens, Tel Aviv, Milan, Lisbon, and Madrid, respectively.

THE FOLLOWING TERMS APPLY TO THE COUNTRY SPECIFIED:

AUSTRIA AND GERMANY

The IBM Warranty for Machines: *The following replaces the first sentence of the first paragraph of this Section:* The warranty for an IBM Machine covers the functionality of the Machine for its normal use and the Machine's conformity to its Specifications.

The following paragraphs are added to this Section:

The minimum warranty period for Machines is six months. In case IBM or your reseller is unable to repair an IBM Machine, you can alternatively ask for a partial refund as far as justified by the reduced value of the unrepaired Machine or ask for a cancellation of the respective agreement for such Machine and get your money refunded.

Extent of Warranty: *The second paragraph does not apply.*

Warranty Service: *The following is added to this Section:* During the warranty period, transportation for delivery of the failing Machine to IBM will be at IBM's expense.

Limitation of Liability: *The following paragraph is added to this Section:* The limitations and exclusions specified in the Statement of Limited Warranty will not apply to damages caused by IBM with fraud or gross negligence and for express warranty.

The following sentence is added to the end of item 2: IBM's liability under this item is limited to the violation of essential contractual terms in cases of ordinary negligence.

EGYPT

Limitation of Liability: *The following replaces item 2 in this Section:* as to any other actual direct damages, IBM's liability will be limited to the total amount you paid for the Machine that is the subject of the claim. For purposes of this item, the term "Machine" includes Machine Code and Licensed Internal Code.

Applicability of suppliers and resellers (unchanged).

FRANCE

Limitation of Liability: *The following replaces the second sentence of the first paragraph of this Section:*In such instances, regardless of the basis on which you are entitled to claim damages from IBM, IBM is liable for no more than: *(items 1 and 2 unchanged).*

IRELAND

Extent of Warranty: *The following is added to this Section:* Except as expressly provided in these terms and conditions, all statutory conditions, including all warranties implied, but without prejudice to the generality of the foregoing all warranties implied by the Sale of Goods Act 1893 or the Sale of Goods and Supply of Services Act 1980 are hereby excluded.

Limitation of Liability: *The following replaces items one and two of the first paragraph of this Section:*1. death or personal injury or physical damage to your real property solely caused by IBM's negligence; and 2. the amount of any other actual direct damages, up to 125 percent of the charges (if recurring, the 12 months' charges apply) for the Machine that is the subject of the claim or which otherwise gives rise to the claim.

Applicability of suppliers and resellers (unchanged).

The following paragraph is added at the end of this Section: IBM's entire liability and your sole remedy, whether in contract or in tort, in respect of any default shall be limited to damages.

ITALY

Limitation of Liability: *The following replaces the second sentence in the first paragraph: In each such instance unless otherwise provided by mandatory law, IBM is liable for no more than: 1. (unchanged) 2. as to any other actual damage arising in all situations involving nonperformance by IBM pursuant to, or in any way related to the subject matter of this Statement of Warranty, IBM's liability, will be limited to the total amount you paid for the Machine that is the subject of the claim. Applicability of suppliers and resellers (unchanged).*

The following replaces the third paragraph of this Section: Unless otherwise provided by mandatory law, IBM and your reseller are not liable for any of the following: (items 1 and 2 unchanged) 3) indirect damages, even if IBM or your reseller is informed of their possibility.

SOUTH AFRICA, NAMIBIA, BOTSWANA, LESOTHO AND SWAZILAND

Limitation of Liability: *The following is added to this Section: IBM's entire liability to you for actual damages arising in all situations involving nonperformance by IBM in respect of the subject matter of this Statement of Warranty will be limited to the charge paid by you for the individual Machine that is the subject of your claim from IBM.*

UNITED KINGDOM

Limitation of Liability: *The following replaces items 1 and 2 of the first paragraph of this Section:*

1. death or personal injury or physical damage to your real property solely caused by IBM's negligence;
2. the amount of any other actual direct damages or loss, up to 125 percent of the charges (if recurring, the 12 months' charges apply) for the Machine that is the subject of the claim or which otherwise gives rise to the claim;

The following item is added to this paragraph: 3. breach of IBM's obligations implied by Section 12 of the Sale of Goods Act 1979 or Section 2 of the Supply of Goods and Services Act 1982.

Applicability of suppliers and resellers (unchanged).

The following is added to the end of this Section: IBM's entire liability and your sole remedy, whether in contract or in tort, in respect of any default shall be limited to damages.

Appendix G. Notices

This publication was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.*

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Edition notice

**© COPYRIGHT INTERNATIONAL BUSINESS MACHINES CORPORATION, 2002.
All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active Memory	Predictive Failure Analysis
Active PCI	PS/2
Active PCI-X	ServeRAID
Alert on LAN	ServerGuide
BladeCenter	
C2T Interconnect	ServerProven
Chipkill	TechConnect
EtherJet	Tivoli
e-business logo	Tivoli Enterprise
FlashCopy	Update Connector
IBM	Wake on LAN
IntelliStation	XA-32
Light Path Diagnostics	XA-64
NetBAY	X-Architecture
Netfinity	Xcel4
NetView	XpandOnDemand
OS/2 WARP	xSeries

Lotus, Lotus Notes, SmartSuite, and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speeds indicate the internal clock speed of the microprocessor; other factors also affect application performance.

CD-ROM drive speeds list the variable read rate. Actual speeds vary and are often less than the maximum possible.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for approximately 1000 bytes, MB stands for approximately 1 000 000 bytes, and GB stands for approximately 1 000 000 000 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity may vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives available from IBM.

Maximum memory may require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven[®], including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software may differ from its retail version (if available), and may not include user manuals or all program functionality.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: 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 using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

Australia and New Zealand Class A statement

Attention: 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.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: 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.

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。

Japanese Voluntary Control Council for Interference (VCCI) statement

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

Index

Numerics

- 802.1Q VLANs Entry Settings - Add window 41
- 802.1Q VLANs Entry Settings - Edit window 42

A

- access levels for user accounts 59, 61, 79
- address table 65
- aging time 23
- assigning privileges to user accounts 59, 61, 79
- authentication failure 21
- authentication protocol 22
- auto-negotiation 133
- avoiding network problems 136

B

- bay locations 7, 19
- blocking state 127
- bridge protocol data unit (BPDU) 122
- Browse MAC Address Table window 65, 94

C

- cable
 - lengths 119
- cable specifications 6
- case-sensitive passwords 76
- Category 3 cable 115, 119
- Category 5 cable 119
- chassis configuration 17
- Class A electronic emission notice 157
- Class of Service Configuration window 51, 102
- Class of Service menu 101
- Class of Service window 51
- cold start 21
- community settings 58
- compatible options Web site 8
- components
 - major 4
- configuration 34, 73, 81
- Configure 802.1Q Port Settings window 109
- Configure Ports window 38, 89
- Configure Spanning Tree menu 99
- Configure Spanning Tree window 48
- configuring the switch module through a Telnet interface 75
- connecting the Telnet interface to the switch module 76, 77

D

- data loop 136
- data transmission rates 5
- default remote-management mode 31, 75

- default settings
 - Factory Reset window 73
 - Reboot menu 81
 - runtime switching software 117
- default spanning-tree configuration 124
- deleting user accounts 83
- disabled state 132
- Display Ports window 38
- distribution method 53
- Distribution Method window 53
- Download Configuration File from TFTP Server window 68, 90
- Download Configuration/Log Files window 72
- dynamic host configuration protocol (DHCP) 29

E

- Edit 802.1Q VLANs window 40, 107
- efficient network operation 136
- egress port 24
- electronic emission Class A notice 157
- Ethernet
 - activity LED 16
 - cable specifications 6
 - interface requirements 7
 - link LED 16
 - port locations 5
 - standards 6
 - switch error LED 16
- external components 15
- external-port remote management 32, 75

F

- Factory Reset values 73, 81
- Factory Reset window 73
- FCC Class A notice 157
- features 5
- filtering
 - ingress 29
- First IGMP Snooping window 45
- first-time connection to the switch module 76
- flash memory 5
- forwarding 56, 101
- forwarding state 130
- full/half duplex mismatch 133

G

- GARP VLAN Registration Protocol (GVRP) 110
- general requirements 5
- Generic Attribute Registration Protocol (GARP) 110
- GVRP Status window 66
- GVRP window 95

H

handling static-sensitive devices 9

I

identification labels 4

identifying a data loop 136

IEEE 802.3ad Link Aggregation menu 113

IGMP Snooping Table window 67

IGMP Snooping window 95, 105

indicators 15

information panel 15

ingress filtering 29

ingress port 24

initial configuration 18

installation

guidelines 8

illustration 10

procedure 10

requirements 7

installing

options 8

switch module 10

Internet protocol (IP) 19

introduction 1

IP address 19

IP Setup 84

IP Setup window 36, 85

L

labels 4

LACP Aggregator Monitoring window 66, 96

learning state 129

LEDs

Ethernet activity 16

Ethernet link 16

Ethernet switch error 16

front view 15

OK 16

power-on 16

link aggregation 52, 53, 110

Link Aggregation Port Setting window 55, 113

Link Aggregation window 111

listening state 128

location

LEDs 15

media access control (MAC) address 4

ports 15

serial number 4

logging onto the switch module 82

Logout window 98

M

MAC address forwarding 56, 101

MAC Address Forwarding window 56, 101

main menu 73, 77, 80, 81

maintenance 68

major components 4

Management Information Base (MIB) 21

Management Station IP Settings window 58

managing the switch module remotely 31, 75

maximum cable lengths 119

media access control (MAC) address 4, 19, 20

Multicasting menu 104

N

negotiation 133

network management

Web-based 32

network monitoring 62

Network Monitoring menu 92

network operation 136

new root 21

normal user privileges 61, 79

notes, important 156

notices

electronic emission 157

FCC, Class A 157

used in this book 4

O

OK LED 16

options

installing 8

Web site 8

overview 17

P

packet corruption 135

packet forwarding 23, 25

password rules 76

performance requirements 5

pin assignments 115

Ping window 92

Port Error Packet window 62, 63

Port Error Packets window 93

Port GVRP Settings window 45

Port Ingress Filter window 44

port locations 5, 15

Port Mirroring Settings window 47, 104

Port Packet Analysis window 64, 94

port priority 125

Port Priority window 43

port specifications 5

port states 122

port transition 123

port trunking 52, 53, 110

Port Trunking window 54, 112

Port Utilization window 62, 93

Port VLAN ID (PVID) window 42

power-on LED 16

privileges for user accounts, assigning 59, 61, 79

protocols 6

R

- Reboot menu 81, 97
- redundancy 17
- remote access 31, 75
- remote management 31, 75
- remote management setup 57
- Remote Management Setup menu 87
- remote reset 73
- removing
 - switch module 12
- resource errors 135
- Restart System window 73
- restarting the switch 73, 97
- restoring default configuration values 73, 81
- RJ-45 pin specifications 115
- Root privileges 59, 61, 79
- runtime switching software default settings 117

S

- Save Changes window 72, 80
- Save Log to TFTP Server window 70, 91
- saving configuration values 73, 80, 81
- serial number 4
- set up user accounts 78
- setting up user accounts 59
- Setup 802.1p Priority Mapping window 52, 102
- Setup Diffserv Mapping window 52, 103
- Setup IEEE 802.1q Multicast Forwarding window 46, 106
- Setup IEEE 802.3ad Link Aggregation window 55
- Setup Trap Receivers window 58
- Setup Trap Recipients window 87
- Setup User Account - Add window 60
- Setup User Account - Edit window 60, 61
- Setup User Accounts window 59, 82, 83
- simple network management protocol (SNMP) 22
- SNMP community names 19
- SNMP Community Settings window 58
- Spanning Tree Algorithm (STA) 22, 23
- Spanning Tree Protocol (STP) 23
- specifications
 - data transmission rates 5
 - network cable 6
 - performance requirements 5
 - ports 5
 - protocols 6
 - RJ-45 pin 115
 - standards 6
 - technical 5
 - topology 6
- stable topology 122
- standard Category 3 cable 115
- standards 6
- static electricity 9
- static-sensitive devices, handling 9
- statistics 62
- STP
 - See Spanning Tree Protocol (STP)
 - STP failure 133

STP illustration

- after applying STA rules 126
- before applying STA rules 125

- STP parameters 121, 124
- STP port parameters 121
- STP Port Settings menu 100
- STP Port Settings window 49
- STP port states 122
- switch bay numbers 19
- Switch History window 67, 96
- Switch Information menu 19, 20, 35
- Switch Information window 84
- switch management operation 17
- Switch Settings window 39, 88
- Switch Utilities menu 89
- system operation 17
- System Reboot Confirmation window 97
- system reliability 8

T

- tagging a packet 24, 28
- tags 26
- technical specifications 5
- Telnet interface 75
- Telnet Settings window 40
- Telnet usage conventions 76
- topology 6, 122
- topology change 21
- trademarks 156
- transmission rates 5
- trap receivers 58
- traps 20, 57, 58
- troubleshooting STP 133

U

- understanding STP 121
- understanding the Ethernet switch subsystem 17
- unidirectional link 134
- United States electronic emission Class A notice 157
- United States FCC Class A notice 157
- untagging a packet 24, 28
- updating user accounts 82
- Upgrade Firmware from TFTP Server window 69, 90
- Upgrade Firmware/Configuration File window 71
- Upload Configuration File to TFTP Server window 70, 91
- user access levels 59, 61, 79
- User name 77
- user privileges 59, 61, 79
- User+ privileges 59, 61, 79

V

- virtual local area network (VLAN) 24
- VLAN ID (VID) 27
- VLAN menu 107

W

warm start 21

Web site

 compatible options 8

 IBM products 1

Web-based network management 31, 32

World Wide Web 1



Part Number: 59P6530

Printed in U.S.A.

(1P) P/N: 59P6530

