BladeCenter 2-Port Fibre Channel Switch Module, HS20 Expansion Card

Hardware Maintenance Manual and Troubleshooting Guide
Note
Before using this information and the product it supports, be sure to read Appendix C, “Notices”, on page 197.
About this manual

This manual contains diagnostic information, a Symptom-to-FRU index, service information, error codes, error messages, and configuration information for the BladeCenter™ 2-Port Fibre Channel Switch Module and HS20 Fibre Channel Expansion Card.

Important safety information

Be sure to read all caution and danger statements in this book before performing any of the instructions. See “Safety information” on page 161.

Lea todas as instruções de cuidado e perigo antes de executar qualquer operação.

注意和危险声明（简体中文）

重要事项:

本书中的所有注意和危险声明之前都有编号。该编号用于英语的注意或危险声明与 Safety Information 一书中可以找到的翻译版本的注意或危险声明进行交叉引用。

例如，如果一个注意声明以编号 1 开始，那么对该注意声明的翻译出现在 Safety Information 一书中的声明 1 中。

在按说明执行任何操作前，请务必阅读所有注意和危险声明。

注意及危险聲明（中文）

重要資訊：

本書中所有「注意」及「危險」的聲明均以數字開始。此一數字是用來作為交叉參考之用，英文「注意」或「危險」聲明可在「安全資訊」(Safety Information) 一書中找到相同內容的「注意」或「危
險」聲明的譯文。

例如，有一「危險」聲明以數字 1 開始，則該「危

險」聲明的譯文將出現在「安全資訊」(Safety

Information) 一書的「聲明」1 中。

執行任何指示之前，請詳讀所有「注意」及「危險」

的聲明。

Prenez connaissance de toutes les consignes de type Attention et Danger avant de procéder aux opérations décrites par les instructions.

Lesen Sie alle Sicherheitshinweise, bevor Sie eine Anweisung ausführen.
Accertarsi di leggere tutti gli avvisi di attenzione e di pericolo prima di effettuare qualsiasi operazione.

WARNING: Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

ADVERTENCIA: El contacto con el cable de este producto o con cables de accesorios que se venden junto con este producto, pueden exponerle al plomo, un elemento químico que en el estado de California de los Estados Unidos está considerado como un causante de cancer y de defectos congénitos, además de otros riesgos reproductivos. Lávese las manos después de usar el producto.

Online support


Support telephone numbers

### Contents

**About this manual** .................................................. iii
**Important safety information** .................................. iii
**Online support** ................................................... iv
**Support telephone numbers** ..................................... iv

**Chapter 1. General information** ................................ 1
**Related publications** ............................................ 1
**Notices used in this book** ....................................... 3

**Chapter 2. BladeCenter 2-Port Fibre Channel Switch Module** .... 5
**Command line interface (CLI)** .................................. 6
  **Logging on to a switch** ....................................... 6
  **Command syntax** ............................................... 7
  **Commands** ........................................................ 7

**Using the SAN Utility** .......................................... 70
  **SAN Utility user interface** ................................... 70
  **Using the Topology window** .................................. 74
  **Using the Faceplate window** ................................ 76
  **Managing fabrics** ............................................. 78
  **Managing switch modules** ................................... 93
  **Managing ports** ................................................ 104

**Switch management utility functions** .......................... 113
  **LED diagnostics** ............................................. 113
  **Port testing** ................................................... 116
  **Fibre Channel switch module monitoring using SNMP** ...... 117
  **Restoring Fibre Channel switch module configuration** .... 118
  **Using the Fabric View application** .......................... 120

**Mapping port locations and software numbering** ............. 122
  **Port mapping** .................................................. 122

**Chapter 3. HS20 Fibre Channel Expansion Card** .................. 125
**Features and specifications** ................................... 125
**Inventory checklist** ............................................. 128
**Notices and statements used in this book** ..................... 128
**Major components of the HS20 Expansion Card** ................. 128
**Installing the HS20 Expansion Card** ............................ 130
  **Installation guidelines** ....................................... 130
  **Installing the HS20 Expansion Card** ........................ 131

**Updating the expansion card BIOS code and NVRAM code and installing device drivers** .................................. 134
  **Creating a BIOS Update Utility diskette** .................... 135
  **Updating the expansion card BIOS code and NVRAM code** .. 136
  **Using the Remote Deployment Manager** ....................... 138
  **Installing the HS20 Expansion Card device drivers** .......... 138

**Using IBM Fast!UTIL** ............................................ 139
  **Starting Fast!UTIL** .......................................... 139
  **Configuration Settings menu options** ........................ 139

**Chapter 4. Diagnostic information** .............................. 145
**General BladeCenter Fibre Channel configuration diagram** ..... 145
**General Checkout** ............................................... 145

**Chapter 5. Symptom-to-FRU index** ............................... 149
Chapter 1. General information

Fibre Channel technology is outlined in the SCSI-3 Fibre Channel Protocol (SCSI-FCP) standard. Fibre Channel is a high-speed data transport technology used for mass storage and networking.

By adding HS20 Expansion Cards to the blade servers and BladeCenter 2-Port Fibre Channel switch modules to the BladeCenter unit, you can attach the blade server to an external storage area network (SAN) through the external 2 Gbps (gigabits per second) optical ports on the switch modules. The HS20 Expansion Card supports data-transfer rates up to 200 MB per second half-duplex and 400 MB per second full-duplex.

Related publications

This *Hardware Maintenance Manual and Troubleshooting Guide* is provided in PDF on the WEB at http://www.ibm.com/pc/support. It contains information to help you solve problems yourself or to provide helpful information to a service technician.

In addition to this *Hardware Maintenance Manual and Troubleshooting Guide*, the following related documentation is provided with your switch module:

- **IBM @server BladeCenter Fibre Channel Switch Management User’s Guide**
  This publication describes how to use the SAN Utility application. In addition, it describes how to start the Telnet CLI and lists the CLI commands and their usage.

- **IBM @server BladeCenter 2-Port Fibre Channel Switch Module Installation Guide**
  This publication contains detailed installation instructions for the switch module. This publication also provides general information about your switch module, including information about features, how to install and set up your switch module, how to install the SAN Utility application, and how to get help.

- **IBM @server BladeCenter Type 8677 Installation and User’s Guide**
  This publication is provided in Portable Document Format (PDF) on the IBM BladeCenter Documentation CD. It contains 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

- **IBM @server BladeCenter HS20 Type 8678 Installation and User’s Guide**
  This publication is provided in PDF on the IBM BladeCenter Documentation CD. It contains 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
IBM Eserver HS20 Fibre Channel Expansion Card Installation and User’s Guide
This publication contains instructions for installing your IBM HS20 Fibre Channel Expansion Card in an IBM BladeCenter HS20 blade server and information about:

– Configuring the HS20 Expansion Card
– Updating the BIOS code and device drivers of the HS20 Expansion card

IBM Eserver BladeCenter SAN Solutions Guide
This publication is provided in PDF on the IBM BladeCenter Documentation CD. It provides a user-oriented discussion of how BladeCenter Fibre Channel options are used to provide different SAN storage solutions for various application requirements. This document also provides an overview and description for backup and restore, business continuance and high availability, and storage consolidation and data sharing solutions.

IBM Eserver BladeCenter Fibre Channel Switch Interoperability Guide
This publication is provided in PDF on the IBM BladeCenter Documentation CD. It provides detailed Fibre Channel switch module configuration data and step-by-step configuration procedures for integrating the BladeCenter unit into other vendor switch fabrics. Each vendor configuration includes an initial integration checklist, configuration limitations, supported switch and firmware versions, specific management application operations, and a successful-integration checklist.

IBM Fibre Channel Problem Determination Guide
This publication provides problem determination and resolution information for the issues most commonly encountered with IBM® Fibre Channel devices and configurations. This manual should be used in conjunction with the Fibre Channel Hardware Maintenance Manual (19K6130), which contains useful component information, such as specifications, replacement and installation procedures, and basic symptom lists.

IBM FASTT Management Suite Java User’s Guide
This publication describes how to use the FASTT MSJ application, including:

– An overview of FASTT MSJ
– FASTT MSJ system requirements
– How to install and start FASTT MSJ
– The features and functions of FASTT MSJ

Rack Installation Instructions
This publication contains the instructions for installing your BladeCenter unit in a rack.

Safety Information
This multilingual publication is provided in PDF on the IBM BladeCenter Documentation CD. It contains translated versions of the caution and danger statements that appear in the documentation. Each caution and danger statement has a number, which you can use to locate the corresponding statement in your language.

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 Eserver BladeCenter Planning and Installation Guide at

Notices used in this book

The following notices are used in this book:

• **Notes**: 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 potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage could occur.
Chapter 2. BladeCenter 2-Port Fibre Channel Switch Module

You can manage and configure your IBM® @server BladeCenter™ 2-Port Fibre Channel Switch Module through a Telnet connection to the embedded command line interface (CLI) or by using the IBM BladeCenter SAN Utility application. The SAN Utility provides an intuitive graphical user interface (GUI) that you can use to configure multiple Fibre Channel switch modules through other connected SAN devices from a single interface. The IBM BladeCenter SAN Utility application is referred to throughout this publication as the SAN Utility. The IBM BladeCenter 2-Port Fibre Channel Switch Module is referred to throughout this publication as the switch module.

This User's Guide provides instructions to:
• Configure your switch module
• Manage fabrics, ports, and switch modules
• Use Telnet and the CLI to configure switch module parameters

You can manage the BladeCenter fabric through an Ethernet network using the SAN Utility or the CLI. The SAN Utility is installed on a Microsoft® Windows® 2000, Red Hat Linux® Advanced Server Version 2.1, Red Hat Linux Version 7.x, or SuSE Linux Professional Version 8.0 network management workstation.

The switch module has an embedded Telnet server through which a Telnet client can connect and manage the switch module using the CLI. See "Command line interface (CLI)" on page 6 for more information about Telnet and CLI commands.

SNMP provides monitoring and trap functions for the fabric. The switch module firmware supports SNMP Versions 1, 2, and 3; the Fibre Alliance Management Information Base (FA-MIB) version 4.0; and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps are formatted using SNMP version 2.

If you are an experienced user, you can use the Telnet CLI to perform the following tasks:
• Manage the switch module from the BladeCenter management module interface to the Telnet client
• Perform single switch management
• Use advanced control commands

If you are a new user or if you need to manage multiple switch modules from a single interface, you can use the SAN Utility GUI to perform the following tasks:
• Manage your switch module from a remote client or network management workstation
• Manage your multiswitch fabric

For information about installing the switch module and the SAN Utility, see the IBM BladeCenter 2-Port Fibre Channel Switch Module Installation Guide that comes with the switch module.

You can obtain up-to-date information about your switch module and other IBM server products at http://www.ibm.com/eserver/bladecenter/.
Command line interface (CLI)

Your switch module contains an embedded Telnet server. This server enables a Telnet client to establish a Telnet session with the switch module to retrieve information or to configure parameters using the CLI. You can use the CLI to perform a variety of fabric and switch management tasks through an Ethernet connection to your BladeCenter unit.

You can access the Telnet interface in two ways:

- In the BladeCenter management module Web interface
- In a command-line window on a connected network management workstation

Important: Before you configure your switch module, be sure that the management modules in your BladeCenter unit are properly configured. In addition, to access and manage your 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. For more detailed information about configuring your switch module, see the IBM Eserver BladeCenter 2-Port Fibre Channel Switch Module Installation Guide on the IBM BladeCenter Documentation CD.

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

Logging on to a switch

To log on to a switch using Telnet, complete the following steps:

1. Open a command-line window on the network management workstation, type one of the following commands, and press Enter.
   
   For switch module bay 3:
   telnet 192.168.70.129
   
   For switch module bay 4:
   telnet 192.168.70.130
   
   A command prompt window opens.

2. At the Login prompt, type the initial default user ID, USERID. At the Password prompt, type the initial default password, PASSW0RD (the sixth character is a zero, not the letter O). The user ID and password are case sensitive.

   This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account. See “Commands” on page 7 for more information about authority levels. See the “User command” on page 60 for information about creating user accounts.

   Note: The switch module supports a combined maximum of 15 logins. This includes the SAN Utility in-band and out-of-band logins, Telnet out-of-band logins, and SNMP out-of-band logins. A maximum of 10 SAN Utility logins are accepted. Additional logins will be refused.
Command syntax

The command syntax is as follows:

```
command
  keyword
  keyword [value]
  keyword [value1] [value2]
```

The command is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are lowercase and case sensitive.
- Required keyword values are shown in standard font: [value]. Optional values are shown in italics: [value].
- The underlined portion of each keyword indicates the abbreviated form that can be used. For example the `Delete` keyword can be abbreviated Del.

Commands

The command set provides for User and Admin authority levels.

- User authority grants viewing access to the fabric and switches using the Show command and other read-only commands.
- Admin authority includes the User authority and grants permission to use the Admin command. The Admin Start command opens an admin session, which provides access to the commands that change switch and fabric configurations. See the "Admin command" on page 9.

Note: Admin authority is enforced only if fabric security is enabled on the switch. By default, fabric security is disabled. See the keywords of the "Set Setup command" on page 38 for information about setting fabric security.

The commands and their page numbers are listed by authority level in Table 1 on page 8. The following Admin session commands have some keywords that are available with User authority:

- Alias
- Config
- Date
- Set
- User
- Zone
- Zoneset
- Zoning
<table>
<thead>
<tr>
<th>User authority commands</th>
<th>Admin authority command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Admin</td>
</tr>
<tr>
<td>History</td>
<td>Admin</td>
</tr>
<tr>
<td>Ps</td>
<td>Admin</td>
</tr>
<tr>
<td>Quit</td>
<td>Admin</td>
</tr>
<tr>
<td>Show</td>
<td>Admin</td>
</tr>
<tr>
<td>Show Config</td>
<td>Admin</td>
</tr>
<tr>
<td>Show Log</td>
<td>Admin</td>
</tr>
<tr>
<td>Show Perf</td>
<td>Admin</td>
</tr>
<tr>
<td>Show Setup</td>
<td>Admin</td>
</tr>
<tr>
<td>Uptime</td>
<td>Admin</td>
</tr>
<tr>
<td>Whoami</td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin session commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
</tr>
<tr>
<td>Config</td>
</tr>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Fallback</td>
</tr>
<tr>
<td>Image</td>
</tr>
<tr>
<td>Lip</td>
</tr>
<tr>
<td>Passwd</td>
</tr>
<tr>
<td>Reset</td>
</tr>
<tr>
<td>Set</td>
</tr>
<tr>
<td>Set Config</td>
</tr>
<tr>
<td>Set Log</td>
</tr>
<tr>
<td>Set Port</td>
</tr>
<tr>
<td>Set Setup</td>
</tr>
<tr>
<td>Shutdown</td>
</tr>
<tr>
<td>Test</td>
</tr>
<tr>
<td>User</td>
</tr>
<tr>
<td>Zone</td>
</tr>
<tr>
<td>Zoneset</td>
</tr>
<tr>
<td>Zoning</td>
</tr>
</tbody>
</table>

"Help command" on page 16.
"History command" on page 17.
"Ps command" on page 20.
"Quit command" on page 21.
"Show command" on page 41.
"Show Config command" on page 48.
"Show Log command" on page 50.
"Show Perf command" on page 52.
"Show Setup command" on page 54.
"Uptime command" on page 59.
"Whoami command" on page 62.
**Admin command**

Opens and closes an admin session. The admin session provides commands that change the fabric and switch configurations. Only one admin session can be open on the switch at any time. An inactive admin session will time out after a period of time that can be changed using the Set Setup System command. See the "Set Setup command" on page 38.

**Authority:** Admin

**Syntax:**

```plaintext
admin
    start
    end
    cancel
```

**Keywords:**

- **start**
  
  Opens the admin session.

- **end**
  
  Closes the admin session. The Logout, Shutdown, and Reset Switch commands will also end an admin session.

- **cancel**
  
  Terminates an admin session opened by another user. Use this keyword with care because it terminates the admin session without warning the other user and without saving pending changes.

**Notes:** Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

**Examples:** The following example shows how to open and close an admin session.

```
FCSM: user1> admin start

FCSM: (admin) user1>
```

```
.
.
.
FCSM (admin): user1> admin end
FCSM: user1>
```
**Alias command**

Creates a named set of ports. Aliases make it easier to assign a set of ports to many zones. An alias cannot have a zone or another alias as a member.

**Authority:** Admin

**Syntax:**

```plaintext
alias
   add [alias] [members]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
   members [alias]
remove [alias] [members]
rename [alias_old] [alias_new]
```

**Keywords:**

**add [alias] [members]**

Specifies one or more ports given by [members] to add to the alias named [alias]. An alias can have a maximum of 2000 members. [members] can have one of the following formats:

- Domain ID and port number pair (domain ID, port number). Domain IDs and port numbers are in decimal format. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)

The application verifies that the [alias] format is correct but does not validate that such a port exists.

**copy [alias_source] [alias_destination]**

Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

**create [alias]**

Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, &, _, and -. The zoning database supports a maximum of 256 aliases.

**delete alias**

Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

**list**

Displays a list of all aliases. This keyword is valid for User authority and does not require a zoning edit session or an admin session.

**members [alias]**

Displays all members of the alias given by [alias]. This keyword is available with User authority and does not require a zoning edit session or an admin session.

**remove [alias] [members]**

Removes the ports given by [members] from the alias given by [alias]. [members] can have one of the following formats:

- Domain ID and port number pair (domain ID, port number). Domain IDs and port numbers are in decimal format. Ports are numbered beginning with 0.
• 6-character hexadecimal device Fibre Channel address (hex)

rename [alias_old] [alias_new]
Renames the alias given by [alias_old] to the alias given by [alias_new].
**Config command**
Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, see the "Set Config command" on page 28.

**Authority:** Admin for all keywords except List

**Syntax:**
```
cfg
  activate [config]
  backup
  cancel
  copy [config_source] [config_destination]
  delete [config]
  edit [config]
  list
  restore
  save [config]
```

**Keywords:**

**activate [config]**
Activates the configuration given by [config]. If you omit the configuration, the currently active configuration is used. Only one configuration can be active at a time.

**backup**
Creates a file named `configdata`, which contains the configuration information. To download this file, open a File Transfer Protocol (FTP) session, log in with account name of `images` and password of `images`, and type `get configdata`.

**cancel**
Terminates the current configuration edit session without saving changes that were made.

**copy [config_source] [config_destination]**
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

**delete [config]**
Deletes the specified configuration file where [config] is a file name.

**edit [config]**
Opens an edit session for the configuration given by [config]. If you omit the configuration name, the currently active configuration is used.

**list**
Displays a list of all available configurations. This keyword is available with User authority.

**restore**
Restores configuration settings to an out-of-band switch from a backup file named `configdata`, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, and then enter the Config Restore command.

**save [config]**
Saves changes made during a configuration edit session in the configuration
given by [config]. If you omit the configuration name value, the configuration you chose for the Config Edit command is used.

**Notes:** If you edit the active configuration, changes will be suspended until you reactivate the configuration or activate another configuration.

**Examples:** The following shows an example of how to open and close a Config Edit session.

```plaintext
FCSM: user1> admin start

FCSM (admin) : user1> config edit
.
.
.
FCSM (admin-config) : user1> config cancel

Configuration mode will be canceled. Please confirm (y/n): [n] y

FCSM (admin) : user1> admin end
```
**Date command**
Displays or sets the blade server date and time. To set the date and time, you must provide the information string in this format: `MMDDhhmmCCYY`, where `MM` = month, `DD` = day, `hh` = hour, `mm` = minute, `CC` = century, and `YY` = year. You must reset the switch for the new date to take effect.

**Authority:** Admin to change the date; user to display the date.

**Syntax:**
date

```bash
[MMDDhhmmCCYY]
```

**Keywords:**

`[MMDDhhmmCCYY]`

Specifies the date – this requires an admin session. If you omit `[MMDDhhmmCCYY]`, the current date is displayed – this is available with User authority.

**Examples:** The following is an example of the Date command.

```
FCSM: user1> date
Thu Sep 26 07:51:24 2002
```
**Fallback command**

Loads the fallback version of the firmware from switch memory. The switch stores two versions of the firmware. This command alternately activates the two versions.

*Authority:*  Admin

*Syntax:*

```
fallback
```

*Notes:*

- The Show Switch command displays the available firmware versions and the currently active version.
- After running the Fallback command, reset the switch for the firmware to be in effect.

*Examples:* The following is an example of the Fallback command.

```
FCSM: user1> admin start
FCSM (admin) : user1> fallback
  Reverting to previous software image. Please confirm (y/n): [n] y
FCSM: user1> admin end
FCSM: user1>
```
Help command
Displays a brief description of the specified command and its keywords.

Authority: User

Syntax:
help
   [command]
   [keyword]

Keywords:
[command]
   A command name. If you omit this value, all available commands from which to choose are displayed.

[keyword]
   A keyword associated with the command named by [command]. If you omit this value, available keywords for the specified command are displayed.

all  Displays a list of all available commands (including command variations).

Examples: The following is an example of the Help Set command.
FCSM: user1> help set
   set SET_OPTIONS
   There are many attributes that can be set.
   Type help with one of the following to get more information:
      set alarm
      set beacon
      set blade
      set config blade
      set config port
      set config ports
      set config switch
      set config threshold
      set config zoning
      set log
      set pagebreak
      set port
      set setup snmp
      set setup system
      set switch

The following is an example of the Help Set Beacon command.
FCSM: user1> help set beacon
   set beacon On | Off
   This command allows the lights on the front of the switch to flash.
   The On option will start and the Off option will stop the flashing.
**History command**  
Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

**Authority:** User

**Syntax:**

`history`

**Notes:**  Use the History command to provide context for the `!` command.
- Enter `![command]` to re-enter the most recent execution of that command.
- Enter `![line number]` to re-execute the corresponding command from the History display.
- Enter `![partial command string]` to re-execute a command that matches the command string.
- Enter `!!` to re-execute the most recent command.

**Examples:** The following is an example of the History command.

FCSM: user1> history  
  1 show switch  
  2 date  
  3 help set  
  4 history  

FCSM: user1> !2  
  date  

Thu Sep 26 11:03:07 2002
**Image command**
Manages and installs switch firmware.

*Authority:* Admin

*Syntax:*

```
image
  cleanup
  fetch [account_name] [ip_address] [file_source] [file_destination]
  list
  unpack [file]
```

*Keywords:*

- **cleanup**
  Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

- **fetch [account_name] [ip_address] [file_source] [file_destination]**
  Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the device with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the device, you are prompted for it.

- **list**
  Displays the list of image files that reside on the switch.

- **unpack [file]**
  Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

**Lip command (for external ports only)**
Reinitializes the specified loop port.

*Authority:* Admin

*Syntax:*

```
lip
  [port_number]
```

*Keywords:*

- **[port_number]**
  The number of the port to be reinitialized.

*Examples:* The following is an example of the Lip command.

```
FCSM (admin) : user1> lip 2
```
**Passwd command**  
Changes the password for a user account.

**Authority:** Admin to change the password for another account; user to change your own.

**Syntax:**

```
passwd
   [account_name]
```

**Keywords:**

[account_name]  
The user account name. You must open an admin session to change the password for an account name other than your own. If you omit [account_name], you are prompted to change the password for the current account name.

**Examples:** The following is an example of the Passwd command.

FCSM (admin) : user1> passwd user2

   Press 'q' and the ENTER key to abort this command.

   account OLD password : 
   account NEW password (4-20 chars) :

   please confirm account NEW password:

   password has been changed.

**Note:** If you lose the password for the account, contact IBM Support (see Appendix A, “Getting help and technical assistance”, on page 159).
**Ps command**  
Displays current blade server process information.

**Authority:** User

**Syntax:**

```
ps
```

**Examples:** The following is an example of the Ps command.

```
FCSM: user1> ps
           PID  PPID  %CPU TIME ELAPSED COMMAND
           341   329   0.0 00:00:00 2-00:58:29 cns
           342   329   0.0 00:00:02 2-00:58:29 ens
           343   329   0.0 00:00:27 2-00:58:29 dlog
           344   329  1.3 00:40:39 2-00:58:29 ds
           345   329  1.4 00:41:38 2-00:58:29 mgmtApp
           346   329   0.0 00:00:06 2-00:58:29 fc2
           347   329  0.5 00:16:35 2-00:58:29 nserver
           348   329  0.4 00:12:20 2-00:58:29 mserver
           349   329  3.6 01:47:29 2-00:58:29 util
           350   329   0.0 00:00:36 2-00:58:29 snmpservicepath
           351   329  0.5 00:15:24 2-00:58:29 eport
           352   329   0.0 00:00:05 2-00:58:29 PortApp
           353   329   0.0 00:00:08 2-00:58:28 port_mon
           354   329  0.2 00:07:14 2-00:58:28 zoning
           355   329   0.0 00:00:00 2-00:58:28 diagApp
           356   329   0.0 00:00:02 2-00:58:18 snmpd
           357   329   0.0 00:00:00 2-00:58:18 snmpmain
```
Quit command
Closes the Telnet session.

**Authority:** User

**Syntax:**
quit, exit, or logout
Reset command
Resets the switch and port configuration parameters.

**Authority:** Admin

**Syntax:**
```
reset
config [config_name]
factory
port [port_number]
snmp
switch (default)
system
zoning
```

**Keywords:**

- `config [config_name]`  
  Resets the configuration given by `[config_name]` to the factory default values for switch, port, alarm threshold, and zoning configuration. This keyword clears all zoning definitions. If `[config_name]` does not exist on the switch, a configuration with that name is created. If you omit `[config_name]`, the active configuration is reset. You must activate the configuration or reset the switch for the changes to take effect. See [Table 2](#) through [Table 4 on page 23](#).

- `factory`  
  Resets switch, alarm threshold, port, SNMP, zoning configuration, and blade server configuration settings to the factory default values. The switch configuration is activated automatically. See [Table 2](#) through [Table 6 on page 24](#).

- `port [port_number]`  
  Reinitializes the port given by `[port_number]`. Ports are numbered beginning with 0. For more information, see [Table 37 on page 122](#).

- `snmp`  
  Resets the SNMP configuration settings to the factory default values. See [Table 5 on page 24](#) for SNMP configuration default values.

- `switch`  
  Reinitializes the switch. This is the default. This command also closes the Telnet session.

- `system`  
  Resets the blade server configuration settings to the factory default values. See [Table 6 on page 24](#) for configuration default values.

- `zoning`  
  Clears the zoning database and deactivates the active zone set. The zoning configuration values remain unchanged.

**Notes:** The following tables specify the various factory default settings.

*Table 2. Switch configuration defaults*

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Online</td>
</tr>
<tr>
<td>Broadcast Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Inband Enable</td>
<td>True</td>
</tr>
</tbody>
</table>
### Table 2. Switch configuration defaults (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain ID</td>
<td>1</td>
</tr>
<tr>
<td>Domain ID Lock</td>
<td>False</td>
</tr>
<tr>
<td>Symbolic Name</td>
<td>Fibre Channel Switch Module</td>
</tr>
<tr>
<td>R_T_TOV</td>
<td>100</td>
</tr>
<tr>
<td>R_A_TOV</td>
<td>10000</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>2000</td>
</tr>
<tr>
<td>FS_TOV</td>
<td>5000</td>
</tr>
<tr>
<td>DS_TOV</td>
<td>5000</td>
</tr>
<tr>
<td>Principal Priority</td>
<td>254</td>
</tr>
<tr>
<td>System Description</td>
<td>IBM BladeCenter 2-Port Fibre Channel Switch Module</td>
</tr>
<tr>
<td>Configuration Last Saved By</td>
<td>Initial</td>
</tr>
<tr>
<td>Configuration Last Saved On</td>
<td>Initial</td>
</tr>
</tbody>
</table>

### Table 3. Port configuration defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>External port (0,15) default</th>
<th>Internal port (1-14) default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Online</td>
<td>Online</td>
</tr>
<tr>
<td>Link Speed</td>
<td>Auto</td>
<td>2 Gbps</td>
</tr>
<tr>
<td>Port Type</td>
<td>GL</td>
<td>F</td>
</tr>
<tr>
<td>TL_Port Mode</td>
<td>TLTARGETMODE</td>
<td>TLTARGETMODE</td>
</tr>
<tr>
<td>ISL Security</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Symbolic Name</td>
<td>Port0 or Port15</td>
<td>Port1 – Port14</td>
</tr>
<tr>
<td>ALFairness</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>ARB_FF</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>InteropCredit</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ExtCredit</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FanEnable</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>LCFEnable</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>MFSEnable</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>MFS_TOV</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>MSEnable</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>NoClose</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>IOSStreamGuard</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>VIEnable</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>CheckAlps</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>

### Table 4. Threshold configuration defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThresholdMonitoringEnabled</td>
<td>True</td>
</tr>
</tbody>
</table>
Table 4. Threshold configuration defaults (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRCErrorsMonitoringEnabled</td>
<td>25</td>
</tr>
<tr>
<td>RisingTrigger</td>
<td>1</td>
</tr>
<tr>
<td>FallingTrigger</td>
<td>10</td>
</tr>
<tr>
<td>SampleWindow</td>
<td></td>
</tr>
<tr>
<td>DecodeErrorsMonitoringEnabled</td>
<td>200</td>
</tr>
<tr>
<td>RisingTrigger</td>
<td>0</td>
</tr>
<tr>
<td>FallingTrigger</td>
<td>10</td>
</tr>
<tr>
<td>SampleWindow</td>
<td></td>
</tr>
<tr>
<td>ISLMonitoringEnabled</td>
<td>2</td>
</tr>
<tr>
<td>RisingTrigger</td>
<td>0</td>
</tr>
<tr>
<td>FallingTrigger</td>
<td>10</td>
</tr>
<tr>
<td>SampleWindow</td>
<td></td>
</tr>
<tr>
<td>LoginMonitoringEnabled</td>
<td>5</td>
</tr>
<tr>
<td>RisingTrigger</td>
<td>1</td>
</tr>
<tr>
<td>FallingTrigger</td>
<td>10</td>
</tr>
<tr>
<td>SampleWindow</td>
<td></td>
</tr>
<tr>
<td>LogoutMonitoringEnabled</td>
<td>5</td>
</tr>
<tr>
<td>RisingTrigger</td>
<td>1</td>
</tr>
<tr>
<td>FallingTrigger</td>
<td>10</td>
</tr>
<tr>
<td>SampleWindow</td>
<td></td>
</tr>
<tr>
<td>LOSMonitoringEnabled</td>
<td>100</td>
</tr>
<tr>
<td>RisingTrigger</td>
<td>5</td>
</tr>
<tr>
<td>FallingTrigger</td>
<td>10</td>
</tr>
<tr>
<td>SampleWindow</td>
<td></td>
</tr>
</tbody>
</table>

Table 5. SNMP configuration defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Undefined</td>
</tr>
<tr>
<td>Location</td>
<td>Undefined</td>
</tr>
<tr>
<td>Description</td>
<td>Undefined</td>
</tr>
<tr>
<td>Trap [1] Address</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>Trap [2-5] Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Trap [1-5] Port</td>
<td>162</td>
</tr>
<tr>
<td>Trap [1-5] Severity</td>
<td>Warning</td>
</tr>
<tr>
<td>Trap [1-5] Enabled</td>
<td>False</td>
</tr>
<tr>
<td>ObjectID</td>
<td>1.3.6.1.4.1.1663.1.1.1.1.1.16</td>
</tr>
<tr>
<td>AuthFailureTrap</td>
<td>False</td>
</tr>
</tbody>
</table>

Table 6. System configuration defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Network IP Address</td>
<td>Switch module bay 3: 192.168.70.129</td>
</tr>
<tr>
<td></td>
<td>Switch module bay 4: 192.168.70.130</td>
</tr>
<tr>
<td>Ethernet Network IP Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Ethernet Gateway Address</td>
<td>10.90.90.254</td>
</tr>
<tr>
<td>Ethernet Network Discovery</td>
<td>Static</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Admin Timeout</td>
<td>30 minutes</td>
</tr>
<tr>
<td>Security Enabled</td>
<td>False</td>
</tr>
<tr>
<td>Local Log Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Remote Log Enabled</td>
<td>False</td>
</tr>
<tr>
<td>Remote Log Host IP Address</td>
<td>10.0.0.254</td>
</tr>
</tbody>
</table>

Table 6. System configuration defaults (continued)
Set command
Sets a variety of port and switch parameters.

Authority: Admin for all keywords except Alarm Clear, Beacon, and Pagebreak which are available with User authority.

Syntax:
set
alarm clear
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]

Keywords:
alarm clear
Clears the alarm log. This keyword is available with User authority.

beacon [state]
Enables or disables the flashing of the Port Logged-in LEDs according to [state]. This keyword is available with User authority. [state] can be one of the following:

On
  Enables the flashing beacon.

Off
  Disables the flashing beacon.

cfg [option]
Sets port, switch, alarm threshold, and zoning configuration parameters. See the “Set Config command” on page 28

log [option]
Specifies the type of entries to be entered in the event log. See the “Set Log command” on page 34

pagebreak [state]
Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword is available with User authority. [state] can be one of the following:

on
  Limits the display of information to 20 lines at a time.

off
  Allows continuous display of information without a break.

port [option]
Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. See the “Set Port command” on page 36

setup [option]
Changes SNMP and blade server configuration settings. See the “Set Setup command” on page 38

switch [state]
Temporarily changes the administrative state for all ports on the switch to the
state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

Online
   Places all ports online

Offline
   Places all ports offline.

Diagnostics
   Prepares all ports for testing.
Set Config command
Sets port, switch, alarm threshold, and zoning configuration parameters.

Authority: Admin authority and a Config Edit session. See the "Config command" on page 12 for information about starting a Config Edit session.

Syntax:
set config
  port [port_number]
  ports [port_number]
  switch
  threshold
  zoning

Keywords:
port [port number]
Initiates an editing session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the BladeCenter unit begins with port 0 and proceeds in order through port 15. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Type q to cancel the configuration for one port, or qq to cancel the configuration for all ports. Table 7 describes the port parameters.

Note: For external ports (0,15), all port parameters apply. For internal ports, only the port state setting is configurable. For information about port numbering and mapping, see Table 37 on page 122.

port [port number]
Initiates an editing session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the BladeCenter unit begins with port 0 and proceeds in order through port 15. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Type q to cancel the configuration for one port, or qq to cancel the configuration for all ports. Table 7 describes the port parameters.

Note: For external ports (0,15), all port parameters apply. For internal ports, only the port state setting is configurable. For information about port numbering and mapping, see Table 37 on page 122.

ports [port number]
Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Type q to cancel the configuration. Table 7 describes the port parameters. For external ports (0,15), all parameters apply. For internal ports (1 through 14) only AdminState applies.

Table 7. Set Config port parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminState</td>
<td>Port administrative state: online, offline, diagnostics, or down.</td>
</tr>
<tr>
<td>LinkSpeed</td>
<td>1 Gbps or 2 Gbps</td>
</tr>
<tr>
<td>PortType</td>
<td>Type of port</td>
</tr>
</tbody>
</table>
Table 7. Set Config port parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLPortMode</td>
<td>Initiates the configuration of external ports attributes. Indicates whether using initiator or target devices on the loop. If you specify [port_number], the display will present attributes for that port only; otherwise, all attributes for all ports will be available for configuration.</td>
</tr>
</tbody>
</table>
| ISLSecurity    | E_Port security. Determines which switches a port will establish a link with.  
|                |  - Any - Will link with any switch.  
|                |  - Ours - Will link only to another BladeCenter Fibre Channel switch module.  
|                |  - None - The port will not establish an ISL link.                                                                                   |
| SymbolicPortName | Descriptive name                                                                                                                            |
| ALFairness     | Default is switch that has priority                                                                                                       |
| ARB_FF         | Use ARB_FF instead of idles on loop FCAL option                                                                                          |
| InteropCredit  | Number of buffer-to-buffer credits per port. 0 means the default (12) is unchanged.                                                        |
| ExtCredit      | Extended credit port                                                                                                                     |
| FANEnable      | Fabric Address Notification. If enabled, notifies logged-in NL_Ports of the FL_Port address, port name, and node name.                     |
| LCFEnable      | Link control frame preference, R_CTL = 0xC                                                                                               |
| MFSEnable      | Multi-frame sequence bundling                                                                                                             |
| MFS_TOV        | MFS limit for camp on                                                                                                                    |
| MSEnable       | Management Server enable on this port                                                                                                    |
| NoClose        | Do not close unless another device arbitrates                                                                                             |
| I/O Stream Guard | Enables or disables the suppression of RSCN messages                                                                                     |
| IVIEnable      | Not applicable                                                                                                                           |
| CheckAlps      | Close before sending frames to new target                                                                                                |

**switch**

Initiates an editing session in which to change switch configuration settings. Each parameter is displayed, one line at a time and prompts you for a value. For each parameter, type a new value or press the Enter key to accept the current value shown in brackets. Type q to cancel the configuration.

Table 8. Set Config switch parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminState</td>
<td>Switch administrative state: online, offline, or diagnostics.</td>
</tr>
<tr>
<td>Broadcast Enable</td>
<td>Enables (True) or disables (False) forwarding if broadcasting frames.</td>
</tr>
</tbody>
</table>
Table 8. Set Config switch parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InbandEnabled</td>
<td>Enables (True) or disables (False) the ability to manage the switch over an ISL.</td>
</tr>
<tr>
<td>DefaultDomainID</td>
<td>Default domain ID setting.</td>
</tr>
<tr>
<td>DomainIDLock</td>
<td>Prevents (True) or allows (False) dynamic reassignment of the domain ID.</td>
</tr>
<tr>
<td>SymbolicName</td>
<td>Descriptive name</td>
</tr>
<tr>
<td>R_T_TOV</td>
<td>Receiver Transmitter Timeout Value. Specifies the number of milliseconds a port is to wait to receive a response from another port. The default is 100.</td>
</tr>
<tr>
<td>R_A_TOV</td>
<td>Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000 msec.</td>
</tr>
<tr>
<td>FS_TOV</td>
<td>Fabric Stability Timeout Value. The default is 5000 msec.</td>
</tr>
<tr>
<td>DS_TOV</td>
<td>Distributed Services Timeout Value (Management Server, Name Server). The default is 5000 msec.</td>
</tr>
<tr>
<td>PrincipalPriority</td>
<td>The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low.</td>
</tr>
<tr>
<td>ConfigDescription</td>
<td>The name for the configuration. The default is undefined.</td>
</tr>
</tbody>
</table>

threshold

Initiates a configuration session by which to generate and log alarms for selected events. Each event, its thresholds, and sampling interval is displayed, one line at a time and you are prompted for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. See the "Config command" on page 12 for information about saving and activating a configuration. Table 9 describes the Set Config threshold parameters.

Table 9. Set Config threshold parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold Monitoring Enabled</td>
<td>Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms.</td>
</tr>
<tr>
<td>CRCErrorsMonitoringEnabled</td>
<td>The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events:</td>
</tr>
<tr>
<td>DecodeErrorsMonitoringEnabled</td>
<td>• CRC errors</td>
</tr>
<tr>
<td>ISLMonitoringEnabled</td>
<td>• Decode errors</td>
</tr>
<tr>
<td>LoginMonitoringEnabled</td>
<td>• ISL connection count</td>
</tr>
<tr>
<td>LogoutMonitoringEnabled</td>
<td>• Login errors</td>
</tr>
<tr>
<td>LOSMonitoringEnabled</td>
<td>• Logout errors</td>
</tr>
<tr>
<td></td>
<td>• Loss-of-signal errors</td>
</tr>
</tbody>
</table>
Table 9. Set Config threshold parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rising Trigger</td>
<td>The event count above which an event is logged. Once the count exceeds the rising threshold, one alarm is logged. The switch will not generate another alarm for that event until the count falls below the falling threshold.</td>
</tr>
<tr>
<td>Falling Trigger</td>
<td>The event count above which an event becomes eligible for logging in the alarm log.</td>
</tr>
<tr>
<td>Sample Window</td>
<td>The period of time in seconds in which to count events.</td>
</tr>
</tbody>
</table>

**zoning**

Initiates an editing session in which to change switch zoning attributes. Each parameter is displayed, one line at a time, and you are prompted for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table 10. Set Config zoning parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoSave</td>
<td>Determines whether zoning changes will be saved to flash (nonvolatile) memory (On) or to RAM (volatile) (Off). The default is On.</td>
</tr>
<tr>
<td>Default</td>
<td>Determines communication among ports/devices in the absence of an active zone set. “All” enables all ports/devices to communicate with one another. “None” prohibits communication among ports/devices.</td>
</tr>
</tbody>
</table>

**Examples:** The following is an example of the Set Config Port command.

FCSM: user1> admin start
FCSM (admin) : user1> config edit
FCSM (admin-config) : user1> set config port 0

A list of attributes with formatting and current values will follow. Enter a new value or simply press the ENTER key to accept the current value. If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.

Configuring Port Number: 0

----------------------------------------
| AdminState          | (1=Online, 2=Offline, 3=Diagnostics, 4=Down) | [Online]   |
| LinkSpeed           | (1=1Gb/s, 2=2Gb/s, 3=Auto) | [Auto]     |
| PortType            | (TL / GL / G / F / FL / Donor) | [GL]       |
| TLPortMode          | (1=TLTargetMode, 2=TLInitiatorMode) | [TLTargetMode] |
| ISLSecurity         | (Any / Ours / None) | [Any]      |
| SymPortName         | (string, max=32 chars) | [Port0]    |
| ALFairness          | (True / False) | [False]    |
| ARB_FF              | (True / False) | [False]    |
| InteropCredit       | (decimal value, 0-255) | [0]        |
| ExtCredit           | (dec value, increments of 11, non-loop only) | [0]        |
| FANEnable           | (True / False) | [True]     |
| LCFEnable           | (True / False) | [False]    |
| MFSEnable           | (True / False) | [True]     |

Chapter 2. BladeCenter 2-Port Fibre Channel Switch Module 31
Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

The following is an example of the Set Config Switch command.
FCSM: user1> admin start
FCSM (admin) : user1> config edit
FCSM (admin-config) : user1> set config switch

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

AdminState (1=Online, 2=Offline, 3=Diagnostics) [Online]
InbandEnabled (True / False) [True]
DefaultDomainID (decimal value, 1-239) [1]
SymbolicName (string, max=32 chars) [Fibre Channel Switch Module]
R_T_TOV (decimal value, 1-1000 msec) [100]
E_D_TOV (decimal value, 10-20480 msec) [2000]
FS_TOV (decimal value, 100-100000 msec) [5000]
DS_TOV (decimal value, 100-100000 msec) [5000]
PrincipalPriority (decimal value, 1-255) [254]
ConfigDescription (string, max=64 chars) [IBM BladeCenter(TM) 2-port
Fibre Channel Switch Module]

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

The following is an example of the Set Config Threshold command.
FCSM (admin-config) : user1> set config threshold

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

ThresholdMonitoringEnabled (True / False) [False]
CRC Errors Monitoring Enabled (True / False) [False]
RisingTrigger (decimal value, 1-1000) [25]
FallingTrigger (decimal value, 0-1000) [1]
SampleWindow (decimal value, 1-1000 sec) [10]
Decode Errors Monitoring Enabled (True / False) [True]
RisingTrigger (decimal value, 1-1000) [200]
FallingTrigger (decimal value, 0-1000) [0]
SampleWindow (decimal value, 1-1000 sec) [10]
ISL Monitoring Enabled (True / False) [True]
RisingTrigger (decimal value, 1-1000) [2]
FallingTrigger (decimal value, 0-1000) [0]
SampleWindow (decimal value, 1-1000 sec) [10]
Login Monitoring Enabled (True / False) [True]
RisingTrigger (decimal value, 1-1000) [5]
FallingTrigger (decimal value, 0-1000) [1]
SampleWindow (decimal value, 1-1000 sec) [10]

LogoutMonitoringEnabled (True / False) [True]
RisingTrigger (decimal value, 1-1000) [5]
FallingTrigger (decimal value, 0-1000) [1]
SampleWindow (decimal value, 1-1000 sec) [10]

LOSMonitoringEnabled (True / False) [True]
RisingTrigger (decimal value, 1-1000) [100]
FallingTrigger (decimal value, 0-1000) [5]
SampleWindow (decimal value, 1-1000 sec) [10]

The following is an example of the Set Config Zoning command.

FCSM: user1> admin start
FCSM (admin) : user1> config edit
FCSM (admin-config) : user1> set config zoning

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

AutoSave (True / False) [True]
Default (All / None) [All]

Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
Set Log command
Specifies the type of entries to be entered in the event log. The log is a storage file contained on the switch. The log can hold a maximum of 200 entries. When the log becomes full, the entries are replaced, starting with the oldest entry, to produce a list of the last 200 events which occurred. Log entries are created for ports, components, and event severity levels.

**Authority:** Admin

**Syntax:**

```plaintext
set log
  archive
  clear
  component [list]
  level [level]
  port [port_list]
  restore
  save
  start (default)
  stop
```

**Keywords:**

**archive**
Archives the log entries to a file on the switch named `logfile` that can be downloaded from the switch using FTP. To download the log file, open an FTP session, log in with an account name of `images` and password of `images`, and type `get logfile`.

**clear**
Clears all log entries.

**component [list]**
Specifies one or more components to monitor for events. Use spaces to delimit values in the list. Use one or more of the following values:

- **All** Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.
- **Blade** Not applicable
- **Chassis** Not applicable
- **Eport** Monitors all E_Ports.
- **Mgmtserver** Monitors management server status.
- **Nameserver** Monitors name server status.
- **None** Monitors none of the component events.
- **Other** Monitors other miscellaneous events.
Port
  Monitors all port events.

Switch
  Monitors switch management events.

Zoning
  Monitors zoning conflict events.

level [level]
  Specifies the severity level given by [level] to use in monitoring events for the
  specified components or ports. [level] can be one of the following values:

  Critical
    Monitors critical events.

  Warn
    Monitors warning events.

  Info
    Monitors informational events. To maintain optimal switch performance, do
    not use this setting with the Component keyword set to All.

  None
    Monitors none of the severity levels.

port [port_list]
  Specifies one or more ports to monitor for events. Use one of the following
  values:

  [port_list]
    Specifies port or ports to monitor. Use spaces to delimit values in the list.
    Ports are numbered beginning with 0.

  All
    Specifies all ports.

  None
    Disables monitoring on all ports.

restore
  Returns the port, component, and level settings to the default values.

save
  Saves the log settings for the component, level, and port. These settings remain
  in effect after a switch reset. The log settings can be viewed using the Show
  Log Settings command. To export log entries to a file, use the Set Log Archive
  command.

start
  Starts the logging of events based on the Port, Component, and Level
  keywords assigned to the current configuration. The logging continues until you
  enter the Set Log Stop command.

stop
  Stops logging of events.

Notes: To maintain optimal switch performance, do not set the Component
  keyword to All and the Level keyword to Info at the same time.
Set Port command
Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters. For information about port numbering and mapping, see Table 37 on page 122.

Note: For external ports (0,15), all port parameters apply. For internal ports, only the port state setting is configurable.

Authority: Admin

Syntax:
set port [port_number]
  • bypass [alpa] (for external ports only)
  • clear
  • enable [alpa] (for external ports only)
  • speed [transmission_speed]
  • state [state]

Keywords:
[port_number]
  Specifies the port. Ports are numbered beginning with 0. For information about port numbering and mapping, see Table 37 on page 122.
bypass [alpa]
  Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.
clear
  Clears the counters on the specified port.
enable [alpa]
  Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.
speed [transmission_speed]
  Specifies the transmission speed for the specified port. Use one of the following port speed values:
  1Gbps
    One gigabit per second.
  2Gbps
    Two gigabits per second.
  Auto
    The port speed is automatically detected.
state [state]
  Specifies the administrative state for the specified port. Use one of the following port state values:
  Online
    Places the port online.
  Offline
    Places the port offline.
Diagnostics
   Prepares the port for testing.

Down
   Disables the port.
Set Setup command
Changes SNMP and blade server configuration settings. The switch maintains one SNMP configuration and one configuration.

**Authority:** Admin

**Syntax:**

```
set setup
    snmp
    system
```

**Keywords:**

**snmp**
Prompts you, line-by-line, to change SNMP configuration settings. Table 11 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Specifies the name of the person to be contacted to respond to trap events. The default is Undefined.</td>
</tr>
<tr>
<td>Location</td>
<td>Specifies the name of the switch location. The default is Undefined.</td>
</tr>
<tr>
<td>Trap [1-5] Address</td>
<td>Specifies the IP address to which SNMP traps are sent.</td>
</tr>
<tr>
<td>Trap [1-5] Port</td>
<td>Specifies the port for which SNMP traps are sent.</td>
</tr>
<tr>
<td>Trap [1-5] Severity</td>
<td>Specifies the severity level to use when monitoring trap events. The default is Warning.</td>
</tr>
<tr>
<td>Trap [1-5] Enabled</td>
<td>Specifies whether traps (event information) are enabled or disabled (default).</td>
</tr>
<tr>
<td>ReadCommunity</td>
<td>Read Community Authentication. A write-only field; the value on the switch and the SNMP management server must be the same.</td>
</tr>
<tr>
<td>WriteCommunity</td>
<td>Write Community Authentication. A write-only field; the value on the switch and the SNMP management server must be the same.</td>
</tr>
<tr>
<td>TrapCommunity</td>
<td>Trap Community Authentication. A write-only field; the value on the switch and the SNMP management server must be the same.</td>
</tr>
<tr>
<td>AuthFailureTrap</td>
<td>Specifies the IP address where a notification is sent in the event of an authentication failure.</td>
</tr>
</tbody>
</table>

**system**
Prompts you, line-by-line, to change blade server configuration settings. Table 12 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0NetworkAddress</td>
<td>Ethernet Internet protocol (IP) address</td>
</tr>
<tr>
<td>Eth0NetworkMask</td>
<td>Ethernet subnet mask address for the Ethernet port.</td>
</tr>
<tr>
<td>Eth0GatewayIPAddress</td>
<td>Ethernet IP address gateway</td>
</tr>
</tbody>
</table>
Table 12. System configuration settings (continued)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth0NetworkDiscovery</td>
<td>Ethernet boot method (1 - Static).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> BootP, DHCP, and RARP do not apply</td>
</tr>
<tr>
<td>AdminTimeout</td>
<td>Specifies the amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30; the maximum is 1440.</td>
</tr>
<tr>
<td>Security Enabled</td>
<td>Enables or disables the enforcement of account names and passwords.</td>
</tr>
<tr>
<td>Remote Log Enabled</td>
<td>Whether remote logging is enabled or disabled. If enabled, log information is saved to a remote host that supports the systole protocol.</td>
</tr>
<tr>
<td>RemoteLogHost IP Address</td>
<td>The IP address of the host that will receive the remote log information if remote logging is enabled.</td>
</tr>
</tbody>
</table>

**Notes:** The two components of security are user authentication and fabric security. The user must be authenticated before gaining access to a switch. If an invalid account name/password combination is entered, that user can not access the switch, and thus cannot gain access to the fabric. If security is enabled (True) and a valid account name/password combination is entered, that user can access the switch but can not execute any command that exceeds their authority (privileges) level. If security is disabled (False) and a valid account name/password combination is entered, that user has access to all switches in the fabric and can execute all commands (both user and admin), regardless of their authority (privileges) level.

**Examples:** The following is an example of the Set Setup SNMP command.

FCSM: user1> admin start
FCSM (admin) : user1> set setup snmp
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.

**Trap Severity Options**
---------------------
unknown, emergency, alert, critical, error, warning, notify, info, debug, mark

<table>
<thead>
<tr>
<th>Contact</th>
<th>(string, max&lt;32 chars)</th>
<th>&lt;sysContact undefined&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>(string, max&lt;32 chars)</td>
<td>&lt;sysLocation undefined&gt;</td>
</tr>
<tr>
<td>Trap1Address</td>
<td>(dot-notated IP Address)</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>Trap1Port</td>
<td>(decimal value)</td>
<td>162</td>
</tr>
<tr>
<td>Trap1Severity</td>
<td>(see allowed options above)</td>
<td>warning</td>
</tr>
<tr>
<td>Trap1Enabled</td>
<td>(True / False)</td>
<td>False</td>
</tr>
<tr>
<td>Trap2Address</td>
<td>(dot-notated IP Address)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Trap2Port</td>
<td>(decimal value)</td>
<td>162</td>
</tr>
<tr>
<td>Trap2Severity</td>
<td>(see allowed options above)</td>
<td>warning</td>
</tr>
<tr>
<td>Trap2Enabled</td>
<td>(True / False)</td>
<td>False</td>
</tr>
<tr>
<td>Trap3Address</td>
<td>(dot-notated IP Address)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Trap3Port</td>
<td>(decimal value)</td>
<td>162</td>
</tr>
<tr>
<td>Trap3Severity</td>
<td>(see allowed options above)</td>
<td>warning</td>
</tr>
<tr>
<td>Trap3Enabled</td>
<td>(True / False)</td>
<td>False</td>
</tr>
<tr>
<td>Trap4Address</td>
<td>(dot-notated IP Address)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Trap4Port</td>
<td>(decimal value)</td>
<td>162</td>
</tr>
<tr>
<td>Trap4Severity</td>
<td>(see allowed options above)</td>
<td>warning</td>
</tr>
<tr>
<td>Trap4Enabled</td>
<td>(True / False)</td>
<td>False</td>
</tr>
<tr>
<td>Trap5Address</td>
<td>(dot-notated IP Address)</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Trap5Port</td>
<td>(decimal value)</td>
<td>162</td>
</tr>
<tr>
<td>Trap5Severity</td>
<td>(see allowed options above)</td>
<td>warning</td>
</tr>
<tr>
<td>Trap5Enabled</td>
<td>(True / False)</td>
<td>False</td>
</tr>
<tr>
<td>Trap6Address</td>
<td>(dot-notated IP Address)</td>
<td></td>
</tr>
<tr>
<td>Trap6Port</td>
<td>(decimal value)</td>
<td></td>
</tr>
<tr>
<td>Trap6Severity</td>
<td>(see allowed options above)</td>
<td></td>
</tr>
<tr>
<td>Trap6Enabled</td>
<td>(True / False)</td>
<td>False</td>
</tr>
</tbody>
</table>
The following is an example of the Set Setup System command.

FCSM: user1> admin start
FCSM (admin) : user1> set setup system

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

- Eth0NetworkAddress (dot-notated IP Address) [10.90.10.93]
- Eth0NetworkMask (dot-notated IP Address) [255.255.252.0]
- Eth0GatewayAddress (dot-notated IP Address) [10.20.8.254]
- Eth0NetworkDiscovery (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp) [Static]
- AdminTimeout (dec value 0-1440 minutes, 0=never) [30]
- SecurityEnabled (True / False) [False]
- LocalLogEnabled (True / False) [True]
- RemoteLogEnabled (True / False) [False]
- RemoteLogHostAddress (dot-notated IP Address) [10.0.0.254]

Do you want to save and activate this system setup? (y/n): [n]
Show command
Displays fabric, switch, and port operational information.

Authority: User

Syntax:
show

about
alarm
broadcast
chassis
cfg

domains
donor
fabric
interface
log [option]
lsdb
mem [count]
ns [option]
pagbreak
perf [option]
port [port_number]
post log
setup [option]
steering [domain_id]
support
switch
topology
users
version

Keywords:
about
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the Version keyword.

alarm
Displays the last 200 alarm entries.

broadcast
Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis
Not applicable

config [option]
Displays switch and port configuration attributes. For more information, see the “Show Config command” on page 48
domains
Displays a list of each domain and its worldwide name in the fabric.

donor
Displays list of current donor configuration for all ports.

fabric
Displays list of each domain, fabric ID, worldwide name, node IP address, port IP address, and symbolic name in the fabric.

interface
Displays the status of the active network interfaces.

log [option]
Displays log entries. See the “Show Log command” on page 50.

lsdb
Displays Link State database information.

mem [count]
Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in units of 1 KB.

Note: This keyword will display memory activity updates until [count] is reached; it cannot be interrupted. Therefore, avoid using large values for [count].

ns [option]
Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all Displays name server information for all switches and ports.
[domain_id]
Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.
[port_id]
Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak
Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

perf [option]
Displays performance information for all ports. See the “Show Perf command” on page 52.

port [port_number]
Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If the port number is omitted, information is displayed for all ports. Table 13 on page 43 describes the port parameters. For information about port numbering and mapping, see Table 37 on page 122.

Note: For external ports (0,15), all parameters apply. For internal ports (1 through 14) only AdminState applies.
<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alinit</td>
<td>Incremented each time the port begins AL initialization.</td>
</tr>
<tr>
<td>AlinitError</td>
<td>Number of times the port entered initialization and the initialization failed.</td>
</tr>
<tr>
<td>ClassXFramesIn</td>
<td>Number of class x frames received by this port.</td>
</tr>
<tr>
<td>ClassXFramesOut</td>
<td>Number of class x frames sent by this port.</td>
</tr>
<tr>
<td>ClassXWordsIn</td>
<td>Number of class x words received by this port.</td>
</tr>
<tr>
<td>ClassXWordsOut</td>
<td>Number of class x words sent by this port.</td>
</tr>
<tr>
<td>DecodeError</td>
<td>Decoding error detected.</td>
</tr>
<tr>
<td>EpConnects</td>
<td>Number of times an E_Port connects through ISL negotiation.</td>
</tr>
<tr>
<td>FBusy</td>
<td>Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_port that is preventing delivery of this frame.</td>
</tr>
<tr>
<td>Flowerrors</td>
<td>Received a frame when there were no available credits.</td>
</tr>
<tr>
<td>FReject</td>
<td>Number of frames from devices that were rejected.</td>
</tr>
<tr>
<td>InvalidCRC</td>
<td>Invalid CRC detected.</td>
</tr>
<tr>
<td>InvalidDestAddr</td>
<td>Invalid destination address detected.</td>
</tr>
<tr>
<td>LIP ALPD ALPS</td>
<td>Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.</td>
</tr>
<tr>
<td>LIPF7ALPS</td>
<td>This LIP is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.</td>
</tr>
<tr>
<td>LIPF8ALPS</td>
<td>This LIP denotes a loop failure detected by the L_port identified by AL_PS.</td>
</tr>
<tr>
<td>LIPF7F7</td>
<td>A loop initialization primitive frame used to acquire a valid AL_PA.</td>
</tr>
<tr>
<td>LIPF8F7</td>
<td>A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.</td>
</tr>
<tr>
<td>Link Failures</td>
<td>Number of optical link failures detected by this port. A link failure is a loss of synchronization for a period of time greater than the value of R_T_TOV or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established by the time specified by R_T_TOV, a link failure is counted. A link reset is performed after a link failure.</td>
</tr>
<tr>
<td>Login</td>
<td>Time when user logged in.</td>
</tr>
<tr>
<td>Logout</td>
<td>Time when user logged out.</td>
</tr>
<tr>
<td>LoopTimeouts</td>
<td>A 2-second timeout as specified by FC-AL-2.</td>
</tr>
<tr>
<td>LossOfSync</td>
<td>Number of synchronization losses (&gt;100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.</td>
</tr>
<tr>
<td>PrimSeqErrors</td>
<td>Primitive sequence errors detected.</td>
</tr>
<tr>
<td>RxLinkResets</td>
<td>Number of link reset primitives received from an attached device.</td>
</tr>
</tbody>
</table>
Table 13. Show Port parameters (continued)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxOfflineSeq</td>
<td>Number of offline sequences received. An OLS is issued for link initialization, a Receive &amp; Recognize Not_Operational (NOS) state, or to enter the offline state.</td>
</tr>
<tr>
<td>TotalErrors</td>
<td>Total number of errors detected.</td>
</tr>
<tr>
<td>TotalLIPsRecvd</td>
<td>Number of loop initialization primitive frames received by this port.</td>
</tr>
<tr>
<td>TotalLinkResets</td>
<td>Total number of link reset primitives.</td>
</tr>
<tr>
<td>TotalOfflineSeq</td>
<td>Total number of Offline Sequences issued by this port.</td>
</tr>
<tr>
<td>TotalRxFrames</td>
<td>Total number of frames received by this port.</td>
</tr>
<tr>
<td>TotalRxWords</td>
<td>Total number of words received by this port.</td>
</tr>
<tr>
<td>TotalTxFrames</td>
<td>Total number of frames issued by this port.</td>
</tr>
<tr>
<td>TotalTxWords</td>
<td>Total number of words issued by this port.</td>
</tr>
<tr>
<td>TxLinkResets</td>
<td>Number of Link Resets issued by this port.</td>
</tr>
<tr>
<td>TxOfflineSeq</td>
<td>Total number of Offline Sequences issued by this port.</td>
</tr>
<tr>
<td>TxWait</td>
<td>Time waiting to transmit when blocked with no credit. Measured in FC Word times.</td>
</tr>
</tbody>
</table>

**post log**
Displays the POST log which contains results from the POST.

**setup [option]**
Displays setup attributes for the system, SNMP, and the switch manufacturer. See the "Show Setup command" on page 54.

**steering [domain_id]**
Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

**support**
Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The following commands are executed:

- Date
- Alias List
- Config List
- Date
- History
- Ps
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Switch, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts
- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

**switch**
Displays switch operational information.

**topology**
Displays all connected devices.

**users**
Displays a list of logged-in users. This is equivalent to the User List command.

**version**
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

**Examples:**
The following is an example of the Show Setup SNMP command.

FCSM: user1> show setup snmp

SNMP Information
----------------
Contact <sysContact undefined>
Location <sysLocation undefined>
Description IBM BladeCenter(TM) 2-port Fibre Channel Switch Module
Trap1Address 10.0.0.1
Trap1Port 162
Trap1Severity warning
Trap1Enabled False
Trap2Address 0.0.0.0
Trap2Port 162
Trap2Severity warning
Trap2Enabled False
Trap3Address 0.0.0.0
Trap3Port 162
Trap3Severity warning
Trap3Enabled False
Trap4Address 0.0.0.0
Trap4Port 162
Trap4Severity warning
Trap4Enabled False
Trap5Address 0.0.0.0
Trap5Port 162
Trap5Severity warning
Trap5Enabled False
ObjectID 1.3.6.1.4.1.1663.1.1.1.1.1.16
AuthFailureTrap False

The following is an example of the Show Topology command.

FCSM: user1> show topology

Unique ID Key
-------------
A = ALPA, D = Domain ID, P = Port ID

<table>
<thead>
<tr>
<th>Loc</th>
<th>Local</th>
<th>Rem</th>
<th>Remote</th>
<th>Unique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type PortWWN</td>
<td>Type NodeWWN</td>
<td>ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>------</td>
<td>--</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>Ext:15 E 20:0f:00:c0:dd:00:90:fb E 10:00:00:c0:dd:00:90:d74 (0x4) D</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following is an example of the Show Topology (for Port #15) command.

FCSM: user1> show topology 15

Local Link Information
----------------------
Port Ext2:15
PortID 020f00
PortWWN 20:0f:00:c0:dd:00:90:fb
Remote Link Information

<table>
<thead>
<tr>
<th>Remote Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortNumber 10</td>
</tr>
<tr>
<td>DomainID 04</td>
</tr>
<tr>
<td>NodeWWN 10:00:00:c0:dd:00:90:d7</td>
</tr>
<tr>
<td>PortType E</td>
</tr>
<tr>
<td>Description Switch</td>
</tr>
<tr>
<td>IPAddress 10.0.0.3</td>
</tr>
</tbody>
</table>

The following is an example of the Show Port command.

```
FCSM: user1> show port 0
Port Number: 0

AdminState: Online  PortID: 640000
AsicNumber: 0     PortWWN: 20:00:00:c0:dd:00:91:03
AsicPort: 0      RunningType: E
ConfigType: GL    SFPPartNumber: FTRJ-8519-3-2.5
DiagStatus: Passed    SFPRevision: X1
EpConnState: Connected    SFPType: 100-M5-SN-I
EpIsoReason: NotApplicable    SFPVendor: FINISAR CORP.
LinkSpeed: 2Gb/s    SFPVendorID: 00659000
LinkState: Active    SymbolicName: Port0
LoginStatus: LoggedIn    SyncStatus: SyncAcquired
MaxCredit: 12     XmitterEnabled: True
OperationalState: Online

ALInit: 11        FlowErrors: 0          PrimSeqErrors: 0
ALInitError: 1    FReject: 0             RxLinkResets: 0
Class2FramesIn: 0 InvalidCRC: 0          RxOfflineSeq: 0
Class2FramesOut: 0 InvalidDestAddr: 0  TotalErrors: 1
Class2WordsIn: 0  LIP_AL_PD_AL_PS: 0      TotalLIPsRecvd: 15
Class2WordsOut: 0  LIP_F7_AL_PS: 0       TotalLinkResets: 0
Class3FramesIn: 0  LIP_F7_F7: 15          TotalRxFrames: 0
Class3FramesOut: 0  LIP_F8_AL_PS: 0       TotalRxWords: 0
Class3Toss: 0     LIP_F8_F7: 0           TotalTxWords: 0
Class3WordsIn: 0  LinkFailures: 0        TotalTxFrames: 0
Class3WordsOut: 0  Login: 7              TotalTxFrames: 0
DecodeErrors: 0   Logout: 6              TxLinkResets: 0
EpConnects: 7     LoopTimeouts: 0         TxOfflineSeq: 0
FBusy: 0          LossOfSync: 1          TxWaits: 0

The following is an example of the Show Switch command.

```
FCSM: user1> show switch
Switch Information

SymbolicName: Fibre Channel Switch Module
SwitchWWN: 10:00:00:c0:dd:00:91:03
SwitchType: BladeCenter
PROMVersion: V1.4.0.1-0 (Thu Sep 12 17:46:41 2002)
CreditPool: 0
DomainID: 1 (0x1)
FirstPortAddress: 010000
FlashSize - MBytes: 128
LogLevel: Critical
MaxPorts: 16
NumberOfResets: 14
ReasonForLastReset: NormalReset
SWImageVersion (1) - build date V1.4.0.18-3 (Thu Sep 19 03:55:16 2002)
SWImageVersion (2) - build date V1.4.0.19-1 (Fri Sep 20 03:56:20 2002)
ActiveConfiguration: default
ActiveSWImage: 02
AdminState: Online
AdminModeActive      False
BeaconOnStatus       False
OperationalState     Online
PrincipalSwitchRole  True
BoardTemp (1) - Degrees Celsius  50
BoardTemp (2) - Degrees Celsius  50
SwitchDiagnosticsStatus Passed
SwitchTemperatureStatus Normal
**Show Config command**
Display port, switch, alarm threshold, and zoning attributes for the current configuration.

**Authority:** User

**Syntax:**
show config
  port [port_number]
  switch
  threshold
  zoning

**Keywords:**

**port [port_number]**
Displays configuration parameters for the port number given by [port_number]. Ports are numbered beginning with 0. If the port value is omitted, all ports are specified.

**switch**
Displays configuration parameters for the switch.

**threshold**
Displays alarm threshold parameters for the switch.

**zoning**
Displays zoning configuration parameters for the switch.

**Examples:** The following is an example of the Show Config Port command.

FCSM: user1> show config port 15
Configuration Name: lei
-------------------
Port Number: 15
-------------
AdminState Online
LinkSpeed Auto
PortType GL
TLPortMode TLTargetMode
ISLSecurity Any
SymbolicName Port15
ALFairness False
ARB_FF False
InteropCredit 0
ExtCredit 0
FANEnable True
LCFEnable False
MFEEnable True
MFS_TOV 10
MSEnable True
NoClose False
IOStreamGuard Disabled
VIEnable False
CheckAlps False

The following is an example of the Show Config Switch command.
FCSM: user1> show config switch
Configuration Name: lei

Switch Configuration Information
-----------------------------
AdminState Online
BroadcastEnabled True
InbandEnabled True
DomainID 1 (0x1)
DomainIDLock False
SymbolicName Fibre Channel Switch Module
R_T_TOV 100
R_A_TOV 10000
E_D_TOV 2000
FS_TOV 5000
DS_TOV 5000
PrincipalPriority 254
ConfigDescription IBM BladeCenter(TM) 2-port Fibre Channel Switch Module
ConfigLastSavedBy Initial
ConfigLastSavedOn Initial

The following is an example of the Show Config Threshold command.
FCSM: user1> show config threshold
Configuration Name: default

Threshold Configuration Information
-------------------------------------
ThresholdMonitoringEnabled True
CRCErrorsMonitoringEnabled True
  RisingTrigger 25
  FallingTrigger 1
  SampleWindow 10
DecodeErrorsMonitoringEnabled True
  RisingTrigger 200
  FallingTrigger 0
  SampleWindow 10
ISLMonitoringEnabled True
  RisingTrigger 2
  FallingTrigger 0
  SampleWindow 10
LoginMonitoringEnabled True
  RisingTrigger 5
  FallingTrigger 1
  SampleWindow 10
LogoutMonitoringEnabled True
  RisingTrigger 5
  FallingTrigger 1
  SampleWindow 10
LOSMonitoringEnabled True
  RisingTrigger 100
  FallingTrigger 5
  SampleWindow 10

The following is an example of the Show Config Zoning command.
FCSM: user1> show config zoning
Configuration Name: default

Zoning Configuration Information
--------------------------------
AutoSave True
Default All
Show Log command
Displays the contents of the log or the parameters used to create entries in the log. The log contains a maximum of 200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority: User

Syntax:
show log
   component
   level
   options
   port
   settings

Keywords:

component
Displays the components currently being monitored for events.

level
Displays the event severity level needed to create an entry in the log. If the severity level occurs on a port or on a component which is not defined, no entry is made in the log.

options
Displays the options used to set the component and log level attributes.

port
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings
Displays the current settings for component, level and port. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples: The following is an example of the Show Log Component command.
FCSM: user1> show log component
  Current setting(s) for log component: NameServer

The following is an example of the Show Log Level command.
FCSM: user1> show log level
  Current settings for log
  ------------------------
  level Critical

The following is an example of the Show Log Options command.
FCSM: user1> show log options

  Allowed options for 'level': Critical,Warn,Info,None
  Allowed options for 'component': All,None,NameServer,MgmtServer,Zoning,Switch, Chassis,Blade,Port,Eport,Snmp,Other
  Current setting(s) for log port: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
The following is an example of the Show Log command.

[327] [Wed Jan 25 09:36:54 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Eport State = E_A0_GET_DOMAIN_ID]
[328] [Wed Jan 25 09:36:54.860 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [FSPF PortUp state=0]
[329] [Wed Jan 25 09:36:54.861 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Sending init hello]
[330] [Wed Jan 25 09:36:54.861 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Processing EFP, oxid= 0x8]
[331] [Wed Jan 25 09:36:54.861 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Eport State = E_A2_IDLE]
[332] [Wed Jan 25 09:36:54.861 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [EFP, WWN= 0x100000c0dd00b845, len= 0x30]
[333] [Wed Jan 25 09:36:54.864 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Sending LSU oxid= 0xc: type= 1]
[334] [Wed Jan 25 09:36:54.864 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Sending Zone Merge Request]
[335] [Wed Jan 25 09:36:54.865 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [LSDB Xchg timer set]
[336] [Wed Jan 25 09:36:54.865 1989] [Eport:0xdd00b8b6.304.4 Port: 0/8] [Setting attribute Oper.UserPort.0.8.EpConnState Connected]
Show Perf command
Displays port performance in frames per second and bytes per second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames per second and bytes per second.

Authority: User

Syntax:
show perf
  byte
  inbyte
  outbyte
  frame
  inframe
  outframe
  errors

Keywords:
byte
  Displays continuous performance data in total bytes per second transmitted and received for all ports. Type q and press the Enter key to stop the display.

inbyte
  Displays continuous performance data in bytes per second received for all ports. Type q and press the Enter key to stop the display.

outbyte [port_number]
  Displays continuous performance data in bytes per second transmitted for all ports. Type q and press the Enter key to stop the display.

frame [port_number]
  Displays continuous performance data in total frames per second transmitted and received for all ports. Type q and press the Enter key to stop the display.

inframe [port_number]
  Displays continuous performance data in frames per second received for all ports. Type q and press the Enter key to stop the display.

outframe [port_number]
  Displays continuous performance data in frames per second transmitted for all ports. Type q and press the Enter key to stop the display.

errors [port_number]
  Displays continuous error counts for all ports. Type q and press the Enter key to stop the display.

Examples: The following is an example of the Show Perf command.

FCSM: user1> show perf

<table>
<thead>
<tr>
<th>Port</th>
<th>Bytes/s (in)</th>
<th>Bytes/s (out)</th>
<th>Bytes/s (total)</th>
<th>Frames/s (in)</th>
<th>Frames/s (out)</th>
<th>Frames/s (total)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ext1:0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ext2:15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bay1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bay2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bay3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Bay</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Bay4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bay14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Show Setup command
Displays the current SNMP and system settings.

**Authority:** User

**Syntax:**
show setup

  mfg
  snmp
  system

**Keywords:**

mfg  Displays manufacturing information about the switch.

snmp  Displays the current SNMP settings.

system  Displays the current system settings.

**Examples:** The following is an example of the Show Setup Mfg command.

```
FCSM: user1> show setup mfg
Manufacturing Information

BoardSerialNumber    P9
BrandName            IBM
BuildDate            Unknown
ChassisPartNumber    Unknown
ChassisSerialNumber  P9
MACAddress            00:c0:dd:00:91:02
PlanarPartNumber     Unknown
SwitchSymbolicName    Fibre Channel Switch Module
SwitchWWN             10:00:00:c0:dd:00:91:03
SystemDescription     IBM BladeCenter(TM) 2-port Fibre Channel Switch Module
SystemObjectID        1.3.6.1.4.1.1663.1.1.1.1.1.16
```

The following is an example of the Show Setup Snmp command.

```
FCSM: user1> show setup snmp
SNMP Information

Contact           <sysContact undefined>
Location          <sysLocation undefined>
Description       IBM BladeCenter(TM) 2-port Fibre Channel Switch Module
Trap1Address      10.0.0.254
Trap1Port         162
Trap1Severity     warning
Trap1Enabled      False
Trap2Address      0.0.0.0
Trap2Port         162
Trap2Severity     warning
Trap2Enabled      False
Trap3Address      0.0.0.0
Trap3Port         162
Trap3Severity     warning
Trap3Enabled      False
Trap4Address      0.0.0.0
Trap4Port         162
Trap4Severity     warning
Trap4Enabled      False
Trap5Address      0.0.0.0
```
The following is an example of the Show Setup System command.

```
FCSM: user1> show setup system
System Information

Eth0NetworkAddress   10.20.8.188
Eth0NetworkMask      255.255.252.0
Eth0GatewayAddress   10.20.8.254
Eth0NetworkDiscovery Static
AdminTimeout         30
SecurityEnabled      False
LocalLogEnabled      True
RemoteLogEnabled     False
RemoteLogHostAddress 10.0.0.254
```

Chapter 2. BladeCenter 2-Port Fibre Channel Switch Module
**Shutdown command**
Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

**Authority:** Admin

**Syntax:**
shutdown

**Notes:** Always use this command to effect an orderly shutdown before removing power from the switch. Failure to do so could damage the flash memory and the switch configuration.
**Test command**
Tests switch module ports using internal (SerDes level), external small form-factor pluggable (SFP), and online loopback tests. Internal and external tests require that the switch module port be placed in diagnostic mode. See the "[Set Port command](#)" on page 36 for information about changing the port administrative state. While the test is running, the remaining ports on the switch remain fully operational. See "Port testing" on page 116 for more information.

**Authority:** Admin

**Syntax:**

test
   port [port_number] [test_type]
cancel
status

**Keywords:**

port [port_number] [test_type]
Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

Internal (for internal and external ports)
   Tests the SerDes. This is the default. The port must be in diagnostics mode to perform this test.

External (for external ports only)
   Tests both the SerDes and SFP. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the SFP.

Online (for internal and external ports)
   Tests one online port.

cancel
   Cancels the online test in progress.

status
   Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

**Examples:** To run Internal (SerDes) or External (SFP) port tests, complete the following steps:

1. To start an admin session, type the following command:
   
      admin start

2. Place the port in Diagnostics mode by typing the following command (x = port number):
   
      set port x state diagnostics

3. Insert the loopback plug into the SFP on the selected port (for external port test only).

4. Choose one of the two types of port loopback tests to run:
   
   - To run an internal loopback test, type the following command:
     
        test x internal
   
   - To run an external loopback test, type the following command. A loopback plug must be installed for this test to pass.
     
        test x external
Note: The external loopback test can be performed only on external switch module ports.

After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.

5. After the test is run, put the port back into online state by typing the following command (x = port number):
   `set port x state online`

6. To verify the port is back online, type the following command. The contents of the **AdminState** field should be **Online**.
   `show port x`

The online node-to-node test can test only one port at a time, and that port must be online and connected to an external device or a blade server Fibre Channel expansion card. To run the online node-to-node test, complete the following steps:

1. To start an admin session, type the following command:
   `admin start`

2. To run the online node-to-node test, type the following command:
   `test x online`

A series of test parameters are displayed on the screen.

3. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

   FCSM (admin) : user1> test x online

   A list of attributes with formatting and current values will follow. Enter a new value or simply press the ENTER key to accept the default value. If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.

   TestLength (decimal value, 1-4294967295) [100 ]
   FrameSize (decimal value, 36-2148) [256 ]
   DataPattern (32-bit hex value or 'Default') [Default]
   StopOnError (True/False) [False ]

   Do you want to start the test? (y/n) [n]

4. After all parameter values are defined, press the Y key to start the test.
**Uptime command**
Displays the elapsed time since the switch was last reset and reset method.

**Authority:** User

**Syntax:**
```
uptime
```

**Examples:** The following is an example of the Uptime command.

```
FCSM: user1> uptime
Elapsed up time : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
Reason last reset: NormalReset
```
**User command**
Administers or displays user accounts.

**Authority:** Admin. The List keyword is available with User authority.

**Syntax:**
```
user
    accounts
        add
            delete [account_name]
        list
```

**Keywords:**
- `accounts` Displays all user accounts that exist on the switch.
- `add` Add a user account to the switch. After this command is executed, the administrator will be prompted for the information needed to establish the user account. A switch can have a maximum of 15 user accounts. Account names are limited to 15 characters; passwords are limited to 31 characters.
- `delete [account_name]` Deletes the account name given by [account_name] from the switch.
- `list` Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is valid for User authority and does not require an admin session.

**Examples:** The following is an example of the User Accounts command.
```
FCSM (admin) : user1> user accounts
Current list of user accounts
-----------------------------
images (admin authority = False)
admin (admin authority = True)
USERID (admin authority = True)
```
The following is an example of the User Add command.
```
FCSM (admin) : user1> user add
Press 'q' and the ENTER key to abort this command.
account name (1-15 chars) : user3
account password (4-20 chars) :
please confirm account password:
should this account have admin authority? (y/n) [n] : y
OK to add user account 'user3' with admin authority? Please confirm (y/n): [n] y
```
The following is an example of the User Delete command.
```
FCSM (admin) : user1> user del user3
The user account will be deleted. Please confirm (y/n): [n] y
```
The following is an example of the User List command.
FCSM (admin) : user1> user list
Current list of users logged in
-----------------------------------
admin@OB-session1 - in admin mode
admin@OB-session2
user1@OB-session3
**Whoami command**
Command
Displays the account name, session number, and switch domain ID for the Telnet session.

*Authority:* User

*Syntax:*

whoami

*Examples:* The following is an example of the Whoami command.

FCSM: user1> whoami
User name : admin@OB-session3
Switch name : Fibre Channel Switch Module
Switch domain ID: 100 (0x64)
Zone command
Manages zones and zone membership on a switch. The Zone command defines members (ports and devices) for a single switch. Zones are members of zone sets.

Authority: Admin authority and a Zoning Edit session. See the "Zoning command" on page 68 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available with User authority and do not require a Zoning Edit session.

Syntax:
zone
  add [zone] [members]
  copy [zone_source] [zone_destination]
  create [zone]
  delete [zone]
  list
  members [zone]
  remove [zone] [members]
  rename [zone_old] [zone_new]
  type [zone] [zone_type]
  zonesets [zone]

Keywords:
add [zone] [members]
Specifies one or more ports given by [members] to add to the zone named [zone]. A zone can have a maximum of 256 members. [members] can have one of the following formats:
  • Domain ID and port number pair (domain ID, port number). Domain IDs and port numbers are in decimal format. Ports are numbered beginning with 0.
  • 6-character hexadecimal device Fibre Channel address (hex)
  • Alias name
The application verifies that the [zone] format is correct, but does not validate that such a port exists.

copy [zone_source] [zone_destination]
Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]
Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, &, _, and -. The zoning database supports a maximum of 256 zones.

delete [zone]
Deletes the specified zone given by [zone] from the zoning database. If the zone is a member of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all zones and the zone sets of which they are members. This keyword is valid for User authority and does not require a zoning edit session.
**members [zone]**
Displays all members of the zone given by [zone]. This keyword is available with User authority and does not require a Zoning Edit session.

**remove [zone] [members]**
Removes the ports given by [members] from the zone given by [zone]. [members] can have one of the following formats:
- Domain ID and port number pair (Domain ID, Port Number). Domain IDs and port numbers are in decimal. Ports are numbered beginning with 0.
- 6-character hexadecimal device Fibre Channel address (hex)
- Alias name

**rename [zone_old] [zone_new]**
Renames the zone given by [zone_old] to the zone given by [zone_new].

**type [zone] [zone_type]**
Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:
- soft
  - Name server zone
- hardacl
  - Access control list hard zone
- hardvpf
  - Virtual private fabric hard zone

**zonesets [zone]**
Displays all zone sets of which the zone given by [zone] is a member. This keyword is available with User authority and does not require a Zoning Edit session.

**Examples:** The following is an example of the Zone List command.

```
FCSM: user1> zone list

Zone     ZoneSet
--------  ---------------
wwn_b0241f  zone_set_1
wwn_23bd31  zone_set_1
wwn_221416  zone_set_1
wwn_2215c3  zone_set_1
wwn_0160ed  zone_set_1
wwn_c001b0  zone_set_1
wwn_401248  zone_set_1
wwn_02402f  zone_set_1
```
The following is an example of the Zone Members command.

FCSM: user1> zone members wwn_b0241f

Current List of Members for Zone: wwn_b0241f
---------------------------------
21:00:00:e0:8b:02:41:2f

The following is an example of the Zone Zonesets command.

FCSM: user1> zone zonesets zone1

Current List of ZoneSets for Zone: wwn_b0241f
----------------------------------
Zoneset command
Manages zone sets and zone set membership across the fabric.

Authority: Admin authority and a Zoning Edit session. See the Zoning command on page 68 for information about starting a Zoning Edit session. The Active, List, Zones keywords are available with User authority. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax:
zoneset
  activate [zone_set]
  active
  add [zone_set] [zone_list]
  copy [zone_set_source] [zone_set_destination]
  create [zone_set]
  deactivate
  delete [zone_set]
  list
  remove [zone_set] [zone_list]
  rename [zone_set_old] [zone_set_new]
  zones [zone_set]

Keywords:
activate [zone_set]
  Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
  Displays the name of the active zone set. This keyword is available with User authority and does not require a Zoning Edit session.

add [zone_set] [zone_list]
  Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Zone and alias names are delimited by spaces in [zone_list]. This keyword requires a Zoning Edit session.

copy [zone_set_source] [zone_set_destination]
  Creates a new zone set named [zone_set_destination] and copies into it the membership from the zone set given by [zone_set_source]. This keyword requires a Zoning Edit session.

create [zone_set]
  Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, &, _, and -. This keyword requires a Zoning Edit session. The zoning database supports a maximum of 256 zone sets.

deactivate
  Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
  Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated. This keyword requires a Zoning Edit session.

list
  Displays a list of all zone sets. This keyword is available with User authority and does not require a Zoning Edit session.
remove [zone_set] [zone_list]
  Removes a list of zones and aliases given by [zone_list] from the zone set
given by [zone_set]. Zone and alias names are delimited by spaces in
[zone_list]. If [zone_set] is the active zone set, the zone will not be removed
until the zone set has been deactivated. This keyword requires a Zoning Edit
session.

rename [zone_set_old] [zone_set_new]
  Renames the zone set given by [zone_set_old] to the name given by
[zone_set_new]. You can rename the active zone set. This keyword requires a
Zoning Edit session.

zones [zone_set]
  Displays all zones that are members of the zone set given by [zone_set]. This
keyword is available with User authority and does not need a Zoning Edit
session.

Notes:
• A zone set must be active for its definitions to be applied to the fabric.
• Only one zone set can be active at one time.
• A zone can be a member of more than one zone set.

Examples: The following is an example of the Zoneset Active command.
FCSM: user1> zoneset active
    The active ZoneSet is: Beta
The following is an example of the Zoneset List command.
FCSM: user1> zoneset list
    Current List of ZoneSets
    ------------------------
    alpha
    beta
The following is an example of the Zoneset Zones command.
FCSM: user1> zoneset zones ssss
    Current List of Zones for ZoneSet: ssss
    ------------------------------
    zone1
    zone2
    zone3
Zoning command
Opens a Zoning Edit session in which to create and manage zone sets and zones. See the “Zone command” on page 63 and the “Zoneset command” on page 66 for information about managing zone and zone sets.

Authority: Admin. The List keyword is available with User authority.

Syntax:
```
zoning active cancel clear edit history limits list restore save
```

Keywords:
active
Displays membership information for the active zone set including member zones and zone members.
cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.
clear
Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword does not affect the nonvolatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the nonvolatile zoning database will be cleared from the switch. The preferred method for clearing the zoning database from the switch is the Reset Zoning command.
edit
Opens a Zoning Edit session.
history
Displays a history of zoning modifications including the following:
• Time of the most recent zone set activation or deactivation and the user who performed it
• Time of the most recent modifications to the zoning database and the user who made them.
• Checksum for the zoning database.
limits
Displays the maximum limits imposed on the zoning database for the number of zone sets, zones, aliases, members per zone, members per alias, and total members.
list
Lists all fabric zoning definitions. This keyword is available with User authority.
restore
Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.
save
Saves changes made during the current Zoning Edit session. The system will inform you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples: The following is an example of the Zoning Edit command.
FCSM: user1> admin start
FCSM (admin) : user1> zoning edit
FCSM (admin-zoning) : user1>
.
FCSM (admin-zoning) : user1> zoning cancel
Zoning edit mode will be canceled. Please confirm (y/n): [n] y
FCSM (admin) : user1> admin end

The following is an example of the Zoning List command.
FCSM: user1> zoning list
Active ZoneSet Information
ZoneSet Zone ZoneMember
--------------------------------
wwn

    wwn_b0241f
       21:00:00:e0:8b:02:41:2f

    wwn_23bd31
       10:00:00:00:c9:23:bd:31

    wwn_221416
       10:00:00:00:c9:22:14:16

    wwn_2215c3
       10:00:00:00:c9:22:15:c3

Configured Zoning Information
ZoneSet Zone ZoneMember
--------------------------------
wwn
    wwn_b0241f
       21:00:00:e0:8b:02:41:2f

    wwn_23bd31
       10:00:00:00:c9:23:bd:31

    wwn_221416
Using the SAN Utility

You can use the SAN Utility application to access and configure switch modules. For information about installing, uninstalling, and starting the SAN Utility application, see the IBM Eserver BladeCenter 2-Port Fibre Channel Switch Module Installation Guide. The SAN Utility application can be installed on a BladeCenter blade server or an external network management workstation configured with one of the operating systems described in the IBM Eserver BladeCenter 2-Port Fibre Channel Switch Installation Guide.

To manage your switch modules and fabrics, the SAN Utility application provides two basic windows: Topology and Faceplate. The SAN Utility user interface, its elements, and the tasks that you can perform from the Faceplate window and Topology window are described in this chapter.

Important: Before you configure your switch module, be sure that the management modules in your BladeCenter unit are properly configured. In addition, to access and manage your 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 Unit 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 at http://www.ibm.com/eserver/bladecenter/ on the World Wide Web for information to help you prepare for system installation and configuration.

SAN Utility user interface

The Topology window and Faceplate window share the following common elements:
- Menu bar
- Toolbar
- Fabric tree
- Graphic window
- Data window and tabs
- Working Status indicator

The Topology window displays all of the switch modules that are enabled and the connections between switch modules and other Fibre Channel devices, as shown in Figure 1 on page 71.
The Faceplate window displays the front of a single switch module and its active ports, as shown in Figure 2.

Menu bar
The menu bar is displayed at the top of the Faceplate window and Topology window. Depending on which window is open, the menu bar has similar menu selections. Figure 3 on page 72 shows menu items that are available in the Topology window. In the Faceplate window, menu items shown with a gray background are available.
Some menu selections have shortcut keys as shown in Table 14.

<table>
<thead>
<tr>
<th>Shortcut key</th>
<th>Menu selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5</td>
<td>View → Refresh</td>
</tr>
<tr>
<td>Ctrl+O</td>
<td>File → Open View File</td>
</tr>
</tbody>
</table>

In addition to the menu bar, both the Topology and Faceplate windows have context-sensitive menus that open when you click in the graphic window with the right mouse button. See “Opening the Faceplate window and pop-up menus” on page 77 for more information about these pop-up menus.

**Toolbar**

The toolbar consists of a row of graphical buttons that you can use to access SAN Utility functions as shown and described in Table 15. The toolbar buttons are an alternative method to using the menu bar.

<table>
<thead>
<tr>
<th>Toolbar button</th>
<th>Toolbar button name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Add Fabric</td>
<td>Adds a new fabric</td>
</tr>
<tr>
<td></td>
<td>Open View File</td>
<td>Opens an existing fabric view file</td>
</tr>
<tr>
<td></td>
<td>Save View As</td>
<td>Saves the current fabric view to a file</td>
</tr>
<tr>
<td></td>
<td>Refresh</td>
<td>Polls the fabric to update the Topology or Faceplate window with the current information</td>
</tr>
<tr>
<td></td>
<td>Help Topics</td>
<td>Opens the online help</td>
</tr>
</tbody>
</table>
Table 15. Toolbar buttons (continued)

<table>
<thead>
<tr>
<th>Toolbar button</th>
<th>Toolbar button name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Edit Zoning</td>
<td>Opens the Edit Zoning window (available only in the Faceplate window)</td>
</tr>
</tbody>
</table>

Fabric tree
The fabric tree, in the FC Fabric pane, lists the managed fabrics and their switch modules. To adjust the window, click and drag the moveable window border. An entry handle to the left of an entry in the tree indicates that you can expand the entry. When you click the handle or double-click the entry, the entry expands to show its member switches. These fabric tree elements are shown in Figure 4.

![Figure 4. Fabric tree](image)

Each fabric tree entry has a small icon next to it that uses color to indicate the following operational status:
- A green switch module entry icon indicates that the switch is in normal operation.
- A green switch module entry icon indicates that the switch has a communications failure.
- A red switch
- A blue switch module entry icon indicates that the switch status is Unknown or that security is enabled on the switch module but security is disabled on the fabric management switch.
- An amber switch module entry icon indicates that the switch is operational with errors.

You can use the fabric tree to access any fabric or switch module using the Topology or Faceplate window. You can click a fabric entry to open the Topology window from the fabric tree. You can click a switch module entry to open the Faceplate window from the fabric tree.

Graphic window
The graphic window as shown in Figure 1 on page 71 shows graphic information about fabrics and switch modules such as the fabric topology and the switch faceplate. To adjust the window length, click and drag the window border that it shares with the data window.

Data window and tabs
The data window as shown in Figure 2 on page 71 displays a table of data and statistics associated with the selected tab. Use the scroll bar to browse through the data. The window length can be adjusted by clicking and dragging the border that it shares with the graphic window.
To adjust the column width, move the pointer over the column heading border shared by two columns until a right/left arrow graphic is displayed. Click and drag the arrow to the desired width. The data window tabs show options for the types of information that you can display in the data window. These options vary depending on the display.

**Working status indicator**
The working status indicator as shown in Figure 1 on page 71 is in the lower-right corner of the Topology window and shows when the network management workstation is exchanging information with the fabric. As conditions change, the fabric forwards this information to the network management workstation where it is reflected in the various displays.

**Using the Topology window**
The Topology window shown in Figure 5 polls the selected fabric and displays its topology. Switch modules and interswitch links (ISL) are displayed in the graphic window and use color to indicate status. The following functional elements are displayed in the Topology window when you click on the Data window tabs:

- Switch module and link status
- Working with switch modules and links
- Topology data windows

**Fibre Channel switch module and link status**
The Fibre Channel switch module icon shape and color provide information about the switch and its operational state. In the Topology window, lines represent links between switch modules. See Table 16 for Fibre Channel switch module and link status and “Fabric status” on page 81 for more information about other Topology window icons.

<table>
<thead>
<tr>
<th>Switch module icon color</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Normal Fibre Channel switch operation</td>
</tr>
<tr>
<td>Amber</td>
<td>Operational with errors</td>
</tr>
<tr>
<td>Red</td>
<td>Inactive or Fibre Channel switch failure</td>
</tr>
<tr>
<td>Blue</td>
<td>Unknown Fibre Channel device</td>
</tr>
</tbody>
</table>
Working with switch modules and links
Switch module and link icons are selectable and moveable and serve as access points for other windows and menus. You select switch modules and links to display information, modify configurations, or delete them from the window. The context-sensitive pop-up menus are accessible through the switch module and link icons.

Click a switch module or link in the graphic window to display its status in the data window. To select multiple switch modules or links, hold down the Ctrl key while selecting. When no switch modules or links are selected, information about all switch modules is displayed. To deselect a switch module or link that is currently selected, click the switch or link.

Different switch module icons will be displayed depending on the different switch vendor products present in the attached fabric. See Table 17 on page 82 for a list of switch module icons and vendors. Attached switch modules that are not manageable through the SAN Utility will be displayed as “third-party manageable” switch icons. The topology configuration in Figure 6 shows an example of a switch fabric with third-party switch modules.

Arranging switch modules in the window: You can use the following two methods to arrange individual switch module icons:

- To move an individual switch module icon, click and drag the icon to another location in the graphic window. Links stretch or contract to remain connected.
- To arrange all switch module icons in the Topology window, click View → Layout Topology.

The Toggle Auto Layout check box in the View menu is selected by default so that the SAN Utility can arrange the icons when you select Layout Topology.

You can save a custom arrangement, or layout, and restore that layout during a SAN Utility session. To create a custom arrangement, arrange the icons; then, click View → Remember Layout. To restore the saved layout, click View, clear the Toggle Auto Layout check box, and click Layout Topology.

Selecting switch modules and links: Selected switch module icons are highlighted in violet. Selected ISLs are highlighted in amber. You can select switch modules and links by performing the following tasks:
To select a switch module or a link, click the icon or link.

To select multiple switch modules or links, hold down the Ctrl key and click the switch modules or links that you want.

To select all switch modules or links, right-click in the graphic window background. Click Select All Switches or click All Links from the pop-up menu.

To cancel a selection, press and hold the Ctrl key, and select the item again. To cancel multiple selections, click in the graphic window background.

**Topology data window tabs**
The Topology Data window contains four tabs at the bottom of the window. When you click a tab, the following information is displayed:

- **Name Server** - Click the Name Server tab to display all devices that are logged with the name server and their location within the current fabric configuration. See “Name Server Data window” on page 108 for more information about your configuration.

- **Active Zoneset** - Click the Active Zoneset tab to display the active zone set for the fabric, including zones and their member ports. See “Active Zoneset Data window” on page 83 for more information about this data window. See “Zoning a fabric” on page 83 for information about zone sets and zones.

- **Switch** - Click the Switch tab to display the current network and switch module configuration data for the selected switches. See “Switch Data window” on page 95 for more information.

- **Link** - Click the Link tab to display the current link status for the selected switch modules in the fabric.

**Using the Faceplate window**
The Faceplate window shown in Figure 7 and described in this section displays the switch module name and operational state and the port status. The following functional elements are displayed in the Faceplate window when you click on the Data window tabs:

- Port views and status
- Working with ports
- Faceplate data windows

![Faceplate window](image-url)
Opening the Faceplate window and pop-up menus
The Faceplate window shows the front of a single switch module and its ports. You can open the Faceplate window and pop-up menus when you are in the Topology window by performing the following tasks:

- To open the Faceplate window when viewing the Topology window, click a switch module entry or icon in the fabric tree, or double-click the switch module graphic.
- To open the fabric pop-up menu when viewing the Topology window, right-click the graphic window background. The fabric pop-up menu displays selections to refresh the fabric, select all switch modules, select all links, or layout topology.
- To open the switch module pop-up menu when viewing the Topology window, right-click the switch module icon in the graphic window. The switch pop-up menu displays selections to refresh the switch, delete the switch from the display, open the Switch Properties window, or open the Network Properties window.
- To open the link pop-up menu, right-click the link. The Link pop-up menu displays a selection to delete the link from the display.
- To open a Faceplate window pop-up menu, right-click the faceplate graphic in the Graphic window. The faceplate pop-up menu displays selections to refresh the switch module, select all ports, manage switch, port, and network properties, extend credits, and run the Port Loopback tests.

Port views and status
Port color and text provides information about the port and its operational state. Green indicates that the port is active, and gray indicates that the port is inactive. The Faceplate window displays the following views of port status corresponding to the View menu options in the Faceplate window:

- Port mode
- Port state
- Port speed
- Port media

See "Monitoring port status" on page 104 for more information about these displays.

Working with ports
Ports are selectable and serve as access points for other windows and menus. You select ports to display information about them in the data window or to modify them. You cannot use the SAN Utility to select internal bays and external ports at the same time; you must select either internal bays or external ports. Context-sensitive pop-up menus and properties windows are accessible through the Faceplate window and port icons.

Selecting ports: When you select a port, the port is highlighted with a white border. You can select ports in the following ways:

- To select one port, click the port in the Faceplate display.
- To select a range of either internal or external consecutive ports, select a port and then press and hold the shift key and select another port. The application selects both end ports and all ports in between in port number.
- To select several nonconsecutive ports, hold the Ctrl key while selecting ports.
- To select all external ports, right-click anywhere on the switch module faceplate, and select Select All Ports from the pop-up menu. To select all internal ports, click any blade server and select All Ports from the pop-up menu.

To cancel a selection, press and hold the Ctrl key and select it again.
**Opening pop-up menus:** You can manage the switch module and its ports using the following methods:

- To open the pop-up menu, right-click anywhere in the graphic window. If no ports are selected, port specific tasks are unavailable in the menu.
- To select one or more ports and open the Port pop-up menu, right-click a port.

**Faceplate data window tabs**
The Faceplate Data window contains six tabs at the bottom of the display. When you click a tab, the following information is displayed:

- **Name Server** - Click the Name Server tab to display all devices connected to the switch module that are logged with the name server.
- **Switch** - Click the Switch tab to display the current switch module configuration data.
- **Port Statistics** - Click the Port Stats tab to display the port performance data for the selected port.
- **Port Information** - Click the Port Info tab to display the port detail information for the selected port.
- **Configured Zonesets** - Click the Configured Zonesets tab to display all zone sets, zones, and zone membership in the zoning database.
- **Alarm Log** - Click the Alarm Log tab to display the system error information.

**Managing fabrics**
This section describes the following four main tasks for managing fabrics:

- Setting up security
- Managing the fabric database
- Displaying fabric information
- Zoning a fabric

**Setting up security**
Access to a switch module and permission to configure a switch is managed through user accounts created by a fabric administrator. A user account consists of an account name, a password, and an authority level. The authority level determines whether an account can merely monitor the switch module and fabric activity (User authority), or change switch module configurations (Administrative authority). See “User command” on page 60 for information about administering user accounts. Fabric security determines the enforcement of user accounts on a switch module. A fabric administrator can enable or disable the fabric security on a switch module using the Set Setup System command.

If fabric security is disabled (default), you can use the SAN Utility to log in to a switch module without an account name and password. The Login name and Password fields in the Add a Fabric window are ignored, and you are granted Admin authority. If fabric security is enabled, you must enter an account name and password to log in to a switch module and add the fabric to the workspace. Having successfully added a fabric, you can perform only those tasks in the SAN Utility that are granted by the authority level for that account. All switch modules in a fabric should use the same fabric security value. See “Set Setup command” on page 38 for information about the System keyword and the Security Enable parameter.

**Note:** A switch module supports a combined maximum of 15 active login sessions. This includes SAN Utility in-band and out-of-band login attempts, Telnet out-of-band login attempts, and SNMP out-of-band login sessions. Of this 15,
there can be a maximum of 10 SAN Utility login attempts included in the 15 total attempts. Additional logins are refused.

Managing the fabric database
A fabric database contains the set of fabrics that you have added during a SAN Utility session. Initially, a Topology window with an empty fabric database opens. This section describes the following fabric database management tasks:

- Adding a fabric
- Removing a fabric
- Opening a fabric view file
- Saving a fabric view file
- Rediscovering a fabric
- Adding a new switch module to a fabric
- Replacing a failed switch module in a fabric
- Deleting switch modules and links

Adding a fabric: Complete the following steps to add a fabric to the database:

1. In the Faceplate window, click **Fabric → Add Fabric**.
   
   The Add a New Fabric window opens, as shown in **Figure 8**.

   ![Figure 8. Add a New Fabric window](image)

2. In the **Fabric name** field, type a fabric name.
3. In the **IP address** field, type the IP address of the switch module through which to manage the fabric.
4. In the **Login name** field, type the initial default login ID, USERID. In the **Password** field, type the initial default password, PASSW0RD (the sixth character is a zero, not the letter O). The user ID and password are case sensitive.

   **Note:** The password is for the switch module and is stored in the switch firmware. You are not required to type a user ID or password if security is disabled. See “Setting up security” on page 78 for information about the Set Setup command on page 38 for information about the Set Setup commands in the Telnet section to log in, and obtain password and security information.

5. Click **Add fabric**.

Removing a fabric: Complete the following steps to delete a fabric file from the database:

2. In the Faceplate window, click **Fabric → Remove Fabric**.
Opening a fabric view file: Complete the following steps to open an existing fabric view file:
1. In the Faceplate window, click File → Open View File, or click the Open icon.
   If there is a change to the fabric you are using, you are prompted to save the changes to the view file before opening a different view file.
   The Open View window opens.
2. In the Open View window, type the name of the file you want to open.
3. Type a file password if necessary.
4. Click Load View File. If the fabric has changed, you are prompted to save the file before opening the new view.

Saving a fabric view file: Complete the following steps to save a fabric view file:
1. In the Faceplate window, click File → Save View As or click the Save icon.
   The Save View window opens.
2. In the Save View window, type a new file name.
3. Click OK.
4. Type a file password, if necessary.

Rediscovering a fabric: After making changes or deleting switch modules from a fabric view, refresh the fabric configuration. Use the Rediscover Fabric option to clear the current fabric information that is displayed and rediscover the switch module information. To rediscover a fabric, in the Faceplate window, click Fabric → Rediscover Fabric.

Adding a new switch module to a fabric: After you install a switch module into your BladeCenter unit, the switch uses the default fabric configuration settings. The default fabric configuration settings are as follows:
- Fabric zoning is sent to the switch module from the fabric.
- All external ports (0,15) are GL_Ports; all internal ports (1 through 14) are F_Ports.
- The default IP addresses are:
  For switch module bay 3:
  192.168.70.129
  For switch module bay 4:
  192.168.70.130

Complete the following steps to add a new switch module to a fabric and not make changes to the default fabric configuration settings:
1. If the switch module is not new, to reset the switch to the factory configuration, in the Faceplate window, click Switch → Restore Factory Defaults.
2. If you want to manage the switch module through the Ethernet port, configure the network SNMP configuration using the Network Properties window. For more information, see “Network properties” on page 101.
3. Configure any special switch settings.

Note: To prevent communication with other switch modules in the fabric until the new switch is configured, in the Zoning Config window, click None in the Default Visibility field. For more information, see “Zoning configuration” on page 85.
4. Connect the interswitch links (ISL), but do not connect the devices.
5. In the Port Properties window, configure the port types for the new switch (GL_Port, TL_Port, Donor).

6. Connect the Fibre Channel devices to the switch module.

7. In the Edit Zoning window, make the necessary zoning changes.

**Replacing a failed switch module in a fabric:** Complete the following steps to replace a failed switch module for which an archive is available. See "Restoring a switch module" on page 119 and "Archiving a switch module" on page 102 for more information.

1. Remove the failed switch module. For more information, see the Installation Guide.

2. Install the new replacement switch module. For more information, see the Installation Guide.

3. Log in to the fabric through the replacement switch module. In the Topology window, select the replacement switch module from the fabric tree.

4. Click **Switch → Restore**.

   The Restore Switch window opens.

5. In the Restore Switch window, type a name or select the archived switch configuration file to copy to the switch module. For more information, see "Archiving a switch module" on page 102.

6. Click **OK** to write the configuration file to the switch module.

**Deleting switch modules and links from the Topology display:** The SAN Utility does not automatically delete switch modules or links that have failed or that are physically removed. In this case, you can delete switch modules and links in the Topology window to bring the display up to date. If you delete a switch or a link that is still active, the SAN Utility restores it automatically. You can also refresh the display.

Complete the following steps to delete a switch module in the Topology window:

1. Select one or more switch modules in the Topology window.

2. Click **Switch → Delete**.

Complete the following steps to delete a link:

1. Select one or more links in the Topology window.

2. Click **Switch → Delete**.

**Displaying fabric information**

The Topology window is the primary tool for monitoring a fabric. The graphics window of the Topology window provides status information for switch modules, interswitch links, and the Ethernet connection to the network management workstation.

The data window tabs show name server, switch, and active zone set information. The **Active Zoneset** tab shows the zone definitions for the active zone set. See "Switch Data window" on page 95 and "Name Server Data window" on page 108 for information about the Switch Data and Name Server Data windows.

**Fabric status:** The fabric updates the Topology and Faceplate windows by forwarding changes in status to the network management workstation as they occur. Use the fabric to update the display status, or you can refresh the display at any time. To refresh the Topology window, use one of the following methods:

- In the Topology window, click **Refresh**.
• Click View → Refresh.
• Press the F5 key.
• Right-click anywhere in the background of the Topology window. Select Refresh Fabric from the pop-up menu.

The Topology window displays switch module and status icons that provide status information about switches, interswitch links, and the Ethernet connection. The switch module icons indicate different vendor switches and switch types. The switch module status icons, displayed on the left side of a switch, vary in shape and color. Each switch module that is managed by an Ethernet Internet protocol (IP) has a colored Ethernet icon that is displayed on the right side of the switch. A green Ethernet icon indicates normal operation, amber indicates operational with errors, and red indicates inactive or failure. Table 17 shows the different switch module icons and their descriptions.

Note: Different switch module icons are displayed depending on the different switch vendor products presented in the attached fabric. For a list of switch module icons and vendors, see Table 17. Attached switch modules that are not manageable through the SAN Utility are displayed as third-party manageable switch icons. The topology configuration in Figure 6 on page 75 shows an example of a switch fabric with third-party switch modules.

Table 17. Topology window switch module and status icons

<table>
<thead>
<tr>
<th>Switch module icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![BladeCenter Fibre Channel switch module]</td>
<td>BladeCenter Fibre Channel switch module</td>
</tr>
<tr>
<td>![QLogic 8-port Fibre Channel switch module]</td>
<td>QLogic 8-port Fibre Channel switch module</td>
</tr>
<tr>
<td>![QLogic 16-port Fibre Channel switch module]</td>
<td>QLogic 16-port Fibre Channel switch module</td>
</tr>
<tr>
<td>![Inrange switch module]</td>
<td>Inrange switch module</td>
</tr>
<tr>
<td>![McData switch module]</td>
<td>McData switch module</td>
</tr>
<tr>
<td>![Brocade switch module]</td>
<td>Brocade switch module</td>
</tr>
<tr>
<td>![Other third-party switch modules]</td>
<td>Other third-party switch modules</td>
</tr>
<tr>
<td>![Switch communication normal (green)]</td>
<td>Switch communication normal (green)</td>
</tr>
<tr>
<td>![Switch is operational with errors (amber)]</td>
<td>Switch is operational with errors (amber)</td>
</tr>
<tr>
<td>![Switch communication interrupted (red)]</td>
<td>Switch communication interrupted (red)</td>
</tr>
<tr>
<td>![Switch management communication unknown (blue)]</td>
<td>Switch management communication unknown (blue)</td>
</tr>
<tr>
<td>![Fabric management switch Ethernet connection normal (green)]</td>
<td>Fabric management switch Ethernet connection normal (green)</td>
</tr>
<tr>
<td>![Fabric management switch Ethernet connection critical (red)]</td>
<td>Fabric management switch Ethernet connection critical (red)</td>
</tr>
<tr>
<td>![Fabric management switch Ethernet connection warning (amber)]</td>
<td>Fabric management switch Ethernet connection warning (amber)</td>
</tr>
</tbody>
</table>
**Active Zoneset Data window:** The Active Zoneset Data window displays the zone membership for the active zone set that resides on the fabric management switch. The active zone set is the same on all switch modules in the fabric. You can confirm this by adding a fabric through another switch module and comparing Active Zone Set displays.

To open the Active Zoneset Data window, click the Active Zoneset tab below the data window in the Topology window. See "Zoning a fabric" for more information about zone sets and zones. See "Configured Zonesets Data window" on page 96 for information about the zone set definitions on a specific switch module.

The Active Zoneset data window, shown in Figure 9, uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle to the left of an entry in the fabric tree indicates that you can expand the entry. Click this handle or double-click the following entries to expand or contract them:
- A zone set entry expands to show its member zones.
- A zone entry expands to show its member ports.
- A port entry expands to show the port Fibre Channel address.
- A Fibre Channel address entry expands to show the port worldwide name.

![Figure 9. Active Zonesets window](image)

**Zoning a fabric**

Fibre Channel fabrics use zoning to restrict or extend access to devices in the fabric. A zone is a named group of devices that can communicate with each other.

You can use zoning to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes. You can set the Auto Save and Default Visibility zoning configuration parameters using the SAN Utility or the **Set Config Zoning** command. See "Auto save" on page 86 for information about the Auto Save parameter, see "Default visibility" on page 86 for information about the Default Visibility parameter, and see "Using the Zoning Config window" on page 86 for information about the Set Config Zoning command.

**Zoning concepts:** The following zoning concepts provide some context for the zoning tasks described in this section:
- Zones
- Aliases
- Zone sets
Zoning database

Zoning configuration

Zones: A zone is a named group of ports or devices that can communicate with each other. Membership in a zone is defined by port number, device Fibre Channel address, or device World Wide Name (WWN). Zone members can communicate only with members of the same zone. Zones can overlap; that is, a port or device can be a member of more than one zone.

There are three zone types that are supported but have restrictive levels of communication. These zone types are:

- Soft zone
- Access control list (ACL) - hard zone
- Virtual private fabric (VPF) - hard zone

Soft zoning: Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. Soft zones that include members from multiple switch modules need not include the ports of the interswitch links. Soft zone boundaries yield to ACL and VPF zone boundaries. Soft zones can overlap; that is, a port can be a member of more than one soft zone. Membership is defined by Fibre Channel address, port ID and domain ID, or worldwide name. Soft zoning supports all port modes.

Access control list zones: Access control list (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Members can communicate with each other and transmit outside the ACL zone but cannot receive inbound traffic from outside the zone. The ACL zone boundary is secure against inbound traffic. ACL zones can overlap; that is, a port can be a member of more than one ACL zone. ACL zones that include members from multiple switch modules need not include the ports of the interswitch links. ACL zone boundaries supersede soft zone boundaries but yield to VPF zone boundaries. Membership can be defined only by port ID and domain ID. ACL zoning supports all port modes except TL_Ports.

Virtual private fabric zones: Virtual private fabric (VPF) zoning divides the fabric for purposes of controlling discovery and both inbound and outbound traffic. This type of zoning is useful for providing security and reserving paths between devices to guarantee bandwidth. VPF zoning is a type of hard zoning that is hardware enforced. Members can transmit to and receive only from members of the same VPF zone. The VPF zone boundary is secure against both inbound and outbound traffic. VPF zones that include members from multiple switch modules must include the ports of the interswitch links. VPF zones cannot overlap; that is, a port can be a member of only one VPF zone. VPF zone boundaries supersede both soft and ACL zone boundaries. Membership can be defined only by port ID and domain ID. VPF zoning supports all port modes.

Note: Domain ID conflicts can result in automatic reassignment of switch module domain IDs. These reassignments are not reflected in zones that use domain ID and port number pairs or Fibre Channel addresses to define their membership. Be sure to reconfigure zones that are affected by a domain ID
change. To prevent zoning definitions from becoming invalid when the membership is defined by domain ID/port number or Fibre Channel address, you must lock domain IDs.

**Aliases:** To make it easier to add a group of ports or devices to one or more zones, you can create an alias. An alias is a named set of ports or devices that are grouped together for convenience. Unlike zones, aliases impose no communication restrictions between its members. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias.

**Zone sets:** A zone set is a named group of zones. A zone can be a member of more than one zone set. All zones that are not members of a zone set belong to the orphan zone set. The orphan zone set is saved to the switch module. Each switch module in the fabric maintains its own zoning database containing one or more zone sets. This zoning database resides in nonvolatile or permanent memory and is therefore retained after a reset. For information about displaying the zoning database, see [“Configured Zonesets Data window” on page 96](#).

To apply zoning to a fabric, select a zone set and activate it. When you activate a zone set, the switch module distributes that zone set to every switch in the fabric. Therefore, every switch module in the fabric will have identical active zone sets. For information about displaying the active zone set, see [“Active Zoneset Data window” on page 83](#).

**Zoning database:** Each switch module has its own zoning database. The zoning database is made up of all aliases, zones, and zone sets that have been created on the switch or received from other switch modules. The switch module maintains two copies of the zoning database: one copy is maintained in temporary memory for editing purposes; the second copy is maintained in permanent memory. Zoning database edits are made on an individual switch basis and are not propagated to other switch modules in the fabric when saved.

The Auto Save zoning configuration parameter controls whether the temporary zoning database is automatically saved in permanent memory. For more information about the Auto Save parameters, see [“Zoning configuration”](#).

The zoning limits for a fabric are:
- Maximum number of zonesets is 256
- Maximum number of zones is 256
- Maximum number of aliases is 256
- Maximum number of members per zone is 2000
- Maximum number of members per alias is 2000
- Maximum total number of zone and alias members is 2000
- Maximum total number of zone set members is 1000

**Zoning configuration:** You can set the zoning configuration parameters using the SAN Utility or the `Set Zoning Config` command. For information about zoning configuration using the SAN Utility, see [“Using the Zoning Config window” on page 86](#) and [“Set Config command” on page 28](#).

The following parameters make up the zoning configuration:
- Auto Save
- Default Visibility
Auto save: The Auto Save parameter determines whether changes to the active zone set that a switch module receives from other switches in the fabric are saved to permanent memory on that switch module. Changes are saved when an updated zone set is activated. Zoning changes are always saved to temporary memory. However, if Auto Save is enabled, the switch module firmware saves changes to the active zone set in both temporary and permanent memory. If Auto Save is disabled, changes to the active zone set are stored only in temporary memory.

Default visibility: The Default Visibility parameter determines the level of communication that is permitted between devices when there is no active zone set. The default visibility parameter can be set differently on each switch module. When default visibility is enabled (set to All) on a switch module, all ports on the switch can communicate with all ports on switch modules that also have the Default Visibility parameter set to Enabled. When default visibility is disabled (set to None) on a switch module, none of the ports on that switch module can communicate with any other switch in the fabric.

Using the Zoning Config window
Use the Zoning Config window to change the Auto Save and Default Visibility configuration parameters. Complete the following steps to open the Zoning Config window and change configuration parameters:

1. In the Faceplate window, click Zoning → Edit Zoning Config. The Zoning Config window opens.

   ![Zoning Config window](image)

   Figure 10. Zoning Config window

2. Make the necessary changes to the Auto Save and Default Visibility fields and click OK.

Restoring default zoning
Restoring the default zoning clears the switch module of all zoning definitions. Complete the following steps to restore the default zoning for a switch module.

Attention: The use of this command will deactivate any active zone set. If the switch module is not isolated from the fabric, this command will deactivate the active zone set for the entire fabric.

1. In the Faceplate window, click Zoning → Restore Default Zoning.
2. Click OK to confirm that you want to restore default zoning and save changes to the zoning database.

Merging fabrics and zoning
If you join two fabrics, the active zone sets from the two fabrics attempt to merge. The fabrics can consist of a single switch module or many switches already connected together. The switch modules in the two fabrics attempt to create a new active zone set containing the union of the active zone set of each fabric. The propagation of zoning information affects only the active zone set, not the configured zone sets.
Zone merge failure: If a zone merge is unsuccessful, the interswitch links between the fabrics will isolate because of a zone merge failure, which generates an alarm log entry. The reason for the E_Port isolation can also be determined by viewing the port information. See the Port Information Data window on page 96 and the Show command on page 41 (Port keyword).

A zone merge will fail if the two active zone sets have member zones with identical names that differ in content or type. For example, consider Fabric A and Fabric B, each with a zone in its active zone set named "ZS1." Fabric A "ZS1" contains a member specified by Domain ID 1 and Port 1; Fabric B "ZS1" contains a member specified by Domain ID 1 and Port 2. In this case, the merge fails, and the interswitch links between the fabrics are isolated.

Zone merge failure recovery: When a zone merge failure occurs, the conflict that caused the failure must be resolved. You can correct a failure due to a zone conflict by deactivating one of the active zone sets or editing the conflicting zones so that their membership is the same. You can deactivate the active zone set on one switch module if the active zone set on the other switch accurately defines your zoning needs. If not, you must edit the zone memberships and reactivate the zone sets. For information about adding and removing zone members, see Managing zones on page 90. To permit the fabrics to join, reset the ports that were isolated. See Resetting a port on page 113.

Using the Edit Zoning window
Use the Edit Zoning window to edit the zoning database for a specific switch module. To edit the zoning database, in the Faceplate window, click Zone → Edit Zoning. The Edit Zoning window opens.

Note: You can make changes only to an active zone set, which is stored in flash (nonvolatile) memory and retained after setting a switch module.

![Edit Zoning window](image)

Figure 11. Edit Zoning window

The Edit Zoning window displays a Zone Sets tree in the left pane and a Port and Device (or members) tree in the right pane, as shown in Figure 11. Both trees use display conventions similar to the fabric tree for expanding and contracting zone sets, zones, and ports. An expanded port shows the port Fibre Channel address; an expanded address shows the port worldwide name. You can select zone sets, zones, and ports in the following ways:

- Click a zone, zone set, or port icon.
• Right-click to select a zone set or zone and open the corresponding pop-up menu.
• Hold down the Shift key while clicking several consecutive icons.
• Hold down the Ctrl key while clicking several nonconsecutive icons.

Using the toolbar, pop-up menus, or a drag-and-drop method, you can create and manage zone sets and zones in the zoning database. Click **Apply** to save your changes to the zoning database without closing the window. Click **OK** to save your changes to the zoning database and close the window.

The following table explains the toolbar buttons and functions.

<table>
<thead>
<tr>
<th>Toolbar button</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![zone set icon]</td>
<td>Create a new zone set.</td>
</tr>
<tr>
<td>![zone icon]</td>
<td>Create a new zone.</td>
</tr>
<tr>
<td>![alias icon]</td>
<td>Create an additional name for a set of objects.</td>
</tr>
<tr>
<td>![insert icon]</td>
<td>Add the selected zone to a zone set, or add the selected port to a zone.</td>
</tr>
<tr>
<td>![remove icon]</td>
<td>Delete the selected zone from a zone set, or delete the selected port from a zone.</td>
</tr>
</tbody>
</table>

### Managing zone sets
Zoning a fabric involves creating a zone set, creating zones as zone set members, then adding devices as zone members. The zoning database supports multiple zone sets to serve the different security and access needs of your storage area network. Only one zone set can be active at one time. Managing zone sets involves the following tasks:

• Creating zone sets
• Activating and deactivating zone sets
• Copying a zone to a zone set
• Removing a zone from one zone set or from all zone sets
• Removing a zone set
• Removing all zoning definitions

**Note:** Changes that you make to the zoning database are limited to the managed switch module and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric-wide, you must edit the zoning databases on the individual switch modules.

**Creating a zone set:** Complete the following steps to create a zone set:

1. In the Faceplate window, click **Zoning → Edit Zoning**.
   The Edit Zoning window opens.
2. Click **Edit → Create Zone Set**.
   The Create Zone Set window opens.
3. Type a name for the zone set, and click OK. The new zone set name is displayed in the Zone Sets window.

4. Complete one of the following tasks to create new zones in a zone set:
   - Right-click a zone set and select Create A Zone from the pop-up menu. In the Create A Zone window, type a name for the new zone, and click OK. The new zone name is displayed in the Zone Sets window.
   - To copy an existing zone into the new zone set, in the Faceplate window, select the zone and drag it into the new zone set.

5. Click Apply to save changes to the zoning database.

**Activating and deactivating a zone set:** You must activate a zone set to apply its zoning definitions to the fabric. Only one zone set can be active at one time. When you activate a zone set, the switch module distributes that zone set to the temporary zoning database on every switch in the fabric, replacing any zone set of the same name. If Auto Save is enabled, the zone set is saved in the permanent zoning database also. For more information, see “Auto save” on page 86.

The purpose of the deactivate function is to suspend all fabric zoning, which results in free communication fabric-wide or no communication, depending on the default visibility setting. For more information, see “Default visibility” on page 86. It is not necessary to deactivate the active zone set before activating a new one.

Complete the following steps to activate a zone set:
1. In the Faceplate window, click Zoning → Activate Zone Set. The Activate Zoneset window opens.
2. In the Select Zone Set menu, click Zone Set → Activate.

Complete the following steps to deactivate a zone set:
1. In the Faceplate window, click Zoning → Deactivate Zone Set. A message warning you about traffic disruption is displayed.
2. Click Yes to confirm that you want to deactivate the active zone.

**Copying a zone to a zone set:** Complete the following steps to copy an existing zone and its membership from one zone set to another:
1. In the Faceplate window, select the zone and drag it to the zone set you want.
2. Click Apply to save your changes to the zoning database.

**Removing a zone from a zone set or from all zone sets:** Complete the following steps to remove a zone from a zone set or from all zone sets in the database:
1. In the Faceplate window, click Zoning → Edit Zoning. The Edit Zoning window opens.
2. In the Zone Sets tree, select the zone you want to remove.
3. Click Edit → Remove to remove the zone from the zone set, or select Remove from All Zones to remove the zone from all zone sets.
4. Click Apply to save changes to the zoning database.

**Note:** You can use shortcut menus to remove a zone from a zone set or from all zone sets in the database.

**Removing a zone set:** Removing a zone set from the database affects the member zones in the following ways:
- Member zones that are members of other zone sets are not affected.
- Member zones that are not members of other zone sets become members of the orphan zone set. The orphan zone set is saved on the switch module.

Complete the following steps to remove a zone set from the database:
1. In the Faceplate window, click **Zoning → Edit Zoning**. The Edit Zoning window opens.
2. In the Zone Sets tree, select the zone set to be removed.
3. Click **Edit → Remove** to remove the zone set.
4. Click **Apply** to save changes to the zoning database.

**Note:** You can use shortcut menus to remove a zone set from the database.

**Removing all zoning definitions:** To remove all zone and zone set definitions from the zoning database, use one of the following methods:
- Click **Edit → Remove All**. In the Remove All window, click **Yes** to confirm that you want to delete all zones and zone sets.
- Right-click the **Zone Sets** heading at the top of the Zone Sets tree, and select **Clear Zoning** from the pop-up menu. Click **Yes** to confirm that you want to delete all zone sets and zones.

**Managing zones**
Managing zones involves the following tasks:
- Creating a zone in a zone set
- Adding zone members
- Renaming a zone or a zone set
- Removing a zone member
- Removing a zone from a zone set
- Removing a zone from all zone sets
- Changing zone types

**Note:** Changes that you make to the zoning database are limited to the managed switch module and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric-wide, you must edit the zoning databases on the individual switch modules.

**Creating a zone in a zone set:** When a zone is created, its zone type is soft. To change the zone type to a hard zone, see "Changing zone types" on page 92 for more information. See "Zones" on page 84 for information on zone types (soft and hard). Complete the following steps to create a zone in a zone set:
1. In the Faceplate window, click **Zoning → Edit Zoning**. The Edit Zoning window opens.
2. Click **Edit → Create a Zone**. The Create a Zone window opens.
3. Type a name for the new zone and click **OK**. The new zone name is displayed in the Zone Sets window.

**Note:** If you type the name of a zone that already exists in the database, the SAN Utility will create a copy of that zone and its membership in the zone set.
4. Use one of the following methods to add ports or devices to the zone:
• In the zone set tree, select the zone set. In the graphic window, select the port to add to the zone. Click Edit → Add Members.
• Select a port by port number, Fibre Channel address, or worldwide name in the Port or Device tree, and drag it into the zone.
• Select a port by port number, Fibre Channel address, or worldwide name in the Port and Device tree. Right-click the zone and select Add Zone Members from the pop-up menu.

5. Click Apply to save your changes to the zoning database.

**Adding zone members:** Adding a zone member to a zone will affect every zone set in which that zone is a member. To add member ports and devices to a zone, choose one of the following methods:
• Select a port by port number, Fibre Channel address, or worldwide name in the Port and Device tree, and drag it into the zone. To select and drag multiple ports and devices, press and hold the Ctrl key while dragging.
• Select one or more ports by port number, Fibre Channel address, or worldwide name in the Port and Device tree. Right-click the zone and select Add Zone Members from the pop-up menu.

Click Apply to save your changes to the zoning database.

**Note:** Domain ID conflicts can result in automatic reassignment of switch module domain IDs. These reassignments are not reflected in zones that use domain ID and port number pair to define their membership. Be sure to reconfigure zones that are affected by a domain ID change.

**Renaming a zone or a zone set:** Complete the following steps to rename a zone:
1. In the Edit Zoning window, in the Zone Sets tree, click the zone or zone set to be renamed.
2. Click Edit → Rename.
3. In the Rename Zone/Rename Zone Set window, type a new name for the zone and zone set.
4. Click OK.

**Removing a zone member:** Removing a zone member will affect every zone and zone set in which that zone is a member. Complete the following steps to remove a member from a zone:
1. In the Edit Zoning window, select the zone member to be removed.
2. Click Edit → Remove.
3. Click OK to save the changes and close the Edit Zoning window.

**Removing a zone from a zone set:** Removing a zone from a zone set will affect every zone set in which that zone is a member. Zones that are no longer members of any zone set are moved to the orphan zone set. The orphan zone set is saved on the switch module.

Complete the following steps to delete a zone from a zone set:
1. In the Edit Zoning window, select the zone to be removed.
2. Click Edit → Remove.
3. Click OK to save the changes and close the Edit Zoning window.

**Removing a zone from all zone sets:** Complete the following steps to delete a zone from all zone sets:
1. In the Edit Zoning window, select the zone to be removed
2. Click **Edit → Remove Zone from All Sets**.
3. Click **OK** to save the changes and close the Edit Zoning window.

*Changing zone types:* Zones that are no longer members of any zone set are moved to the orphan zone set. The orphan zone set is saved on the switch module.

Complete the following steps to change a zone type:
1. In the Faceplate window, select the switch module with the zone type you want to change.
2. Click **Zoning → Edit Zoning** or click the **Zoning** icon to open the Edit Zoning window.
3. In the Zone Sets tree, select the zone to change.
4. Click **Edit → Set Zone Type**.
   The Set Zone Type window opens.
5. Click **Zone Type → Soft, ACL (hard zoning), or VPF (hard zoning).**
   - Soft zoning is the least restrictive type of zoning.
   - ACL zoning is hard zoning and is enforced by hardware and defines access to a given port. ACL zones need not include interswitch links.
   - VPF zoning is hard zoning that defines ports that can communicate with each other. VPF zones must include interswitch links.

For more information about zone types, see "Zones" on page 84.

*Managing aliases:* An alias is a named set of ports or devices that are grouped together for convenience. An alias is not a zone and cannot have a zone or another alias as a member. This section describes how to create, remove, and add a member to an alias.

**Note:** Changes that you make to the zoning database are limited to the managed switch module and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switch modules.

*Creating an alias:* Complete the following steps to create an alias:
1. In the Faceplate window, click **Zoning → Edit Zoning**.
   The Edit Zoning window opens.
2. Click **Edit → Create Alias**.
   The Create Alias window opens.
3. Type a name for the alias and click **OK**. The alias name is displayed in the Zone Sets window.
4. Click **OK** to save the alias name to the zoning database.

*Adding a member to an alias:* To add a member to an alias, use one of the following methods:
- Drag-and-drop method
- Menu options

Complete the following steps to add a member to an alias using the drag-and-drop method:
1. In the right pane of the Faceplate window, click and hold down the mouse button on the member to be added to the alias.
2. Drag the selected member from the right pane to the alias in the left pane.

Complete the following steps to add a member to an alias using the menu options:
1. Click **Zoning → Edit Zoning**.
   
   The Edit Zoning window opens.
2. In the left pane of the Edit Zoning window, select an alias.
3. In the right pane, select the member to add to the selected alias.
4. Use one of the following actions:
   • Click **Edit → Add Members**.
   • Click **Insert**.
5. Click **OK** to save the changes and close the Edit Zoning window.

**Removing an alias from all zones:** Complete the following steps to remove an alias from all zones:
1. In the Zone Sets tree of the Edit Zoning window, select the alias to be removed.
2. Click **Edit → Remove Alias from All Zones**.
3. In the Remove window, click **Yes**.

**Managing switch modules**

This section describes the following tasks that manage switch modules in the fabric:
• Displaying switch module information
• Managing alarms
• Exporting name server information to a file
• Paging a switch module
• Setting the switch module date and time
• Resetting a switch module
• Configuring a switch module
• Archiving a switch module
• Managing firmware

**Displaying switch module information**

The Faceplate window and data windows provide the following specific switch module information:
• Name server information
• Switch module specifications and addresses
• Configuration parameters
• Performance statistics
• Configured zone sets
• Alarm log information
A fabric updates the Topology and Faceplate windows by forwarding changes in status to the network management workstation as they occur. You can use the fabric to update the switch module status, or you can refresh the switch status at any time. To refresh a switch module status that is displayed, use one of the following actions:

- Click **Refresh**.
- Click **View → Refresh**.
- Press the F5 key.
- Right-click a switch module in the Topology window and click **Refresh Switch**.
- Right-click in the graphic window in the Faceplate window, and click **Refresh Switch**.

**Name Server data window:** The Name Server data window displays information about the devices that are logged in to the fabric. Click the **Name Server** tab below the data window to display name server information for all devices that are logged in to the selected fabric. To narrow the display to devices that are logged in to specific switch modules, select one or more switches in the fabric tree or the Topology window. For a description of the entries in the Name Server Data window, see Table 19. For exporting name server information, see “Exporting alarm log information to a file” on page 98.

**Note:** Internal ports 1 through 14 are fixed.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device number in the fabric</td>
</tr>
<tr>
<td>Switch</td>
<td>Switch module name</td>
</tr>
<tr>
<td>Port</td>
<td>Port number: Ext1:0, Ext2:15</td>
</tr>
<tr>
<td>Address</td>
<td>Fibre Channel address</td>
</tr>
<tr>
<td>Type</td>
<td>Node type</td>
</tr>
<tr>
<td>NWWN</td>
<td>Node worldwide name</td>
</tr>
<tr>
<td>PWWN</td>
<td>Port worldwide name</td>
</tr>
<tr>
<td>Vendor</td>
<td>Host bus adapter and device vendor</td>
</tr>
<tr>
<td>FC-4 types</td>
<td>Device Fibre Channel protocol types</td>
</tr>
<tr>
<td>Active zones</td>
<td>Zones in the current active zone set that contains the device</td>
</tr>
</tbody>
</table>
Switch Data window: The Switch Data window displays current network and switch module information for the selected switches. For more information about the switch data window, see "Configuring a switch module" on page 99. To open the Switch Data window, select one or more switch modules in the Topology window and click the Switch tab below the window. You can also open the Switch Data window from the Faceplate window.

Table 20. Switch data window entries

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FcAddress</td>
<td>Switch module Fibre Channel address</td>
</tr>
<tr>
<td>World Wide name</td>
<td>Switch module worldwide name</td>
</tr>
<tr>
<td>Reason for status</td>
<td>Additional status information</td>
</tr>
<tr>
<td>User name</td>
<td>Name of user</td>
</tr>
<tr>
<td>Login level</td>
<td>Security level</td>
</tr>
<tr>
<td>Security enabled</td>
<td>Fabric security on the switch module that enforces account names and passwords</td>
</tr>
<tr>
<td>Vendor</td>
<td>Switch module manufacturer</td>
</tr>
<tr>
<td>Flash version</td>
<td>Active flash</td>
</tr>
<tr>
<td>Inactive flash version</td>
<td>Inactive firmware version</td>
</tr>
<tr>
<td>PROM/Flasher version</td>
<td>Firmware version</td>
</tr>
<tr>
<td>MAC address</td>
<td>Media access control address</td>
</tr>
<tr>
<td>IP address</td>
<td>Internet protocol address</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Mask that determines the IP address subnet</td>
</tr>
<tr>
<td>Gateway</td>
<td>Gateway address</td>
</tr>
<tr>
<td>Negotiated domain ID</td>
<td>The domain ID currently in use by the fabric</td>
</tr>
<tr>
<td>Configured domain ID</td>
<td>The domain ID defined by the network administrator</td>
</tr>
<tr>
<td>Domain ID lock</td>
<td>Domain ID lock status. Prevents (True) or permits (False) dynamic domain ID reassignment</td>
</tr>
<tr>
<td>Number of ports</td>
<td>Number of ports on the switch module</td>
</tr>
<tr>
<td>Switch type</td>
<td>IBM Fibre Channel switch module model</td>
</tr>
<tr>
<td>Operational state</td>
<td>Switch module operational state: Online, offline, and diagnostic</td>
</tr>
<tr>
<td>Administrative state</td>
<td>Current switch module administrative state: Online, offline, and diagnostic</td>
</tr>
<tr>
<td>Configured Admin State</td>
<td>Switch module administrative state that is stored in the switch configuration</td>
</tr>
<tr>
<td>MFS timeout</td>
<td>Multiframe sequencing timeout value</td>
</tr>
<tr>
<td>RA timeout</td>
<td>Resource allocation timeout value</td>
</tr>
<tr>
<td>RT timeout</td>
<td>Receiver transmitter timeout value</td>
</tr>
<tr>
<td>ED timeout</td>
<td>Error detect timeout value</td>
</tr>
<tr>
<td>Zoning merge mode</td>
<td>Active zone set merge or all zone set merge</td>
</tr>
<tr>
<td>Zoning merge auto save</td>
<td>Zoning auto save status. Saves zoning updates in temporary and permanent memory (True) or only in temporary memory (False).</td>
</tr>
<tr>
<td>Zoning default visibility</td>
<td>Zoning visibility status. Permits (ALL) or prevents (None) communication with other switch modules in the absence of an active zone set.</td>
</tr>
</tbody>
</table>
Table 20. Switch data window entries (continued)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Fan 1 status</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Fan 2 status</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Fan 3 status</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Power supply 1 status</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Power supply 2 status</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Beacon status</td>
<td>Beacon status. Port Logged-in LEDs are flashing (On) or not (Off).</td>
</tr>
<tr>
<td>Broadcast support</td>
<td>Broadcast support status. Broadcast support is enabled or disabled (default).</td>
</tr>
<tr>
<td>Inband enabled</td>
<td>Inband management status. Permits (True) or prevents (False) a switch module from being managed over an ISL.</td>
</tr>
<tr>
<td>Switch date</td>
<td>Switch module time and date</td>
</tr>
</tbody>
</table>

**Link data window:** The Link data window displays information about all switch module links in the fabric or selected links. This information includes the switch module name and port number at the end of each link. To open the Link data window, click the **Link** tab below the window.

**Fabric view port graphing application:** You can use the Fabric View application to view port performance as graphs. The Fabric View window displays data communication rates and total errors for selected ports as shown in Figure 23 on page 120. You can graph communication data rates in frames per second or KB per second. See “Using the Fabric View application” on page 120 for information about tasks that can be performed when using the Fabric View application.

**Port Statistics Data window:** The Port Statistics Data window displays port performance data for the selected ports. To open the Port Statistics Data window, click the **Port Stats** tab below the data window in the Faceplate window. For a description of the Port Statistics Data window entries, see Table 28 on page 106.

The Statistics menu is accessible in the Port Statistics Data window, and provides different ways to view detailed port information. Click the down arrow to open the Statistics menu. In the Statistics menu, you can:

- Click **Absolute** to view the total count of statistics since the last switch module reset.
- Click **Rate** to view the number of statistics counted per second over the polling period.
- Click **Baseline** to view the total count of statistics since the last time the baseline was set.
- Click **Clear Baseline** to set the current baseline.

**Port Information Data window:** The Port Information Data window displays port detail information for the selected ports. To open the Port Information Data window, click the **Port Info** tab below the data window in the Faceplate window. For a description of the Port Information Data window entries, see Table 29 on page 108.

**Configured Zonesets Data window:** The Configured Zonesets Data window displays all zone sets, zones, and zone membership in the zoning database. To
open the Configured Zonesets Data window, click the **Configured Zonesets** tab below the data window in the Faceplate window shown in [Figure 13](#).

![Figure 13. Zonesets Data window](image)

The Configured Zonesets Data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle to the left of an entry in the tree indicates that you can expand the entry. Click this handle or double-click the following entries to expand or contract them:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its members by port number, worldwide name, or Fibre Channel address.

**Alarm Log Data window:** The Alarm Log Data window displays switch module event information. To open the Alarm Log Data window, click the **Alarm Log** tab below the data window in the Faceplate window.

**Managing alarms**

You can configure the switch module to generate and log alarms. To display the Alarm Log, click the **Alarm Log** tab in the Faceplate window. For information about the alarm log, see [Alarm Log Data window](#). You can also export the alarm log to a file in XML format.

**Configuring alarms:** Configuring an alarm involves choosing an event type, rising and falling thresholds, a sampling interval, and then enabling or disabling the alarm.

Complete the following steps to configure an alarm:

1. In the Faceplate window, click **Switch → Configure Alarm Thresholds**.
2. The Alarm Threshold Configuration window shown in [Figure 14 on page 98](#) prompts you to select an event, set thresholds, set a sampling interval, and enable or disable the alarm.
3. Select an event type from the **Alarm Threshold** pull-down menu. Choose from the following options:
   - CRC error monitoring
   - Decode error monitoring
   - ISL monitoring
   - Login monitoring
   - Logout monitoring
   - Loss of signal monitoring

4. Enter a value in the **Falling Threshold** field. The falling threshold is the event count above which an event becomes eligible for logging in the alarm log.

5. Enter a value in the **Rising Threshold** field. The rising threshold is the event count above which an event is logged. After the count exceeds the rising threshold, one alarm is logged. The switch module will not generate another alarm for that event until the count falls below the falling threshold and rises again above the rising threshold.

6. Enter a sample interval, in milliseconds. The sample interval defines the period of time in which to count events.

7. Select the **Enable** check box to make the alarm eligible for use.

8. Repeat step 3 through step 7 for each alarm you want to configure or enable.

9. Select the **Enable Alarm Threshold Generation** check box to activate all alarms enabled in step 7.

10. Click **OK** to save all changes.

**Exporting alarm log information to a file:** Complete the following steps to save the switch module alarm log to a file:

1. In the Faceplate window, click **Switch** → **Export Alarm Log**.
2. Type a file name in the Save window.
3. Click **Save**.

**Exporting name server information to a file**

Complete the following steps to save switch module name server information to a file:

1. In the Topology window, click **Switch** → **Export Name Server**.
2. Type a file name in the Save window.
3. Click **Save**.
Paging a switch module
You can use the beacon feature to page a switch module. The beacon feature causes both external port Logged-in LEDs to flash, making it easier to locate the switch module you are paging. To page a switch, in the Faceplate window, click Switch → Toggle Beacon. To cancel the beacon, click Toggle Beacon.

Setting the date and time
Complete the following steps to set the date and time on a switch module:
1. Select a switch in the Topology window and open the Faceplate window.
2. In the Faceplate window, click Switch → Set Date/Time
3. Type the year, month, day and time in the Switch Date and Time window, and then click OK. The system prompts you to reset the switch module to implement the new date and time.

Resetting a switch module
Resetting a switch module restarts the switch using configuration parameters in memory. You can reset a switch module using the following methods:
- Select the switch module to be reset in the fabric tree. Click Switch → Reset Switch.
- Remove and then reinsert the Fibre Channel switch module in the BladeCenter unit.

Configuring a switch module
The SAN Utility is used to configure the switch module. Switch module configuration is divided into two areas: chassis configuration and network configuration. Chassis configuration specifies parameters that relate to switch module identity on the Fibre Channel network. Network configuration specifies parameters that relate to switch module identity on the Ethernet network. To open the Switch Properties window, click Switch → Switch Properties. You can also right-click a switch graphic in the Topology window or Faceplate window and click Switch Properties.

Switch module properties: Use the Switch Properties window shown in Figure 15 to change the module name, administrative state and domain ID; to enable or disable broadcast support; and to enable or disable inband management. The timeout values are displayed for reference purposes only when the switch module is online. These fields become active when the switch module is taken offline. After making changes, click OK to put the new values into effect.

Figure 15. Switch Properties window
Symbolic name: The symbolic name is a user-defined name that identifies the switch module.

Switch module administrative state: The switch module administrative state determines the operational state of the switch and its ports. The switch module administrative state exists in two forms: the configured administrative state and the current administrative state. The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. The SAN Utility always makes changes to the configured administrative state. The current administrative state is the state that is applied to the switch module for temporary purposes and is not retained across switch resets. The current administrative state is set using the Set Switch command. For more information about the Set Switch command, see "Set command" on page 26.

Table 21. Switch module administrative states

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online</td>
<td>The switch module is available.</td>
</tr>
<tr>
<td>Offline</td>
<td>The switch module is unavailable.</td>
</tr>
<tr>
<td>Test</td>
<td>The switch module is in diagnostics mode and is unavailable.</td>
</tr>
</tbody>
</table>

Domain ID and Domain ID Lock: The domain ID is a unique Fibre Channel identifier for the switch module. The Fibre Channel address consists of the domain ID, port ID, and the Arbitrated Loop Physical Address (ALPA). The maximum number of switch modules within a fabric is 239, with each switch having a unique domain ID.

Switch modules come from the factory with the domain IDs unlocked. This means that if there is a domain ID conflict in the fabric, the switch module with the highest principal priority, or the principal switch, will reassign any domain ID conflicts and establish the fabric. If you lock the domain ID on a switch module and a domain ID conflict occurs, the switch module with the higher WWN will be isolated as a separate fabric, and the Logged-in LEDs on both switch modules will flash to show the affected ports. See "Set Config command" on page 28 for information about the switch module keyword and the Domain ID Lock and Principal Priority parameters.

If you connect a new switch module to an existing fabric with its domain ID unlocked and a domain conflict occurs, the new switch module will be isolated as a separate fabric. However, you can remedy this by resetting the new switch module or taking it offline then back online. The principal switch module will reassign the domain ID, and the switch will join the fabric.

Note: Domain ID reassignment is not reflected in zoning that is defined by domain ID and port number pair. You must reconfigure zones that are affected by domain ID reassignment.

Broadcast support: Broadcast is supported by the switch module, which enables TCP/IP support. Broadcast is implemented using the proposed standard specified in Multi-Switch Broadcast for FC-SW-3, T11 Presentation Number T11/02-031v0. The FSPF is used to set up a fabric spanning tree used in transmission of broadcast frames. Broadcast frames are retransmitted on all ISLs indicated in the spanning tree and all online F/FL_Ports. Broadcast zoning is supported with ACL and VPF hard zones. When a broadcast frame is received, these hard zones are enforced at the F/FL_Port. If the originator of the broadcast is in a hard zone, the frame is
retransmitted on all online F/FL_Ports within the hard zone. If the originator of the broadcast frame is not in a hard zone, the frame is retransmitted on online F/FL_Ports that are not in a hard zone.

**In-band management:** In-band management is the ability to manage switch modules across interswitch links. If you disable in-band management on a particular switch module, you can no longer communicate with that switch module by means other than a direct Ethernet or serial connection.

**Timeout values:** The switch module timeout values determine the timeout values for all external ports on the switch. Table 22 describes the switch module timeout parameters. R_A_TOV, R_T_TOV, or E_D_TOV values must be the same for all switch modules in the fabric.

**Note:** Timeout values can be changed only if the switch module operational state is offline.

**Table 22. Timeout values**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R_A_TOV</td>
<td>Resource Allocation Timeout. Represents the maximum time a frame can be delayed in the fabric and still be delivered. The default is 10000 milliseconds.</td>
</tr>
<tr>
<td>R_T_TOV</td>
<td>Receiver Transmitter Timeout. The amount of time that Sync can be lost between two ports before Link Failure is detected. The default is 100 milliseconds.</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>Error Detect Timeout. Represents the maximum round trip time that an operation between two N_Ports requires. The default is 2000 milliseconds.</td>
</tr>
</tbody>
</table>

**Network properties**

Use the Network Properties window shown in Figure 16 on page 102 to change IP and SNMP configuration parameters. After making changes, click OK to put the new values into effect. To open the Network Properties window, click **Switch → Network Properties**.

**Note:** The Read Community, Trap Community, and Write Community settings are like passwords; therefore, they are write-only fields. The current settings are not displayed.
IP configuration: The IP configuration identifies the switch module on the Ethernet network and determines which start (boot) method to use. Start methods described in the following table are for external and internal ports. Table 23 describes the IP configuration parameters.

Table 23. IP configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Internet protocol (IP) address for the Ethernet port.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>When the BladeCenter unit is turned on, the management module loads the following factory default Ethernet IP addresses:</td>
</tr>
<tr>
<td></td>
<td>• Switch module bay 3: 192.168.70.129</td>
</tr>
<tr>
<td></td>
<td>• Switch module bay 4: 192.168.70.130</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Subnet mask address for the Ethernet port. The default value is 255.255.255.0.</td>
</tr>
<tr>
<td>Boot method</td>
<td>Static - Uses the IP configuration parameters entered in the Switch</td>
</tr>
<tr>
<td></td>
<td>Properties window.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP gateway address. The default value is 10.90.90.254.</td>
</tr>
</tbody>
</table>

Remote logging: The Remote Logging (syslog) feature enables saving of the log information to a remote host that supports the syslog protocol. When enabled, the log entries are sent to the syslog host at the IP address that you specify in the **Logging Host IP Address** field. Log entries are saved in the internal switch module log whether this feature is enabled or not.

To save log information to a remote host, you must edit the syslog.conf file and then restart the syslog daemon. The syslog.conf file on the remote host must contain an entry that specifies the name of the log file in which to save error messages. Add the following line to the syslog.conf file:

```
local0.info <tab> /var/adm/messages.name
```

Use <tab> to separate the selector field (local0.info) and action field, which contains the log file path name (/var/adm/messages/messages.name).

Archiving a switch module
You can create an XML archive file containing the switch module configuration parameters. Archived parameters include the following:
Switch module properties and statistics
IP configuration
SNMP configuration
Port properties and statistics
Zoning configuration

You can use this archive file to restore the configuration on the same switch module or on a replacement switch. You can also use the archive file as a template for configuring new switch modules to add to a fabric. Security settings and user account information are not archived. You can use the archive later to restore the switch module. For more information, see "Restoring a switch module" on page 119.

Complete the following steps to archive a switch module configuration:
1. In the Faceplate window, click Switch → Archive.
2. In the Save window, type a file name.
3. Click Save.

Managing firmware
The switch module memory is partitioned for two firmware images. This is useful when you are upgrading firmware so that both the old and new firmware are maintained on the switch module. When you load new firmware, the currently active firmware is preserved and the new firmware becomes the second image or the fallback version. You can activate either firmware image. If you activate the fallback firmware, the current firmware becomes the fallback version.

Loading firmware: The switch module does not have to be offline for you to download firmware. However, the switch module must be reset to activate the new firmware, which requires administrative authority. The SAN Utility prompts you to reset the switch module after the firmware is loaded.

Complete the following steps to load firmware to a switch module:
1. In the Faceplate window, click Switch → Load Firmware.
   The Firmware Upload window opens.
2. In the Firmware Upload window, click Select to browse and select the firmware file to be uploaded.
3. Click Start to begin the firmware install process.
4. When the installation is complete, click Close. The Firmware Upload window closes.
5. The SAN Utility prompts you to reset the switch module. Click OK to reset the switch and activate the new firmware.

Activating the fallback firmware: Complete the following steps to activate the fallback firmware:
1. In the Faceplate window, click Switch → Firmware Fallback.
2. The Firmware Fallback window displays the file name of the current firmware and the fallback firmware versions. Click Yes to select the fallback firmware or No to cancel.
3. The SAN Utility prompts you to reset the switch module. Click OK to reset the switch and activate the new fallback firmware.
Managing ports

This section describes the following tasks that manage ports and devices:

- Displaying port information
- Configuring ports

**Displaying port information**

Port information is available primarily in the Faceplate window shown in Figure 17. Faceplate Display Data windows provide information and statistics for switch modules and ports. Use the Topology window to show the status information for links between switch modules.

![Faceplate Display Data window](image)

**Figure 17. Faceplate Display Data window**

**Monitoring port status:** The Faceplate window provides the following port related information:

- SNMP configuration (see “Fibre Channel switch module monitoring using SNMP” on page 117 for more information)
- Port mode
- Port operational state
- Port speed
- Port media

To display port number and status information for a port, position the cursor over a port displayed in the Faceplate window. The status information changes, depending on the View menu option that you select.

**Displaying port modes:** To display port mode status, from the Faceplate window, click **View → View Port Modes.** Table 24 lists the available port modes and their descriptions.

**Table 24. Port mode descriptions**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Fabric port</td>
</tr>
<tr>
<td>FL</td>
<td>Fabric loop port</td>
</tr>
<tr>
<td>TL</td>
<td>Translated loop port</td>
</tr>
<tr>
<td>G</td>
<td>Generic port</td>
</tr>
<tr>
<td>GL</td>
<td>Generic fabric loop port</td>
</tr>
<tr>
<td>E</td>
<td>Expansion port</td>
</tr>
</tbody>
</table>
Table 24. Port mode descriptions (continued)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Donor port</td>
</tr>
</tbody>
</table>

Displaying port operational states: To display the operational state of each port, in the Faceplate window, click **View** → **View Port States**. Table 25 lists and describes the available operational states. The port operational state refers to the actual port state and not the administrative state you might assign.

Table 25. Port operational states

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On</td>
<td>Online - The port is active and ready to send data.</td>
</tr>
<tr>
<td>la</td>
<td>Inactive - The port operational state is Offline, but the administrative state is Online.</td>
</tr>
<tr>
<td>Off</td>
<td>Offline - The port is active and can receive a signal but cannot accept a device login.</td>
</tr>
<tr>
<td>Tst</td>
<td>Diagnostics - The port is in Diagnostics mode in preparation for testing.</td>
</tr>
<tr>
<td>Dn</td>
<td>Down – The port is inactive or disabled; it is not receiving a signal and cannot be logged in to.</td>
</tr>
</tbody>
</table>

Displaying port speeds: To display the speed of each port in the Faceplate window, click **View** → **View Port Speeds**. Table 26 lists the available speeds.

Table 26. Port speeds

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gb</td>
<td>1 Gbps (gigabits per second) transmission speed</td>
</tr>
<tr>
<td>2 Gb</td>
<td>2 Gbps transmission speed</td>
</tr>
</tbody>
</table>

Displaying SFP module media status: To display SFP module media status, click **View** → **View Port Media**. Table 27 lists and describes the available media states.

Table 27. SFP module media view

<table>
<thead>
<tr>
<th>Media icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>The SFP module is online (green)</td>
</tr>
<tr>
<td>*</td>
<td>The SFP module is offline (gray)</td>
</tr>
<tr>
<td>None</td>
<td>The port is empty; no SFP module is detected or installed</td>
</tr>
</tbody>
</table>

Port graphing and Fabric View application:

You can use the Fabric View application to view port performance as graphs. The Fabric View window displays data communication rates and total errors for selected ports as shown in **Figure 23 on page 120**. You can graph communication data rates using either frames per second or KB per second. For more information about port graphing, see **Using the Fabric View application** on page 120.
**Port Statistics Data window:** The Port Statistics Data window displays statistics about port performance. To open the Port Statistics Data window, select one or more ports in the Faceplate window and click the Port Stats tab in the data pane of the Faceplate window. Table 28 describes the Port Statistics Data window entries. See Table 37 on page 122 for information about port numbering and mapping.

The Statistics menu is available on the Port Statistics Data window. Click the down arrow to open the Statistics menu and then use one of the following methods to view the detailed port information:

- Click **Absolute** to view the total count of statistics since the last switch module reset.
- Click **Rate** to view the number of statistics counted per second over the polling period.
- Click **Baseline** to view the total count of statistics since the last time the baseline was set.

When viewing baseline statistics, click **Clear Baseline** to set the current baseline.

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start time</td>
<td>The beginning of the period of time for which the statistics apply. The start time for the Absolute view is not applicable. The start time for the Rate view is the beginning of the polling interval. The start time for the Baseline view is the last time the baseline was set.</td>
</tr>
<tr>
<td>End time</td>
<td>The last time the statistics were updated on the display.</td>
</tr>
<tr>
<td>Total time</td>
<td>Total time period from start time to end time.</td>
</tr>
<tr>
<td>Login count</td>
<td>Number of logins that have occurred on the switch module.</td>
</tr>
<tr>
<td>Logout count</td>
<td>Number of logouts that have occurred on the switch module.</td>
</tr>
<tr>
<td>AI init count</td>
<td>Number of times the port entered the initialization state.</td>
</tr>
<tr>
<td>Invalid destination address</td>
<td>Number of address identifiers (S_ID, D_ID) found to be in error.</td>
</tr>
<tr>
<td>Total LIP received</td>
<td>Number of loop initialization primitive frames received.</td>
</tr>
<tr>
<td>LIP F7F7 count</td>
<td>A loop initialization primitive frame used to acquire an Arbitrated Loop Physical Address (AL_PA).</td>
</tr>
<tr>
<td>LIP F8F7 count</td>
<td>Currently not used.</td>
</tr>
<tr>
<td>LIP F7AIPs count</td>
<td>This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, might have noticed a performance degradation and is trying to restore the loop.</td>
</tr>
<tr>
<td>LIP F8AIPs Count</td>
<td>This LIP denotes a loop failure detected by the L_Port identified by AL_PS.</td>
</tr>
<tr>
<td>LIP AIPdAIPs Count</td>
<td>Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.</td>
</tr>
<tr>
<td>Class 2 In Frames</td>
<td>Number of class 2 frames received by this port.</td>
</tr>
<tr>
<td>Class 2 Out Frames</td>
<td>Number of class 2 frames transmitted by this port.</td>
</tr>
<tr>
<td>Class 2 Words In</td>
<td>Number of class 2 words received by this port.</td>
</tr>
<tr>
<td>Class 2 Words Out</td>
<td>Number of class 2 words transmitted by this port.</td>
</tr>
<tr>
<td>Class 3 In Frames</td>
<td>Number of class 3 frames received by this port.</td>
</tr>
<tr>
<td>Class 3 Out Frames</td>
<td>Number of class 3 frames transmitted by this port.</td>
</tr>
<tr>
<td>Class 3 Words In</td>
<td>Number of class 3 words received by this port.</td>
</tr>
<tr>
<td>Entry</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Class 3 Words Out</td>
<td>Number of class 3 words transmitted by this port.</td>
</tr>
<tr>
<td>Decode Error Count</td>
<td>Number of invalid transmission words detected during decoding. Decoding is from the 10-bit characters and special K characters.</td>
</tr>
<tr>
<td>Loss Of Sync Count</td>
<td>Number of synchronization losses (&gt;100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.</td>
</tr>
<tr>
<td>Invalid CRC Count</td>
<td>Number of invalid CRC frames detected.</td>
</tr>
<tr>
<td>Tx Wait Count</td>
<td>Number of times the port entered a wait state because it was out of buffer-to-buffer credits.</td>
</tr>
<tr>
<td>Class 3 Toss Count</td>
<td>Number of class 2 and class 3 sequences that were discarded by this port. A sequence can be discarded because of detection of a missing frame (based on SEQ_CNT), detection of an E_D_TOV timeout, receiving a reject frame, receiving frames for a stopped sequence, or other causes.</td>
</tr>
<tr>
<td>FReject Count</td>
<td>Number of frames, from devices, that have been rejected. Frames can be rejected for many reasons.</td>
</tr>
<tr>
<td>FBusy Count</td>
<td>Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.</td>
</tr>
<tr>
<td>Link Failures</td>
<td>Number of optical link failures detected by this port. A link failure is a loss of synchronization for a period of time greater than the value of R_T_TOV or by loss of signal while not in the offline state. A loss of signal causes the switch module to attempt to reestablish the link. If the link is not reestablished by the time specified by R_T_TOV, a link failure is counted. A link reset is performed after a link failure.</td>
</tr>
<tr>
<td>Primitive Sequence Errors</td>
<td>Number of bad primitives received by the port.</td>
</tr>
<tr>
<td>Rx Link Resets</td>
<td>Number of link reset primitives received from an attached device.</td>
</tr>
<tr>
<td>Tx Link Resets</td>
<td>Number of link reset primitives sent from this port to an attached port.</td>
</tr>
<tr>
<td>Rx Offline Sequences</td>
<td>Number of offline sequence primitives received by the port.</td>
</tr>
<tr>
<td>Tx Offline Sequences</td>
<td>Number of offline primitives transmitted by the port.</td>
</tr>
<tr>
<td>Total Errors</td>
<td>Total number of primitive and nonprimitive port link errors.</td>
</tr>
<tr>
<td>Total Tx Frames</td>
<td>Total number of frames transmitted by the port.</td>
</tr>
<tr>
<td>Total Rx Frames</td>
<td>Total number of frames received by the port.</td>
</tr>
<tr>
<td>Total Tx Words</td>
<td>Total number of words transmitted by the port.</td>
</tr>
<tr>
<td>Total Rx Words</td>
<td>Total number of words received by the port.</td>
</tr>
<tr>
<td>Total Link Resets</td>
<td>Number of link-reset primitives that are transmitted by the port.</td>
</tr>
<tr>
<td>Total Offline Sequences</td>
<td>Total number of offline sequences transmitted and received by the port.</td>
</tr>
</tbody>
</table>

See [Table 37 on page 122](#) for information about port numbering and mapping.

**Port Information data window:** The Port Information data window displays port detail information for the selected port. To open the Port Information data window,
click the **Port Info** tab below the data window in the Faceplate window.

**Table 29. Port Information Data window entries**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Address</td>
<td>Port Fibre Channel address.</td>
</tr>
<tr>
<td>Administrative Port Mode</td>
<td>The current administrative port mode: GL, G, FL, F, TL.</td>
</tr>
<tr>
<td>Operational Port Mode</td>
<td>The operational port mode.</td>
</tr>
<tr>
<td>Administrative Port State</td>
<td>The current administrative port state: online, offline, diagnostics, or down.</td>
</tr>
<tr>
<td>Operational Port State</td>
<td>The operational port state.</td>
</tr>
<tr>
<td>Configured Administrative Port State</td>
<td>The port administrative state that is stored in the switch module configuration.</td>
</tr>
<tr>
<td>Logged In</td>
<td>Indicates whether logged in or not.</td>
</tr>
<tr>
<td>E Port Connection Status</td>
<td>Indicates whether the E_Port connection is enabled.</td>
</tr>
<tr>
<td>E Port Isolation Reason</td>
<td>Indicates why the E_Port is isolated.</td>
</tr>
<tr>
<td>MFS Mode</td>
<td>Port tuning indicator.</td>
</tr>
<tr>
<td>I/O Stream Guard</td>
<td>Whether RSCN suppression is enabled or disabled.</td>
</tr>
<tr>
<td>Administrative Port Speed</td>
<td>The speed requested by the user.</td>
</tr>
<tr>
<td>Operational Port Speed</td>
<td>The speed actually used by the port.</td>
</tr>
<tr>
<td>TLMODE</td>
<td>Indicates if TL target or TL initiator is used.</td>
</tr>
<tr>
<td>BB Credits</td>
<td>Indicates whether the buffer-to-buffer credits are set.</td>
</tr>
<tr>
<td>Ext Credits Requested</td>
<td>Indicates whether the extended credits are requested for ports.</td>
</tr>
<tr>
<td>Medium</td>
<td>The SFP module type.</td>
</tr>
</tbody>
</table>

**Name Server Data window**: The Name Server Data window displays information about the port and the connected device. To open the Name Server Data window, select one or more switch modules in the Topology window and click the **Name Server** tab below the data window. You can also open the Name Server Data window in the Faceplate window. See [Table 19 on page 94](#) for a description of the Name Server Data window entries.

**Configuring ports**

**Note**: For external ports (0, 15), all port parameters apply. For internal ports, only the port state setting is configurable.

The external Fibre Channel ports are self-configuring GL_Ports that auto-negotiate transmission speeds of 1 Gbps or 2 Gbps depending on the connected device. A GL_Port connects to a loop of public devices or a single device and configures itself as a fabric loop port (FL_Port), fabric port (F_Port), or an expansion port (E_Port). Each external port has 12 buffer credits. This enables a cable length up to 20 km at 1 Gbps or 10 km at 2 Gbps. Eleven credits from one port can be borrowed by the other port to extend transmission distances.

The buffer credit flow control mechanism provides a way to ensure full use of the media, regardless of length, by providing for frame streaming. With frame streaming, the sender can transmit as many frames as there are credits without
having to wait for a response to one frame before transmitting the next frame. The media can then be continuously in use at its rated capacity.

The external port (0,15) settings or characteristics are configured using the Port Properties window shown in Figure 18. To open the Port Properties window, select one or more external ports and click **Port → Port Properties**.

![Figure 18. External Port Properties window](image)

The Port Properties window displays the switch module name and the selected external ports. Use the Port Properties window to change the following parameters:

- Port state
- Port speed
- Port mode
- TL mode
- Port buffer credits
- I/O stream guard (RSCN suppression)

Internal port (1 through 14) configuration is limited to the port state as shown in Figure 19. To open the Port Properties window, select one or more internal ports and click **Port → Port Properties**.

![Figure 19. Internal Port Properties window](image)

**Changing port administrative states:** The Port Administrative state determines the operational state of a port. The port administrative state exists in two forms: the configured administrative state and the current administrative state.
The Configured Administrative state is the state that is saved in the switch module configuration and is preserved across switch module resets. The SAN Utility always makes changes to the configured administrative state.

The Current Administrative state is the state that is applied to the port for temporary purposes and is not preserved across switch module resets. The current administrative state is set using the Set Port command. See "Set Port command" on page 36 for more information. See Table 30 for additional port administrative state descriptions.

The Port Administrative state determines the internal and external port operational state. The port administrative state refers to the requested state in the SAN Utility or through a Telnet command. The port operational state refers to the state actually used by the port.

Complete the following steps to change the port administrative state:
1. Select one or more ports in the Faceplate window.
2. Click Port → Port Properties. The Port Properties window opens.
3. Click the Port States that corresponds to the port state you want.
4. Click OK to write the new port state to the switch module.

<table>
<thead>
<tr>
<th>Table 30. Port administrative states</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
</tr>
<tr>
<td>Online</td>
</tr>
<tr>
<td>Offline</td>
</tr>
<tr>
<td>Test</td>
</tr>
</tbody>
</table>

**Changing port speeds (external ports only):** The switch module external ports (0,15) are capable of transmitting and receiving at 1 Gbps or 2 Gbps. The ports are configured for either transmission speed or to sense the transmission speed of the device to which it is connected. Internal ports (1 through 14) are fixed at 2 Gbps. Table 31 describes the port speeds. Complete the following steps to change the port speed:
1. Select one or more ports in the Faceplate window.
2. Click Port → Port Properties.
3. Select the speed that you want.
4. Click Apply to write the new port speed to the switch module.

<table>
<thead>
<tr>
<th>Table 31. Port speeds</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
</tr>
<tr>
<td>Auto-detect</td>
</tr>
<tr>
<td>1 Gb</td>
</tr>
<tr>
<td>2 Gb</td>
</tr>
</tbody>
</table>

**Changing port modes (external ports only):** The switch module external ports (0,15) support both public and private devices as single devices or in loops. External ports can be configured to self-discover the proper mode to match the
device or switch module to which it is connected. Internal ports (1 through 14) are fixed as F_Ports. Table 32 describes the port modes. Complete the following steps to change the port mode:

1. Select one or more ports in the Faceplate window.
2. Click Port → Port Properties. The Port Properties window opens.
3. Select the Port Mode speed that you want.
4. Click OK to write the new port mode to the switch module.

Table 32. Port modes

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F_Port</td>
<td>Fabric port - Supports a single public device (N_Port).</td>
</tr>
<tr>
<td>FL_Port</td>
<td>Fabric loop port - Supports a loop of up to 126 public devices (NL_Port).</td>
</tr>
<tr>
<td>TL_Port</td>
<td>Translated loop port - Supports a loop of up to 124 private target devices or 125 private initiator devices capable of communicating with up to 63 off-loop initiator devices or 64 off-loop target devices.</td>
</tr>
<tr>
<td>G_Port</td>
<td>Generic port - Self-discovers as an F_Port or an E_Port.</td>
</tr>
<tr>
<td>GL_Port</td>
<td>Generic loop port - Self-discovers as an F_Port, FL_Port, or an E_Port.</td>
</tr>
<tr>
<td>Donor</td>
<td>Donor port - Allows buffer credits to be used by another port.</td>
</tr>
</tbody>
</table>

Configuring translated loop (TL) modes (external ports only): You can configure an external (0,15) TL_Port to support a loop of private target devices or a loop of private initiator devices.

- For a loop of up to 124 private target devices, click TL Target. This enables up to 63 initiator devices anywhere in the fabric to automatically connect with the private devices on the TL_Port. Group the TL_Port and up to 63 initiators in the same soft or ACL zone using the worldwide name or domain ID and port ID membership, to limit the number of possible initiators to 63.
- For a loop of up to 125 private initiator devices, click TL Initiator. This enables the private initiators on the TL_Port to automatically connect to up to 64 target and initiator devices in the same soft or ACL zone. You must group the TL_Port and the target devices in the same soft or ACL zone using the worldwide name or domain ID and port ID membership. If there are more than 65 members in the zone, the TL_Port is unable to communicate with the fabric.

Changing buffer-to-buffer credits (external ports only): Each switch module external port (0,15) has a receive buffer capacity of 12 Fibre Channel frames or credits, which is equal to approximately 24 KB. Port buffer credits can be changed on ports to accommodate connections to other switch modules that have different port buffer capacities. Complete the following steps to change external port buffer credits:

1. Select one or more ports in the Faceplate window.
2. Click Port → Port Properties.
3. In the E_Port BB Credits field, type the new number.
4. Click OK to write the new buffer-to-buffer setting to the switch module.

I/O stream guard: The I/O Stream Guard feature suppresses registered state control notification (RSCN) messages on external ports (0,15).
Extending port credits: Each external port (0,15) is supported by a data buffer with a 12-credit capacity; that is, 12 maximum sized frames. For fiber-optic cables, this enables full bandwidth class 2 service over a distance of 20 km (12.4 mi) at 1 Gbps (0.6 credits per km), or 10 km (6.2 mi) at 2 Gbps (1.2 credits per km). Longer distances can be spanned at full bandwidth by borrowing credits from designated donor ports; therefore, pooling the buffer capacities. This is called credit extension. Each donor port contributes 11 credits to the pool from which the recipient ports can draw. Only external ports (0,15) can be donor or recipient ports. For example, one donor port contributes 11 credits to the pool from which a recipient draws for a total of 23 credits (11+12). This provides approximately 38 Km (23.6 mi) at 1 Gbps (23÷0.6) or 19 km (11.8 mi) at 2 Gbps (23÷1.2).

Complete the following steps to extend port buffer credits:

1. In the Faceplate window, select the ports that are to serve as donor ports. Click Port → Port Properties. In the Port Properties window, click Donor → OK.

   Note: Donor ports are incapable of transmitting or receiving data.

2. In the Faceplate window, select the recipient port. Recipient ports must be external ports configured as G_Ports or F_Ports. Click Port → Extended Credits. The Extended Credits window opens as shown in Figure 20.

3. Distribute the borrowed credits by incrementing the Ext Credits Requested field for the recipient ports up to the total credits in the pool. Click OK. If you exceed this total, a message is entered in the alarm log indicating that some recipient ports did not receive the requested credits.

4. To confirm that the requested credits were received, reopen the Extended Credits window and match the number of credits in the Ext Credits Requested column with the number in the Donated to Port column.

   Note: As credits are used, the Logged-in LEDs on the corresponding donor ports are lit continuously. In addition, donor port Activity LEDs will reflect the same
traffic as the recipient port. Donor ports whose credits are being used are unavailable to devices that are connected to them.

**Resetting a port:** The Reset Port option reinitializes the port using configuration parameters stored in memory. Complete the following steps to reset a port:
1. In the Faceplate window, select the ports to be reset.
2. Click Port ➤ Reset Port.

To run an internal, external, or online port loopback test on an external port, see “Port testing” on page 116.

---

**Switch management utility functions**

This chapter contains information about the following topics:

- LED diagnostics
- Port testing
- Fibre Channel switch module monitoring using SNMP
- Restoring Fibre Channel switch module configuration defaults
- Using the Fabric View application

**LED diagnostics**

The BladeCenter Fibre Channel switch module performs a POST as part of its power-on procedure. The POST diagnostic program performs the following tests:
- Checksum tests on the boot firmware in PROM and the switch module firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the switch module ASIC

During the POST, the switch module logs any errors encountered. Some POST errors are fatal; others are non-fatal. The switch module uses the heartbeat LED and the logged-in LED to indicate switch and port status. A fatal error disables the switch module so that it will not operate. If a non-fatal error occurs, the switch module can still operate but disables the ports that have errors. Regardless of whether the problem is fatal or nonfatal, contact your IBM technical support representative.

If there are no POST errors, the heartbeat LED flashes at a steady rate of once per second. If a fatal error occurs, the heartbeat LED will show an error flash pattern. If there are non-fatal errors, the switch module disables the failed ports and flashes the associated logged-in LEDs. See “Heartbeat LED patterns” on page 114 for more information about heartbeat LED flash patterns.

There are three sets of LEDs on the information panel. The first row of LEDs at the top of the switch module represent switch module status and include OK, ♥ (heartbeat), and ! (Fibre Channel switch fault). The second and third sets of LEDs represent status for external Fibre Channel port 2 and external Fibre Channel port 1. The port LEDs include port logged-in, port activity, and port fault. Figure 21 on page 114 shows the location of these LEDs on the switch module. For more information about switch module LEDs, see the IBM @server BladeCenter 2-Port Fibre Channel Switch Module Installation Guide.
Heartbeat LED patterns
The heartbeat LED uses different flash patterns to indicate the following conditions:

- Normal
- Internal firmware failure
- Fatal error
- Configuration file system error

**Normal (all pass) LED flash pattern:** If POST diagnostics pass and the switch module processor is operating correctly, the switch will go to normal operation, and the heartbeat LED will flash at a steady rate of one flash per second.

**Internal firmware failure LED flash pattern:** An internal firmware failure flash pattern is two flashes per second followed by a 2-second pause, as shown in the following illustration. The two-flash error pattern indicates that the firmware has failed and that the switch module must be reset.

![Two flash error pattern](image)

**Fatal error LED flash pattern:** A fatal error flash pattern is three flashes per second followed by a 2-second pause, as shown in the following illustration. The three-flash error pattern indicates that a fatal error has made the switch module inoperable. If a fatal error occurs, contact your IBM technical support representative.

![Three flash error pattern](image)

**Configuration file system error LED flash pattern:** A configuration file system error flash pattern is four flashes per second followed by a 2-second pause, as shown in the following illustration. The four-flash error pattern indicates that a
configuration file system error has occurred.

Switch module fault LED flash pattern
The amber Switch Fault LED is lit to indicate one or more of the following conditions:

- POST failure
- Over temperature condition
- Port operational test failure. See “Port fault LED flash patterns” on page 116 for information about port operational tests.

If the Switch Fault LED is lit for reasons other than a port operational test failure, take the BladeCenter Fibre Channel switch module offline and contact your IBM technical support representative.

Switch module OK LED
The green OK LED is lit to indicate that the switch module has completed POST diagnostics without errors. If this LED is not lit when you turn on the BladeCenter unit or turns off during operation, remove the switch module and inspect the connector for damage.

Port logged-in LED flash patterns
The Port Logged-in LED has the following flash patterns:

- Logged in - The logged-in LED is lit continuously.
- Logging in - The logged-in LED flashes once per second as shown in the following illustration.
- Set beacon - Enables or disables the flashing of the Port Logged-in LEDs according to [state]. For information about the set beacon command, see “Set command” on page 26.
- Error - The logged-in LED flashes at twice per second as shown in the following illustration.

Logging in

<table>
<thead>
<tr>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Second</td>
</tr>
</tbody>
</table>

A logged-in LED error indication is often the result of E_Port isolation. Table 33 describes the causes and remedies for E_Port isolation conditions. An isolated E_Port is indicated by a red link in the Topology window. See “Timeout values” on page 101, “Domain ID and Domain ID Lock” on page 100, and “Zoning a fabric” on page 83 for information about how to set IDs, timeout values, and edit zoning.

Table 33. E-port isolation causes and fixes

<table>
<thead>
<tr>
<th>Isolation cause</th>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two switch modules in the same fabric have the same domain ID</td>
<td>Correct the domain IDs on the malfunctioning switch modules. Domain IDs are decimal numbers in the range from 1 to 239. Domain IDs must be unique.</td>
</tr>
<tr>
<td>All switch modules in the fabric do not have the same timeout values</td>
<td>Correct the timeout values on the malfunctioning switch modules.</td>
</tr>
<tr>
<td>Isolation cause</td>
<td>Fix</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>When merging two fabrics, the active zone sets contain zones with the same names but different membership.</td>
<td>Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same. The conflicting zones have the same name but different membership. Take the affected ports offline then back online to restore the interswitch links.</td>
</tr>
</tbody>
</table>

**Port fault LED flash patterns**

The amber port fault LED is lit to indicate that the port has failed one of the following port operational tests performed with the SAN Utility or the CLI:

- Internal
- External
- Online

If the port fault LED is lit, take the port offline and contact your IBM technical support representative.

**Port testing**

The port loopback tests verify correct port operation by sending a test data frame out through the loop and then verifying that the frame received matches the frame that was sent. You can perform the following port tests from the Port Loopback window:

- **Internal SerDes test (internal and external ports)** - The SerDes (serializer/deserializer) level test verifies internal and external port circuitry. The SerDes level test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected internal ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received.
  
  **Note:** A loopback plug is required to perform an external SFP test.

- **External SFP test (external ports only)** - The SFP level test also verifies port circuitry. The SFP level test sends a test frame from the ASIC through the SerDes chip, through the SFP module fitted with the loopback plug, and back to the ASIC for the selected external ports. The external port passes the test if the test frame that was sent by the ASIC matches the test frame that was received.

- **Online node-to-node test (internal ports)** - The node-to-node test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a device. The port passes the test if the test frame that was sent matches the test frame that was received.
Note: The internal SerDes and external SFP level tests disrupt communication on the selected port. The online node-to-node level test does not disrupt communication, because it requires that the port is online.

Complete the following steps to run the internal, external, or online port loopback test on an external port:

1. In Faceplate window, select the external port to be tested.
2. Click **Port → Port Loopback Test**.
   - The Port Loopback Test window opens.
3. In the test selection pane, select the type of loopback test (internal, external, or online) to be run. If you want to run the internal or external test, the SAN Utility prompts you to confirm that the port state needs to be changed to the diagnostic state. Click **OK**. The SAN Utility changes the port state.
4. Type the frame count, frame size, and select a test pattern. You can use the default pattern or type an 8-digit pattern (hexadecimal). For online tests, click the **Terminate Test Upon Error** check box if you want the test to stop when encountering an error.
5. Click **Start Test** to begin the test. The test results pane displays the test status, number of frames sent, and number of errors found.

**Fibre Channel switch module monitoring using SNMP**

This section describes SNMP configuration and trap parameters. The switch module SNMP agent enables external network management monitoring and notification of switch module status.

**SNMP configuration**

SNMP configuration defines how authentication traps are managed. Table 34 describes the SNMP configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>Specifies the name of the person to contact for trap events. The default is undefined.</td>
</tr>
</tbody>
</table>
Table 34. SNMP configuration parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read community</td>
<td>Read Community Authentication. A write-only field; the value on the switch module and the SNMP management server must be the same. The default value is Public.</td>
</tr>
<tr>
<td>Trap community</td>
<td>Trap Community Authentication. A write-only field; the value on the switch module and the SNMP management server must be the same. The default value is Public.</td>
</tr>
<tr>
<td>Location</td>
<td>Specifies the switch module location. The default is undefined.</td>
</tr>
<tr>
<td>Authentication trap</td>
<td>Enables or disables the reporting of SNMP authentication failures. If enabled, and the incorrect community string values are used, an authentication failure event occurs and a notification trap is sent to the configured trap addresses. The default value is False.</td>
</tr>
<tr>
<td>Write community</td>
<td>Write Community Authentication. A write-only field; the value on the switch module and the SNMP management server must be the same. The default value is Private.</td>
</tr>
</tbody>
</table>

SNMP trap configuration

The SNMP trap configuration defines how traps are set. Table 35 describes the SNMP trap configuration parameters.

Table 35. SNMP trap configuration parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap enabled</td>
<td>Select this check box to enable or disable the trap.</td>
</tr>
<tr>
<td>Trap address</td>
<td>Specifies the IP address to which SNMP traps are sent. The default is 10.0.0.1 for trap 1 and 0.0.0.0 for traps 2–5. A maximum of five trap addresses are supported.</td>
</tr>
<tr>
<td>Trap port</td>
<td>The port number on which the trap is set.</td>
</tr>
<tr>
<td>Trap severity</td>
<td>Specifies a severity level to assign to the trap. Open the menu and select a level. Traps must be enabled to access this menu. Trap severity levels include Unknown, Emergency, Alert, Critical, Error, Warning, Notify, Info, Debug, and Mark.</td>
</tr>
</tbody>
</table>

Restoring Fibre Channel switch module configuration

This section describes switch module configuration restoration tasks that are performed using the Telnet CLI interface and the management module.

Configuration backup

Changes made to the switch module since it was manufactured can be saved to a file in nonvolatile memory. However, the backup file is lost if the switch module is reset. Use the File Transfer Protocol (FTP) user images procedures to save the configdata file to the network management workstation. (In FTP, no directory listing is available. The configuration backup file is always named configdata.) For information about SNMP configuration, see "SNMP configuration" on page 117 and "SNMP trap configuration".

Configuration restore

Switch module configurations can be duplicated to easily propagate an identical configuration to other switch modules. Use the FTP User Images procedures with the Put command to send the previously saved (using config backup) configdata file to the switch module. In Telnet, use the Config Restore command to return the
switch module configuration to the previously saved configuration. The switch module is automatically reset after a successful restore.

**Restoring the factory default configuration**
You can restore the switch module and port configuration settings to the factory default values. To restore the factory configuration on a switch module, click **Switch → Restore Factory Defaults**. [Table 36](#) lists the factory default switch module configuration settings. Restoring the switch module to the factory default configuration does not restore the login name and password settings.

**Table 36. Factory default configuration settings**

<table>
<thead>
<tr>
<th>Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module name</td>
<td>Fibre Channel switch module</td>
</tr>
<tr>
<td>Administrative state</td>
<td>Online</td>
</tr>
<tr>
<td>Domain ID</td>
<td>1</td>
</tr>
<tr>
<td>Resource allocation timeout (RA_TOV)</td>
<td>10000 milliseconds</td>
</tr>
<tr>
<td>Receiver transmitter timeout (RT_TOV)</td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>Error detect timeout (ED_TOV)</td>
<td>2000 milliseconds</td>
</tr>
<tr>
<td>IP address</td>
<td>Switch module bay 3: 192.168.70.129</td>
</tr>
<tr>
<td></td>
<td>Switch module bay 4: 192.168.70.130</td>
</tr>
<tr>
<td>Subnet mask address</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway address</td>
<td>10.90.90.254</td>
</tr>
<tr>
<td>Boot method</td>
<td>Static</td>
</tr>
<tr>
<td>Contact</td>
<td>Undefined</td>
</tr>
<tr>
<td>Location</td>
<td>Undefined</td>
</tr>
<tr>
<td>Trap address</td>
<td>Trap 1: 10.0.0.1; Traps 2–5: 0.0.0.0</td>
</tr>
<tr>
<td>Trap community</td>
<td>Public</td>
</tr>
<tr>
<td>Read community</td>
<td>Public</td>
</tr>
<tr>
<td>Write community</td>
<td>Private</td>
</tr>
<tr>
<td>Port state</td>
<td>Online - external ad internal ports</td>
</tr>
<tr>
<td>Port speed</td>
<td>Auto-detect - external; 2G - internal</td>
</tr>
<tr>
<td>Port mode</td>
<td>GL - external; F - internal</td>
</tr>
</tbody>
</table>

**Reinitializing the configuration file system**
If the heartbeat LED on the switch module is showing the four-flash pattern, the configuration file system might be damaged. To recover the factory switch module configuration, use the **Config Restore** Telnet command. The heartbeat LED four-flash pattern continues until a previous switch module configuration is successfully restored. The heartbeat LED is not reflected in the SAN Utility.

**Restoring a switch module**
Restoring a switch module loads the archived switch configuration parameters to the switch module. The switch module configuration must be archived before it can be restored. See “Archiving a switch module” on page 102 for more information.

1. Log in to the fabric through the switch module you want to restore. You cannot restore a switch module over an ISL.
2. In the Faceplate window, click **Switch → Restore**.
3. In the Restore window, type the archive file name or browse for the file.
4. Click **Restore**.

**Using the Fabric View application**

You can use the Fabric View application to view port performance as graphs. The Fabric View window displays data communication rates and total errors for selected ports as shown in Figure 23. You can graph communication data rates using either frames per second or KB per second.

This section provides the instructions you need to perform the following tasks in the Fabric View window:

- Start the Fabric View application
- Display port performance graphs
- Arrange and size port performance graphs
- Customize port performance graphs

---

**Starting the Fabric View application**

To start Fabric View using the SAN Utility, open the Faceplate window and click **Start Fabric View** from the Switch menu.

**Displaying port performance graphs**

Complete the following steps to display port performance graphs:

1. Click **Fabric** and select **Add Fabric** or click the **Add** button. Type a **fabric name** and an **IP address** in the Add a New Fabric window. Include a login name and a password if required.

2. Set the graphing options and polling frequency. By default, the Fabric View application plots total bytes transmitted and received at a polling frequency of once per second. See "Customizing port performance graphs" on page 121 for information about changing what is plotted and how it is plotted.
3. Select a switch module icon in the Fabric Tree to display a graph for each logged-in port on that switch module; or display a graph for a single port by clicking on the switch module entry handle and selecting one or more ports.

4. You can move graphs around individually by clicking and dragging, or you can arrange them as a group. See “Arranging and sizing port performance graphs” for more information.

5. To remove a graph, click Close. To remove all graphs, click View and click Close All Graphs.

Fabric View can access only one fabric at a time. To access another fabric, you must first remove the current fabric. To remove a fabric, click Fabric and select Remove Fabric or click the Remove button.

Arranging and sizing port performance graphs
Complete the following steps to arrange and size graphs in the Fabric View window:
1. Click View and select Tile Graphs Vertically. Tiling vertically sizes and arranges the graphs in the longest columns possible.
2. Click View and select Tile Graphs Horizontally. Tiling horizontally sizes and arranges the graphs in the longest rows possible.
3. Click View and select Cascade Graph Panels. Cascading overlaps the graphs so that all graphs are at least partially visible.

Customizing port performance graphs
You can customize the graph polling frequency, what is plotted in the graphs, and the graph color scheme. Complete the following steps to customize the port performance graphs:
1. To set the polling frequency for all graphs, click Graph and click Set Polling Frequency.
2. Type an interval, in seconds (0 through 60), and click OK.
3. To select what is to be plotted, click Graph and click Options. The Modify Graph Display window opens.

4. To modify the graph display, select the units for the graph:
   - Select the Show Bytes Data on Graph check box to plot data in KB per second.
   - Select the Show Frames Data on Graph check box to plot data in frames per second.

Figure 24. Modify Graph Display window
5. Choose what data type to plot. For example, if you selected Show Frames Data on Graph in step 4 on page 121, you can plot one or all of the following:

- Total frames transmitted and received (Total Frames)
- Total frames transmitted (Total Tx Frames)
- Total frames received (Total Rx Frames)

In addition to these, you can also plot total errors by selecting the Total Errors check box.

6. Display or hide the unit grid. Select the Display Grid on Graph check box to display the unit grid.

7. Choose the color scheme for the graph. You can select the color for each data type, the unit grid, and the background by clicking the corresponding color field or button. In each case, you can choose a color using the swatches, Red-Green-Blue (RGB), or Hue-Saturation-Brightness (HSB):

- Swatches – Click the Swatches tab. Select a swatch from the palette and click OK.
- RGB – Click the RGB tab. Select a color by moving the slides to adjust the values for red, blue, and green; or type values in the fields. Click OK.
- HSB – Click the HSB tab. Select a color using any of the following methods and click OK:
  - Click in the color palette.
  - Select H, S, or B and use the slide to vary the selected value.
  - Type values in the H, S, or B fields.

### Mapping port locations and software numbering

Your switch module has two external Fibre Channel ports (external Fibre Channel port 1 and external Fibre Channel port 2) and 14 internal Fibre Channel ports that connect to each of the 14 blade server bays (ports 1 to 14). The SAN Utility and CLI for the switch module require port numbering from 0 to 15. The SNMP monitoring agent for the switch module numbers the ports from 1 to 16.

### Port mapping

Table 37 shows the mapping of switch module port numbering and whether the port has the capability to be configured.

<table>
<thead>
<tr>
<th>Switch module physical port connection</th>
<th>SAN Utility and CLI logical port number</th>
<th>SNMP port numbering</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>External port 1</td>
<td>0 (Ext1:0*)</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Blade server bay 1</td>
<td>1</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 2</td>
<td>2</td>
<td>3</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 3</td>
<td>3</td>
<td>4</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 4</td>
<td>4</td>
<td>5</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 5</td>
<td>5</td>
<td>6</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 6</td>
<td>6</td>
<td>7</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 7</td>
<td>7</td>
<td>8</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 8</td>
<td>8</td>
<td>9</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 9</td>
<td>9</td>
<td>10</td>
<td>No</td>
</tr>
</tbody>
</table>
### Table 37. Port mapping (continued)

<table>
<thead>
<tr>
<th>Switch module physical port connection</th>
<th>SAN Utility and CLI logical port number</th>
<th>SNMP port numbering</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blade server bay 10</td>
<td>10</td>
<td>11</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 11</td>
<td>11</td>
<td>12</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 12</td>
<td>12</td>
<td>13</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 13</td>
<td>13</td>
<td>14</td>
<td>No</td>
</tr>
<tr>
<td>Blade server bay 14</td>
<td>14</td>
<td>15</td>
<td>No</td>
</tr>
<tr>
<td>External port 2</td>
<td>15 (Ext2:15*)</td>
<td>16</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Indicates a symbolic port name if it is different from the logical port number.

**Note:** The Fibre Channel ports that connect to each of the blade server bays (1 through 14) are fixed 2 Gbps F_Port configurations. Only the administrative state for these ports can be changed.
Chapter 3. HS20 Fibre Channel Expansion Card

This *Installation and User's Guide* contains instructions for installing your IBM HS20 Fibre Channel Expansion Card in an IBM @server BladeCenter™ HS20 blade server. This publication contains information about:

- Installing and configuring the HS20 Expansion Card
- Updating the BIOS code and device drivers of the HS20 Expansion card

The IBM HS20 Fibre Channel Expansion Card is a 2 Gb Fibre Channel device that has two configurable adapter ports. Communication signals are routed from the blade server through the Fibre Channel high-speed connector on the HS20 Expansion Card to switch-module bay 3 and bay 4 in the BladeCenter unit. This provides a high-performance connection between the 64-bit PCI-X bus in the blade server and the two IBM BladeCenter 2-Port Fibre Channel Switch Modules in the BladeCenter unit.

**Note:** The modules in switch-module bay 3 and bay 4 in the BladeCenter unit must be IBM @server BladeCenter 2-Port Fibre Channel Switch Modules.


Packaged with this *Installation and User's Guide* is a software CD that helps you to configure hardware and install device drivers.

This *Installation and User's Guide* and other publications that provide detailed information about your BladeCenter unit, blade server, and available options are provided in Portable Document Format (PDF) on the IBM BladeCenter Documentation CD, which comes with the HS20 blade server.

For service or assistance, see Appendix A, “Getting help and technical assistance,” on page 159.

The IBM HS20 Fibre Channel Expansion Card is referred to throughout this book as the HS20 Expansion Card or the expansion card.

### Features and specifications

The HS20 Expansion Card has the following features:

- Compliance with Third Generation Fibre Channel Physical and Signaling Interface (PC-PH-3), revision 9.2
- Compliance with U.S. and international safety and emissions standards
- Support for direct memory access (DMA)
- Support for bus mastering
- Fast!UTIL basic input/output system (BIOS) utility program to customize the configuration parameters on the HS20 Expansion Card and attached drives
- Support for Fibre Channel protocol SCSI (FCP-SCSI) and Fibre Channel Internet protocol (FCP-IP)
- Support for point-to-point fabric connection (F-port fabric login)
- Support for Fibre Channel service (classes 2 and 3)
The following list and table provide a summary of the specifications of your HS20 Fibre Channel Expansion Card.

**Temperature and altitude**
- Blade server on: 10°C to 35°C (50°F to 95°F) at an altitude of 0 to 914 m (2998.69 ft)
- Blade server on: 10°C to 32°C (50°F to 89.6°F) at an altitude of 914 m to 2134 m (2998.69 ft to 7000 ft)
- Blade server off: -40°C to 60°C (-40°F to 140°F)
- Shipping temperature: -40°C to 60°C (-40°F to 140°F)
- Storage altitude: 0 to 2133 m (6998 ft)
**Humidity**

- Blade server on: 8% to 80%
- Blade server off: 5% to 80%

*Table 38. HS20 Expansion Card specifications*

<table>
<thead>
<tr>
<th>Type</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expansion card bus</td>
<td>Supports subset of PCI local bus specification, revision 2.2 and the PCI-X specification 1.0a</td>
</tr>
<tr>
<td>PCI/PCI-X signaling environment</td>
<td>Supports 3.3 V only</td>
</tr>
<tr>
<td>PCI/PCI-X transfer rate</td>
<td>The burst transfer rate is based on the input clock speed multiplied by the number of bytes (8).&lt;br&gt;  - PCI - 66 = 525 MB per second  &lt;br&gt;  - PCI-X - 100 = 800 MB per second</td>
</tr>
</tbody>
</table>

**Fibre Channel specifications**

- Bus transfer rate: 200 MB per second maximum at half-duplex and 400 MB per second maximum at full-duplex<br>  - Support for both FCP-SCSI and IP protocols<br>  - Support for point-to-point fabric connection: F-Port Fabric Login<br>  - Support for FCAL public loop profile: FL-Port Login<br>  - Support for Fibre Channel services class 2 and 3<br>  - Support for FCP SCSI initiator and target operation<br>  - Support for full-duplex operation<br>  - Copper interface ac coupled

**Processor**

- Single-chip design with two completely independent 2 Gb serial Fibre Channel ports. Each port provides:<br>  - RISC processor<br>  - Integrated serializer/deserializer<br>  - Receive direct memory access (DMA) sequencer<br>  - Frame buffer<br>  - Five-channel DMA controller

**Host data transfer**

- 64-bit, 100 MHz bus-master DMA data transfers to 800 MB per second

**RAM**

- 512 KB sync burst SRAM per channel supporting parity protection

**BIOS ROM**

- BIOS ROM 128 KB of flash memory (the flash is field programmable)

**NVRAM**

- NVRAM 256 bytes, field programmable

**Onboard DMA**

- Five-channel DMA controller for each port: transmit, receive, command, auto-request, and auto-response

**Frame buffer FIFO**

- Integrated 4 KB transmit and 6 KB receive frame buffer FIFO for each data channel

**Connectors (internal only)**

- Board-to-board Molex HSM type for serial interfaces<br>  - 200 pin board-to-board for PCI-X interface

**Dimensions**

- Approximately 9.35 cm x 13.14 cm (3.683 in. x 5.275 in.)

**Operating power**

- Less than 12 watts
Inventory checklist

The HS20 Expansion Card option package contains the following items:

- HS20 Expansion Card
- I/O expansion option tray
- IBM HS20 Fibre Channel Expansion Card Installation and User’s Guide
- IBM HS20 Fibre Channel Expansion Card Support CD

Notices and statements used in this book

The caution and danger statements used in this book are also in the multilingual Safety Information book provided on the IBM BladeCenter Documentation CD. Each caution and danger statement is numbered for reference to the corresponding statement in the Safety Information book.

The following types of 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 HS20 Expansion Card

The following illustration shows the top of the HS20 Expansion Card.
Note: The illustrations in this document might differ slightly from your hardware.

**ISP2312 chip (U5):** The ISP2312 chip provides a PCI-X local bus interface and two completely independent 2 Gb serial Fibre Channel ports. Each port has a RISC processor, an integrated serializer/deserializer (SERDES), a receive DMA sequencer, frame buffer, five-channel DMA controller, and an external memory interface in a single-chip solution.

*Figure 25. HS20 Expansion Card (top)*
The following illustration shows the components on the bottom of the HS20 Expansion Card.

**PCI-X connector (J3):** This connector is a 64-bit PCI-X interface with a 200-pin board-to-board connector that is connected to the blade server.

**Fibre Channel high-speed connector (J2):** Communication signals are routed from the blade server through the Fibre Channel high-speed connector on the HS20 Expansion Card to switch-module bay 3 and bay 4 in the BladeCenter unit.

---

**Figure 26. HS20 Expansion Card (bottom)**

**Installing the HS20 Expansion Card**

This chapter provides detailed instructions for installing the HS20 Expansion Card in your blade server.

**Installation guidelines**

Before you begin installing the HS20 Expansion Card in your blade server, read the following information:

- Read “Safety information” on page 161 and “Handling electrostatic discharge-sensitive devices” on page 164. This information will help you work safely with your blade server and options.
- Have a small flat-blade screwdriver and a Phillips screwdriver available.

**Handling static-sensitive devices**

**Attention:** Static electricity can damage electronic devices, including your blade server. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.
To reduce the possibility of damage from 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 circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to an unpainted metal part of the BladeCenter unit for at least 2 seconds. This drains static electricity from the package and from your body.
- Remove the device from its package and install it directly into the blade server without setting down the device. If it is necessary to set down the device, place it back into its static-protective package. Do not place the device on your blade server cover or on a metal surface.
- Take additional care when handling devices during cold weather. Heating reduces indoor humidity and increases static electricity.

**Installing the HS20 Expansion Card**

Complete the following steps to install the HS20 Expansion Card in a blade server:

1. Read **“Safety information” on page 161**
2. Read **“Handling static-sensitive devices” on page 130**
3. Ensure that one IBM BladeCenter 2-Port Fibre Channel Switch Module is installed in switch-module bay 3 or bay 4 in the BladeCenter unit. See the *IBM BladeCenter 2-Port Fibre Channel Switch Module Installation Guide* for detailed installation instructions.

**Note:** You must install at least one Fibre Channel switch module in the BladeCenter unit when you install the IBM HS20 Fibre Channel Expansion Card in a blade server. Installing a second Fibre Channel switch module in the BladeCenter unit provides a backup switch in case one switch module fails.

4. If the blade server is operating, press the power-control button (behind the blade server control panel door) to shut down the operating system and turn
off the blade server. For the location of the control panel door, see the illustration on page 134. Wait at least 30 seconds, until the drives stop spinning, before proceeding to the next step.

5. Open the two release levers. The blade server moves out of the bay approximately 0.6 cm (0.25 inch).

6. Pull the blade server out of the blade bay. Spring-loaded doors further back in the bay move into place to cover the bay temporarily.

7. Place either a filler blade or another blade server in the bay within 1 minute. The recessed spring-loaded doors will move out of the way as you insert the blade or filler blade.

8. Lay the blade server down on a flat, nonconductive surface, with the cover side up.

9. Press the blade-cover release on each side of the blade server. Open the cover and lay it flat, or lift it from the blade server.

Statement 21:

CAUTION:

Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

10. If an IDE hard disk drive is in IDE connector 2, remove the drive and tray (save the screws that secure the tray to the system board); otherwise, remove the two screws near IDE connector 2 that secure the system board to the chassis.

11. Install the I/O expansion option tray, which comes with the HS20 Expansion Card. Secure the tray to the system board using a Phillips screwdriver and the
12. Remove the HS20 Expansion Card from the static-protective package.
13. Slide the narrow end of the HS20 Expansion Card into the raised hook on the tray.
14. Align the HS20 Expansion Card connectors with the network-interface option connector and the PCI-X expansion slot.
15. Gently press the card into the connectors.

**Important**: The blade server cannot be inserted into the BladeCenter unit until the cover is installed and closed. Do not attempt to override this protection.
16. Lower the cover so that the slots at the rear slide down onto the pins at the rear of the blade server, as shown in the illustration.
17. Pivot the cover to the closed position as shown in the illustration, until it clicks into place.
Statement 21:

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.

18. Ensure that the release levers on the blade server are in the open position (perpendicular to the blade server).

19. Slide the blade server into the bay until it stops. The spring-loaded doors that are further back in the bay and cover the bay opening move out of the way as you insert the blade server into the BladeCenter unit.

20. Push the release levers on the front of the blade server to close them.

21. Turn on the blade server. Press the keyboard/mouse/video select button.

Note: The blade server control panel door is shown in the closed (normal) position in the illustration.

22. If the information displayed on the monitor screen is similar to the following text, update the BIOS code if necessary and install the expansion card device drivers. If the information displayed on the monitor screen is not similar to this text and you have checked the expansion card configuration, go to “General Checkout” on page 145.

QL2312 PCI Fibre Channel ROM BIOS Version X.XX
Copyright (C) QLogic Corporation 1993-2002 All Rights Reserved.
www.qlogic.com
Press <Ctrl+Q> for Fast!UTIL
BIOS for Adapter 0 is disabled
ROM BIOS not installed

Updating the expansion card BIOS code and NVRAM code and installing device drivers

After you install the HS20 Expansion Card, be sure that the latest BIOS code and the nonvolatile random access memory (NVRAM) code are installed; then, install the device drivers.
Before you can update the BIOS code and NVRAM code, you must create a BIOS Update Utility diskette. You will use the diskette to update the BIOS code and NVRAM code. For more information about creating a diskette, see “Creating a BIOS Update Utility diskette”.

To install the device drivers, see “Installing the HS20 Expansion Card device drivers” on page 138.

Note: For the latest information about supported operating systems, versions of device drivers, utilities, and documentation, go to http://www.ibm.com/pc/support/.

Creating a BIOS Update Utility diskette

To create a BIOS Update Utility diskette, you can copy the image from the HS20 Fibre Channel Expansion Card Support CD or download the image from http://www.ibm.com/pc/support/. You can create a BIOS Update Utility diskette for the following operating systems:

- Microsoft® Windows® 2000
- Red Hat Linux®
- SuSE Linux

For Microsoft Windows 2000

Complete the following steps to create a BIOS Update Utility diskette for Microsoft Windows 2000 from the HS20 Fibre Channel Expansion Card Support CD:

1. To associate the CD-ROM drive and the diskette drive with the blade server, press the CD/diskette/USB select button on the blade server. For the location of the CD/diskette/USB button, see the illustration on page 134. The LED on the button flashes while the request is being processed, then is steady when the ownership of the CD-ROM or diskette drive is transferred to the blade server.

2. To associate the keyboard port, mouse port, and video port with the blade server, press the keyboard/mouse/video select button. The LED on this button flashes while the request is processed, then is steady when the ownership of the keyboard, mouse, and video is transferred to the blade server.

3. Insert the support CD into the CD-ROM drive.

4. Insert a diskette into the diskette drive.

5. Restart the blade server.

6. At the command prompt, type:

   `e:\tools\dsk4w32 e:\bios\hs20__xxx.img a:

   where e is the CD-ROM drive letter, a is the diskette drive letter, and xxx is the latest BIOS code version. For the latest BIOS code version, see the readme file on the HS20 Fibre Channel Expansion Card Support CD.

7. Press Enter.

8. Remove the CD from the CD-ROM drive.

9. Remove the diskette from the diskette drive and label the diskette.

10. To update the HS20 Expansion Card BIOS code and NVRAM code, go to “Updating the expansion card BIOS code and NVRAM code” on page 136.

For Red Hat Linux and SuSE Linux

Complete the following steps to create a BIOS Update Utility diskette for Red Hat Linux or SuSE Linux from the HS20 Fibre Channel Expansion Card Support CD:
1. To associate the CD-ROM drive and the diskette drive with the blade server, press the CD/diskette/USB select button on the blade server. For the location of the CD/diskette/USB button, see the illustration on page 134. The LED on the button flashes while the request is being processed, then is steady when the ownership of the CD-ROM or diskette drive is transferred to the blade server.

2. To associate the keyboard port, mouse port, and video port with the blade server, press the keyboard/mouse/video select button. The LED on this button flashes while the request is processed, then is steady when the ownership of the keyboard, mouse, and video is transferred to the blade server.

3. Insert the support CD into the CD-ROM drive.

4. Insert a diskette into the diskette drive.

5. Restart the blade server.

6. At the command prompt, type
   
   ```
   mount -t iso9660 /dev/cdromdevicefile /mnt
   ```
   
   where `cdromdevicefile` is the specific device file for the CD-ROM block device. Press Enter.

7. Type
   
   ```
   dd if=/mnt/bios/hs20_xxx.img of=/dev/diskettedevicefile bs=32
   ```
   
   where `xxx` is the BIOS code version on the CD. For more information, see the readme file on the HS20 Fibre Channel Expansion Card Support CD. Press Enter.

8. To unmount the CD file, type the following command and press Enter.
   
   ```
   unmount /mnt
   ```

9. Remove the CD from the CD-ROM drive.

10. Remove the diskette from the diskette drive and label the diskette.

11. To update the HS20 Expansion Card BIOS code and NVRAM code, go to "Updating the expansion card BIOS code and NVRAM code"

### Updating the expansion card BIOS code and NVRAM code

**Attention:** Do not turn off or restart the blade server during the BIOS code or NVRAM code update process.

To update the HS20 Expansion Card BIOS code and NVRAM code, use one of the following methods:

- Use the flasutil command prompt method to type command-line options.
- Use the flasutil BIOS Update Utility menu to select a command-line option.

### Using the flasutil command prompt

Complete the following steps to update the HS20 Expansion Card BIOS code and NVRAM code using the flasutil command prompt:

1. To associate the diskette drive with the blade server, press the CD/diskette/USB select button on the blade server. For the location of the CD/diskette/USB button, see the illustration on page 134. The LED on the button flashes while the request is processed, then is steady when the ownership of the CD-ROM or diskette drive is transferred to the blade server.

2. To associate the keyboard port, mouse port, and video port with the blade server, press the keyboard/mouse/video select button. The LED on this button flashes while the request is processed, then is steady when the ownership of the keyboard, mouse, and video is transferred to the blade server.
3. Insert the diskette you created from the support CD into the diskette drive.
4. Restart the blade server. The blade server starts to a DOS prompt.
5. To update the BIOS code and the NVRAM code on the HS20 Expansion Card, at the DOS prompt, type the following command and press Enter:

```
flasutil /i /f /i
```

**Notes:**
- You must add /i to each command for correct vendor recognition.
- Commands are not case sensitive.
6. To review additional command-line options that you can use, see “Command-line options”; then, return to step 6.
7. Remove the diskette from the diskette drive and restart the blade server.
8. Go to "Installing the HS20 Expansion Card device drivers" on page 138

**Command-line options**
To view a list of supported command-line options, at the DOS prompt, type the following command and press Enter:

```
flasutil /?
```

The following command-line options are displayed:
- **/F xxxx** = Write Flash, adapter address = xxxx
  - If no address specified then write Flash to all adapters
- **/W xxxx** = Copy Flash to file: QLxxRIM.SAV, adapter type = xxxx
- **/O <filename.ext>** = Use <filename.ext> instead of QLxxROM.BIN
- **/I** = IgnoreSubsystem ID
- **/M** = Program all adapters
- **/Q** = Quiet Mode, no messages will be displayed
- **/V xxxx** = Display current version number of BIOS on adapters at address xxxx
  - If no address specified then display the BIOS version of all adapters
- **/C xxxx** = Verify Flash of adapter at address xxxx
  - If no address specified verify the Flash of all adapters
- **/Y xxxx** = Display port name of adapter at address xxxx
  - If no address specified then display port name of all adapters
- **/i** = Vendor recognition

**Using the flasutil BIOS Update Utility menu**
Complete the following steps to update the HS20 Expansion Card BIOS code and NVRAM code using the flasutil BIOS Update Utility menu:

1. To associate the diskette drive with the blade server, press the CD/diskette/USB select button on the blade server. For the location of the CD/diskette/USB button, see the illustration on page 134. The LED on the button flashes while the request is being processed, then is steady when the ownership of the CD-ROM or diskette drive is transferred to the blade server.
2. To associate the keyboard port, mouse port, and video port with the blade server, press the keyboard/mouse/video select button. The LED on this button flashes while the request is being processed, then is steady when the ownership of the keyboard, mouse, and video is transferred to the blade server.
3. Insert the diskette you created from the support CD into the diskette drive.
4. Restart the blade server. The blade server starts to a DOS prompt.
5. From the DOS prompt, type the following command and press Enter:

```
flasutil /i
```

The HS20 Expansion Card has two I/O addresses. Both port I/O addresses are displayed.
6. At the **Enter adapter I/O address** prompt, type the I/O address of the port for which you want to update the BIOS code and NVRAM code. Press Enter.
7. The following option menu is displayed:
   L = Write NVRAM
   F = Write Flash
   W = Copy Flash to file: QLxxROM.SAV
   S = Display serial number
   V = Display current BIOS version
   C = Verify Flash
   X = Verify NVRAM
   Y = Display port name

8. At the Enter Option prompt, type l and press Enter.

9. At the DOS prompt, type the following command and press Enter:
   flasutil /i

10. At the Enter adapter I/O address prompt, type the same I/O address that you
typed in step 5 on page 137.
    The following option menu is displayed:
    L = Write NVRAM
    F = Write Flash
    W = Copy Flash to file: QLxxROM.SAV
    S = Display serial number
    V = Display current BIOS version
    C = Verify Flash
    X = Verify NVRAM
    Y = Display port name

11. At the Enter Option prompt, type f and press Enter.

12. For each additional option that you want for the same I/O address, repeat step
8 on page 138 through step 11 on page 138 substituting the option letter for f.

13. Repeat step 4 on page 137 through step 12 on page 138 for the second I/O
    address.

14. Remove the diskette from the diskette drive and restart the blade server.

15. Go to “Installing the HS20 Expansion Card device drivers”

Using the Remote Deployment Manager

You can use the Remote Deployment Manager (RDM) program to install a
supported Microsoft Windows operating system on a blade server only if the blade
server patch has been applied to RDM. Follow the instructions in the documentation
that comes with the RDM program. To download the RDM software and user’s
guide, go to:


Installing the HS20 Expansion Card device drivers

The device drivers and installation instructions for the following supported operating
systems are provided on the HS20 Fibre Channel Expansion Card Support CD:

- Microsoft Windows 2000 Server and Advanced Server (requires SP 3)
- Red Hat Linux 7.3
- Red Hat Advanced Server 2.1
- SuSE Linux 8.0 Professional

The installation instructions are in a file in the applicable operating-system directory.
Using IBM Fast!UTIL

This chapter provides detailed configuration information for advanced users who want to customize the configuration of the HS20 Expansion Card. You can configure the expansion card using the Fast!UTIL utility.

Starting Fast!UTIL

Start or restart the blade server. On the blade server control panel, press the keyboard/video/mouse select button. To access Fast!UTIL, press Ctrl+Q during the expansion card BIOS initialization (it might take a few seconds for the Fast!UTIL menu to be displayed). The HS20 Expansion Card has dual adapter ports that can be configured separately with Fast!UTIL. After changing the settings that are described in the "Configuration Settings menu options", Fast!UTIL restarts the blade server to enable the new parameters.

Important: If the configuration settings are incorrect, the HS20 Expansion Card might not function properly. Do not modify the default configuration settings unless you are instructed to do so by an IBM technical-support representative or in the installation instructions.

Configuration Settings menu options

Note: For information about Remote Boot options, contact your IBM technical-support representative.

Use the options described in this section to configure the HS20 Expansion Card. The Configuration Settings menu displays several options that you can use to configure your expansion card.

Select host adapter
Use this option to select, configure, or view either of the two I/O port addresses on the HS20 Expansion Card.

Host Adapter Settings
To access this option, select Host Adapter Settings. The default settings and the modifiable settings for the expansion card are listed in Table 39 and are described in this section. The HS20 Expansion Card is always point-to-point connected in the blade server with the 2-port Fibre Channel switch module.

Note: The loop reset delay, adapter hard loop ID, and hard loop ID settings are not applicable.

Table 39. Modifiable expansion card default settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host adapter BIOS</td>
<td>Enabled or disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Frame size</td>
<td>512, 1024, 2048</td>
<td>2048</td>
</tr>
<tr>
<td>Loop reset delay</td>
<td>0-60 seconds</td>
<td>5 seconds</td>
</tr>
<tr>
<td>Adapter hard loop ID</td>
<td>Enabled or disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Table 39. Modifiable expansion card default settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard loop ID</td>
<td>0-125</td>
</tr>
<tr>
<td></td>
<td>125</td>
</tr>
<tr>
<td>Spin up delay</td>
<td>Enabled or disabled</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Host adapter BIOS:** When this option is disabled, the read-only memory (ROM) BIOS code on the HS20 Expansion Card is disabled, freeing space in upper memory. The default is **Disabled**.

**Frame size:** This setting specifies the maximum frame length supported by the HS20 Expansion Card. The default size is 2048. If you are using F-port (point-to-point) connections, use the default size for maximum performance.

**Spin up delay:** When this option is enabled, the BIOS code waits up to 5 minutes to find the first drive. The default is **Disabled**.

**Note:** The HS20 Expansion Card settings and default values will vary, based on the version of BIOS code installed for the expansion card.

There are specific expansion card settings that you cannot modify. Table 40 describes these settings and gives examples.

**Note:** See the device-driver installation instructions for the required operating-system-specific modifications to the NVRAM.

Table 40. Nonmodifiable expansion card settings and examples

<table>
<thead>
<tr>
<th>Setting</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS address</td>
<td>CD400</td>
</tr>
<tr>
<td>Revision</td>
<td>1.25</td>
</tr>
<tr>
<td>Adapter serial number</td>
<td>E59719</td>
</tr>
<tr>
<td>Interrupt level</td>
<td>3</td>
</tr>
<tr>
<td>Adapter port name</td>
<td>21000E08B07C703</td>
</tr>
</tbody>
</table>

**BIOS address:** The BIOS address is the HS20 Expansion card I/O address where the BIOS code is stored when you press Ctrl+Q. This is the address of the BIOS code in ROM shadow memory.

**Revision:** The BIOS revision is the revision number of the loaded BIOS code on the HS20 Expansion Card.

**Adapter Serial Number:** This number is for manufacturing use only. It does not correlate to external labels or to the adapter port name of the HS20 Expansion Card.

**Interrupt level:** The interrupt level is the interrupt that is used by the HS20 Expansion Card. The interrupt level can change when the operating system is installed.

**Adapter port name:** This is the worldwide port name of the expansion card.

**Selectable Boot Settings**

To access this option, select **Selectable Boot Settings**. For more information about boot settings, contact your IBM technical-support representative.
Restore Default Settings
This option is in the Configuration Settings menu. It restores the HS20 Expansion Card default NVRAM settings.

Raw NOVRAM data
This option displays the HS20 Expansion Card NVRAM contents in hexadecimal format. This is a troubleshooting tool; you cannot modify the data.

Advanced Adapter Settings
Use this option to view and set advanced adapter settings. The default settings for the HS20 Expansion Card are listed in Table 41 and are described in this section.

Table 41. Advanced Adapter Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execution throttle</td>
<td>1-256</td>
<td>256</td>
</tr>
<tr>
<td>&gt;4GByte addressing</td>
<td>Enabled or Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>LUNs per target</td>
<td>0, 8, 16, 32, 64, 128, 256</td>
<td>0</td>
</tr>
<tr>
<td>Enable LIP reset</td>
<td>Yes or No</td>
<td>No</td>
</tr>
<tr>
<td>Enable LIP full login</td>
<td>Yes or No</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable target reset</td>
<td>Yes or No</td>
<td>Yes</td>
</tr>
<tr>
<td>Login retry count</td>
<td>0-255</td>
<td>30</td>
</tr>
<tr>
<td>Port down retry count</td>
<td>0-255</td>
<td>30</td>
</tr>
<tr>
<td>IOCB allocation</td>
<td>1-512 buffers</td>
<td>256 buffers</td>
</tr>
<tr>
<td>Extended error logging</td>
<td>Enabled or Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Execution throttle: This setting specifies the maximum number of commands that can run on any one port. When a port reaches its execution throttle, Fast!UTIL does not run any new commands until the current command is completed. The valid options for this setting are 1 through 256. The default (optimum) is 256.

>4GByte addressing: Enable this setting when the blade server has more than 4 GB of memory available. The default is Disabled.

LUNs per target: This setting specifies the number of logical unit numbers (LUNs) per device. Multiple LUN support is typically for redundant array of independent disks (RAID) enclosures that use LUNs to map drives. The default is 0.

Enable LIP reset: This setting determines the type of loop initialization process (LIP) reset that is used when the operating system initiates a bus reset routine. When this option is set to Yes, the device driver initiates a global LIP reset to clear the target device reservations. When this option is set to No, the device driver initiates a global LIP reset with full login. The default is No.

Enable LIP full logon: This setting instructs the application specific integrated circuit (ASIC) chip to log in to all ports after any LIP. The default is Yes.

Enable target reset: This setting enables the device drivers to issue a Target Reset command to all devices on the loop when a SCSI Bus Reset command is issued. The default is Yes.

Login retry count: This setting specifies the number of times the software tries to log in to a device. The default is 30 retries.
Port down retry count: This setting specifies the number of times the software retries a command to a port that is returning port-down status. The default is 30.

IOCB allocation: This setting specifies the maximum number of buffers from the firmware buffer pool that are allocated to any one port. The default setting is 256.

Extended error logging: When set to Enabled, this setting provides additional error and debugging information to the Windows operating system event error log. The default is Disabled.

Extended Firmware Settings
Use this option to view and set extended firmware settings. The default settings for the HS20 Expansion Card are listed in Table 42 and are described in this section.

Table 42. Extended firmware settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIO operation mode</td>
<td>0, 5</td>
<td>0</td>
</tr>
<tr>
<td>Connection Options</td>
<td>0, 1, 2</td>
<td>2</td>
</tr>
<tr>
<td>Fibre Channel tape support</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Interrupt delay timer</td>
<td>0-255</td>
<td>0</td>
</tr>
<tr>
<td>Data rate</td>
<td>0, 1, 2</td>
<td>2</td>
</tr>
</tbody>
</table>

RIO operation mode: This setting specifies the reduced interrupt operation (RIO) mode, if supported by the software device driver. When the expansion card is in the RIO mode you can post multiple command completions in a single interrupt (see Table 43). The default is 0.

Table 43. RIO options and operation modes

<table>
<thead>
<tr>
<th>Option</th>
<th>Operation mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No multiple responses</td>
</tr>
<tr>
<td>5</td>
<td>Multiple responses with minimal interrupts</td>
</tr>
</tbody>
</table>

Connection options: This setting defines the type of connection (loop or point-to-point) or connection preference (see Table 44). The default is 2.

Table 44. Connection options

<table>
<thead>
<tr>
<th>Option</th>
<th>Type of connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Loop only</td>
</tr>
<tr>
<td>1</td>
<td>Point-to-point only</td>
</tr>
<tr>
<td>2</td>
<td>Loop preferred; otherwise, point-to-point</td>
</tr>
</tbody>
</table>

Fibre Channel tape support: This setting is reserved for Fibre Channel tape support. The default is Disabled.

Interrupt delay timer: This setting contains the value (in 100-microsecond increments) used by a timer to set the wait time between accessing a set of handles and generating an interrupt using direct memory access (DMA). The default is 0.
Data rate: This setting determines the data rate. The default setting is 2.

Table 45. Data rate options

<table>
<thead>
<tr>
<th>Option</th>
<th>Data rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1 GB per second</td>
</tr>
<tr>
<td>1</td>
<td>2 GB per second</td>
</tr>
<tr>
<td>2</td>
<td>Auto select</td>
</tr>
</tbody>
</table>

Scan Fibre Channel devices

Use this option to scan and list all the connected devices. Information about each device is listed, for example, vendor name, product name, and revision. This information is useful when you are configuring the HS20 Expansion Card and attached devices.

Fibre Channel disk utility

The Fibre Channel disk utility is not supported in the IBM BladeCenter Fibre Channel Options

Use this option to scan the Fibre Channel loop bus and list all the connected devices by loop ID. You can select a disk device and perform a low-level format or verify the disk media or data.

Attention: Performing a low-level format removes all data on the disk.

Loopback data test

This option is not available with your BladeCenter configuration. Use the Online Port Loopback Test in the BladeCenter SAN Utility to test communication between the HS20 Expansion Card and the BladeCenter 2-Port Fibre Channel Switch Module. See "Port testing" on page 116.

ExitFast!UTIL

After you complete the configuration, use this option to exit the menu and restart the blade server.
Chapter 4. Diagnostic information

If you are having a problem, use the following information to help you determine the cause of the problem and the action to take.


General BladeCenter Fibre Channel configuration diagram

Refer to the following diagram and note the differences between a BladeCenter Fibre Channel installation and other Fibre Channel installations:

The HS20 Expansion Card contains two virtual adapters on a single card. One virtual adapter is connected to the BladeCenter 2-Port Fibre Channel Switch Module in switch module bay 3 and the other virtual adapter is connected to the Blade Center 2-Port Fibre Channel Switch Module in switch module bay 4.

One or two 16-port switched (2-Port Fibre Channel Switch Modules) can be installed in the BladeCenter chassis. 14 of the ports are internal ports and the remaining two are external ports.

The HBA (HS20 Expansion Card) and the switch (BladeCenter 2-Port Fibre Channel Switch Module) have internal connections through the mid-plane of the BladeCenter chassis. No SFPs or cables are required for this connection. External Loopback testing is not supported on the internal ports.

General Checkout

The following four types of problems might cause your BladeCenter Fibre Channel installation to function incorrectly:

- Hardware problems
- Software problems
- System configurations problems
- Fibre Channel problems
Use the following procedure to checkout the HS20 Expansion Card and 2-Port Fibre Channel Switch module.

1. Run the FastT MSJ program to verify the HS20 Expansion Card is functioning correctly.
2. Run the BladeCenter SAN utility to verify the BladeCenter 2-Port Fibre Channel Switch Modules are functioning correctly.
3. Use management utilities supplied by the manufacturer to verify the attached Fibre Channel devices are functioning correctly.

**Hardware problems**
To determine whether your installation problem is caused by the hardware, perform the following tasks:

1. Verify any recent hardware changes.
2. Verify that the HS20 Expansion Card is installed correctly and is fully seated in the network-interface option connector and the PCI-X expansion connector. (Refer to Installing the HS20 Expansion Card on p. 137).
3. Verify that the blade server is turned on.
4. Verify that the HS20 data-rate setting is correct. Use Fast!UTIL (see Using IBM Fast!UTIL on page 139) or FASTT MSJ (see the FASTT Management Suite Java User’s Guide). The Fibre Channel ports of the IBM 2-Port Fibre Channel Switch Module that connect to each of the blade server bays (1 through 14) are fixed at the 2 Gbps data rate.
5. Verify that the IBM 2-Port Fibre Channel Switch Module for the BladeCenter unit is installed in switch module bay 3, switch module bay 4, or both.
6. Verify that all LEDs for the switch module information panel and the switch module external Fibre Channel ports do not indicate a fault. See “LED diagnostics” on page 123.
7. Verify that all SFP optical transceivers and cables are installed and securely connected to the correct connectors.
8. Verify that all peripheral devices are turned on and connected through the Fibre Channel Switch Module. For information about displaying attached Fibre Channel devices see “Scan Fibre Channel Devices:” on page 151 or the FASTT Management Suite Java User’s Guide.

**Software problems**
To determine whether your installation problem is caused by the software, perform the following tasks:

1. Verify any recent software changes.
2. Verify that the software utilities, FastT MSJ and BladeCenter SAN Utility, are at the latest level.
3. Verify that the correct HS20 device driver is installed.
4. Verify that the BIOS code in the HS20 expansion card is at the latest level.
5. Verify that you have the correct HS20 expansion card NVRAM settings for your storage area network (SAN) and operating system.
6. Verify that the firmware on the BladeCenter 2-Port Fibre Channel Switch Module is at the latest level.

**System configuration problems**
To determine whether your installation problem is caused by the system configuration, perform the following tasks:
1. Check the HS20 Expansion Card to ensure it is configured properly. For more information, see “Configuration Settings menu options” on page 147 or the FASiT Management Suite Java User’s Guide.

2. Check the BladeCenter 2-Port Fibre Channel Switch Module to ensure it is configured properly. For more information, see chapter 2 “BladeCenter 2-Port Fibre Channel Switch Module”.

3. The BladeCenter 2-Port Fibre Channel Switch Module supports zoning, make sure that your peripheral device is configured to the same switch zone as the HS20 expansion card. For more information, refer to Chapter 2, BladeCenter 2-Port Fibre Channel Switch Module.

**Fibre channel problems**

To determine whether your installation problem is caused by an attached Fibre Channel device, perform the following tasks:

1. Verify that all the Fibre Channel devices were turned on before you turned on the blade server.

2. Ensure that all cables are connected properly.

3. Verify that you configured your RAID storage subsystem using the utilities provided by the manufacturer.

If you still have a Fibre Channel problem, refer to the IBM *IBM Fibre Channel Problem Determination Guide*. The IBM Fibre Channel Problem Determination Guide provides detailed maintenance analyst procedures (MAPs) for troubleshooting Fibre Channel problems. The following modifications need to be made to the maps for them to support the BladeCenter chassis and blade servers:

1. The FastT MSJ loopback test is not supported in the BladeCenter since the HS20 Expansion Card does not have an external port. Use the BladeCenter SAN Utility Online Port Loopback Test to verify communication between the HS20 Expansion Card and the BladeCenter 2-Port Fibre Channel Switch Module (refer to "Port testing" on page 116). Port testing should only be used on ports that are not actively transmitting data.

2. The crossPort Test referred to on the Hub/Switch PD maps is replaced by the Online Port Loopback Test and the External Port Loopback Test in the BladeCenter SAN Utility (refer to "Port testing" on page 116). Port testing should only be used on ports that are not actively transmitting data.
Chapter 5. Symptom-to-FRU index

This index supports the @server BladeCenter 2-Port Fibre Channel Switch Module and HS20 Fibre Channel Expansion Card.

**Notes:**
1. Check the configuration before you replace a FRU. Configuration problems can cause false errors and symptoms.
2. For IBM® devices not supported by this index, refer to the manual for that device.
3. Blade switch modules and management modules must be replaced during service within two minute.

The symptom-to-FRU index lists symptoms, errors, and the possible causes. The most likely cause is listed first. Use this symptom-to-FRU index to help you decide which FRUs to have available when servicing the computer.

The left-hand column of the tables in this index lists error codes or messages, and the right-hand column lists one or more suggested actions or FRUs to replace.

**Note:** In tables with more than two columns, multiple columns are required to describe the error symptoms.

Take the action (or replace the FRU) suggested first in the list of the right-hand column, then try the server again to see if the problem has been corrected before taking further action.

**Note:** Try reseating a suspected component or reconnecting a cable before replacing the component.
Fast!UTIL utility status codes

You can use the following information to find solutions to problems that have definite symptoms.

Attention: If diagnostic status messages appear that are not listed in the following tables, make sure that your BladeCenter unit has the latest level of firmware code installed.

If you have just added a new option and your system is not working, complete the following procedure before using the troubleshooting charts:
1. Remove the option that you just added.
2. Run the diagnostic tests to determine if your system is running correctly.
3. Reinstall the new device.

Note: See Chapter 6, “Parts listing”, on page 157 to determine which components should be replaced by a field service technician.

<table>
<thead>
<tr>
<th>Error code</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Configuration completed successfully. Successful operation, no action required.</td>
</tr>
</tbody>
</table>
| 1          | Error status returned for several reasons: Correct issue and retry.  
- Failure to open, read or write a file needed by Fast!UTIL.  
- Bad or missing command line parameter.  
- Bad data entered at command prompt. |
| 2          | CTRL-C detected. Keyboard sequence acknowledged, no action required. |
| 3, 4, 5, 6, 7 | Error reading flash.  
1. Remove and reinsert the fibre channel switch  
2. Retry the operation.  
3. If the problem remains, replace the fibre channel switch. |

Switch error messages

Note: See Chapter 6, “Parts listing”, on page 157 to determine which components should be replaced by a field service technician.

<table>
<thead>
<tr>
<th>Message</th>
<th>Action</th>
</tr>
</thead>
</table>
| Switch fault x | 1. Reseat switch x.  
2. Replace switch x. |
| Switch module x was removed | Information only. Take action as required. |
| Switch module x was installed | Information only. Take action as required. |
| Switch module x was powered on | Information only. Take action as required. |
| Switch module x was powered on | Information only. Take action as required. |
| Switch System running nonredundant switch modules | Information only. Take action as required. |
Note: See Chapter 6, “Parts listing”, on page 157 to determine which components should be replaced by a field service technician.

<table>
<thead>
<tr>
<th>Message</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch module%d IP configuration was changed</td>
<td>Information only. Take action as required.</td>
</tr>
<tr>
<td>ENET [X] DHCP HSTN=X, DN=X, IP @= XXX.XXX.XXX.XXXGW @= XXX.XXX.XXX.XXX, SN= XXX.XXX.XXX.XXX, DNS1@= XXX.XXX.XXX.XXX</td>
<td>Ethernet configuration information. Take action as required.</td>
</tr>
<tr>
<td>ENET [X] IP Cfg:HstName= XXXX, IP@= XXX.XXX.XXX.XXX ,GW@= XXX.XXX.XXX.XXX, NetMsk= XXX.XXX.XXX.XXX Switch module x was installed</td>
<td>Ethernet configuration information. Take action as required.</td>
</tr>
<tr>
<td>LAN: Ethernet [x] interface is no longer active</td>
<td>Check cables to switch.</td>
</tr>
<tr>
<td>LAN: Ethernet [x] interface now longer active</td>
<td>Information only. Take action as required.</td>
</tr>
</tbody>
</table>

### Expansion card error messages

Note: See Chapter 6, “Parts listing”, on page 157 to determine which components should be replaced by a field service technician.

<table>
<thead>
<tr>
<th>Message</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the HS20 Expansion Card BIOS screen the message “ERROR PC CONFIGURATION ERROR” appears.</td>
<td>1. Replace the HS20 Expansion Card 2. Replace the Blade server 3. 4. 5.</td>
</tr>
</tbody>
</table>

### Management module error messages

Note: See Chapter 6, “Parts listing”, on page 157 to determine which components should be replaced by a field service technician.

<table>
<thead>
<tr>
<th>Message</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application posted alert to ASM</td>
<td>The alert button on the web interface was tested. Information only. Take action as required.</td>
</tr>
<tr>
<td>System log 75% full</td>
<td>Information only. Take action as required.</td>
</tr>
<tr>
<td>System log full</td>
<td>Information only. Take action as required.</td>
</tr>
<tr>
<td>Management module network initialization complete</td>
<td>Information only. Take action as required.</td>
</tr>
<tr>
<td>Remote login successful. Login ID</td>
<td>Information only. Take action as required.</td>
</tr>
<tr>
<td>ASM reset was caused by restoring default values</td>
<td>The management module assembly was reset after restoring the default settings. Information only. Take action as required.</td>
</tr>
<tr>
<td>ASM reset was initiated by the user</td>
<td>Information only. Take action as required.</td>
</tr>
</tbody>
</table>
### Message Action

<table>
<thead>
<tr>
<th>Message</th>
<th>Action</th>
</tr>
</thead>
</table>
| Pushbutton reset activated: Ethernet configuration reset to default values and MM ASM reset due to watchdog timeout | 1. Reseat the management module.  
2. Reflash the management module firmware.  
3. Replace the management module. |
| ASM reset due to XXXXX, instruction fault: XXXXXXXX YYYYYYY ZZZZZZ | 1. Reseat the management module.  
2. Reflash the management module firmware.  
3. Replace the management module. |
| ASM reset reason unknown | Information only. |
| Possible ASM reset occurred reason unknown | Information only. |
| Remote access attempt failed. Invalid userid or password received. User is XXX from CMD mode client at IP@=XXX.XXX.XXX.XXX | Failed attempt to log into the management module. |
| Remote access attempt failed. Invalid userid or password received. User is XXX from WEB browser IP@=XXX.XXX.XXX.XXX | Failed attempt to log into the management module. |
| DHCP [X] failure, no IP @ assigned (retry X), rc=X | Failed to get IP address by DHCP server. Check the DHCP server connection and settings. |
| LAN: Command mode tamper triggered. Possible break in attempt. | Unsuccessful attempt to access the management module in command mode. Information only. Take action as required. |
| LAN: WEB server tamper delay triggered. Possible break in attempt. | Unsuccessful attempt to access the management module in command mode. Information only. Take action as required. |
| System log cleared. | Information only. Take action as required. |

### Switch diagnostic information

The following LED error codes, I2C diagnostic register definitions, and alarms support the 2-Port Fibre Channel Switch Module.

### LED error codes

<table>
<thead>
<tr>
<th>Heartbeat LED error codes</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 blinks</td>
<td>Internal application failure (switch is inoperable, reset is required)</td>
</tr>
<tr>
<td>3 blinks</td>
<td>Fatal POST error (switch is inoperable)</td>
</tr>
<tr>
<td>4 blinks</td>
<td>Corrupt flash or configuration (&quot;config restore&quot; required to clear fault condition)</td>
</tr>
</tbody>
</table>

---

**Note:** See Chapter 6, “Parts listing”, on page 157 to determine which components should be replaced by a field service technician.
Port LED error codes

| Fast blink | Port is inoperable (either hardware problem detected by POST, E_Port isolated, or user set the port to "down" state) |

I2C diagnostic register definitions

<table>
<thead>
<tr>
<th>Progress indicators</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01 - Initialization</td>
<td>N/A</td>
</tr>
<tr>
<td>0x10 - Serial PROM test</td>
<td>N/A</td>
</tr>
<tr>
<td>0x20 - ASIC Register test</td>
<td>N/A</td>
</tr>
<tr>
<td>0x40 - Loopback test group 1</td>
<td>N/A</td>
</tr>
<tr>
<td>0x50 - Loopback test group 2</td>
<td>N/A</td>
</tr>
<tr>
<td>0x60 - Loopback test group 3</td>
<td>N/A</td>
</tr>
<tr>
<td>0x70 - Creating test results summary (determining compromised vs. failed)</td>
<td>N/A</td>
</tr>
<tr>
<td>0xff - POST complete</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Failures</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x80 - Internal port failure</td>
<td>?????????</td>
</tr>
<tr>
<td>0xa0 - External port failure</td>
<td>?????????</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarms</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised failure (single port failure)</td>
<td>POST has detected a partial failure. Use <code>show post log</code> for more information.</td>
</tr>
<tr>
<td>0xa0 - External port failure</td>
<td>Fatal error POST detected a fatal error. The blade is not operational. Use <code>show post log</code> for more information.</td>
</tr>
</tbody>
</table>

Undetermined problems

Use the information in this section if the diagnostic tests did not identify the failure, the devices list is incorrect, or the system is inoperative.

Notes:
1. When troubleshooting a BladeCenter problem, you must determined if the problem is actually a blade server problem.
   - If the BladeCenter unit contains more then one blade server installed and only one of the blade servers exhibits the symptom, most likely it is a blade server problem.
• If all blade servers exhibit the same symptom, most likely it is a BladeCenter unit problem.

2. Damaged data in CMOS can cause undetermined problems.

3. Damaged data in BIOS code can cause undetermined problems.

Check the LEDs on all the power supplies. If the LEDs indicate the power modules are working correctly and reseating the BladeCenter components does not correct the problem, remove or disconnect the BladeCenter components one at a time to a minimal configuration or until you locate the problem. You do not need to remove power from the system. Complete the following steps to remove the components.

1. Remove the acoustic attenuation models, if attached.
2. Shut down the operating system on all blade server.
3. Turn off the blade servers; then, open the release lever on each blade server and slid it out of the bay approximately 1 inch.
4. Disconnect power modules 2, 3, and 4 one at a time. To do this, first remove the power cord; then, pull the release lever all the way down. Slide the power module out of its bay approximately 1 inch.
5. Disconnect the switch modules one at a time. To do this, remove all cables connected to the switch module; then, pull the release lever all the way down. Slide the switch module out of the bay approximately 1 inch.

**Note:** The minimum configuration is:

• 8677 unit (media tray may be connected).
• power module in bay 1.
• management module.

The BladeCenter unit can be checked with the management module WEB interface at each stage as components are removed, and will work in the minimal configuration. If the minimal configuration does not work, do the following.

1. Recheck the management module network settings.
2. Disconnect the media tray and slid it out of the bay approximately 1 inch.

**Note:** The front and rear panel LEDs will not function with the media tray removed.

3. Move the power module to bay 2.
4. Remove and reconnect the power cord to the power module.
5. Replace the management module.
6. Replace the power module.
7. Replace the midplane.

### Problem determination tips

Due to the variety of hardware and software combinations that can be encountered, use the following information to assist you in problem determination. If possible, have this information available when requesting assistance from Service Support and Engineering functions.

• Machine type and model
• Microprocessor or hard disk upgrades
• Failure symptom
  – Do diagnostics fail?
  – What, when, where, single, or multiple systems?
– Is the failure repeatable?
– Has this configuration ever worked?
– If it has been working, what changes were made prior to it failing?
– Is this the original reported failure?

• Diagnostics version
  – Type and version level

• Hardware configuration
  – Print (print screen) configuration currently in use
  – BIOS level

• Operating system software
  – Type and version level

**Note:** To eliminate confusion, identical systems are considered identical only if they:

1. Are the exact machine type and models
2. Have the same BIOS level
3. Have the same adapters/attachments in the same locations
4. Have the same address jumpers/terminators/cabling
5. Have the same software versions and levels
6. Have the same diagnostics code (version)
7. Have the same configuration options set in the system
8. Have the same setup for the operation system control files

Comparing the configuration and software set-up between “working” and “non-working” systems will often lead to problem resolution.
Chapter 6. Parts listing

This parts listing supports the IBM BladeCenter 2-Port Switch Module and HS20 Expansion Card.

**Note:** Field replaceable units (FRUs) should be serviced only by qualified field service technicians. Customer replaceable units can be replaced by the customer.

### BladeCenter 2-Port Switch Module

<table>
<thead>
<tr>
<th>Option</th>
<th>FRU No.</th>
<th>CRU/FRU</th>
</tr>
</thead>
<tbody>
<tr>
<td>BladeCenter 2-Port Switch Module</td>
<td>59P6621</td>
<td>CRU</td>
</tr>
</tbody>
</table>
## HS20 Expansion Card

<table>
<thead>
<tr>
<th>Option</th>
<th>FRU No.</th>
<th>CRU/FRU</th>
</tr>
</thead>
<tbody>
<tr>
<td>HS20 Expansion Card</td>
<td>59P6624</td>
<td>CRU</td>
</tr>
</tbody>
</table>

PCI-X connector (J3)

Fibre Channel high-speed connector (J2)
Appendix A. 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 appendix contains information about where to go for additional information about IBM and IBM products, what to do if you experience a problem with your BladeCenter unit, 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.ibmlink.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 B. Related service information

Note: The service procedures are designed to help you isolate problems. They are written with the assumption that you have model-specific training on all computers, or that you are familiar with the computers, functions, terminology, and service information provided in this manual.

Safety information

The following section contains the safety information that you need to be familiar with before servicing an IBM computer.

General safety

Follow these rules to ensure general safety:

- Observe good housekeeping in the area of the machines during and after maintenance.

- When lifting any heavy object:
  1. Ensure you can stand safely without slipping.
  2. Distribute the weight of the object equally between your feet.
  3. Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
  4. Lift by standing or by pushing up with your leg muscles; this action removes the strain from the muscles in your back. Do not attempt to lift any objects that weigh more than 16 kg (35 lb) or objects that you think are too heavy for you.

- Do not perform any action that causes hazards to the customer, or that makes the equipment unsafe.

- Before you start the machine, ensure that other service representatives and the customer's personnel are not in a hazardous position.

- Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the machine.

- Keep your tool case away from walk areas so that other people will not trip over it.

- Do not wear loose clothing that can be trapped in the moving parts of a machine. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.

- Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconductive clip, approximately 8 centimeters (3 inches) from the end.

- Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing.

  Remember: Metal objects are good electrical conductors.

- Wear safety glasses when you are: hammering, drilling soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.

- After service, reinstall all safety shields, guards, labels, and ground wires. Replace any safety device that is worn or defective.

- Reinstall all covers correctly before returning the machine to the customer.
Electrical safety

CAUTION: Electrical current from power, telephone, and communication cables can be hazardous. To avoid personal injury or equipment damage, disconnect the attached power cords, telecommunication systems, networks, and modems before you open the server covers, unless instructed otherwise in the installation and configuration procedures.

Observe the following rules when working on electrical equipment.

Important: Use only approved tools and test equipment. Some hand tools have handles covered with a soft material that do not insulate you when working with live electrical currents.

Many customers have, near their equipment, rubber floor mats that contain small conductive fibers to decrease electrostatic discharges. Do not use this type of mat to protect yourself from electrical shock.

- Find the room emergency power-off (EPO) switch, disconnecting switch, or electrical outlet. If an electrical accident occurs, you can then operate the switch or unplug the power cord quickly.
- Do not work alone under hazardous conditions or near equipment that has hazardous voltages.
- Disconnect all power before:
  - Performing a mechanical inspection
  - Working near power supplies
  - Removing or installing main units
- Before you start to work on the machine, unplug the power cord. If you cannot unplug it, ask the customer to power-off the wall box that supplies power to the machine and to lock the wall box in the off position.
- If you need to work on a machine that has exposed electrical circuits, observe the following precautions:
  - Ensure that another person, familiar with the power-off controls, is near you.
  - Use only one hand when working with powered-on electrical equipment; keep the other hand in your pocket or behind your back.
  - When using testers, set the controls correctly and use the approved probe leads and accessories for that tester.
  - Stand on suitable rubber mats (obtained locally, if necessary) to insulate you from grounds such as metal floor strips and machine frames.

Observe the special safety precautions when you work with very high voltages; these instructions are in the safety sections of maintenance information. Use extreme care when measuring high voltages.

- Regularly inspect and maintain your electrical hand tools for safe operational condition.
- Do not use worn or broken tools and testers.
• Never assume that power has been disconnected from a circuit. First, check that it has been powered-off.

• Always look carefully for possible hazards in your work area. Examples of these hazards are moist floors, nongrounded power extension cables, power surges, and missing safety grounds.

• Do not touch live electrical circuits with the reflective surface of a plastic dental mirror. The surface is conductive; such touching can cause personal injury and machine damage.

• Do not service the following parts with the power on when they are removed from their normal operating places in a machine:
  – Power supply units
  – Pumps
  – Blowers and fans
  – Motor generators and similar units. (This practice ensures correct grounding of the units.)

• If an electrical accident occurs:
  – Use caution; do not become a victim yourself.
  – Switch off power.
  – Send another person to get medical aid.

Safety inspection guide

The intent of this inspection guide is to assist you in identifying potentially unsafe conditions on these products. Each machine, as it was designed and built, had required safety items installed to protect users and service personnel from injury. This guide addresses only those items. However, good judgment should be used to identify potential safety hazards due to attachment of non-IBM features or options not covered by this inspection guide.

If any unsafe conditions are present, you must determine how serious the apparent hazard could be and whether you can continue without first correcting the problem.

Consider these conditions and the safety hazards they present:

• Electrical hazards, especially primary power (primary voltage on the frame can cause serious or fatal electrical shock).

• Explosive hazards, such as a damaged CRT face or bulging capacitor

• Mechanical hazards, such as loose or missing hardware

The guide consists of a series of steps presented in a checklist. Begin the checks with the power off, and the power cord disconnected.

Checklist:
1. Check exterior covers for damage (loose, broken, or sharp edges).
2. Turn off the computer. Disconnect the power cord.
3. Check the power cord for:
   a. A third-wire ground connector in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and frame ground.
   b. The power cord should be the appropriate type as specified in the parts listings.
   c. Insulation must not be frayed or worn.
4. Remove the cover.
5. Check for any obvious non-IBM alterations. Use good judgment as to the safety of any non-IBM alterations.
6. Check inside the unit for any obvious unsafe conditions, such as metal filings, contamination, water or other liquids, or signs of fire or smoke damage.
7. Check for worn, frayed, or pinched cables.
8. Check that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

Handling electrostatic discharge-sensitive devices
Any computer part containing transistors or integrated circuits (Is) should be considered sensitive to electrostatic discharge (ESD). ESD damage can occur when there is a difference in charge between objects. Protect against ESD damage by equalizing the charge so that the server, the part, the work mat, and the person handling the part are all at the same charge.

Notes:
1. Use product-specific ESD procedures when they exceed the requirements noted here.
2. Make sure that the ESD-protective devices you use have been certified (ISO 9000) as fully effective.

When handling ESD-sensitive parts:
• Keep the parts in protective packages until they are inserted into the product.
• Avoid contact with other people.
• Wear a grounded wrist strap against your skin to eliminate static on your body.
• Prevent the part from touching your clothing. Most clothing is insulative and retains a charge even when you are wearing a wrist strap.
• Use the black side of a grounded work mat to provide a static-free work surface. The mat is especially useful when handling ESD-sensitive devices.
• Select a grounding system, such as those in the following list, to provide protection that meets the specific service requirement.

Note: The use of a grounding system is desirable but not required to protect against ESD damage.
– Attach the ESD ground clip to any frame ground, ground braid, or green-wire ground.
– Use an ESD common ground or reference point when working on a double-insulated or battery-operated system. You can use coax or connector-outside shells on these systems.
– Use the round ground-prong of the ac plug on ac-operated computers.

Grounding requirements
Electrical grounding of the computer is required for operator safety and correct system function. Proper grounding of the electrical outlet can be verified by a certified electrician.

Safety notices (multi-lingual translations)
The caution and danger safety notices in this section are provided in the following languages:
• English
Important: All caution and danger statements in this IBM documentation begin with a number. This number is used to cross reference an English caution or danger statement with translated versions of the caution or danger statement in this section.

For example, if a caution statement begins with a number 1, translations for that caution statement appear in this section under statement 1.

Be sure to read all caution and danger statements before performing any of the instructions.

- 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.

<table>
<thead>
<tr>
<th>To Connect</th>
<th>To Disconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Turn everything OFF.</td>
<td>1. Turn everything OFF.</td>
</tr>
<tr>
<td>2. First, attach all cables to devices.</td>
<td>2. First, remove power cords from outlet.</td>
</tr>
<tr>
<td>3. Attach signal cables to connectors.</td>
<td>3. Remove signal cables from connectors.</td>
</tr>
<tr>
<td>4. Attach power cords to outlet.</td>
<td>4. Remove all cables from devices.</td>
</tr>
<tr>
<td>5. Turn device ON.</td>
<td></td>
</tr>
</tbody>
</table>
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-ROM 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
• 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 10

CAUTION:
Do not place any object weighing more than 82 kg (180 lbs.) on top of rack-mounted devices.

- Statement 20

CAUTION:
To avoid personal injury, before lifting the unit, remove all the blades to reduce the weight.

- Statement 21

CAUTION:
Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade.
Importante:

Todas as instruções de cuidado e perigo da IBM documentation começam com um número. Este número é utilizado para fazer referência cruzada de uma instrução de cuidado ou perigo no idioma inglês com as versões traduzidas das instruções de cuidado ou perigo encontradas nesta seção.

Por exemplo, se uma instrução de cuidado é iniciada com o número 1, as traduções para aquela instrução de cuidado aparecem nesta seção sob a instrução 1.

Certifique-se de ler todas as instruções de cuidado e perigo antes de executar qualquer operação.

Instrução 1

PERIGO

A corrente elétrica proveniente de cabos de alimentação, de telefone e de comunicações é perigosa.

Para evitar risco de choque:

- Não conecte ou desconecte cabos e não realize instalação, manutenção ou reconfiguração deste produto durante uma tempestade com raios.
- Conecte todos os cabos de alimentação a tomadas elétricas corretamente instaladas e aterradas.
- Conecte todos os equipamentos ao qual esse produto será conectado a tomadas corretamente instaladas.
- Sempre que possível, utilize apenas uma das mãos para conectar ou desconectar cabos de sinal.
- Nunca ligue qualquer equipamento quando existir evidência de danos por fogo, água ou na estrutura.
- Desconecte cabos de alimentação, sistemas de telecomunicação, redes e modems antes de abrir as tampas dos dispositivos, a menos que especificado de maneira diferente nos procedimentos de instalação e configuração.
- Conecte e desconecte cabos conforme descrito na seguinte tabela, ao instalar ou movimentar este produto ou os dispositivos conectados, ou ao abrir suas tampas.

<table>
<thead>
<tr>
<th>Para Conectar:</th>
<th>Para Desconectar:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. DESLIGUE Tudo.</td>
<td>1. DESLIGUE Tudo.</td>
</tr>
<tr>
<td>2. Primeiramente, conecte todos os cabos aos dispositivos.</td>
<td>2. Primeiramente, remova os cabos de alimentação das tomadas.</td>
</tr>
<tr>
<td>3. Conecte os cabos de sinal aos conectores.</td>
<td>3. Remova os cabos de sinal dos conectores.</td>
</tr>
<tr>
<td>4. Conecte os cabos de alimentação às tomadas.</td>
<td>4. Remova todos os cabos dos dispositivos.</td>
</tr>
<tr>
<td>5. LIGUE os dispositivos.</td>
<td></td>
</tr>
</tbody>
</table>
Instrução 2

CUIDADO:

Ao substituir a bateria de lítio, utilize apenas uma bateria IBM, Número de Peça 33F8354 ou uma bateria de tipo equivalente, recomendada pelo fabricante. Se o seu sistema possui um módulo com uma bateria de lítio, substitua-o apenas pelo mesmo tipo de módulo, do mesmo fabricante. A bateria contém lítio e pode explodir se não for utilizada, manuseada e descartada de maneira correta.

Não:
- Jogue ou coloque na água
- Aqueça a mais de 100°C (212°F)
- Conserte nem desmonte

Para descartar a bateria, entre em contato com a área de atendimento a clientes IBM, pelo telefone (011) 889-8986, para obter informações sobre como enviar a bateria pelo correio para a IBM.

Instrução 3

PRECAUCIÓN:

Quando produtos a laser (unidades de CD-ROM, unidades de DVD, dispositivos de fibra ótica, transmissores, etc.) estiverem instalados, observe o seguinte:
- Não remova as tampas. A remoção das tampas de um produto a laser pode resultar em exposição prejudicial à radiação de laser. Nenhuma peça localizada no interior do dispositivo pode ser consertada.
- A utilização de controles ou ajustes ou a execução de procedimentos diferentes dos especificados aqui pode resultar em exposição prejudicial à radiação.

PERIGO

Alguns produtos a laser contêm um diodo laser da Classe 3A ou Classe 3B embutido. Observe o seguinte:

Radiação de laser quando aberto. Não olhe diretamente para o raio a olho nu ou com instrumentos óticos, e evite exposição direta ao raio.

Laser Klasse 1.

Instrução 4

CUIDADO:

Ao levantar a máquina, faça-o com segurança.
Instrução 5

CUIDADO:

Os botões Liga/Desliga localizados no dispositivo e na fonte de alimentação não desligam a corrente elétrica fornecida ao dispositivo. O dispositivo também pode ter mais de um cabo de alimentação. Para remover toda a corrente elétrica do dispositivo, assegure que todos os cabos de alimentação estejam desconectados da fonte de energia elétrica.

Instrução 10

CUIDADO:

Não coloque nenhum objeto com peso superior a 82 kg (180 lbs.) sobre dispositivos montados em rack.

Instrução 20

CUIDADO:

Para prevenir acidentes, antes de erguer a unidade, remova todas as láminas para reduzir o peso.

Instrução 21

CUIDADO:

A energia é uma ameaça quando a lámina estiver conectada à fonte de alimentação. Sempre substitua a cobertura da lámina antes de efetuar a instalação.
重要:

Server Library 中的所有提要和危险条款前都带有一个标志，该标志是用来交叉引用一个英文的提要和危险条款及本部分中的用之对应的已翻译成其它文字的提要和危险条款。

例如，如果一个提要条款前的数字为 1，则本部分中相应的提要也带有符号 1。

在执行任何指示的操作之前，请确保您已经阅读了全部提要和危险条款。

声明 1

危险

电源、电话和通信电路中带有危险电流。

为避免触电:

- 禁止在没有拆线的情况下安装、维修及重新配置本产品。
- 将所有电源线连接至正确布线并已接地的电源插座上。
- 确保与本产品连接的所有设备连接至正确布线的插座上。
- 尽量只使用单手操作信号电缆。
- 如发生火警、水患及电箱破损时，请勿打开任何设备。
- 在安装配置过程中有明确指示，否则，打开设备机箱前应断开并关闭电源。
- 确保从系统中拔出电源线。
- 在安装配置设备的机箱时，应按下表操作步骤来拔插和断开电缆。

连接时:

1. 关闭所有设备。
2. 首先将所有电源线拔出设备。
3. 将信号电缆拔出接口。
4. 将电源线拔出电源插座。

断开连接时:

1. 关闭所有设备。
2. 首先从系统中拔出电源线。
3. 从接口拔下信号电缆。
4. 将电源线拔出电源插座。
声 警 2

警告：
更换锂电池时，只能使用 IBM 产品号 33F8354 或金泰力电池来更换原装电池。
如果电池盒中未有锂电池，则只能使用同一厂商制造的同一型号的电池。
更换过程中，电池中含有的微量电池可能会发生爆炸。

请勿对电池进行如下操作：
- 以火或火石点燃
- 加热超过 100°C (212°F)
- 进行物理或化学分解
- 避免电池被要求处理电池。
Laser Klass 1.

Appendix B. Related service information

173
声明 7

警告：
如果设备带有外门，拆卸或移动设备时应将其拆卸或固定以避免造成人员伤害。外门支撑不了设备的重量。

声明 8

警告：
不要拆除机架外盖或标有下标记号的任何部件。

警告：
标有此标记的组件内部存在高电压、高电流的危险。此组件中没有用户可维修的部件。如果怀疑其中的部件存在问题，应与服务技术人员联系。

声明 9

警告：
为避免人员伤害，拆卸设备上的风扇前应拔下热插拔风扇电缆。

声明 10

警告：

机架安装的设备上不得放置重于 62kg（135 磅）的物品。

> 62 kg (135 lb)
声明 11

警告:
下面的标签表明附近有锋利的边、角或接头。

声明 12

警告:
下面的标签表明附近有高温表面。

• 声明 20

警告:
为避免人身伤害，请在抬起设备之前卸下所有刀片服务器以减轻重量。

• 声明 21

警告:
当刀片服务器连接到电源时会有危险的能量，请始终在安装刀片服务器之前重新装上刀片服务器机箱。
重要資訊：

Server Library 中所有「注意」及「危險」的聲明均以數字開
始。此一数字是用作参考之用，英文「注意」或「危險」聲
明可在本節中找到相同內容的「注意」或「危險」聲明的頁
面。

例如，有一「危險」聲明以數字 1 開始，則該「危險」聲明的譯文將
出現在本節的「聲明」1 中。

執行任何指示之前，請詳閱所有「注意」及「危險」的聲明。

### 告警

**注意**

- 重要：注意後面的數字將用於指示相關的注意事項。
- 重要：注意事項內容的詳細說明，請參阅相關的手冊或資料庫。
- 重要：注意事項中的重點語句，請務必仔細閱讀。
- 重要：注意事項中的詳細資料，請參閱相關的手冊或資料庫。

### 告警 2

**注意**

- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。

### 告警 3

**注意**

- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。

### 注意

有某些問題可能會出現在 Class 3A 或 Class 3B 電磁相容性環境中，每次更換電力部分時請務必確認詳細資料庫中的數值，並配合相關的手冊或資料庫。

### 告警

- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
- 註釋：請務必仔細閱讀，並配合相關的手冊或資料庫。
Luokan 1 Laserlaite

警告 4

！

注意：
抬起裝置時，請注意安全措施。

警告 5

！

注意：
装置上的電源控制按鈕及電源供應器上的電源開關均無法關閉装置上的電源。
本装置可能有一個以上的電源線。如果移除装置上的所有電源，請確認所有電源線已被電源分離。

警告 10

！

注意：
移除任何重量超過32公斤（70.5磅）的物資時，勿在電源或電源供應器上方。

警告 20

！

警告：
為了避免人身傷害，抬起裝置之前，請先卸下所有的螺栓，以減輕重量。

警告 21

！

警告：
當螺栓鎖連接到電源時可能有危險之虞。安裝螺栓鎖之前，請先更換螺栓鎖外蓋。
Important:

Toutes les consignes Attention et Danger indiquées dans la bibliothèque IBM documentation sont précédées d’un numéro. Ce dernier permet de mettre en correspondance la consigne en anglais avec ses versions traduites dans la présente section.

Par exemple, si une consigne de type Attention est précédée du chiffre 1, ses traductions sont également précédées du chiffre 1 dans la présente section.

Prenez connaissance de toutes les consignes de type Attention et Danger avant de procéder aux opérations décrites par les instructions.

Notice n° 1

DANGER

Le courant électrique passant dans les câbles de communication, ou les cordons téléphoniques et d’alimentation peut être dangereux.

Pour éviter tout risque de choc électrique:

- Ne manipulez aucun câble et n’effectuez aucune opération d’installation, d’entretien ou de reconfiguration de ce produit au cours d’un orage.
- Branchez tous les cordons d’alimentation sur un socle de prise de courant correctement câblé et mis à la terre.
- Branchez sur des socles de prise de courant correctement câblés tout équipement connecté à ce produit.
- Lorsque cela est possible, n’utilisez qu’une seule main pour connecter ou déconnecter les câbles d’interface.
- Ne mettez jamais un équipement sous tension en cas d’incendie ou d’inondation, ou en présence de dommages matériels.
- Avant de retirer les carters de l’unité, mettez celle-ci hors tension et déconnectez ses cordons d’alimentation, ainsi que les câbles qui la reliant aux réseaux, aux systèmes de télécommunication et aux modems (sauf instruction contraire mentionnée dans les procédures d’installation et de configuration).
- Lorsque vous installez ou que vous déplacez le présent produit ou des périphériques qui lui sont raccordés, reportez-vous aux instructions ci-dessous pour connecter et déconnecter les différents cordons.

<table>
<thead>
<tr>
<th>Connexion</th>
<th>Déconnexion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mettez les unités hors tension.</td>
<td>1. Mettez les unités hors tension.</td>
</tr>
<tr>
<td>2. Commencez par brancher tous les cordons sur les unités.</td>
<td>2. Débranchez les cordons d’alimentation des prises.</td>
</tr>
<tr>
<td>5. Mettez les unités sous tension.</td>
<td></td>
</tr>
</tbody>
</table>
Notice n° 2

ATTENTION:

Remplacez la pile au lithium usagée par une pile de référence identique exclusivement - voir la référence IBM - ou par une pile équivalente recommandée par le fabricant. Si votre système est doté d’un module contenant une pile au lithium, vous devez le remplacer uniquement par un module identique, produit par le même fabricant. La pile contient du lithium et présente donc un risque d’explosion en cas de mauvaise manipulation ou utilisation.

- Ne la jetez pas à l’eau.
- Ne l’exposez pas à une température supérieure à 100° C.
- Ne cherchez pas à la réparer ou à la démonter.

Pour la mise au rebut, reportez-vous à la réglementation en vigueur.

Notice n° 3

ATTENTION:

Si des produits laser sont installés (tels que des unités de CD-ROM ou de DVD, des périphériques contenant des fibres optiques ou des émetteurs-récepteurs), prenez connaissance des informations suivantes:

- N’ouvrez pas ces produits pour éviter une exposition directe au rayon laser. Vous ne pouvez effectuer aucune opération de maintenance à l’intérieur.
- Pour éviter tout risque d’exposition au rayon laser, respectez les consignes de réglage et d’utilisation des commandes, ainsi que les procédures décrites dans le présent document.

DANGER

Certains produits laser contiennent une diode laser de classe 3A ou 3B. Prenez connaissance des informations suivantes:

Rayonnement laser lorsque le carter est ouvert. évitez de regarder fixement le faisceau ou de l’observer à l’aide d’instruments optiques. évitez une exposition directe au rayon.

Appareil A Laser de Classe 1.

Notice n° 4

ATTENTION:

≥18 kg (37 lbs)  ≥32 kg (70.5 lbs)  ≥55 kg (121.2 lbs)
ATTENTION:

Le bouton de mise sous tension/hors tension de l'unité et l'interrupteur d'alimentation du bloc d'alimentation ne coupent pas l'arrivée de courant électrique à l'intérieur de la machine. Il se peut que votre unité dispose de plusieurs cordons d'alimentation. Pour isoler totalement l'unité du réseau électrique, débranchez tous les cordons d'alimentation des socles de prise de courant.

ATTENTION:

Ne posez pas d’objet dont le poids dépasse 82 kg sur les unités montées en armoire.

ATTENTION:

Pour éviter tout risque de blessure, retirez tous les Serveurs lame de l'unité avant de la soulever.

ATTENTION:

Un courant électrique dangereux est présent lorsque le Serveur lame est connecté à une source d'alimentation. Remettez toujours en place le carter du Serveur lame avant d'installer le Serveur lame.
Wichtig:


Wenn z. B. ein Sicherheitshinweis mit der Nummer 1 beginnt, so erscheint die übersetzung für diesen Sicherheitshinweis in diesem Abschnitt unter dem Hinweis 1.

Lesen Sie alle Sicherheitshinweise, bevor Sie eine Anweisung ausführen.

Hinweis 1

VORSICHT

Elektrische Spannungen von Netz-, Telefon- und Datenübertragungsleitungen sind gefährlich.

Aus Sicherheitsgründen:

• Bei Gewitter an diesem Gerät keine Kabel anschließen oder lösen. Ferner keine Installations-, Wartungs- oder Rekonfigurationsarbeiten durchführen.
• Gerät nur an eine Schutzkontaktsteckdose mit ordnungsgemäß geerdetem Schutzkontakt anschließen.
• Alle angeschlossenen Geräte ebenfalls an Schutzkontaktsteckdosen mit ordnungsgemäß geerdetem Schutzkontakt anschließen.
• Signalkabel möglichst einhändig anschließen oder lösen.
• Keine Geräte einschalten, wenn die Gefahr einer Beschädigung durch Feuer, Wasser oder andere Einflüsse besteht.
• Nur nach den nachfolgend aufgeführten Anweisungen arbeiten, die für Installation, Transport oder öffnen von Gehäusen von Personal Computern oder angeschlossenen Einheiten gelten.

<table>
<thead>
<tr>
<th>Kabel anschließen:</th>
<th>Kabel lösen:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Gerät einschalten.</td>
<td></td>
</tr>
</tbody>
</table>

Hinweis 2
ACHTUNG:


Die Batterie nicht:
• mit Wasser in Berührung bringen.
• über 100 °C erhitzen.
• reparieren oder zerlegen.

Die örtlichen Bestimmungen für die Entsorgung von Sondermüll beachten.

Hinweis 3

ACHTUNG:

• Steuer- und Einstellelemente sowie Verfahren nur entsprechend den Anweisungen im vorliegenden Handbuch einsetzen. Andernfalls kann gefährliche Laserstrahlung auftreten.

VORSICHT

Manche CD-ROM-Laufwerke enthalten eine eingebaute Laserdiode der Klasse 3A oder 3B. Die nachfolgend aufgeführten Punkte beachten.


Hinweis 4

ACHTUNG:

Beim Anheben der Maschine die vorgeschriebenen Sicherheitsbestimmungen beachten.

Hinweis 5
ACHTUNG:


Hinweis 10

ACHTUNG:

Keine Gegenstände, die mehr als 82 kg wiegen, auf Rack-Einheiten ablegen.

Hinweis 20

ACHTUNG:

Um Verletzungen zu vermeiden, entfernen Sie vor dem Anheben der Einheit zur Verringerung des Gewichts alle Blades.

Hinweis 21

ACHTUNG:

Wenn das Blade an eine Stromquelle angeschlossen ist, besteht die Gefahr eines Stromschlags. Bringen Sie die Abdeckung der Blades immer an, bevor Sie sie installieren.
**Importante:**

Tutti gli avvisi di attenzione e di pericolo riportati nella pubblicazione IBM documentation iniziano con un numero. Questo numero viene utilizzato per confrontare avvisi di attenzione o di pericolo in inglese con le versioni tradotte riportate in questa sezione.

Ad esempio, se un avviso di attenzione inizia con il numero 1, la relativa versione tradotta è presente in questa sezione con la stessa numerazione.

Prima di eseguire una qualsiasi istruzione, accertarsi di leggere tutti gli avvisi di attenzione e di pericolo.

**Avviso 1**

**PERICOLO**

La corrente elettrica circolante nei cavi di alimentazione, del telefono e di segnale è pericolosa.

Per evitare il pericolo di scosse elettriche:

- Non collegare o scollegare i cavi, non effettuare l’installazione, la manutenzione o la riconfigurazione di questo prodotto durante i temporali.
- Collegare tutti i cavi di alimentazione ad una presa elettrica correttamente cablata e munita di terra di sicurezza.
- Collegare qualsiasi apparecchiatura collegata a questo prodotto ad una presa elettrica correttamente cablata e munita di terra di sicurezza.
- Quando possibile, collegare o scollegare i cavi di segnale con una sola mano.
- Non accendere qualsiasi apparecchiatura in presenza di fuoco, acqua o se sono presenti danni all’apparecchiatura stessa.
- Scollegare i cavi di alimentazione, i sistemi di telecomunicazioni, le reti e i modem prima di aprire i coperchi delle unità, se non diversamente indicato nelle procedure di installazione e configurazione.
- Collegare e scollegare i cavi come descritto nella seguente tabella quando si effettuano l’installazione, la rimozione o l’apertura dei coperchi di questo prodotto o delle unità collegate.

<table>
<thead>
<tr>
<th>Per collegare:</th>
<th>Per scollegare:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. SPEGNERE tutti i dispositivi.</td>
<td>1. SPEGNERE tutti i dispositivi.</td>
</tr>
<tr>
<td>2. Collegare prima tutti i cavi alle unità.</td>
<td>2. Rimuovere prima i cavi di alimentazione dalle prese elettriche.</td>
</tr>
<tr>
<td>3. Collegare i cavi di segnale ai connettori.</td>
<td>3. Rimuovere i cavi di segnale dai connettori.</td>
</tr>
<tr>
<td>4. Collegare i cavi di alimentazione alle prese elettriche.</td>
<td>4. Rimuovere tutti i cavi dalle unità.</td>
</tr>
<tr>
<td>5. ACCENDERE le unità.</td>
<td></td>
</tr>
</tbody>
</table>

**Avviso 2**

**ATTENZIONE:**
Quando si sostituisce la batteria al litio, utilizzare solo una batteria IBM con numero parte 33F8354 o batterie dello stesso tipo o di tipo equivalente consigliate dal produttore. Se il sistema di cui si dispone è provvisto di un modulo contenente una batteria al litio, sostituire tale batteria solo con un tipo di modulo uguale a quello fornito dal produttore. La batteria contiene litio e può esplodere se utilizzata, maneggiata o smaltita impropriamente.

Evitare di:
• Gettarla o immergerla in acqua
• Riscaldarla ad una temperatura superiore ai 100°C
• Cercare di ripararla o smontarla

Smaltire secondo la normativa in vigore (D.Lgs 22 del 5/2/9) e successive disposizioni nazionali e locali.

Avviso 3

ATTENZIONE:

Quando si installano prodotti laser come, ad esempio, le unità DVD, CD-ROM, a fibre ottiche o trasmettitori, prestare attenzione a quanto segue:
• Non rimuovere i coperchi. L’apertura dei coperchi di prodotti laser può determinare l’esposizione a radiazioni laser pericolose. All’interno delle unità non vi sono parti su cui effettuare l’assistenza tecnica.
• L’utilizzo di controlli, regolazioni o l’esecuzione di procedure non descritti nel presente manuale possono provocare l’esposizione a radiazioni pericolose.

PERICOLO

Alcuni prodotti laser contengono all’interno un diodo laser di Classe 3A o Classe 3B. Prestare attenzione a quanto segue:

Aprendo l’unità vengono emesse radiazioni laser. Non fissare il fascio, non guardarlo direttamente con strumenti ottici ed evitare l’esposizione diretta al fascio.

Avviso 4

ATTENZIONE:

Durante il sollevamento della macchina seguire delle norme di sicurezza.

Avviso 5
ATTENZIONE:

Il pulsante del controllo dell'alimentazione situato sull'unità e l'interruttore di alimentazione posto sull'alimentatore non disattiva la corrente elettrica fornita all'unità. L'unità potrebbe disporre di più di un cavo di alimentazione. Per disattivare la corrente elettrica dall'unità, accertarsi che tutti i cavi di alimentazione siano scollegati dalla sorgente di alimentazione.

Avviso 10

ATTENZIONE:

Non poggiare oggetti che pesano più di 82 kg sulla parte superiore delle unità montate in rack.

Avviso 20

ATTENZIONE:

Per evitare incidenti, prima di sollevare l'unità, rimuovere tutte le lame in modo da ridurre il peso.

Avviso 21

ATTENZIONE:

Quando la lama è collegata alla sorgente elettrica è presente una tensione pericolosa. Sostituire sempre il coperchio della lama prima di installarla.
危険

電気を防止するため、常に発生時には、いかなるケーブルの
取り付けまたは取り外しも行わないでください。また導入、
保守、再構成などの作業も行わないでください。

電気を防止するため:
- 電源コードは正しく接続および配線が行われている
 電源に接続してください。
- 本製品が接続されるすべての装置もまた正しく配線
 された電源に接続されている必要があります。

できれば、信頼ケーブルを取り付けまたは取り外しのとき
は外音のまわりに行いためにしてください。これにより、
電位差のある二つの表面に触ることによる感電を防ぐことが
できます。

電源コード、電話ケーブル、通信ケーブルからの電流は身体に
危険を及ぼします。設置、移動、または製品のカバーを取ったり
装置を接続したりするには、以下のようにケーブルの接続、
取り外しを行ってください。

接続するには
1. すべての電源を切る
2. まず、装置にすべての
 ネクターに接続する。
3. さらに、通信ケーブルを
 コネクターに接続する。
4. その後、電源コンセントに
 電源コードを接続する。
5. 装置の電源を入れる。

取り外すには
1. すべての電源を切る
2. まず、電源コンセントから
 電源コードを取り外す。
3. 次に、通信ケーブルを
 コネクターから取り外す。
4. その後、装置からすべての
 ケーブルを取り外す。
注意

本製品には、システム・ボード上にリチウム電池が使用されています。電池の交換方法や取り扱いを誤ると、発熱、発火、破壊のおそれがあります。

電池の交換には、IBM部品番号3383854の電池またはメーカー推薦の同等の電池を使用してください。

交換用電池の購入については、お買い求めの販売店または弊社の営業担当までお問い合わせください。

電池は幼児の手の届かない所に置いてください。

万一、幼児が電池を飲み込んだときは、直ちに医師に相談してください。

以下の行為は絶対にしないでください。
- 水にぬらすこと
- 100度C以上の過熱や焼却
- 分解や充電
- ショート

電池を接触する場合、および保存する場合にはテープなどで絶縁してください。他の金属や電池と混ざると発火、破壊の原因となります。電池は地方自治体の条例、または規則に従って廃棄してください。ごみ廃棄を処分されるごみの中に捨てないでください。

注意

レーザー製品（CD-ROM、DVD、または光ファイバーベーキングまたは光学デバイス）が組み込まれている場合には、次のことに注意してください。
- ここに記載されている制御方法、調節方法、または性能を超えて使用すると、危険な放射線を放射する可能性があります。
- ドライブのカバーを開けると、わずかな放射線を受ける可能性があります。
- ドライブの内部に触れないために交換可能な部品はありません。カバーを開けないでください。

危険

CD-ROMドライブは、Class 1AまたはClass 1Bレーザー・ダイオードを使用しています。次のことに注意してください。

CD-ROMドライブのカバーを開けるとレーザーが放射されます。
光線をみつめたり、光線を反射させて直接見たりしないでください。また、光線を反射させないようにしてください。

注意

10kg以上
30kg以上
100kg以上

装置を持ち上げる場合は、安全に持ち上げる方法に従ってください。
注意

サーバーの前面にある電源制御ボタンは、サーバーに供給された電流を遮断しません。
サーバーには、複数の電源コードが接続されているかもしれません。
サーバーから電流を完全に遮断するために、すべての電源コードが電源から取り外されていることを確認してください。

注意

ラック・モデルのサーバーの上に 82 Kg 以上の物を置かないでください。

危険

怪我を避けるため、ユニットを持ち上げる場合は、その前にすべてのブレード・サーバーを取り外して重量を軽くしてください。

危険

ブレード・サーバーを差し込んだ状態では感電する危険性があります。ブレードを差し込む前に、ブレードのカバーは必ず取り付けておいてください。
주의:
본 Server Library에 있는 모든 주의 및 위험 경고문은 번역 없이
시작합니다. 이 번역은 영문 주의 및 위험 경고문과 이 절에 나오는
반역된 방의 주의 또는 위험 경고문을 성공적으로 하는 데 사용됩니다.

여러 가지 주의 경고문 번역 1로 시작하며, 번역된 해당 주의 경고문은 본 절의 경고문 1에서 찾아볼 수 있습니다.

모든 지시사항을 수행하기 전에 반드시 모든 주의 및 위험 경고문을 읽으십시오.

경고문 1

⚠️ ⚠️ 위험
전원 공급 및 통신 케이블로부터 훼손 또는 정류는 위험합니다.

전기 촉격을 피하려면:
- 납욕물을 놓고 있는 케이블과 연결되지 않도록 하십시오. 이 케이블은
플러그, 유에서 또는 프레임을 장착해야 합니다.
- 모든 전원 코드를 적절히 배속 및 접속하여 합니다.
- 이 장치가 연결되어 있지 않은 케이블을 떼거나, 연결된 케이블의
연결 부분을 잡아 주십시오.
- 모든 활동은 신속하게 완료한 후에 연결하거나 사용하십시오.
- 정해지거나 이 장치의 손상이 있을 경우 장비를 가져
해당자로.
- 저전류 전용 또는 구조적 손상이 있을 경우 장비를 가져
해당자로.
- 분리 및 구성 보호소의 단동 놓어서 연결이 없는 장치 또는
볼과 함께 조립할 때만 올르니다. 왜건 또는 통신 시스템, 테크닉으로
모든 활동을 해야 합니다.
- 장비 또는 접속용 장치를 삽입, 이동 및 완전히 몇 개
다음 항목에 있던 케이블을 연결하거나 해제하십시오.

경고문 2

⚠️ 주의
경고! 바이러스나 장치를 포함한 IBM 백업 백업 93F9365 또는 프로토콜에 따라 시스템에 설치되어 있는 케이블을 사용하거나, 사용자 또는
배터리 케이블을 사용하지 않는 이상, 경고나 전력이 있을 경우 이 장치를 사용하기 전에 배터리 케이블에 작업해야 합니다.

다음의 주의사항:
- 장치가 불안정해지지 않도록 하십시오.
- 모든 바이러스나 장치를 포함한 IBM 백업 백업 93F9365 또는 프로토콜에 따라 시스템에 설치되어 있는 케이블을 사용하거나, 사용자 또는
배터리 케이블을 사용하지 않는 이상, 경고나 전력이 있을 경우 이 장치를 사용하기 전에 배터리 케이블에 작업해야 합니다.
- 지역 법령이나 규정의 요구에 따라 배터리를 제거해야 합니다.

190 BladeCenter 2-Port Fibre Channel Switch Module, HS20 Expansion Card: Hardware Maintenance Manual and Troubleshooting Guide
## 경고문 3

- **주의:**
  - 고유한 관리자나 사용자만이 결함을 진단하고 수리를 할 수 있는 권한을 가지고 있음을 의미합니다.
  - 서비스를 요청할 경우, 당사에 연락이 필요합니다.

### 참고

**추가 안내사항:**
- 문제 해결을 위해 서비스를 요청할 때, 가능한 한 상세한 자세한 사용 상황을 설명해 주시기 바랍니다.
- 당사에서 필요한 경우, 추가적인 도움이나 설명서 등을 제공하기위해 서비스를 요청할 수 있습니다.

## 경고문 4

### 주의사항:
- 올바른 방법을 사용하여 빌트인 또는 보조 인증서를 사용해 보세요.
- 사용자는 저장 및 복사에 대한 권한이 없을 경우 사용하지 마세요.
- 본 권장 사항은 사용자의 안전을 위해 필요할 경우 최적의 방법을 제공하며 개인의 권한에 따라 사용자가 안전하게 사용할 수 있도록 권장합니다.

| 2.8 kg (37 lbs) | ≥ 32 kg (70.5 lbs) | ≥ 55 kg (121.2 lbs) |

### 주의:
- 기계를 들 때는 안전하게 들고 올리십시오.

## 경고문 5

### 주의사항:
- 전산의 보안 및 안전을 위한 권장 사항: 보안을 위해 이 사용을 권장하지 않습니다. 보안을 위해 이 사용을 권장하지 않습니다. 보안을 위해 이 사용을 권장하지 않습니다.
- 사용자는 필요한 경우, 추가적인 도움이나 설명서 등을 제공하기위해 서비스를 요청할 수 있습니다.

| 2 | 1 |

### 경고문 10

### 주의:
- 서더용 물의 질서 상단에 ≥ 8 kg(18 lbs.)이 넘는 물체를 올리지 마십시오.

| ≥ 8 kg (18 lbs) |
경고문 20

⚠️

주의:
부품을 들어올리기 전에 모든 블레이드를 제거하여 두개를 중어야 위험하지 않겠습니다.

경고문 21

⚠️ ⚠️

주의:
블레이드를 전면에 연결할 때 감전 등의 위험이 있을 수 있습니다.
블레이드를 설치하기 전에 항상 블레이드 덮개를 교체하십시오.
**Importante:**

Todas las declaraciones de precaución de esta IBM documentation empiezan con un número. Dicho número se emplea para establecer una referencia cruzada de una declaración de precaución o peligro en inglés con las versiones traducidas que de dichas declaraciones pueden encontrarse en esta sección.

Por ejemplo, si una declaración de peligro empieza con el número 1, las traducciones de esta declaración de precaución aparecen en esta sección bajo Declaración 1.

Lea atentamente todas las declaraciones de precaución y peligro antes de llevar a cabo cualquier operación.

**Declaración 1**

**PELIGRO**

La corriente eléctrica de los cables telefónicos, de alimentación y de comunicaciones es perjudicial.

Para evitar una descarga eléctrica:

- No conecte ni desconecte ningún cable ni realice las operaciones de instalación, mantenimiento o reconfiguración de este producto durante una tormenta.
- Conecte cada cable de alimentación a una toma de alimentación eléctrica con conexión a tierra y cableado correctos.
- Conecte a tomas de alimentación con un cableado correcto cualquier equipo que vaya a estar conectado a este producto.
- Si es posible, utilice una sola mano cuando conecte o desconecte los cables de sent.al.
- No encienda nunca un equipo cuando haya riesgos de incendio, de inundación o de daños estructurales.
- Desconecte los cables de alimentación, sistemas de telecomunicaciones, redes y módems conectados antes de abrir las cubiertas del dispositivo a menos que se indique lo contrario en los procedimientos de instalación y configuración.
- Conecte y desconecte los cables tal como se describe en la tabla siguiente cuando desee realizar una operación de instalación, de traslado o de apertura de las cubiertas para este producto o para los dispositivos conectados.

<table>
<thead>
<tr>
<th>Para la conexión</th>
<th>Para la desconexión</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. APÁGUELO todo.</td>
<td>1. APÁGUELO todo.</td>
</tr>
<tr>
<td>2. En primer lugar, conecte los cables a los dispositivos.</td>
<td>2. En primer lugar, retire cada cable de alimentación de la toma de alimentación.</td>
</tr>
<tr>
<td>3. Conecte los cables de señal a los conectores.</td>
<td>3. Retire los cables de señal de los conectores.</td>
</tr>
<tr>
<td>4. Conecte cada cable de alimentación a la toma de alimentación.</td>
<td>4. Retire los cables de los dispositivos.</td>
</tr>
<tr>
<td>5. ENCIENDA el dispositivo.</td>
<td></td>
</tr>
</tbody>
</table>

Appendix B. Related service information 193
Declaración 2

PRECAUCIÓN:

Cuando desee sustituir la batería de litio, utilice únicamente el número de pieza 33F8354 de IBM o cualquier tipo de batería equivalente que recomiende el fabricante. Si el sistema tiene un módulo que contiene una batería de litio, sustitúyalo únicamente por el mismo tipo de módulo, que ha de estar creado por el mismo fabricante. La batería contiene litio y puede explotar si el usuario no la utiliza ni la maneja de forma adecuada o si no se desprende de la misma como corresponde.

No realice las acciones siguientes:

- Arrojarla al agua o sumergirla
- Calentarla a una temperatura que supere los 100°C (212°F)
- Repararla o desmontarla

Despréndase de la batería siguiendo los requisitos que exija el reglamento o la legislación local.

Declaración 3

PRECAUCIÓN:

Cuando instale productos láser (como, por ejemplo, CD-ROM, unidades DVD, dispositivos de fibra óptica o transmisores), tenga en cuenta las advertencias siguientes:

- No retire las cubiertas. Si retira las cubiertas del producto láser, puede quedar expuesto a radiación láser perjudicial. Dentro del dispositivo no existe ninguna pieza que requiera mantenimiento.
- El uso de controles o ajustes o la realización de procedimientos que no sean los que se han especificado aquí pueden dar como resultado una exposición perjudicial a las radiaciones.

PELIGRO

Algunos productos láser contienen un diodo de láser incorporado de Clase 3A o de Clase 3B. Tenga en cuenta la advertencia siguiente.

Cuando se abre, hay radiación láser. No mire fijamente el rayo ni lleve a cabo ningún examen directamente con instrumentos ópticos; evite la exposición directa al rayo.

Declaración 4

≥18 kg  ≥32 kg  ≥55 kg
PRECAUCIÓN:

Tome medidas de seguridad al levantar el producto.

Declaración 5

1

PRECAUCIÓN:

El botín de control de alimentación del dispositivo y el interruptor de alimentación de la fuente de alimentación no apagan la corriente eléctrica suministrada al dispositivo. Es posible también que el dispositivo tenga más de un cable de alimentación. Para eliminar la corriente eléctrica del dispositivo, asegúrese de desconectar todos los cables de alimentación de la fuente de alimentación.

Declaración 10

PRECAUCIÓN:

No coloque ningún objeto que pese más de 82 kg (180 libras) encima de los dispositivos montados en bastidor.

Declaración 20

PRECAUCIÓN:

Para prevenir ferimentos pessoais, antes de levantar a unidade retire todas as láminas para diminuir o peso.

Declaración 21

PRECAUCIÓN:

Existe energia perigosa quando a lámina está ligada à fonte de alimentação. Substitua sempre a cobertura da lámina antes de instalar a mesma.
Appendix C. 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 about 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 states 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:

<table>
<thead>
<tr>
<th>Term</th>
<th>Trademark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Memory</td>
<td>PS/2</td>
</tr>
<tr>
<td>Active PCI</td>
<td>ServeRAID</td>
</tr>
<tr>
<td>Active PCI-X</td>
<td>ServerGuide</td>
</tr>
<tr>
<td>Alert on LAN</td>
<td>ServerProven</td>
</tr>
<tr>
<td>BladeCenter</td>
<td>TechConnect</td>
</tr>
<tr>
<td>Predictive Failure Analysis</td>
<td>Tivoli</td>
</tr>
<tr>
<td>Chipkill</td>
<td>Tivoli Enterprise</td>
</tr>
<tr>
<td>EtherJet</td>
<td>Update Connector</td>
</tr>
<tr>
<td>e-business logo</td>
<td>Wake on LAN</td>
</tr>
<tr>
<td>HelpWare</td>
<td>XA-32</td>
</tr>
<tr>
<td>IBM</td>
<td>XA-64</td>
</tr>
<tr>
<td>IntelliStation</td>
<td>X-Architecture</td>
</tr>
<tr>
<td>Light Path Diagnostics</td>
<td>XceL4</td>
</tr>
<tr>
<td>NetBAY</td>
<td>XpandOnDemand</td>
</tr>
<tr>
<td>NetView</td>
<td>xSeries</td>
</tr>
<tr>
<td>OS/2 WARP</td>
<td></td>
</tr>
</tbody>
</table>

Lotus and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

Intel, Celeron, MMX, LANDesk, Pentium, Pentium II Xeon, Pentium III Xeon, and Xeon 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 the 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 1000000 bytes, and GB stands for approximately 1000000000 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.

Unless otherwise stated, 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 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.

Taiwan electrical emission 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。
Part Number: 73P8584