BROCADE

Advanced Web Tools

Administrator’s Guide

Supporting Fabric OS v4.4.0

Supporting SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, 24000

Publication Number: 53-0000522-07
Publication Date: 9/15/2004

Publication Number: 53-0000522-07

Brocade, the Brocade B weave logo, Secure Fabric OS, and SilkWorm are registered trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. FICON, IBM @server BladeCenter are registered trademarks of IBM Corporation in the U.S. and other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Export of technical data contained in this document may require an export license from the United States Government.

Brocade Communications Systems, Incorporated

Corporate Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Latin America Headquarters
Brocade Communications System, Inc.
5201 Blue Lagoon Drive
Miami, FL 33126
Tel: 1-305-716-4165
E-mail: latinam-sales@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour A - 2ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 56 40
Fax: +41 22 799 56 41
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems K.K.
Shiroyama JT Trust Tower 36th FL.
4-3-1 Toranomon, Minato-ku
Tokyo, Japan 105-6036
Tel: +81-3-5402-5300
Fax: +81-3-5402-5399
E-mail: japan-info@brocade.com

Document History

The following table lists all versions of the *Brocade Advanced Web Tools Administrator's Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
Web Tools User's Guide v2.0	53-0001536-01	NA	September 1999
Web Tools User's Guide v2.2	53-0001558-02	NA	May 2000
Web Tools User's Guide v2.3	53-0000067-02	NA	December 2000
Web Tools User's Guide v3.0	53-0000130-03	NA	July 2001
Web Tools User's Guide v2.6	53-0000197-02	NA	December 2001
Advanced Web Tools User's Guide v3.0 / v4.0	53-0000185-02	NA	March 2002
Advanced Web Tools User's Guide v4.0.2	53-0000185-03	NA	September 2002
Advanced Web Tools User's Guide v3.1.0	53-0000503-02	NA	April 2003
Advanced Web Tools User's Guide v4.1.0	53-0000522-02	NA	April 2003
Advanced Web Tools User's Guide v4.1.2	53-0000522-04	Insistent Domain ID Mode. Port Swapping information. Minor editorial changes	October 2003
Advanced Web Tools Administrator's Guide, v4.2.0	53-0000522-05	Updates to support new switch types: SilkWorm 3250, 3850, 24000. Structural changes, Support changes, Installation changes.	December 2003
Advanced Web Tools User's Guide	53-0000522-06	Clarifications on software and hardware support, minor enhancements in procedure text, minor rearranging of content.	March 2004
Advanced Web Tools Administrator's Guide	53-0000522-07	Updates to support new switch types (3016, 4100) and Fabric OS v4.4.0, including Ports on Demand, user administration, and zoning wizards.	September 2004

Contents

About This Document

Chapter 1 Introducing Web Tools

Chapter 2 Requirements, Installation, and Support

Chapter 3 Managing Your Fabrics, Switches, and Ports

Chapter 5 Zone Administration

Chapter 6 Performance Monitoring Administration

Chapter 7 Fabric Watch Administration

Chapter 8 Administering and Managing FICON CUP Fabrics

Chapter 9 Limitations

Glossary

Index

About This Document

This document is an administrator's guide written to help you monitor and modify your switches and fabrics from a Web-based graphical user interface. This document is specific to Brocade Fabric OS v4.4.0 and all switches running Fabric OS v4.4.0, including:

- Brocade SilkWorm 3016 switch
- Brocade SilkWorm 3250 switch
- Brocade SilkWorm 3850 switch
- Brocade SilkWorm 3900 switch
- Brocade SilkWorm 4100 switch
- Brocade SilkWorm 12000 director
- Brocade SilkWorm 24000 director

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

"About This Document" contains the following sections:

- "How This Document Is Organized," next
- "Supported Hardware and Software" on page xii
- "What's New in This Document" on page xiii
- "Document Conventions" on page xiv
- "Additional Information" on page xiv
- "Getting Technical Help" on page xvii
- "Document Feedback" on page xvii

How This Document Is Organized

This document is organized to help you find the particular information that you want as quickly and easily as possible.

This document provides both concepts and procedures. If you are already familiar with the Web Tools interface, you might want to forgo reading Chapter 1, "Introducing Web Tools".

Because this document primarily tells you how to perform administrative tasks in Web Tools, it is arranged in a loosely chronological order, beginning with prerequisites to getting started and ending with troubleshooting information.

The document contains the following topics:

- Chapter 1, “Introducing Web Tools”, provides some basic information about the Web Tools interface and offers recommendations for working with Web Tools.
- Chapter 2, “Requirements, Installation, and Support”, provides information about Web Tools system and switch requirements, as well as how to install Web Tools.
- Chapter 3, “Managing Your Fabrics, Switches, and Ports”, provides information on how to manage your entire fabric, including switches and ports, using the Web Tools interface.
- Chapter 4, “Monitoring Your Fabrics, Switches, and Ports”, provides information on how to monitor your entire fabric, including switches and ports, using the Web Tools interface, without any special licenses.
- Chapter 5, “Zone Administration”, provides information on how to use the Brocade Advanced Zoning feature to partition your storage area network (SAN) into logical groups of devices that can access each other. For example, you can partition your SAN into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage.
- Chapter 6, “Performance Monitoring Administration”, provides information on how to use the Brocade Advanced Performance Monitoring feature to monitor your fabric performance.
- Chapter 7, “Fabric Watch Administration”, provides information on how to use the Fabric Watch feature to monitor the performance and status of switches and alert you when problems arise.
- Chapter 8, “Administering and Managing FICON CUP Fabrics”, provides information on how to administer and manage FICON CUP fabrics. You can enable FMS mode, edit and create configurations, and edit FMS parameters.
- Chapter 9, “Limitations”, discusses the limitations of and provides workarounds for using Web Tools.
- The glossary defines both terms specific to Brocade technology and common industry terms with uses specific to Brocade technology.
- The index points you to the exact pages on which specific information is located.

Supported Hardware and Software

This document has been updated to include information specific to the Brocade SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000 switches running Brocade Fabric OS v4.4.0, including:

- Additional functionality or support in the software from Brocade Fabric OS v4.2.0.
- Changes to functionality or support in the software from Brocade Fabric OS v4.2.0.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for the Brocade Fabric OS v4.4.0 release, documenting all possible configurations and scenarios is beyond the scope of this document; however, this document does specify when procedures or steps of procedures apply only to specific switches.

This document does not support all 4.x Fabric OS versions. This document is specific to the Fabric OS v4.4.0 release. To obtain information about an OS version other than v4.4.0, refer to the documentation specific to your OS version.

What's New in This Document

The following changes have been made since this document was last released:

- Information that was added:
  - Added Chapter 8, "Administering and Managing FICON CUP Fabrics", to document the support of FICON CUP fabrics by Web Tools.
  - Added a section to Chapter 5, "Zone Administration", to document the four zoning wizards.
  - Added information on managing user accounts.
  - Added information on managing trace dumps.
  - Added information about the Ports on Demand licensed feature. A new column, **Licensed Port**, has been added to the Ports panel in the Switch Admin module.
  - Added information on configuring RADIUS servers.
  - Screen shots have been updated.
- Information that was changed:
  - Requirements, installation, and support information was updated. Refer to Chapter 2, "Requirements, Installation, and Support", for more information.
  - Updated procedures throughout the document to support the Fabric OS v4.4.0 feature set.
  - Made template and editorial changes throughout.

For further information, refer to the Brocade Fabric OS Release Notes.

Document Conventions

This section describes text formatting conventions and important notices formats.

Text Formatting

The narrative-text formatting conventions that are used in this document are as follows:

bold text	Identifies command names Identifies GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, Cautions, and Warnings

The following notices appear in this document.

Note
A note provides a tip, emphasizes important information, or provides a reference to related information.

Caution
A caution alerts you to potential damage to hardware, firmware, software, or data.

Warning
A warning alerts you to potential danger to personnel.

Additional Information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade Resources

The following related documentation is provided on the Brocade Documentation CD-ROM and on the Brocade Web site, through Brocade Connect.

Note

Go to *http://www.brocade.com* and click **Brocade Connect** to register at no cost for a user ID and password.

Fabric OS

- *Brocade Fabric OS Features Guide*
- *Brocade Fabric OS Procedures Guide*
- *Brocade Fabric OS Command Reference Manual*
- *Brocade Fabric OS MIB Reference Manual*
- *Brocade Fabric OS System Error Message Reference Manual*

Fabric OS Optional Features

- *Brocade Fabric Watch User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Secure Fabric OS QuickStart Guide*

SilkWorm 24000

- *SilkWorm 24000 QuickStart Guide*
- *SilkWorm 24000 Hardware Reference Manual*

SilkWorm 12000

- *SilkWorm 12000 QuickStart Guide*
- *SilkWorm 12000 Hardware Reference Manual*

SilkWorm 4100

- *SilkWorm 4100 Hardware Reference Manual (for v4.4.x and later software)*
- *SilkWorm 4100 QuickStart Guide (for v4.4.x and later software)*

SilkWorm 3900

- *SilkWorm 3900 Hardware Reference Manual (for v4.x software)*
- *SilkWorm 3900 QuickStart Guide (for v4.x software)*

SilkWorm 3250/3850

- *SilkWorm 3250/3850 Hardware Reference Manual (for v4.x software)*
- *SilkWorm 3250/3850 QuickStart Guide (for v4.x software)*

SilkWorm 3016

- *SilkWorm 3016 Hardware Reference Manual (for v4.2.x and later software)*

- *SilkWorm 3016 QuickStart Guide (for v4.2.x and later software)*
- *Brocade Enterprise and Entry SAN Switch Modules for IBM eServer BladeCenter Design, Deployment and Management Guide* (DDM)

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

http://www.brocade.com

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

Other Industry Resources

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, as well as other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

http://www.fibrechannel.org

Getting Technical Help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. **General Information**
   - Technical Support contract number, if applicable
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem and specific questions
   - Description of any troubleshooting steps already performed and results
2. **Switch Serial Number**

   The switch serial number and corresponding bar code are provided on the serial number label, as shown here:

   The serial number label is located as follows:
   - *SilkWorm 3016 switch:* Side of switch module.
   - *SilkWorm 3250, 3850, and 3900 switches*: Bottom of chassis.
   - *SilkWorm 4100 switches:* On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side).
   - *SilkWorm 12000 and 24000 directors:* Inside the front of the chassis, on the wall to the left of the ports.
3. **World Wide Name (WWN)**
   - *SilkWorm 3016, 3250, 3850, 3900, and 4100 switches and SilkWorm 12000 and 24000 directors:* Provide the license ID. Use the **licenseIDShow** command to display the license ID.
   - *All other SilkWorm switches:* Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Document Feedback

Because quality is our first concern at Brocade, we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to *documentation@brocade.com*. Provide the title and version number and as much detail as possible about your issue, including the topic heading and page number and your suggestions for improvement.

Chapter

1

Introducing Web Tools

Brocade Web Tools is a graphical user interface (GUI) that enables administrators to monitor and manage single or small fabrics, switches, and ports from a standard workstation. It is an optionally licensed product that runs on Brocade Fabric OS.

Web Tools provides the administrative control point for Brocade Advanced Fabric Services, including Advanced Zoning, ISL Trunking, Advanced Performance Monitoring, and Fabric Watch. Web Tools also provides an interface to telnet commands to perform special switch functions and diagnostics that are available only through the telnet interface.

This chapter contains the following sections:

- "Launching Web Tools," next
- "Switch Explorer" on page 1-2
- "Displaying Switches in the Fabric" on page 1-10
- "Web Tools and Secure Mode" on page 1-10
- "Recommendations When Working with Web Tools" on page 1-12

Launching Web Tools

You can launch Web Tools on any workstation with a compatible Web browser installed. For a list of Web browsers compatible with Fabric OS v4.4.0, refer to "Requirements" on page 2-1. Web Tools also supports HTTPS protocol, if that protocol is enabled for the switch. For more information on enabling the HTTPS protocol on your switch, refer to the *Brocade Fabric OS Procedures Guide*.

To launch Web Tools

1. Launch the Web browser and type the IP address of the licensed switch in the Location/Address field:

   ```
   http://123.123.123.123
   ```

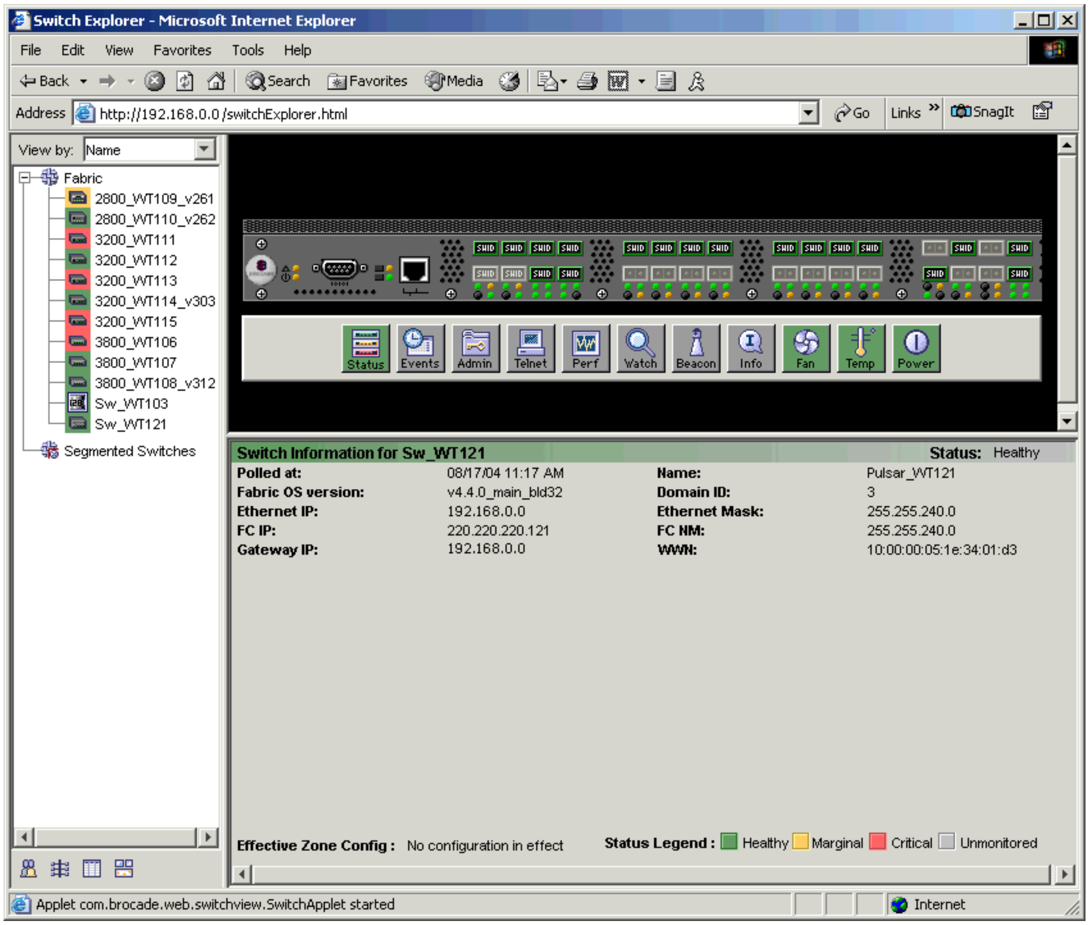
   or

   ```
   https://123.123.123.123
   ```

2. Press **Enter**.

Web Tools launches, as shown in Figure 1-1 on page 1-2.

Figure 1-1 Web Tools Switch Explorer for a SilkWorm 4100 Switch



Address http://192.168.0.0/switchExplorer.html

Switch Information for Sw_WT121 **Status:** Healthy

Polled at:	08/17/04 11:17 AM	**Name:**	Pulsar_WT121
Fabric OS version:	v4.4.0_main_bld32	**Domain ID:**	3
Ethernet IP:	192.168.0.0	**Ethernet Mask:**	255.255.240.0
FC IP:	220.220.220.121	**FC NM:**	255.255.240.0
Gateway IP:	192.168.0.0	**WWN:**	10:00:00:05:1e:34:01:d3

Effective Zone Config : No configuration in effect **Status Legend :** 🟩 Healthy 🟨 Marginal 🟥 Critical □ Unmonitored

Applet com.brocade.web.switchview.SwitchApplet started

Switch Explorer

The first thing you see when you log in to a switch with Web Tools is the Switch Explorer (see Figure 1-1 on page 1-2). The Switch Explorer is divided into several areas that provide access to and information about the switch and fabric. You should familiarize yourself with these areas, as the procedures in this guide refer to them as follows:

- Fabric Tree, which displays a list of all the switches in the fabric
- Fabric Toolbar, which provides access to fabric-wide management interfaces, such as Name Server, and events
- Switch View**,** which displays an interactive graphical representation of the switch
- Switch View Button Menu, which displays buttons providing switch information such as status, event information, access to telnet, switch administration, switch performance, beaconing, and much more
- Switch Information View, which displays information about the switch such as name, status, Fabric OS version, domain ID, IP address, and WWN
- Status Legend, which defines the meaning of the colors visible in the background of various icons in the Switch Explorer

These areas are described further in the sections that follow.

Clicking some of the buttons and icons in the Switch Explorer opens up a separate module, from which you can perform management tasks. In this document, a *module* is a collection of related tabs or "views" that display in a single browser window.

The format of the Switch Explorer varies, depending on the hardware type. Figure 1-2 on page 1-4 through Figure 1-5 on page 1-7 show Switch Explorer examples for several SilkWorm switches. The SilkWorm 3250 Switch Explorer view (shown in Figure 1-4) is a good example of how the SilkWorm 3850, 3900, and 4100 Switch Explorer views look.

Note that the figures are grayed out so that you can more easily see the areas of the Switch Explorer.

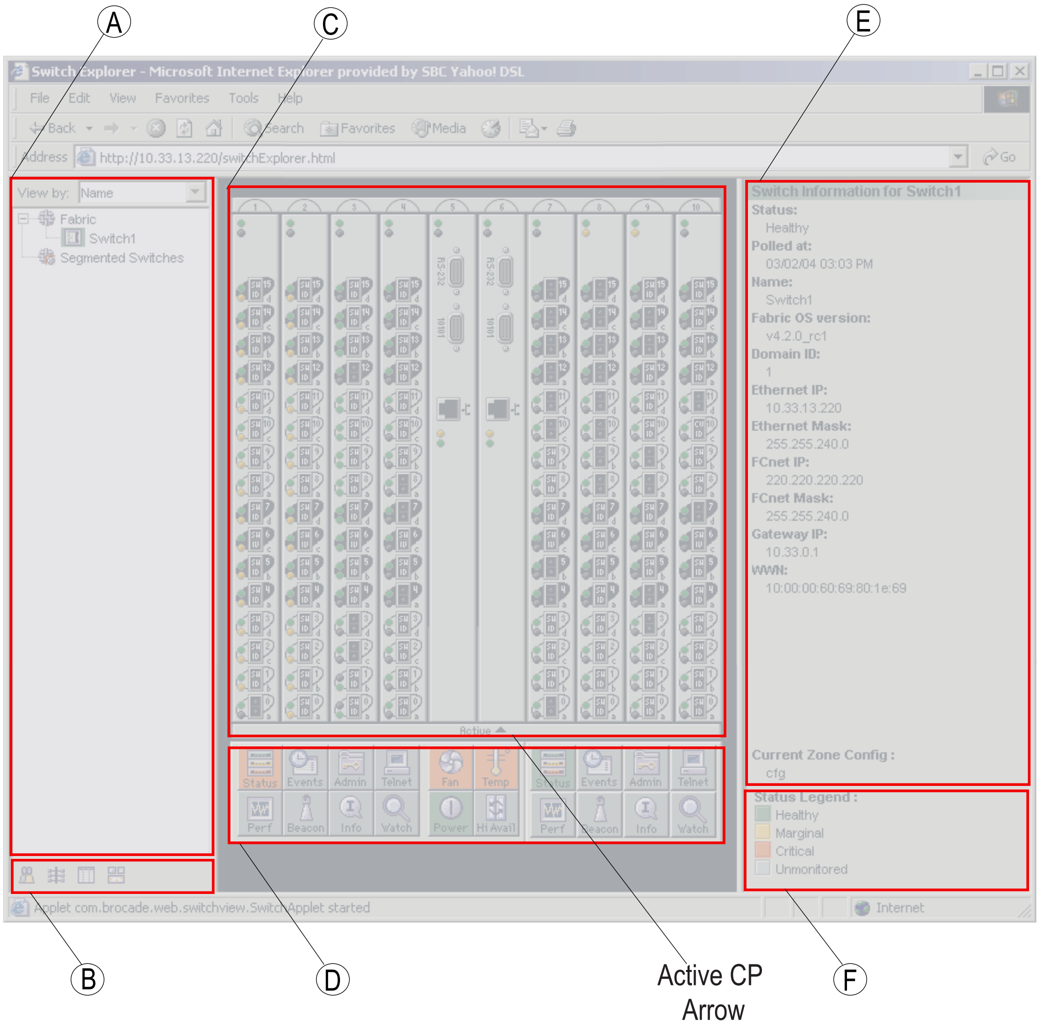
In Figure 1-2 through Figure 1-5, the letters A through F call out the different areas within the Switch Explorer. Table 1-1 is a key for these callouts.

Table 1-1 Key to Figure 1-2 through Figure 1-4

Callout Letter	Area of Switch Explorer View
A	Fabric Tree
B	Fabric Toolbar
C	Switch View
D	Switch View Button Menu
E	Switch Information View
F	Status Legend

Figure 1-2 shows an example of the Web Tools Switch Explorer for a SilkWorm 12000 director.

Figure 1-2 Web Tools Switch Explorer for a SilkWorm 12000 Director



http://10.33.13.220/switchExplorer.html

Switch Information for Switch1

Status:
Healthy

Polled at:
03/02/04 03:03 PM

Name:
Switch1

Fabric OS version:
v4.2.0_rc1

Domain ID:
1

Ethernet IP:
10.33.13.220

Ethernet Mask:
255.255.240.0

FCnet IP:
220.220.220.220

FCnet Mask:
255.255.240.0

Gateway IP:
10.33.0.1

WWN:
10:00:00:60:69:80:1e:69

Current Zone Config :
cfg

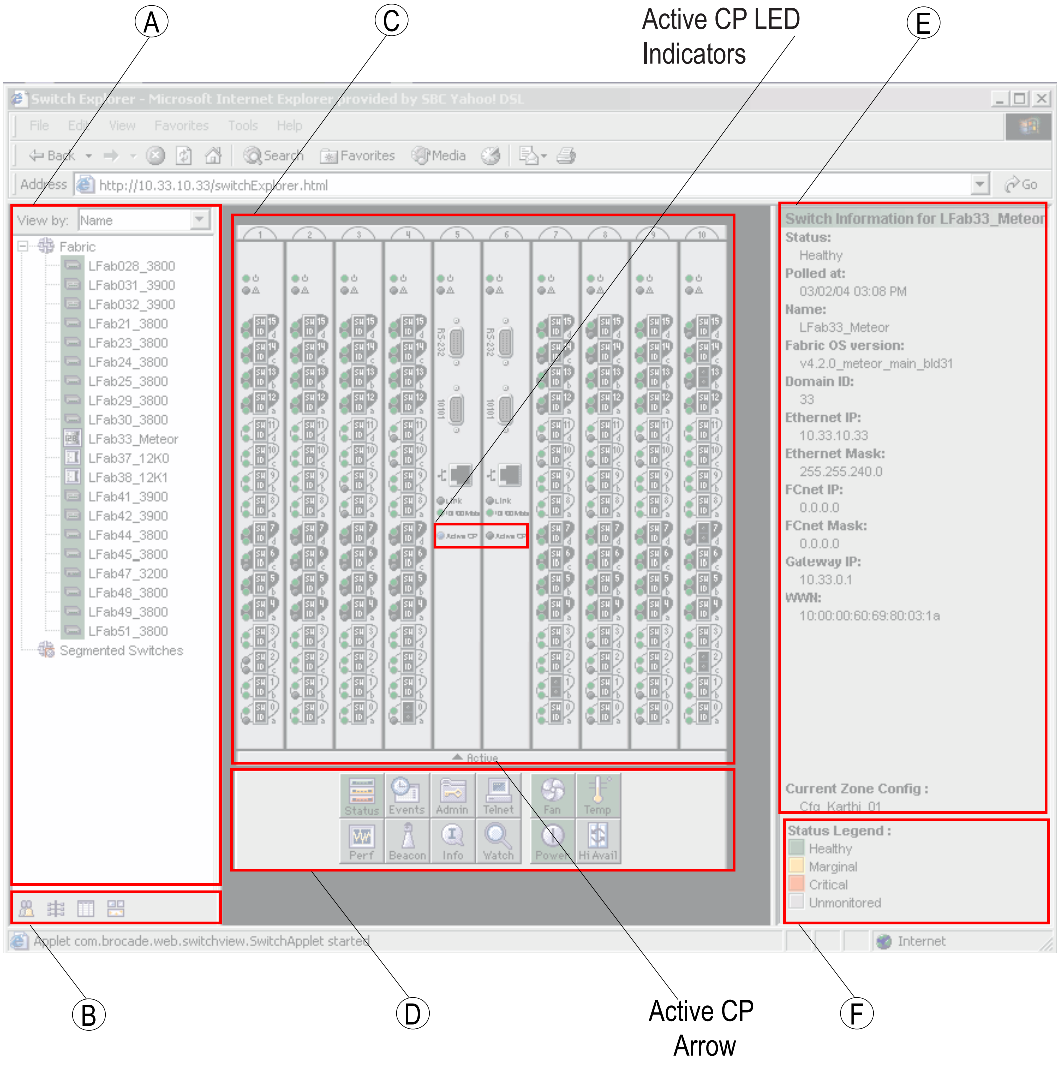
Status Legend :
🟩 Healthy
🟨 Marginal
🟥 Critical
□ Unmonitored

Applet com.brocade.web.switchview.SwitchApplet started

In this figure, the SilkWorm 12000 director has two domains; there is a separate set of Switch View buttons per logical switch. When only one domain exists, there is one shared set of Switch View buttons, as displayed in Figure 1-3 on page 1-5. The active CP in the SilkWorm 12000 director is labeled with a small arrow at the bottom of the CP display.

Figure 1-3 shows an example of the Web Tools Switch Explorer for a SilkWorm 24000 director.

Figure 1-3 Web Tools Switch Explorer for a SilkWorm 24000 Director



Switch Information for LFab33_Meteor

Status:
Healthy

Polled at:
03/02/04 03:08 PM

Name:
LFab33_Meteor

Fabric OS version:
v4.2.0_meteor_main_bld31

Domain ID:
33

Ethernet IP:
10.33.10.33

Ethernet Mask:
255.255.240.0

FCnet IP:
0.0.0.0

FCnet Mask:
0.0.0.0

Gateway IP:
10.33.0.1

WWN:
10:00:00:60:69:80:03:1a

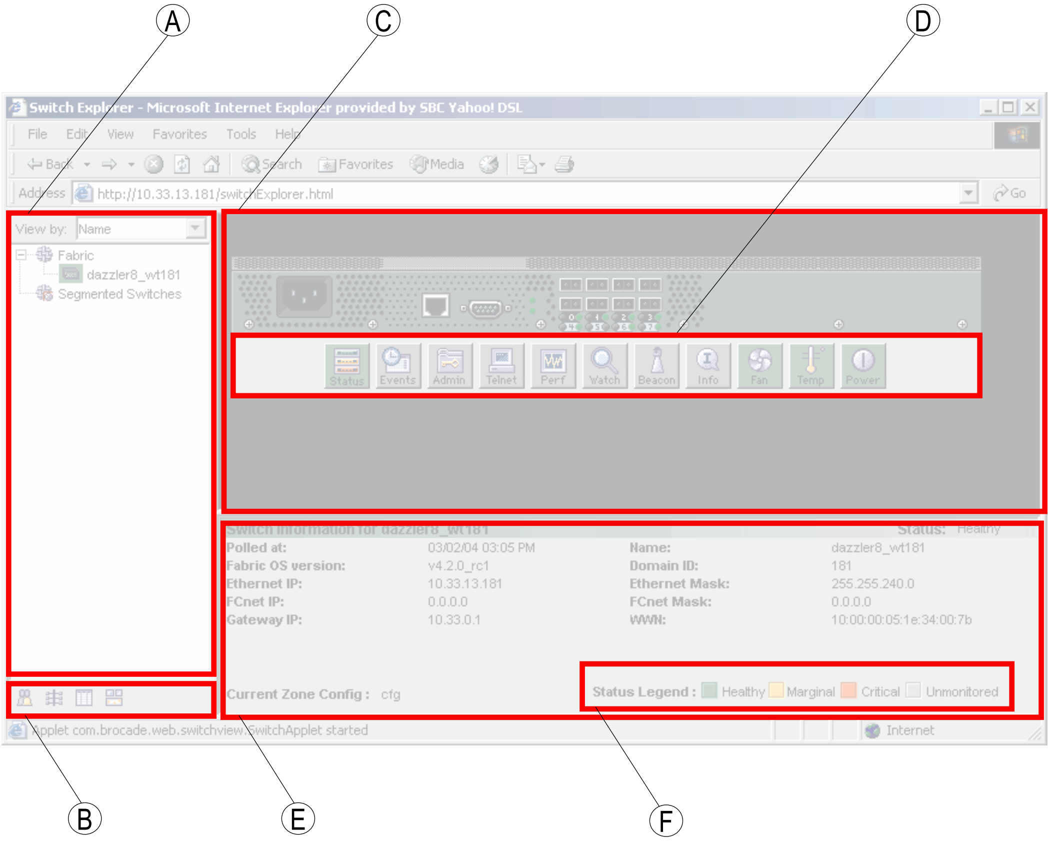
Current Zone Config :
Cfg_Karthi_01

Status Legend :
- 🟩 Healthy
- 🟨 Marginal
- 🟥 Critical
- □ Unmonitored

The active CP in the SilkWorm 24000 director is labeled with a small arrow at the bottom of the CP display. The SilkWorm 24000 active CP is also indicated with the blue Active CP LED indicator, as shown in the figure.

Figure 1-4 shows an example of the Web Tools Switch Explorer for a SilkWorm 3250 switch. This is the same format of the Switch Explorer used in Web Tools for the SilkWorm 3850, 3900, and 4100 switches.

Figure 1-4 Web Tools Switch Explorer for a SilkWorm 3250 Switch



Switch Information for dazzler8_wt181 Status: Healthy

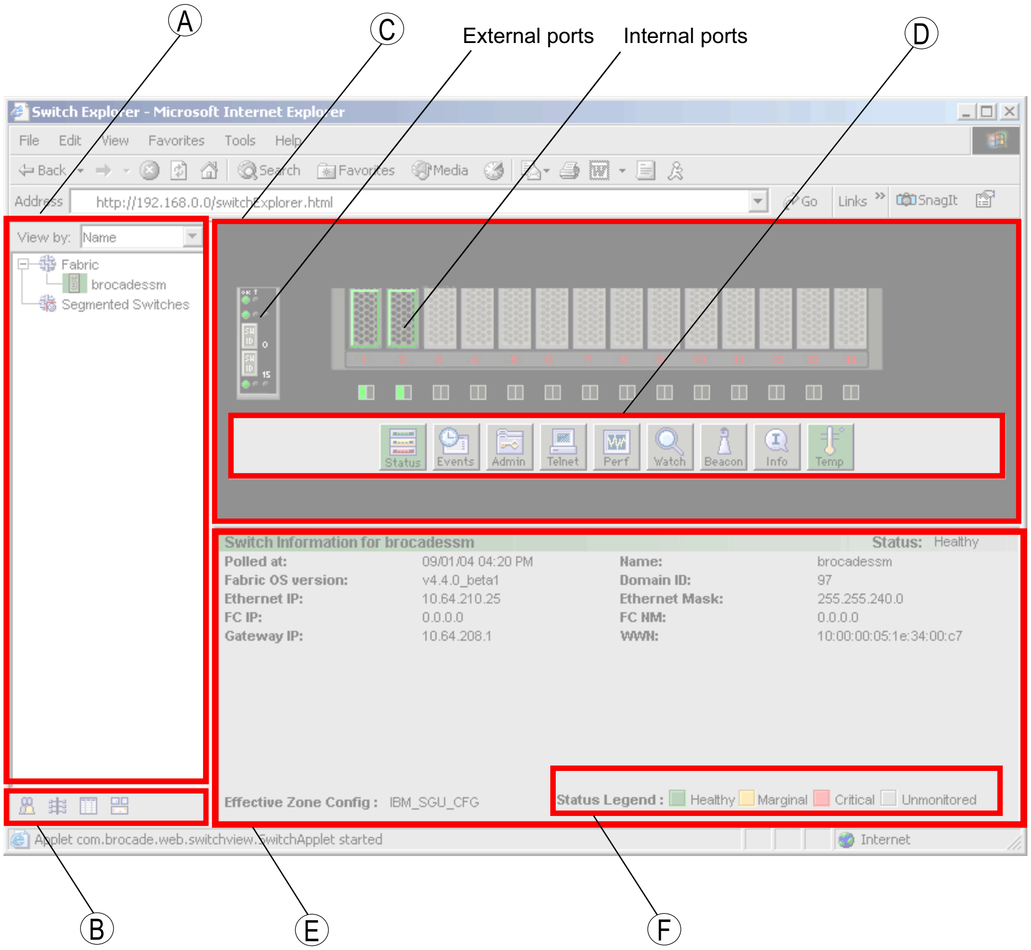
Polled at:	03/02/04 03:05 PM	Name:	dazzler8_wt181
Fabric OS version:	v4.2.0_rc1	Domain ID:	181
Ethernet IP:	10.33.13.181	Ethernet Mask:	255.255.240.0
FCnet IP:	0.0.0.0	FCnet Mask:	0.0.0.0
Gateway IP:	10.33.0.1	WWN:	10:00:00:05:1e:34:00:7b

Current Zone Config : cfg

Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical □ Unmonitored

Figure 1-5 shows an example of the Web Tools Switch Explorer for a SilkWorm 3016 switch.

Figure 1-5 Web Tools Switch Explorer for a SilkWorm 3016 Switch


A
C
External ports
Internal ports
D
Switch Explorer - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.0.0/switchExplorer.html
Go Links SnagIt
View by: Name
Fabric
brocadessm
Segmented Switches
Status Events Admin Telnet Perf Watch Beacon Info Temp
Applet com.brocade.web.switchview.SwitchApplet started
Internet
B
E
F

Switch Information for brocadessm Status: Healthy

Polled at:	09/01/04 04:20 PM	Name:	brocadessm
Fabric OS version:	v4.4.0_beta1	Domain ID:	97
Ethernet IP:	10.64.210.25	Ethernet Mask:	255.255.240.0
FC IP:	0.0.0.0	FC NM:	0.0.0.0
Gateway IP:	10.64.208.1	WWN:	10:00:00:05:1e:34:00:c7

Effective Zone Config : IBM_SGU_CFG

Status Legend : 🟩 Healthy 🟨 Marginal 🟥 Critical □ Unmonitored

Different panels of Web Tools refresh at different rates. Table 1-2 lists the polling rates for the various panels in Web Tools.

Table 1-2 Polling Rate in the Switch Explorer Window

Switch Explorer Area	Polling Rate
Name Server	User-defined; 15 seconds minimum
Zoning Database	60 seconds
Fabric Watch	15 seconds
Performance Monitor	30 seconds

Fabric Tree

The Fabric Tree is the left panel of the Switch Explorer. The Fabric Tree displays all switches in the fabric, including switches that do not have a Web Tools license. Any switches segmented before Web Tools is launched are not displayed.

Although all switches in the fabric are *displayed*, only switches that have a Web Tools license installed can be *managed* through Web Tools. Other switches must be managed through the Fabric OS command line interface (CLI) or another management application. For information on adding a Web Tools license to a switch, see "Installing a Web Tools License" on page 2-3.

Use the drop-down menu at the top of the panel to view switches in the Fabric Tree by switch name, IP address, or WWN. The background color of the switch icon indicates the current status of the switch.

The Fabric Tree is updated at time intervals depending on the number of switches in the fabric. On average, for a fabric with up to 12 switches, the Fabric Tree is updated every 30 seconds. For every additional 12 switches in the fabric, it takes an additional 30 seconds to update the Fabric Tree. The Switch Information View displays a field, "Polled At", that identifies the last time the information was updated.

You can also manually refresh the status of a switch within the fabric by right-clicking that switch in the Fabric Tree and clicking **Refresh**.

Fabric Toolbar

The Fabric Toolbar at the bottom of the Fabric Tree enables you to access fabric-wide administration tasks quickly. The Fabric Toolbar icons provide access to:

- Fabric events

  This information is collected from the launch switch. Refer to "Monitoring Events" on page 4-1 for more information.

- Topology module

  This information is collected from the selected switch. Refer to "Displaying a Fabric Topology Report" on page 4-7 for more information.

- Name Server information

  This information is collected from the selected switch. Refer to "Displaying the Name Server Entries" on page 4-8 for more information.

- Zone Administration module

  This information is collected from the selected switch. This icon is displayed only if a Brocade Advanced Zoning license is installed on the switch. If secure mode is enabled, zoning can be administered only from the primary FCS switch. If the selected switch has a zoning license installed but is not the primary switch, the Zone Admin icon is displayed but not activated. Refer to "Managing Zoning with Advanced Web Tools" on page 5-2 for more information.

It is important to note that the information displayed is gathered from different areas; switches in the fabric might be running different versions of Fabric OS, and different versions of Fabric OS support different features, so the information displayed might not always be the same for switches running different versions of Fabric OS.

Switch View

The Switch View displays a graphical representation of the selected switch, including a real-time view of switch and port status. This view is accessed by selecting a switch icon in the Fabric Tree.

Note

The Switch View display is updated approximately once every 15 seconds. However, the initial display of the Switch Explorer might take from 30 to 60 seconds after the switch is booted.

The layout of information is different for the Switch View of different switch types. See Figure 1-2 through Figure 1-4 for examples of different Switch Views.

Switch View Button Menu

The Switch View button menu is the launch point for the Switch Events screen, telnet interface, Fabric Watch module, Switch Admin module, Performance Monitor module, and High Availability (HA) Admin module. Some of these functions require a license key to activate. The Switch View button menu also includes buttons that display the status of the switch fans, temperature monitors, switch information, power supply, and beacon.

It is important to note that certain Fabric OS features are available only on particular switch types; therefore, the icons for those features are displayed only for those switch types. For example, the High Availability feature is available only on the SilkWorm 12000 and SilkWorm 24000 directors; therefore, the HA Admin button displays in the Switch View button menu only for SilkWorm 12000 and 24000 directors.

The following buttons have a color-coded background, which indicates status for that area:

- Status
- Fan
- Temp
- Power
- Hi Avail (HA)

The colors follow the status legend (see “Status Legend” on page 1-10).

Switch Information View

The Switch Information View displays vital switch information such as name, status, Fabric OS version, domain ID, IP address, WWN, and current zone configuration.

The Switch Information View is located beside the graphic representation of the switch for the SilkWorm 12000 and 24000 directors. For all other switch types (SilkWorm 3016, 3250, 3850, 3900, and 4100), the Switch Information View is located beneath the graphic representation of the switch.

Note

The information in the Switch Information View is polled every 15 seconds.

For more information, refer to “Displaying Detailed Switch Information” on page 4-13.

Status Legend

The Status Legend is included in the Switch Information View and defines the meaning of colors visible in the background of the various icons in the Switch Explorer.

Each color indicates a different operational state:

- Green: healthy
- Yellow: marginal
- Red: critical
- Gray: unknown or unmonitored

Note
For all status displays based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

Displaying Switches in the Fabric

If your fabric has more than one switch, you can launch Web Tools from one switch and then access other switches.

To access the Switch Explorer for a particular switch

1. Launch Web Tools (refer to "Launching Web Tools" on page 1-1 for instructions).

   The Switch Explorer is displayed for the switch you logged in to. The Fabric Tree is expanded by default when you first launch Web Tools.

2. If the Fabric Tree is not expanded, click the "+" in the Fabric Tree to view all the switches in the fabric.

3. Click a switch in the Fabric Tree.

   The graphic of the selected switch is displayed in the Switch View. Additional switch information is displayed in the Switch Information View.

Web Tools and Secure Mode

When secure mode is enabled on switches you manage through Web Tools, there are certain requirements and scenarios of which you should be aware. You should read through the requirements and scenarios in this section if you plan to use Web Tools to manage any switches that have secure mode enabled.

Web Tools Access and HTTP_POLICY

When secure mode is enabled, access to the Web Tools interface is controlled by HTTP_POLICY. If secure mode is enabled and HTTP_POLICY has been defined, your workstation IP address must be included in this policy or you will not have access to Web Tools for any switch in the fabric. If your workstation IP is not included in this policy, the Interface Disabled page is displayed when you attempt to access a switch. For instructions on including your workstation in HTTP_POLICY, refer to the *Brocade Secure Fabric OS User's Guide*.

Note

If a secure mode change is made in the fabric—that is, secure mode is enabled, secure mode is disabled, or there is a change to the primary FCS—you must exit and relaunch Web Tools. If Web Tools is kept open after a secure mode change occurs, behavior is undefined.

Opening Modules in a Secure Fabric

When opening modules in a secure fabric, log in to one module at a time, and complete the entire login process before proceeding to any other task. For example, if you want to access both the Zone Admin and the Switch Admin modules, open one of the modules, log in, and wait for it to load completely before opening the second module. Abnormal behavior might occur if you attempt to open two modules simultaneously in a fabric with secure mode enabled.

Certain Web Tools features are limited or disabled when secure mode is enabled on a fabric. For more information about secure mode, refer to the *Brocade Secure Fabric OS User's Guide*.

Primary-FCS-Only Functionality

The following Web Tools functionality is reserved for the primary FCS when secure mode is enabled:

- Zoning administration is allowed only from the primary FCS switch when secure mode is enabled. For all other switches in a secure fabric, the Zoning button is disabled.
- SNMP community strings can be modified only from the primary FCS switch when secure mode is enabled. For non-FCS switches, you can view the SNMP community strings, but they are read-only, and the SNMP access control lists on the SNMP tab are not displayed.
- User account administration is allowed only from the primary FCS switch when secure mode is enabled. The changes are then propagated to all switches in the fabric.

Disabled Functionality

Telnet access to a switch and the Telnet button in Web Tools are both disabled when secure mode is enabled for a fabric. You must use sectelnet or SSH to access the Fabric OS CLI in a secure fabric. These capabilities are not accessible from Web Tools. For more information on sectelnet or SSH, refer to the *Brocade Secure Fabric OS User's Guide*.

The SNMP Access Control List is replaced with RSNMP_POLICY and WSNMP_POLICY when secure mode is enabled for a fabric. The SNMP Access Control List is not displayed in Web Tools.

Recommendations When Working with Web Tools

Listed below are recommendations when working with Web Tools:

- When using a mixed fabric—that is a fabric containing switches and directors running v4.x, v3.x, and v2.x firmware—use the most advanced switches or directors to control the fabric. For example, use the v4.x switches or directors as the primary FCS, the location to perform zoning tasks, and the time server (CLI). You should use the most recently released firmware on your switches.
- If switches are accessed simultaneously from different connections (for example, Web Tools, CLI, and API), changes from one connection might not be updated to the other, and some modifications might be lost. Make sure when connecting with simultaneous multiple connections that you do not overwrite the work of another connection.
- Several tasks in Web Tools make fabric-level changes: for example, the tasks in the Zone Admin module. When executing fabric-level configuration tasks, wait until you have received confirmation that the changes are implemented before executing any subsequent tasks. For a large fabric, this can be up to a few minutes.
- Many of the Switch View windows are automatically closed when you select a different switch in the Fabric Tree. This is normal behavior and is designed to prevent configuration changes being performed on the wrong switch.
- A maximum of five simultaneous HTTP sessions to any one switch is recommended. An HTTP session is considered a Fabric Manager or Web Tools connection to the switch.

Chapter

2

Requirements, Installation, and Support

Before you install Web Tools on your workstation, verify that your switches and workstation meet the Web Tools requirements listed in this chapter.

This chapter contains the following sections:

- "Requirements," next
- "Installing a Web Tools License" on page 2-3
- "Value Line Licenses" on page 2-5
- "Switch Support" on page 2-5

Requirements

Web Tools requires any browser that conforms to HTML version 4.0, JavaScript version 1.0, and Java Plug-in 1.4.2_03 or higher.

Brocade has certified and tested Web Tools on the platforms shown in Table 2-1.

Table 2-1 Certified and Tested Platforms

Operating System	Browser	Java Plug-In
Solaris 2.8	Mozilla 1.6	1.4.2_03
Solaris 2.9	Mozilla 1.6	1.4.2_03
Windows 2000	Internet Explorer 6.0	1.4.2_03
Windows 2003	Internet Explorer 6.0	1.4.2_03
Windows XP	Internet Explorer 6.0	1.4.2_03

In addition, Brocade has tested Web Tools on the platforms shown in Table 2-2.

Table 2-2 Tested Platforms

Operating System	Browser	Java Plug-In
RedHat Linux 9.0	Mozilla 1.6	1.4.2_03

Note
Some browsers must be configured to work with Web Tools. For information about how to do this, refer to "Configuring Internet Explorer" on page 2-2.

Adequate RAM is required on Windows systems:

- 256 MB or more RAM for fabrics comprising 15 switches or less
- 512 MB or more RAM for fabrics comprising more than 15 switches

A minimum of 8 MB of video RAM is also recommended.

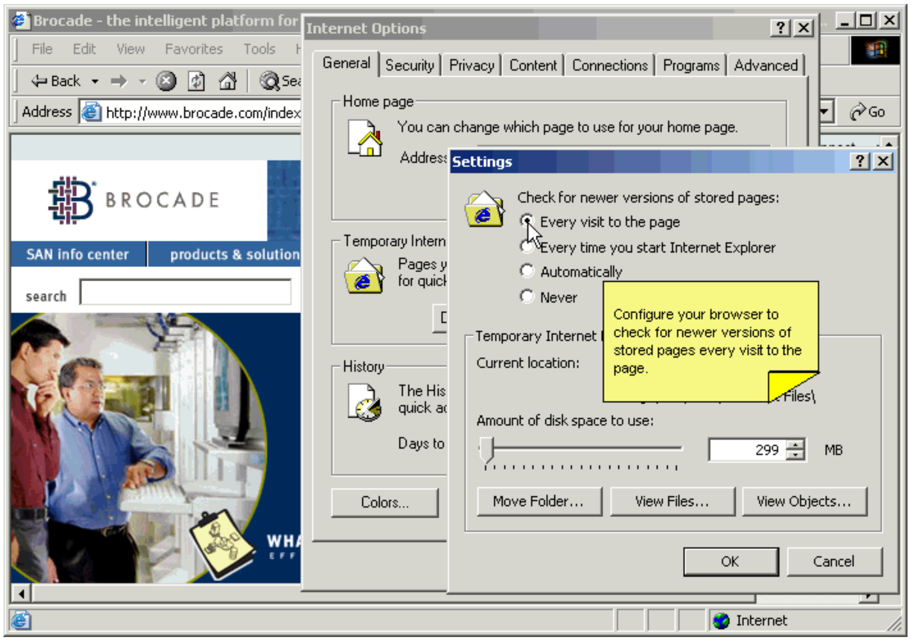
Configuring Internet Explorer

Correct operation of Web Tools with Internet Explorer requires specifying the appropriate settings for browser refresh frequency and process model. Browser pages should be refreshed frequently to ensure the correct operation of Web Tools.

To set the refresh frequency

1. Click **Tools** > **Internet Options** in the browser.
2. Click the **General** tab and click **Settings** (under "Temporary Internet Files").
3. Click **Every visit to the page** under "Check for newer versions of stored pages," as shown in Figure 2-1.

Figure 2-1 Configuring Internet Explorer


Brocade - the intelligent platform for
File Edit View Favorites Tools
Back Search
Address http://www.brocade.com/index
Go
BROCADE
SAN info center
products & solution
search
Internet Options
General Security Privacy Content Connections Programs Advanced
Home page
Temporary Intern
History
Colors...
Internet

Home page: You can change which page to use for your home page.

Settings

Check for newer versions of stored pages:
● Every visit to the page
○ Every time you start Internet Explorer
○ Automatically
○ Never

Temporary Internet Files folder
Current location:
Amount of disk space to use: 299 MB

Configure your browser to check for newer versions of stored pages every visit to the page.

Installing Java on the Workstation

A Java Plug-in must be installed on the workstation for the correct operation of Web Tools. The required version depends on the operating system. Refer "Requirements" on page 2-1 for a list of tested browsers on supported operating systems, and the Java runtime environment (JRE) they require.

To install the JRE on your Solaris or Linux client workstation

1. Locate the JRE on the Internet, at the following URL:

   http://java.sun.com/

   Note
   This URL is subject to change without notice.

2. Follow the instructions to install the JRE.
3. Create a symbolic link from this location...:

   $MOZILLA/plugins/libjavaplugin_oji.so

   ...to this location:

   $JRE/plugin/$ARCH/ns600/libjavaplugin_oji.so

To install patches on Solaris

1. Search for any required patches for your current version of the JRE at the following Web site:

   http://java.sun.com/j2se/1.4.2/install_solaris.html

   Note
   This URL is subject to change without notice.

2. Follow the link to download the patch, and exit the browser when done.
3. Install the patch and reboot the system.

To install the Java Plug-in on Windows

1. Click **Start Menu** > **Settings** > **Control Panel** and select the Java Plug-in Control Panel.
2. Click the **About** tab.
3. Determine whether the correct Java Plug-in version is installed:
   - If the correct version is installed, Web Tools is ready to use.
   - If no Java Plug-in is installed, point the browser toward a switch running Fabric OS v4.x, follow the link to the Sun Microsystems Web site, download the correct Java Plug-in, and double-click the downloaded file to install the plug-in.
   - If an outdated version is currently installed, uninstall it, relaunch the browser, and enter the address of a switch running Fabric OS v4.4.0 or later. Web Tools will guide you through the steps to download the proper Java Plug-in.

Installing a Web Tools License

You can install a Web Tools license either through telnet or over the Web.

All licenses, including Web Tools licenses, are installed on a chassis basis. For example, if you install a Web Tools license on logical switch 0 in a SilkWorm 12000 director, you do not need to install an additional Web Tools license on logical switch 1 of that SilkWorm 12000 director.

To determine whether a license is already installed on a switch, follow the instructions provided under "Installing a Web Tools License Through Telnet," next. If a license is not installed, contact your switch supplier to obtain a license key.

Installing a Web Tools License Through Telnet

Use the following procedure to determine whether a Web Tools license is installed on your switch and, if not, install it.

To install a Web Tools license through telnet

1. Log in to the switch via telnet (refer to the *Brocade Fabric OS Procedures Guide* for more information), using an account that has administrative privileges.
2. To determine whether a Web Tools license is already installed on the switch, type **licenseShow** on the telnet command line.

   A list displays, showing all the licenses currently installed on the switch:

   ```
   switch:admin> licenseshow
   1A1AaAaaaAAAA1a: ]-- This is the license key. The installed feature is listed below.
       Zoning license
   1A2AaAbbbBBBA1a:
       SES license
   1A3AaAbcbBBCC1d:
       QuickLoop license
   ```

   If the Web Tools license is not included in the list or is incorrect, continue with step 3.
3. On the command line, type the following...:

   ```
   licenseadd key
   ```

   ...where `key` is the license key. The license key value is case-sensitive and must be entered exactly as given.
4. Verify that the license was added by typing the following command:

   ```
   licenseshow
   ```

   If the Web Tools license is listed, the feature is available. If the license is not listed, repeat step 3.

Installing a Web Tools License Through the Web

Launching Web Tools from any nonlicensed switch automatically displays the license dialog box. If the fabric already contains at least one licensed switch, you can use Web Tools to view and license other switches from the licensed switch.

To install the first license through the Web

1. Launch the Web browser and type the IP address of the switch in the **Location/Address** field:

   ```
   http://123.123.123.123
   ```

2. Press **Enter**.

If a Web Tools license is already installed on the switch, Web Tools launches. If no license is installed, a license dialog displays.

3. If the license dialog displays, follow the instructions provided.

To install additional licenses through the Web

1. Launch the Web browser and type the IP address of the licensed switch in the **Location/Address** field:

   ```
   http://123.123.123.123
   ```

2. Press **Enter**.

   Web Tools opens, displaying the Switch Explorer.

3. Click the icon for the switch to which you want to add a license.

   A licensing window displays.

4. Follow the instructions provided.

Value Line Licenses

If your fabric includes a switch with a limited switch license and you are launching Web Tools using that switch, if the fabric exceeds the switch limit indicated in the license, Web Tools allows a 45-day "grace period" in which you can still monitor the switch through Web Tools. However, Web Tools will display warning messages periodically.

These messages warn you that your fabric size exceeds the supported switch configuration limit and tells you how long you have before Web Tools will be disabled. After the 45-day grace period, you will no longer be able to launch Web Tools from the switch with the limited switch license if that switch is still exceeding the switch limit.

Switch Support

You can use Web Tools v4.4.0 with the following hardware:

- SilkWorm 3016 switch
- SilkWorm 3250 switch
- SilkWorm 3850 switch
- SilkWorm 3900 switch
- SilkWorm 4100 switch
- SilkWorm 12000 director
- SilkWorm 24000 director

Web Tools is part of the Fabric OS of a switch. When you launch Web Tools on a switch, you can manage other switches in the fabric that have lower or higher firmware versions. It is important to note that when accessing these switches you are opening the remote switch's version of Web Tools, and the functionality available for those switches might vary.

Chapter

3

Managing Your Fabrics, Switches, and Ports

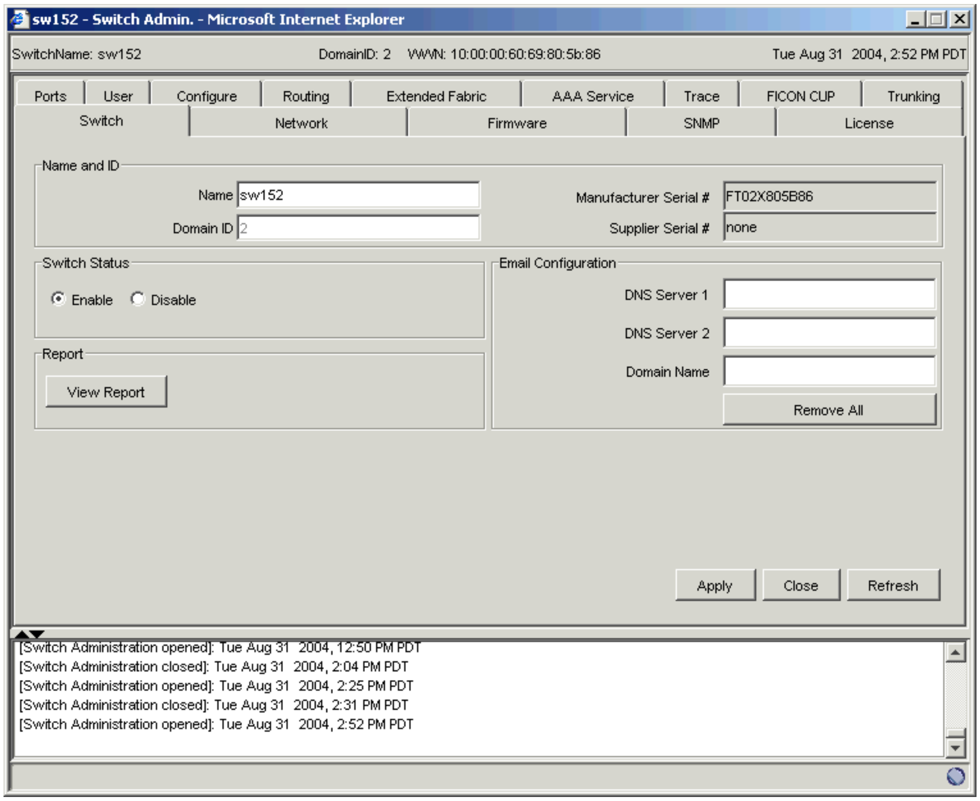
This chapter contains the following sections:

Managing Fabrics, Switches, and Ports Using Web Tools

You can perform most of management tasks described in this chapter through the Switch Admin module. Information in the Switch Admin module is retrieved from the selected switch.

Click the **Admin** button in the Switch View to access the Switch Admin module. Figure 3-1 on page 3-2 shows the Switch Admin module.

Figure 3-1 Switch Admin Module



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 2:52 PM PDT

Name: sw152

Domain ID: 2

Manufacturer Serial #: FT02X805B86

Supplier Serial #: none

● Enable ○ Disable

DNS Server 1:

DNS Server 2:

Domain Name:

```
[Switch Administration opened]: Tue Aug 31  2004, 12:50 PM PDT
[Switch Administration closed]: Tue Aug 31  2004, 2:04 PM PDT
[Switch Administration opened]: Tue Aug 31  2004, 2:25 PM PDT
[Switch Administration closed]: Tue Aug 31  2004, 2:31 PM PDT
[Switch Administration opened]: Tue Aug 31  2004, 2:52 PM PDT
```

When you click the **Admin** button from the Switch View, you must log in as an admin to launch the Switch Admin module. Information displayed in the Switch Admin module is *not* updated automatically by Web Tools. To update the information displayed in the Switch Admin module, refer to "Refreshing the Switch Admin Module" on page 3-3.

Caution
Any changes you make in the Switch Admin module are in a buffered environment and are *not* applied to the switch until you save the changes. (The exception to this is the License tab, where changes are applied immediately and there is no **Apply** button.) If you close the Switch Admin module without saving your changes, your changes are lost. To save the buffered changes you make in the Switch Admin module to the switch, click **Apply** before closing the module or before switching to another tab.

Some of the management tasks for the SilkWorm 12000 and 24000 directors are performed through the Hi Avail module. This module and the associated tasks are described in "Administering High Availability" on page 3-36.

You can also use telnet commands to perform management tasks. Refer to "Launching the Telnet Window" on page 3-3 for information on how to launch a telnet window through Web Tools.

The remainder of this section describes basic Switch Admin module procedures that are useful for many switch-management operations.

Launching the Switch Admin Module

Most of the management procedures in this chapter are performed from the Switch Admin module.

To access the Switch Admin module

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Admin** button from the Switch View.

   The login dialog box displays.

3. Type the user name of an account with the admin role.

4. Type the password.

The Switch Admin module displays (as shown in Figure 3-1 on page 3-2).

Refreshing the Switch Admin Module

You can refresh the fabric element information displayed at any time using the following procedure. Note that when you click a different tab in the Switch Admin module, the information in the newly selected tab is automatically refreshed.

To refresh the fabric information

1. Click the **Refresh** button in any tabbed page of the Switch Admin module.

Launching the Telnet Window

When you launch a telnet window for the SilkWorm 12000 or 24000 directors it is on a logical-switch basis. This means that for each logical switch, you must launch a separate telnet window. Refer to the *Brocade Fabric OS Command Reference Manual* for information about the telnet commands.

Note

Web Tools does not support telnet on the Mozilla browser. You must use an external command line interface if using Mozilla.

Telnet access to a switch and the **Telnet** button in Web Tools are both disabled when secure mode is enabled for a fabric. You must use **sectelnet** or **SSH** to access the Fabric OS CLI in a secure fabric. These capabilities are not accessible from Web Tools. For more information on sectelnet or SSH, refer to the *Brocade Secure Fabric OS User's Guide*.

To access telnet through Web Tools

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Telnet** button from the Switch View.

   The Telnet window displays.

3. To close the session when you are done, type the **exit** command at the telnet prompt.

Configuring IP and Netmask Information

When you configure IP and netmask information for the SilkWorm 12000 or 24000 director, it is on a logical-switch basis. This means that for each logical switch, you must also configure IP and subnet mask information individually.

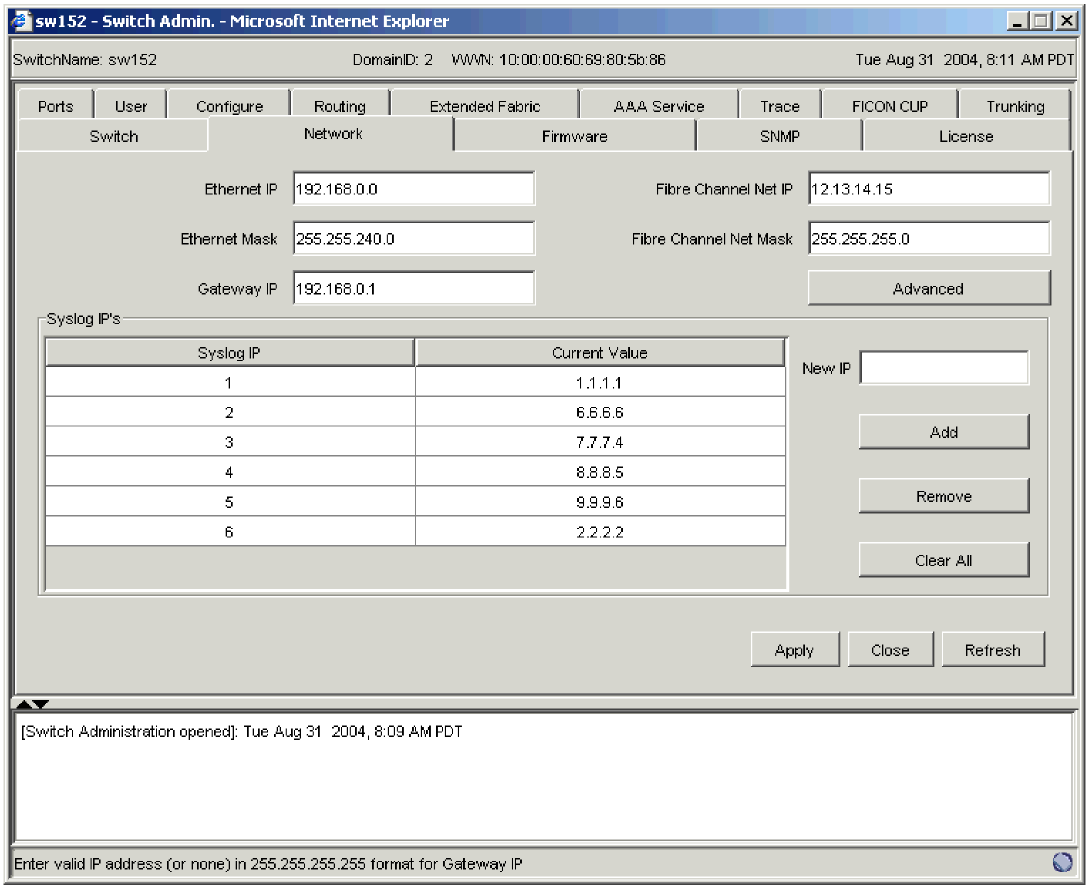
To configure IP and netmask information

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Network** tab (see Figure 3-2 on page 3-5).
3. Type a new value in the appropriate field (for example, 123.123.123.123).
4. For the SilkWorm 12000 and 24000 directors only:
   a. Click **Advanced**.
   b. Type valid IP addresses for the Ethernet IP and subnet mask for CP0 and CP1.
   c. Click **OK** to return to the Network tab.
5. Click **Apply**.
6. Exit and relaunch Web Tools to continue working.

Note

When changing the Ethernet IP/netmask, the Gateway IP, or the Fibre Channel net IP/net mask from Web Tools, there is a normal loss of network connection to the switch. If the IP properties have changed, you must close all current windows and restart Web Tools with the new IP address.

Figure 3-2 Network Tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 8:11 AM PDT

Ethernet IP: 192.168.0.0
Ethernet Mask: 255.255.240.0
Gateway IP: 192.168.0.1
Fibre Channel Net IP: 12.13.14.15
Fibre Channel Net Mask: 255.255.255.0
New IP:

Syslog IP	Current Value
1	1.1.1.1
2	6.6.6.6
3	7.7.7.4
4	8.8.8.5
5	9.9.9.6
6	2.2.2.2

```
[Switch Administration opened]: Tue Aug 31  2004, 8:09 AM PDT
```

Enter valid IP address (or none) in 255.255.255.255 format for Gateway IP

Configuring a syslog IPAddress

The syslog IP represents the IP address of the server that is running the syslog process. The syslog daemon reads and forwards system messages to the appropriate log files and/or users, depending on the system configuration. When one or more IP addresses are configured, the switch forwards all error log entries to the syslog on the specified servers. Up to six servers are supported. Refer to *Fabric OS Procedures Guide* for more information on configuring the syslog daemon.

When you configure a syslog IP address for the SilkWorm 12000 director or for a SilkWorm 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure a syslog IP address individually.

To configure the syslog IP address

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Network** tab (see Figure 3-2).
3. Enter a valid IP address in the **New IP** field (for example, 123.123.123.123).
4. Click **Add**.

   The configured IP is displayed in the Syslog IP window.
5. Click **Apply**.

To remove a syslog IP address

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Network** tab.
3. Select a syslog IP from the table.
4. Click **Remove**.
5. *Optional*: Click **Clear All** to remove all of the syslog IP addresses.
6. Click **Apply**.

Performing a Firmware Download

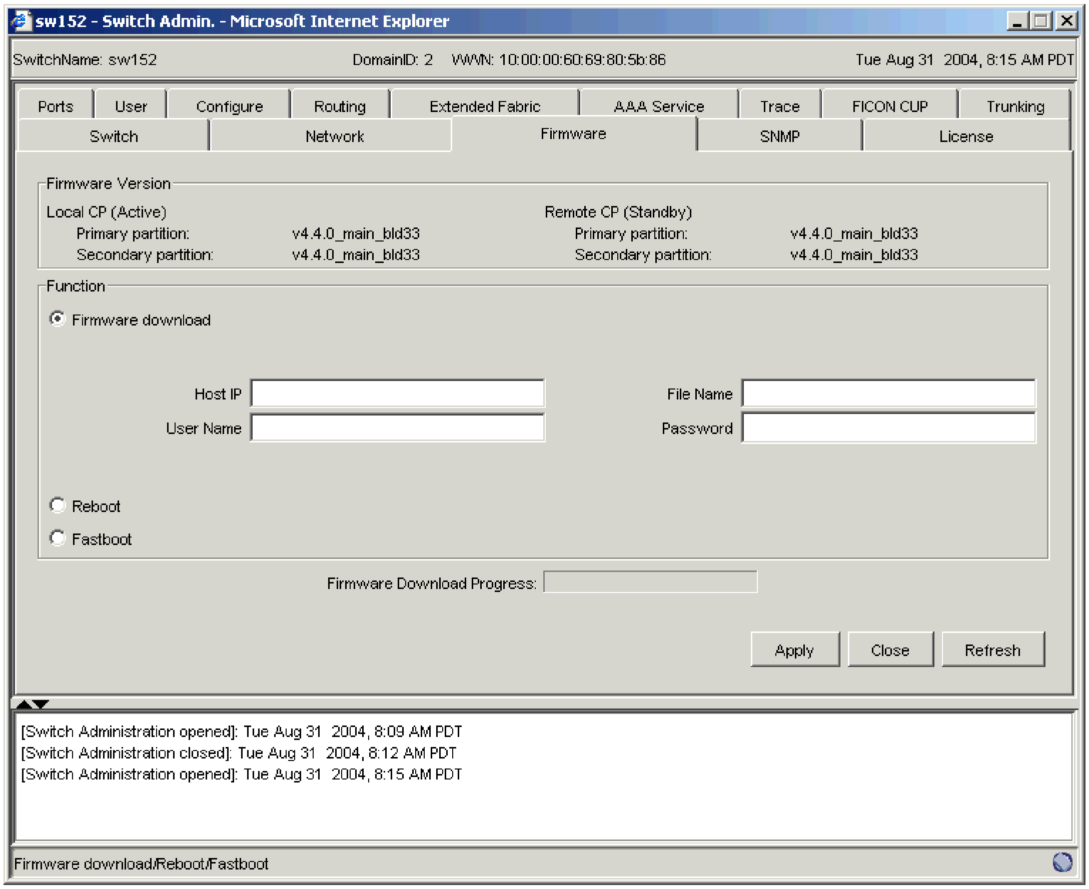
When you request a firmware download, the system first checks the file size that is to be downloaded. If the compact flash does not have enough space, Web Tools displays a message and the download does not occur.

To download a new version of the firmware

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Firmware** tab.
3. Click the **Firmware Download** radio button.
4. Type the host IP address, user name, password, and fully qualified path to the file name.
5. Click **Apply**.

The firmware download begins. You can monitor the firmware download status on the Firmware Download progress bar.

Figure 3-3 Firmware Tab



sw152 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 8:15 AM PDT

Firmware Version

Local CP (Active)
Primary partition: v4.4.0_main_bld33
Secondary partition: v4.4.0_main_bld33

Remote CP (Standby)
Primary partition: v4.4.0_main_bld33
Secondary partition: v4.4.0_main_bld33

Function

● Firmware download

○ Reboot

○ Fastboot

```
[Switch Administration opened]: Tue Aug 31  2004, 8:09 AM PDT
[Switch Administration closed]: Tue Aug 31  2004, 8:12 AM PDT
[Switch Administration opened]: Tue Aug 31  2004, 8:15 AM PDT
```

Firmware download/Reboot/Fastboot

Configuring a Switch

Use the **Switch** tab of the Switch Admin module to perform basic switch configuration. Figure 3-1 on page 3-2 shows an example of the **Switch** tab.

Enabling and Disabling a Switch

You can identify if a switch is enabled or disabled in the Switch Admin module by looking at the bottom right corner: the ○ icon means that the switch is enabled, and the ⊘ icon means that the switch is disabled.

Use the following procedure to enable or disable a switch.

To enable or disable a switch

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Switch** tab.
3. Click the **Enable** radio button in the **Switch Status** section to enable the switch, or click the **Disable** radio button to disable the switch.
4. Click **Apply**.

Changing the Switch Name

Switches can be identified by IP address, domain ID, World Wide Name (WWN), or by customized switch names that are unique and meaningful.

Switch names can be a maximum of 15 characters long for Fabric OS v4.4.0. They must begin with an alpha character, but otherwise can consist of any combination of alphanumeric and underscore characters.

To change the switch name

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Switch** tab.
3. Type a new name in the **Name** field.
4. Click **Apply**.

Note
Beginning with Fabric OS v4.4.0, it is recommended that you customize the chassis name for each switch. Some system messages identify a switch service by chassis name, so if you assign meaningful chassis names in addition to meaningful switch names, logs will be more useful. You change the chassis name using the CLI. Refer to the *Brocade Fabric OS Procedures Guide* for instructions on changing the chassis name.

Changing the Switch Domain ID

Although domain IDs are assigned dynamically when a switch is enabled, you can request a specific ID to resolve a domain ID conflict when you merge fabrics.

To change the switch domain ID

1. Launch the Switch Admin module as described on page 3-2.
2. Disable the switch, as described in "Enabling and Disabling a Switch" on page 3-7.
3. Click the **Switch** tab.
4. Type a new domain ID in the **Domain ID** field.

   The domain ID is an integer between 1 and 239.
5. Click **Apply**.
6. Enable the switch, as described in "Enabling and Disabling a Switch" on page 3-7.

Viewing and Printing a Switch Report

The switch report includes the following information:

- a list of switches in the fabric
- switch configuration parameters

- a list of ISLs and ports
- Name Server information
- zoning information
- SFP serial ID information

To view or print a switch report

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Switch** tab.
3. Click **View Report**.

   A switch report displays in a new window.
4. View or print the report using your browser.

Rebooting the Switch

When you reboot the switch, the reboot takes effect immediately.

Performing a Fast Boot

A fast boot reduces boot time significantly by bypassing power-on self test (POST).

To perform a switch fast boot

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Firmware** tab (see Figure 3-3).
3. Click the **Fastboot** radio button.
4. Click **Apply**.

Performing a Reboot

Use the following procedure to reboot the CP and execute the normal power-on booting sequence.

To perform a switch reboot

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Firmware** tab (see Figure 3-3 on page 3-7).
3. Click the **Reboot** radio button.
4. Click **Apply**.

Configuring Fabric Parameters

When you configure fabric parameters for the SilkWorm 12000 director or for a SilkWorm 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure fabric parameters individually.

Note

You must disable the switch before you can configure fabric parameters.

You can configure the following fabric parameters with the **Configure** tab and **Fabric** subtab of the Switch Admin module (as shown in Figure 3-4 on page 3-11):

- **BB Credit**

  Configure the number of buffers that are available to attached devices for frame receipt. The default BB Credit is 16. The range is 1 through 27.

- **R_A_TOV**

  Resource allocation timeout value (in milliseconds). This variable works with the E_D_TOV to determine switch actions when presented with an error condition. The default is 10000. The possible range is 4000 through 120000.

- **E_D_TOV**

  Error detect timeout value (in milliseconds). This timer is used to flag a potential error condition when an expected response is not received within the set time. The valid range is 1000 through 5000.

- **Datafield size**

  The largest possible data field size (in bytes). The valid range is 256 through 2112.

- **Switch PID Format**

  Select a switch PID format from one of the following:

  - Format 1 (0-base, 256 encoding)
  - Format 2 (16-base, 256 encoding)

- **Sequence Level Switching**

  Check this box to enable frames of the same sequence from a particular group to be transmitted together. When this option is not selected, frames are transmitted interleaved among multiple sequences. Under normal circumstances, sequence-level switching should be disabled for better performance. However, some host adapters have issues when receiving interleaved frames among multiple sequences.

- **Disable Device Probing**

  Set this mode only if the switch N_Port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail. When set, devices that do not register with the Name Server are not present in the Name Server data base. Set this mode only if the switch N_Port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail.

- **Per-Frame Routing Priority**

  Choose to select or deselect per-frame routing priority. When enabled, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.

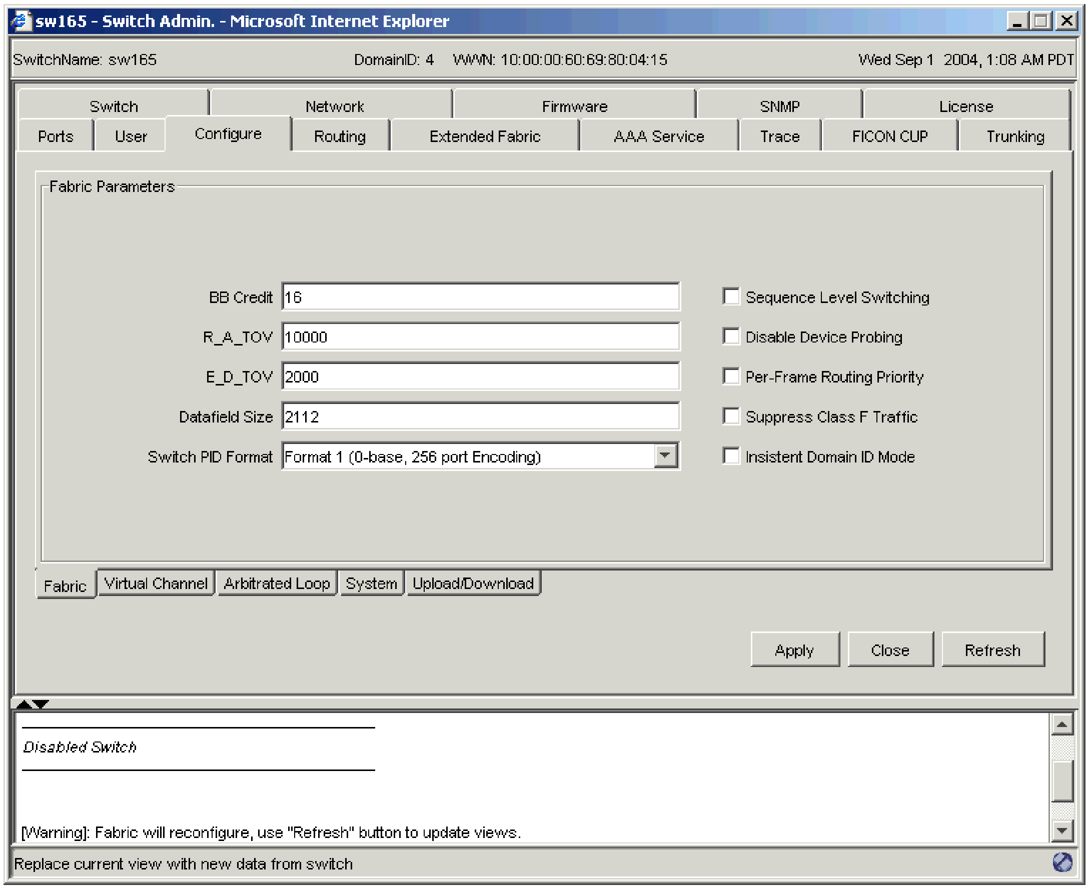
- **Suppress Class F Traffic**

  Applies only if VC-encoded address mode is also set. When checked, translative addressing (which allows private devices to communicate with public devices) is disabled.

- **Insistent Domain ID Mode**

  Set this mode to make the current domain ID insistent across reboots, power cycles, and failovers. This mode is required fabric wide to transmit FICON® data.

Figure 3-4 Configure Tab, Fabric Subtab



sw165 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw165 DomainID: 4 WWN: 10:00:00:60:69:80:04:15 Wed Sep 1 2004, 1:08 AM PDT

Fabric Parameters

BB Credit 16

R_A_TOV 10000

E_D_TOV 2000

Datafield Size 2112

Switch PID Format Format 1 (0-base, 256 port Encoding)

□ Sequence Level Switching

□ Disable Device Probing

□ Per-Frame Routing Priority

□ Suppress Class F Traffic

□ Insistent Domain ID Mode

Disabled Switch

[Warning]: Fabric will reconfigure, use "Refresh" button to update views.

Replace current view with new data from switch

To configure fabric parameters

1. Launch the Switch Admin module as described on page 3-2.
2. Disable the switch (refer to “Enabling and Disabling a Switch” on page 3-7).
3. Click the **Configure** tab.
4. Click the **Fabric** subtab.
5. Make the fabric parameter configuration changes.
6. Click **Apply**.
7. Enable the switch (refer to “Enabling and Disabling a Switch” on page 3-7).

Enabling Insistent Domain ID Mode

When insistent domain ID mode is enabled, the current domain setting for the switch is insistent; that is, the same ID is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfigurations. If the fabric does not assign the insistent domain ID, the switch segments from the fabric.

When you enable insistent domain ID mode for the SilkWorm 12000 director, it is on a logical-switch basis. This means that for each logical switch, you must enable insistent domain ID mode individually.

To enable insistent domain ID mode

1. Launch the Switch Admin module as described on page 3-2.
2. Disable the switch (refer to “Enabling and Disabling a Switch” on page 3-7).
3. Click the **Configure** tab.
4. Click the **Fabric** subtab.
5. Check the **Insistent Domain ID Mode** checkbox.
6. Click **Apply**.
7. Enable the switch (refer to “Enabling and Disabling a Switch” on page 3-7).

Configuring FAN Frame Notification Parameters

You can specify whether fabric access notification (FAN) frames are sent to public loop devices to notify them of their node ID and address.

When you configure FAN frame notification parameters for the SilkWorm 12000 director or for a SilkWorm 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure FAN frame notification parameters individually.

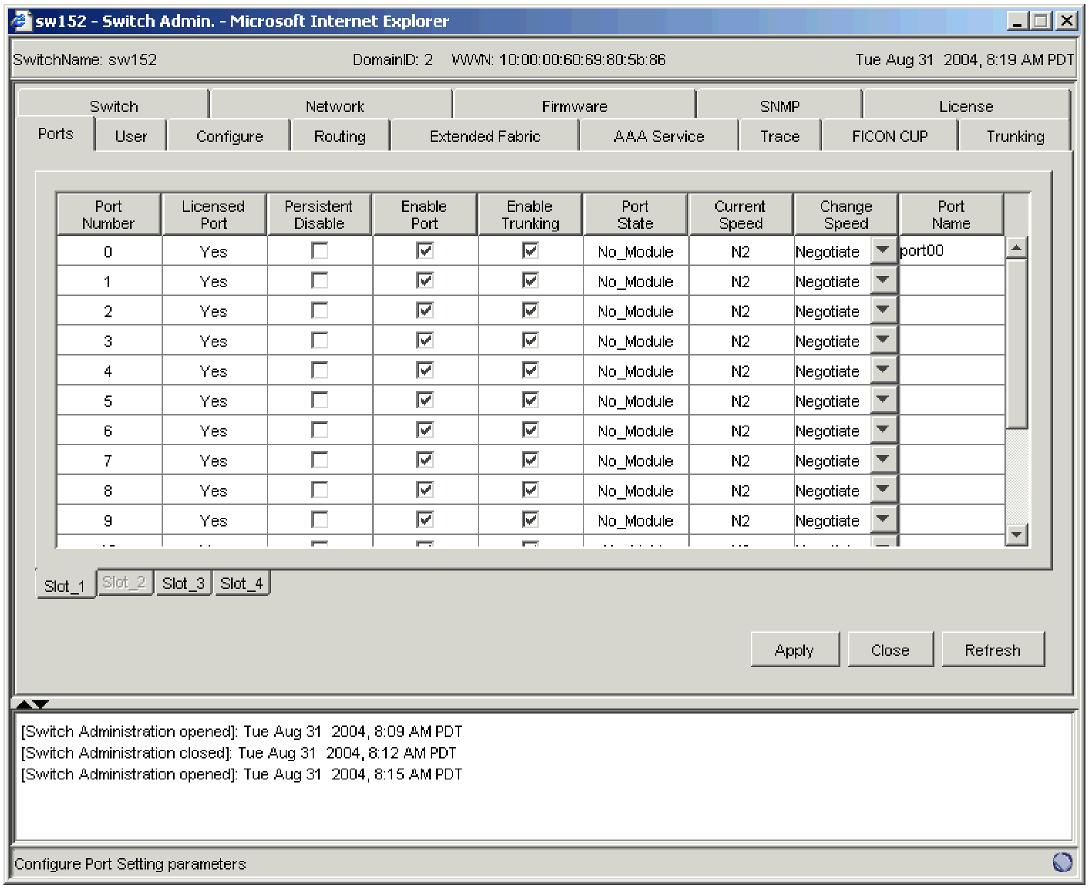
To configure FAN frame notification parameters

1. Launch the Switch Admin module as described on page 3-2.
2. Disable the switch (refer to “Enabling and Disabling a Switch” on page 3-7).
3. Select the **Configure** tab.
4. Select the **Arbitrated Loop** subtab.
5. Check the **Send FAN Frames** box.
6. Click **Apply**.
7. Enable the switch (refer to “Enabling and Disabling a Switch” on page 3-7).

Configuring Ports

Use the **Ports** tab of the Switch Admin module to perform the basic port configuration procedures described in this section. Figure 3-5 on page 3-13 shows an example of the **Ports** tab.

Figure 3-5 Ports tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 8:19 AM PDT

Port Number	Licensed Port	Persistent Disable	Enable Port	Enable Trunking	Port State	Current Speed	Change Speed	Port Name
0	Yes	□	☑	☑	No_Module	N2	Negotiate	port00
1	Yes	□	☑	☑	No_Module	N2	Negotiate	
2	Yes	□	☑	☑	No_Module	N2	Negotiate	
3	Yes	□	☑	☑	No_Module	N2	Negotiate	
4	Yes	□	☑	☑	No_Module	N2	Negotiate	
5	Yes	□	☑	☑	No_Module	N2	Negotiate	
6	Yes	□	☑	☑	No_Module	N2	Negotiate	
7	Yes	□	☑	☑	No_Module	N2	Negotiate	
8	Yes	□	☑	☑	No_Module	N2	Negotiate	
9	Yes	□	☑	☑	No_Module	N2	Negotiate	

```
[Switch Administration opened]: Tue Aug 31  2004, 8:09 AM PDT
[Switch Administration closed]: Tue Aug 31  2004, 8:12 AM PDT
[Switch Administration opened]: Tue Aug 31  2004, 8:15 AM PDT
```

Configure Port Setting parameters

Configuring Port Speed

The Current Speed column in the Ports tab indicates the current speed of the port. Use the following procedure to change the port speed.

To configure port speed

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Ports** tab.
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, select the subtab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed directly to the next step.
4. Select a port speed from the Change Speed drop-down list corresponding to the port for which you want to change the speed.
5. Click **Apply**.

Assigning a Name to a Port

Port names are optional. You can assign a name to a port to make port grouping easier. The Port Name column in the Ports tab displays the port name, if one exists.

The SilkWorm 3016 switch is preconfigured with port names; you can change them to suit your needs.

To name a port

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Ports** tab.
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, select the slot subtab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed directly to the next step.
4. Double-click in the **Port Name** field for the port you want to change.
5. Type a name for the port. Port names can be from 0 through 32 alphanumeric characters, unless FICON Management Server (FMS) mode is enabled; if FMS mode is enabled, port names should be limited from 0 through 24 alphanumeric characters. Although it is not required that port names be unique, it is recommended.
6. Click **Apply**.

Disabling a Port over Reboots

Use the following procedure to disable a port so that it remains disabled if the switch reboots.

To disable a port so that it remains disabled over reboots

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Ports** tab.
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, select the slot subtab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed directly to the next step.
4. Check the **Persistent Disable** checkbox for that port you want to keep disabled over reboots.
5. Click **Apply**.

Enabling and Disabling a Port

All licensed ports are enabled by default. You can disable and reenable them as necessary.

If a port is not licensed you cannot enable it until you install the Ports on Demand license. (Refer to "Activating Ports on Demand" for more information.) The **Licensed Port** column indicates whether a port is licensed.

Note

If you disable a *principal* ISL port (an ISL port that is used to communicate with the principal switch), the fabric reconfigures. If the port was connected to a device, that device is no longer accessible from the fabric. For more information, refer to the *Brocade Fabric OS Features Guide*.

To enable or disable a port

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Ports** tab.
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, select the slot subtab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed directly to the next step.
4. Check the box in the Enable Port column that corresponds to the port you want to enable. Uncheck the box in the Enable Port column that corresponds to the port you want to disable.
5. Click **Apply**.
6. Review the log at the bottom of the tab for information regarding the switch configuration changes.

Activating Ports on Demand

The SilkWorm 4100 model can be purchased with 16, 24, or 32 licensed ports. As your needs increase, you can activate unlicensed ports by purchasing and installing the Brocade Ports on Demand optional licensed product.

Ports on Demand is ready to be unlocked in the switch firmware. Its license might be part of the licensed Paper Pack supplied with switch software, or you can purchase the license separately from your switch vendor, who will provide you with a key to unlock it.

By default, ports 0–15 are enabled on the SilkWorm 4100 switch. To enable ports 16–23, install and enable the Ports On Demand license key. To enable ports 24–31, install and enable another Ports on Demand license. The first license key must be already installed before you can use the second license.

Once you have installed the license keys, you must enable the ports. You can do so without disrupting switch operation, as described in “Enabling and Disabling a Port” on page 3-14. Alternatively, you can disable and reenable the switch to activate all ports as described in “Enabling and Disabling a Switch” on page 3-7.

To unlock a Ports on Demand license, you can either use the supplied license key or generate a license key. If you need to generate a key, launch an Internet browser and go to the Brocade Web site at www.brocade.com. Click **products**> **Software**>**Software License Keys** and follow the instructions to generate the key.

To enable Ports on Demand

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Ports** tab.

   In the **Ports** tab, the Licensed Port column indicates whether the port is licensed or not.

3. Install the Brocade Ports on Demand licensed product.

   For instructions, refer to "Maintaining Licensed Features" on page 3-24.

4. Enable the ports, as described in "Enabling and Disabling a Port" on page 3-14.

If you remove a Ports on Demand License, the licensed ports will become disabled after the next platform reboot or the next port deactivation.

Configuring a Port for Long Distance

The **Extended Fabric** tab of the Switch Admin module displays information about the port speed, long distance setting, and buffer credits, as shown in Figure 3-6 on page 3-17. Use this tab to configure the long-distance setting of a port. For detailed information on managing extended fabrics, refer to the *Brocade Fabric OS Procedures Guide*.

When you configure a long-distance ISL, ensure that the ports on both sides of the ISL have the same configuration to avoid fabric segmentation.

The port speed is displayed as follows:

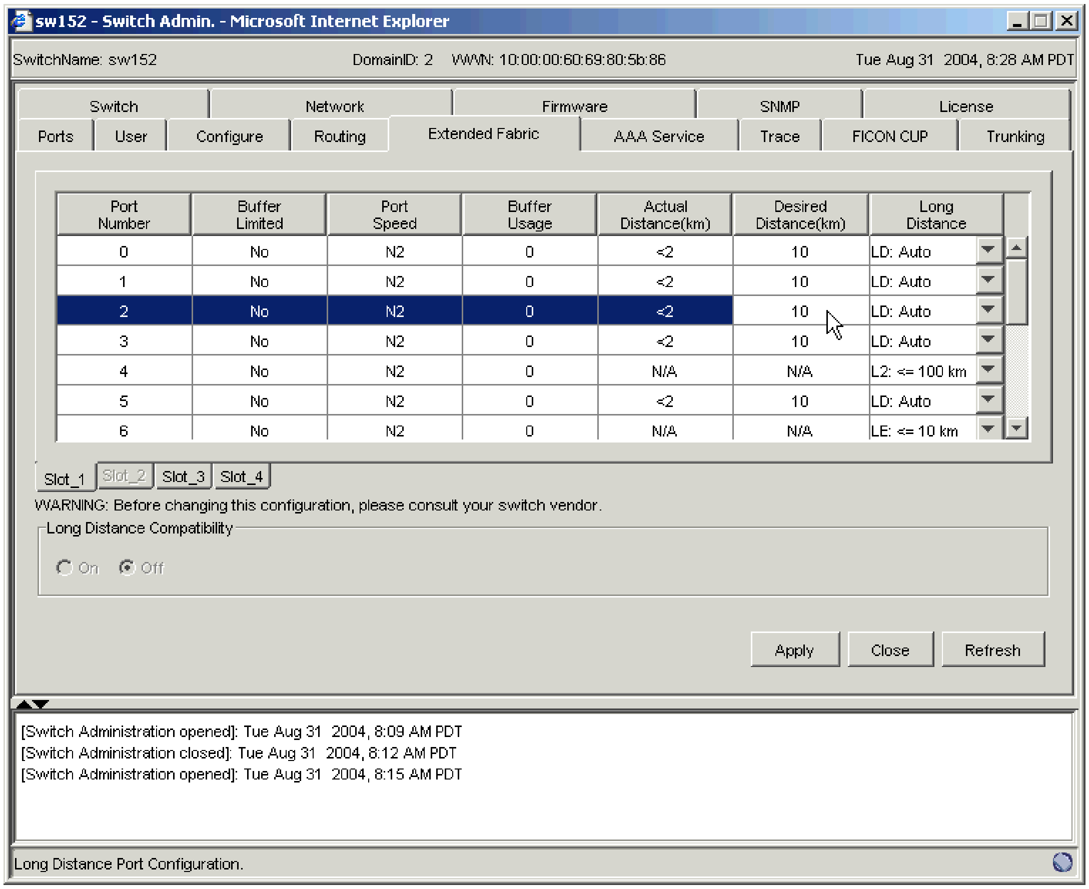
1G	1 Gbit/second
2G	2 Gbit/second
4G	4 Gbit/second
N1	Negotiated 1 Gbit/second
N2	Negotiated 2 Gbit/second
N4	Negotiated 4 Gbit/second
Auto-Negotiation	

Table 3-1 describes the long-distance settings and identifies which settings require a Brocade Extended Fabrics license.

Table 3-1 Long-Distance Settings and License Requirements

Value	Description	Requires Extended Fabrics License?
L0	No long-distance setting is enabled. The maximum supported link distance is 10 km, 5 km, or 2.5 km for ports at speeds of 1 Gbit/sec, 2 Gbit/sec, and 4 Gbit/sec, respectively.	No
LE	Extended normal setting is enabled, 10 km (6 miles) or less.	No
L0.5	25 km (15.5 miles) or less.	Yes
L1	Medium long-distance setting is enabled, 50 km (31 miles) or less.	Yes
L2	Long-distance setting is enabled, 100 km (62 miles) or less.	Yes
LD	Dynamic setting is enabled. The LD-level link can operate at distances up to 500 km at 1 Gbit/sec, 250 km at 2 Gbit/sec, or 125 km at 4 Gbit/sec, depending on the availability of frame buffers within the port group.	Yes

Figure 3-6 Extended Fabric Tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 8:28 AM PDT

Port Number	Buffer Limited	Port Speed	Buffer Usage	Actual Distance(km)	Desired Distance(km)	Long Distance
0	No	N2	0	<2	10	LD: Auto
1	No	N2	0	<2	10	LD: Auto
2	No	N2	0	<2	10	LD: Auto
3	No	N2	0	<2	10	LD: Auto
4	No	N2	0	N/A	N/A	L2: <= 100 km
5	No	N2	0	<2	10	LD: Auto
6	No	N2	0	N/A	N/A	LE: <= 10 km

WARNING: Before changing this configuration, please consult your switch vendor.

Long Distance Compatibility

○ On ● Off

[Switch Administration opened]: Tue Aug 31 2004, 8:09 AM PDT
[Switch Administration closed]: Tue Aug 31 2004, 8:12 AM PDT
[Switch Administration opened]: Tue Aug 31 2004, 8:15 AM PDT

Long Distance Port Configuration.

To configure a port for long-distance connection

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Extended Fabric** tab.
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, select the slot subtab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed directly to the next step.

Note
The SilkWorm 3016 switch has some limitations on the ling distance settings of its external ports. Refer to the *Brocade Fabric OS Procedures Guide* for more information.

4. Select a port by clicking anywhere in the row for that port.
5. Select a distance from the **Long Distance** drop-down list that corresponds to the port.

   Depending on the distance selected, this might require an optional license. For information about the various distances, refer to Table 3-1 on page 3-16.

If you select a long-distance setting of LD, you must also type a value in the **Desired Distance** column for that port number:

a. Double-click the **Desired Distance** field for the port, as shown in Figure 3-6.

b. Type a number in the field to indicate the distance in kilometers.

   For 1 Gbit/sec ports, type a number between 10 and 500, inclusive.
   For 2 Gbit/sec ports, type a number between 10 and 250, inclusive.
   For 4 Gbit/sec ports, type a number between 10 and 125, inclusive.

   This value is the upper limit for calculating buffer availability for other ports in the same port group. If the actual distance is more than the desired distance, the port operates in buffer-limited mode.

c. Press **Enter** or click another port entry for the value to be accepted.

6. *Optional*: To enable long-distance compatibility so that ISLs in a fabric can be up to 100 km long (the exact distance level is determined by the per-port configuration on the E_Ports of each ISL), click the **On** radio button for Long Distance Compatibility.

   The switch must be disabled before you can select this option.

   If you select this option, you must have an Extended Fabrics license, and both E_Ports in an ISL must be configured with the same long-distance compatibility setting.

7. Click **Apply**.

Configuring Routes

Routing policies are configured from the command line interface (CLI). For Fabric OS v4.4.x, the supported routing policies are:

- port-based
- device-based (SilkWorm 4100 only)
- exchanged-based (SilkWorm 4100 only)

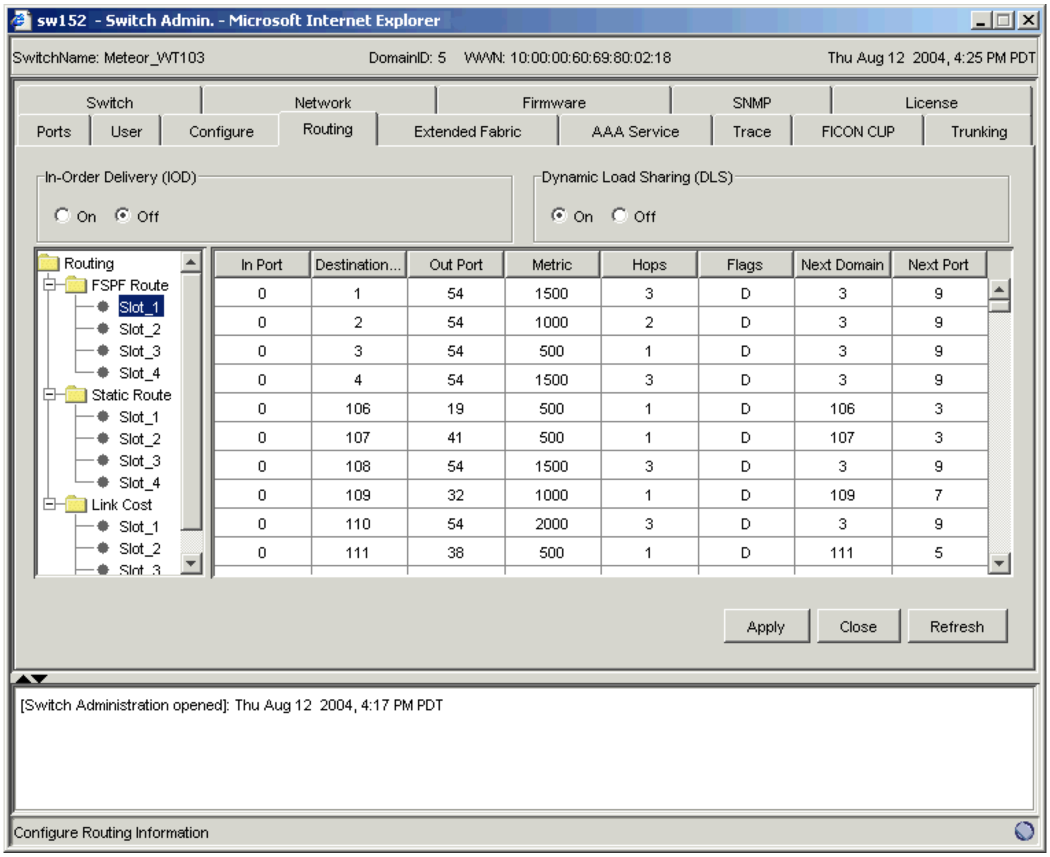
For the SilkWorm 4100, the exchange-based routing policy is the default.

To optimize port-based routing, the dynamic load sharing feature (DLS) can be enabled to balance the load across the available output ports within a domain. Device-based and exchange-based routing *require* the use of DLS; when these policies are in effect, you cannot disable the DLS feature.

Using port-based routing, you can assign a *static route*, in which the path chosen for traffic never changes. In contrast, device-based and exchange-based routing policies always employ *dynamic path selection*, in which the software chooses a path based on current traffic conditions. Refer to the *Brocade Fabric OS Procedures Guide* for more information.

The **Routing** tab of the Switch Admin module displays routing information. Figure 3-7 on page 3-19 shows a Routing tab when the port-based routing policy is enabled. When a device-based or exchange-based routing policy is enabled, the interface is different: the Static Route information and the Dynamic Load Sharing radio buttons are not displayed.

Figure 3-7 Routing Tab for Port-Based Routing Policy



SwitchName: Meteor_WT103 DomainID: 5 WWN: 10:00:00:60:69:80:02:18 Thu Aug 12 2004, 4:25 PM PDT

In-Order Delivery (IOD) ○ On ● Off

Dynamic Load Sharing (DLS) ● On ○ Off

In Port	Destination...	Out Port	Metric	Hops	Flags	Next Domain	Next Port
0	1	54	1500	3	D	3	9
0	2	54	1000	2	D	3	9
0	3	54	500	1	D	3	9
0	4	54	1500	3	D	3	9
0	106	19	500	1	D	106	3
0	107	41	500	1	D	107	3
0	108	54	1500	3	D	3	9
0	109	32	1000	1	D	109	7
0	110	54	2000	3	D	3	9
0	111	38	500	1	D	111	5

[Switch Administration opened]: Thu Aug 12 2004, 4:17 PM PDT

Configure Routing Information

Displaying FSPF Routing

The **Routing** tab of the Switch Admin module displays information about routing paths.

To view FSPF routing

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Routing** tab.
3. This step is switch-type specific:

   For SilkWorm 12000 or 24000 directors, click a slot number under the FSPF Route category in the navigation tree.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, click the FSPF Route category in the navigation tree.

Configuring a Static Route

A static route can be assigned only when the active routing policy is port-based. When device-based or exchange-based routing is active, you cannot disable DLS and you cannot view and configure static routes.

When you configure a static route for a SilkWorm 12000 director or for a SilkWorm 24000 configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure a static route individually.

To configure a static route

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Routing** tab.
3. This step is switch-specific:

   For SilkWorm 12000 or 24000 directors, click a slot number under the Static Route category in the navigation tree. Click **Add**.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, click the Static Route category in the navigation tree. Click **Add**.

   A new blank line appears in the window.

   Note that when device-based or exchange-based routing policies are in effect, the Static Route category does not display in the navigation tree.
4. Type the **In Port** number for the route.
5. Type the **Destination Domain**. The destination domain IDs match the outports in the cell.
6. Type the **Out Port** number for the route.
7. Click **OK** to add the static route.
8. Click **Apply**.

Enabling/Disabling Dynamic Load Sharing

The device-based and exchange-based routing policies depend on the Fabric OS dynamic load sharing feature (DLS) for dynamic routing path selection. When these policies are in force, DLS is always enabled and cannot be disabled.

When the port-based policy is in force, you can enable DLS to optimize routing. When DLS is enabled, it shares traffic among multiple equivalent paths between switches. DLS recomputes load sharing either when a switch boots up or each time an E_Port or Fx_Port goes online or offline. Enabling this feature allows a path to be discovered automatically by the FSPF path-selection protocol.

For more information regarding DLS, refer to the **dlsset** command in the *Brocade Fabric OS Command Reference Manual*.

When you enable or disable dynamic load sharing for the SilkWorm 12000 director or for a SilkWorm 24000 configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must enable or disable dynamic load sharing individually.

To configure the DLS setting

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Routing** tab.
3. Click **On** in the Dynamic Load Sharing area to enable dynamic load sharing.
   Click **Off** in the Dynamic Load Sharing area to disable dynamic load sharing.

   Note that when device-based or exchange-based routing policies are in effect, the DLS radio buttons do not display in the **Routing** tab
4. Click **Apply**.

Specifying Frame Order Delivery

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for example, if a link goes down), traffic is rerouted around the failure, and some frames could be delivered out of order.

By default, frame delivery is out-of-order across topology changes. However, if the fabric contains destination devices that do not support out-of-order delivery, you can force in-order frame delivery across topology changes.

Enabling in-order delivery (IOD) guarantees that frames are either delivered in order or dropped. For more information regarding IOD, refer to the *Brocade Fabric OS Procedures Guide*.

When you enable or disable IOD for the SilkWorm 12000 director or for a SilkWorm 24000 configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you enable or disable IOD individually.

To configure the IOD setting

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Routing** tab.
3. Click **On** in the In-Order Delivery area to force in-order frame delivery across topology changes.
   Click **Off** in the In-Order Delivery area to restore out-of-order frame delivery across topology changes.

   Note
   Enabling in-order delivery can cause a delay in the establishment of a new path when a topology change occurs, and therefore should be used with care.
4. Click **Apply**.

Configuring Link Cost

When you configure link cost for the SilkWorm 12000 director, or for a SilkWorm 24000 configured for two logical switches, it is on a logical-switch basis. This means that for each logical switch, you configure link cost individually.

For information regarding link cost, refer to the **linkCost** command in the *Brocade Fabric OS Command Reference Manual*.

To configure the link cost for a port

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Routing** tab.
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, click the slot number of the logical switch under **Link Cost** in the navigation tree.

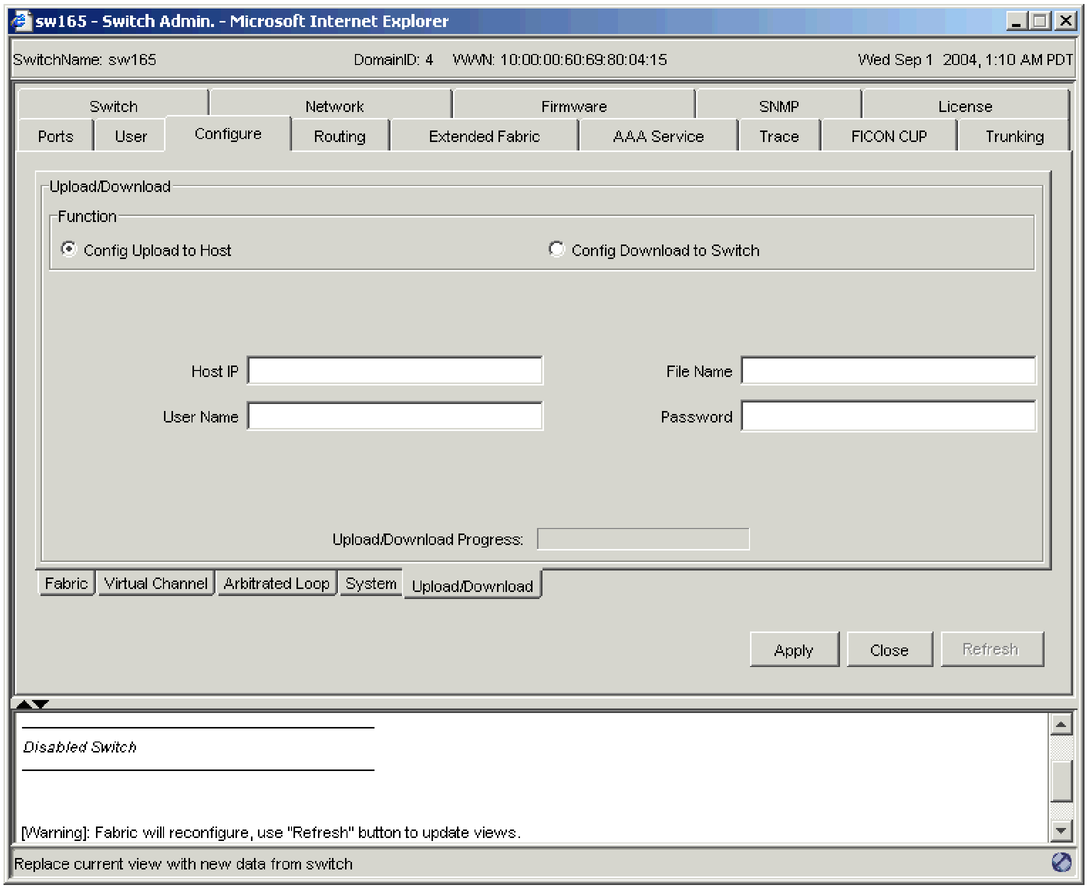
   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, click **Link Cost** in the navigation tree.
4. Double-click in the row in the **Cost** column that corresponds to the appropriate port.
5. Type the link cost. For a 1 Gbit/sec ISL, the default cost is 1000. For a 2 Gbit/sec or a 4 Gbit/sec ISL, the default cost is 500. Valid values for link cost are from 1 through 9999. Setting the value to 0 sets the link cost to the default value for that port.
6. Click **Apply**.

Maintaining Configurations

It is important to maintain consistent configuration settings on all switches in the same fabric, because inconsistent parameters (such as inconsistent PID formats) can cause fabric segmentation. As part of standard configuration maintenance procedures, it is recommended that you back up configuration data for every switch on a host computer server for emergency reference.

The following sections contain procedures for basic switch configuration maintenance. Use the **Configure** tab and **Upload/Download** subtab of the Switch Admin module to perform these tasks. (See Figure 3-8 on page 3-23.)

Figure 3-8 Configure Tab, Upload/Download Subtab



sw165 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw165 DomainID: 4 WWN: 10:00:00:60:69:80:04:15 Wed Sep 1 2004, 1:10 AM PDT

Upload/Download

Function

● Config Upload to Host ○ Config Download to Switch

Host IP

User Name

File Name

Password

Upload/Download Progress:

Disabled Switch

[Warning]: Fabric will reconfigure, use "Refresh" button to update views.

Replace current view with new data from switch

Backing Up a Configuration File

Keep a backup copy of the configuration file in case the configuration is lost or unintentional changes are made. You should keep individual backup files for all switches in the fabric. You should avoid copying configurations from one switch to another.

When you back up a configuration file for the SilkWorm 12000 director or for a SilkWorm 24000 configured with two logical switches, it is on a logical-switch basis. This means that you must back up a separate configuration file for each logical switch.

To back up a configuration file

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Configure** tab.
3. Click the **Upload/Download** subtab (see Figure 3-8).
4. Click the **Config Upload to Host** radio button.
5. Type the user name, password, and host IP information.
6. Type the configuration file with a fully qualified path.

7. Click **Apply**.

You can monitor the progress by looking at the Upload/Download Progress bar on the Configure tab.

Restoring a Configuration

Restoring a configuration involves overwriting the configuration on the switch by downloading a previously saved backup configuration file. Perform this procedure during a planned down time.

Make sure that the configuration file you are downloading is compatible with your switch model, because configuration files from other model switches might cause your switch to fail.

To download a configuration to the switch

1. Launch the Switch Admin module as described on page 3-2.
2. Disable the switch, as described in "Enabling and Disabling a Switch" on page 3-7.

   You can download configurations only to a disabled (offline) switch.
3. Click the **Configure** tab.
4. Click the **Upload/Download** subtab (see Figure 3-8 on page 3-23).
5. Click the **Config Download to Switch** radio button.
6. Type the user name, password, and host IP information.
7. Type the configuration file with a fully qualified path.
8. Click **Apply**.

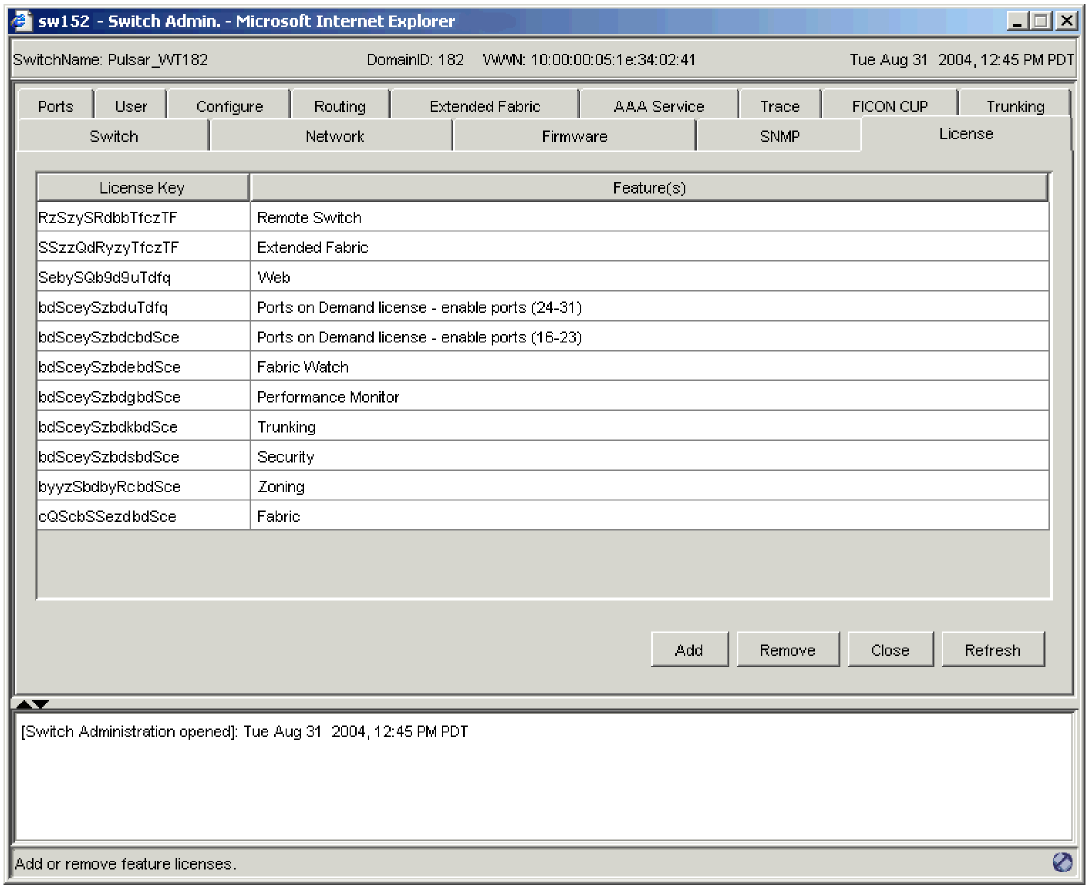
   You can monitor the progress by looking at the Upload/Download Progress bar on the Configure tab.
9. Enable the switch, as described in "Enabling and Disabling a Switch" on page 3-7.

Maintaining Licensed Features

Feature licenses might be supplied with switch software, or you can purchase licenses separately from your switch vendor, who will provide you with keys to unlock the features. License keys are provided on a per-chassis basis, so for products that support multiple logical switches (domains), a license key applies to all domains within the chassis.

The licensed features currently installed on the switch are listed in the License tab of the Switch Admin module, as shown in Figure 3-9. If the feature is listed, it is installed and immediately available. When you enable some licenses, such as ISL Trunking, you might need to change the state of the port to enable the feature on the link.

Figure 3-9 License Tab



SwitchName: Pulsar_WT182 DomainID: 182 WWN: 10:00:00:05:1e:34:02:41 Tue Aug 31 2004, 12:45 PM PDT

License Key	Feature(s)
RzSzySRdbbTfczTF	Remote Switch
SSzzQdRyzyTfczTF	Extended Fabric
SebySQb9d9uTdfq	Web
bdSceySzbduTdfq	Ports on Demand license - enable ports (24-31)
bdSceySzbdcbdSce	Ports on Demand license - enable ports (16-23)
bdSceySzbdebdSce	Fabric Watch
bdSceySzbdgbdSce	Performance Monitor
bdSceySzbdkbdSce	Trunking
bdSceySzbdsbdSce	Security
byyzSbdbyRcbdSce	Zoning
cQScbSSezdbdSce	Fabric

[Switch Administration opened]: Tue Aug 31 2004, 12:45 PM PDT

Add or remove feature licenses.

Activating a License on a Switch

Before you can unlock a licensed feature, you must obtain a license key. You can either use the license key provided in the Paper Pack supplied with switch software or refer to the *Brocade Fabric OS Procedures Guide* for instructions on how to obtain a license key at the Brocade Web site (www.brocade.com).

To activate a license on a switch

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **License** tab.
3. Click **Add**.

   The Add License dialog displays.
4. Paste or type a license key in the field.
5. Click **Add License**.
6. Click **Refresh** to display the new licenses in the License tab.

Note
Some licenses (for example, Trunking) do not take effect until the switch is rebooted.

Removing a License from a Switch

Caution
Removing the Web Tools license from a switch makes that switch unavailable from Web Tools. If you remove the Web Tools license from a SilkWorm 12000 or 24000 director, it makes both logical switches unavailable from Web Tools.

To remove a license from a switch

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **License** tab.
3. Click the license you want to remove.
4. Click **Remove**.

Administering ISL Trunking

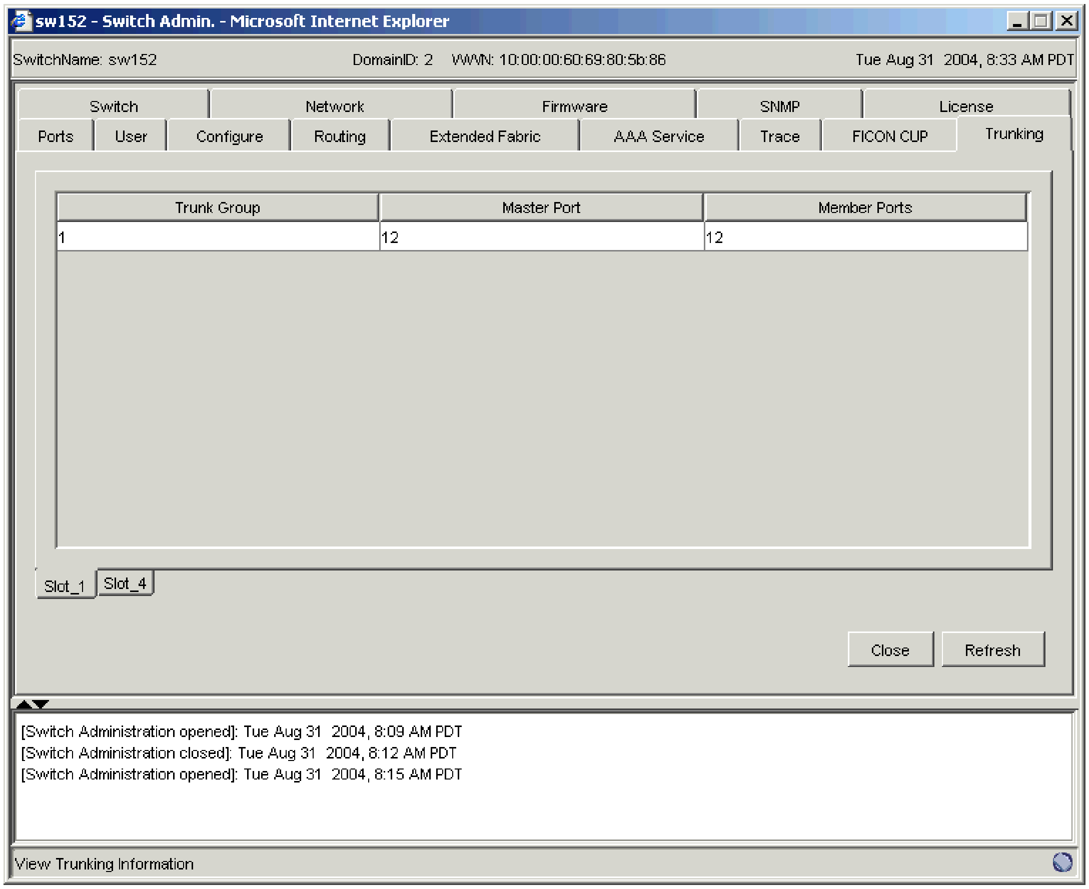
Interswitch link (ISL) trunking optimizes network performance by forming trunking groups that can distribute traffic across a shared bandwidth.

A trunking license is required on each switch that participates in the trunk. (For details on obtaining and installing licensed features, refer to "Maintaining Licensed Features" on page 3-24.)

For additional background information about ISL Trunking, refer to the *Brocade Fabric OS Features Guide*.

Use the Trunking tab of the Switch Admin module to view and manage trunks through Web Tools (see Figure 3-10 on page 3-27).

Figure 3-10 Trunking Tab


sw152 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 8:33 AM PDT

Trunk Group	Master Port	Member Ports
1	12	12

```
[Switch Administration opened]: Tue Aug 31  2004, 8:09 AM PDT
[Switch Administration closed]: Tue Aug 31  2004, 8:12 AM PDT
[Switch Administration opened]: Tue Aug 31  2004, 8:15 AM PDT
```

View Trunking Information

Displaying Trunk Group Information

Use this procedure to display the following information about ISL Trunking groups:

- Trunk group number identifier
- Master port
- Member ports

To view information on a trunk group

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Trunking** tab.
3. *Optional*: Click **Refresh** to refresh the information.

Disabling or Reenabling Trunking Mode on a Port

When the trunking license is activated, trunks are automatically established on eligible ISLs and trunking capability is enabled by default on all ports. Use the following procedure to disable trunking on a port or to reenable trunking if it has been disabled.

Note
The SilkWorm 3016 switch has two external ports that are available for ISL Trunking. The 14 internal ports have ISL Trunking disabled as they attach only to host devices. Refer to the *Brocade Fabric OS Procedures Guide* for additional details.

To disable or reenable trunking mode on a port

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Ports** tab (see Figure 3-5 on page 3-13).
3. This step is switch-specific:

   For SilkWorm 12000 and 24000 switches: Select the slot subtab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches: Proceed directly to the next step.
4. To enable trunking mode on a port, click the checkbox in the **Enable Trunking** column that corresponds to the port you want to trunk.

   To disable trunking mode on a port, uncheck the box.
5. Click **Apply**.

Managing Trace Dumps

A trace dump is a snapshot of the running behavior within the SilkWorm switch. The dump can be used by developers and troubleshooters at Brocade to help understand what might be contributing to a specific switch behavior when certain internal events are seen. For example, a trace dump can be created each time a certain error message is logged to the system error log. Developers can then examine what led up to the message event by studying the traces.

Tracing is always “on.” As software on the switch executes, the trace information is placed into a circular buffer in system RAM. Periodically, the trace buffer is “frozen” and saved. This saved information is a *trace dump*.

A trace dump is generated when:

- it is triggered manually (use the **traceDump** command)
- a critical-level LOG message occurs
- a particular LOG message occurs (use the **traceTrig** command to set up the conditions for this)
- a kernel panic occurs
- the hardware watchdog timer expires

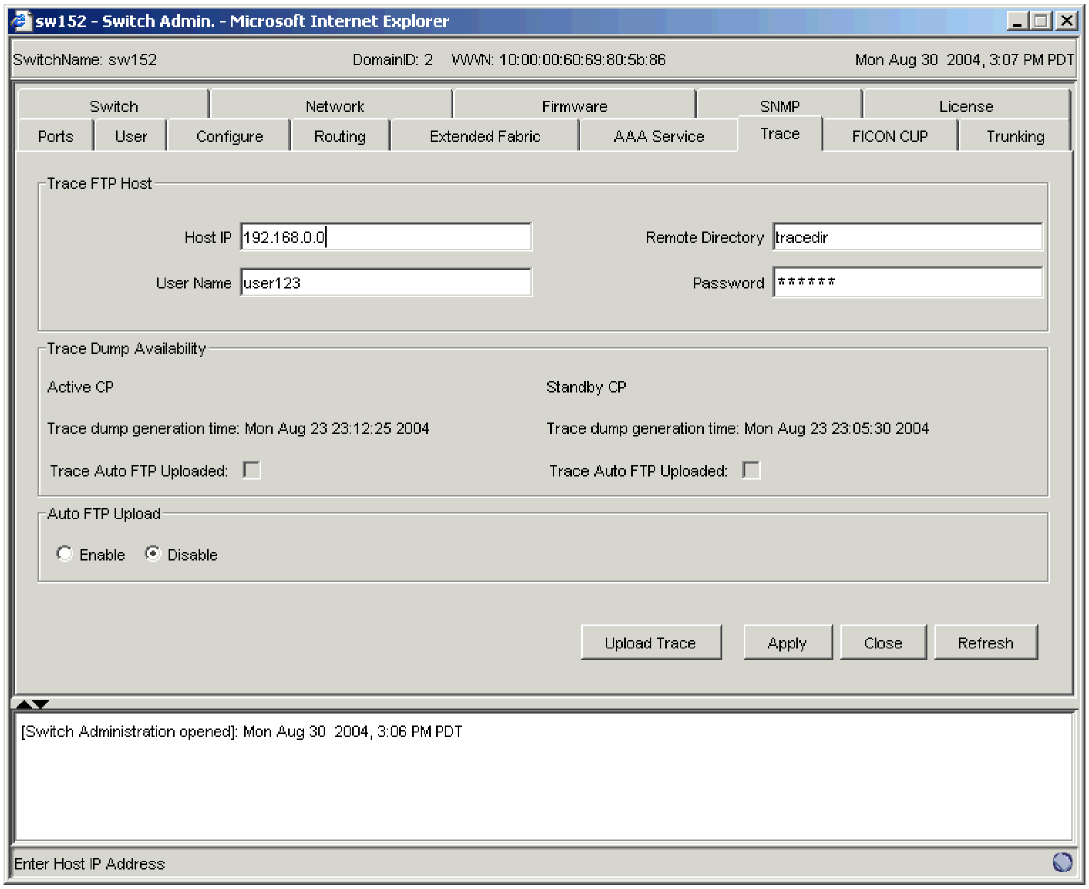
(For information about the **traceDump** and **traceTrig** commands, refer to the *Brocade Fabric OS Command Reference Manual*.)

The trace dump is maintained on the switch until either it is uploaded to the FTP host or another trace dump is generated. If another trace dump is generated before the previous one is uploaded, the previous dump is overwritten.

When a trace dump is generated, it is automatically uploaded to an FTP host if automatic FTP uploading is enabled.

Using the **Trace** tab of the Switch Admin module, you can view and configure the trace FTP host target, enable or disable automatic trace uploads, and manually upload a trace dump (see Figure 3-11 on page 3-29).

Figure 3-11 Trace Tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Mon Aug 30 2004, 3:07 PM PDT

Trace FTP Host

Host IP 192.168.0.0

Remote Directory tracedir

User Name user123

Password ******

Trace Dump Availability

Active CP

Trace dump generation time: Mon Aug 23 23:12:25 2004

Trace Auto FTP Uploaded: □

Standby CP

Trace dump generation time: Mon Aug 23 23:05:30 2004

Trace Auto FTP Uploaded: □

Auto FTP Upload

○ Enable ● Disable

[Switch Administration opened]: Mon Aug 30 2004, 3:06 PM PDT

Enter Host IP Address

How a Trace Dump Is Used

The generation of a trace dump causes a CRITICAL message to be logged to the system error log. When a trace dump is detected, issue the **supportSave** command on the affected switch. This command packages all error logs, the **supportShow** output, and trace dump, and moves these to your FTP server. You can also configure your switch to automatically copy trace dumps to your FTP server (refer to "Setting Up Automatic Trace Dump Transfers," next).

In addition to automatic generation of trace dumps on faults, you can also generate a trace dump manually or when certain system error messages are logged. This is normally done with assistance from Brocade customer support when diagnosing switch behavior.

For details on the commands, refer to the *Brocade Fabric OS Command Reference Manual*.

Setting Up Automatic Trace Dump Transfers

You can set up a switch so that diagnostic information is transferred automatically to a remote server. Then, if a problem occurs you can provide your customer support representative with the most detailed information possible. To ensure the best service, you should set up for automatic transfer as part of standard switch configuration, before a problem occurs.

Setting up for automatic transfer of diagnostic files involves the following tasks:

- Specify a remote server to store the files.
- Enable the automatic transfer of trace dumps to the server. (Trace dumps overwrite each other by default; sending them to a server preserves information that would otherwise be lost.)

You should also set up a periodic checking of the remote server so that you are alerted if the server becomes unavailable and you can correct the problem. Refer to the *Brocade Fabric OS Procedures Guide* for additional information.

The following procedures describe in detail the tasks for setting up automatic transfer.

To specify a remote server

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Trace** tab.
3. Type the FTP host IP address, path of the remote directory in which to store the trace dump files, FTP user name, and FTP password in the appropriate fields.

   The password is optional if you log in as an anonymous user.
4. Click **Apply**.

To enable automatic transfer of trace dumps

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Trace** tab.
3. Click **Enable** in the **Auto FTP Upload** section to enable automatic uploading of the trace dump to the FTP host.
4. Click **Apply**.

Disabling Automatic Trace Uploads

If automatic uploading of a trace dump is disabled, you must manually upload the trace dump or else the information is overwritten when a subsequent trace dump is generated.

To disable automatic uploading of the trace dump

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Trace** tab.
3. Click **Disable** in the **Auto FTP Upload** section to disable automatic uploading of the trace dump to the FTP host.
4. Click **Apply**.

Uploading a Trace Dump Manually

You can manually upload a trace dump when automatic uploading is not enabled.

To upload the trace dump

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **Trace** tab.

   The **Trace Dump Availability** section displays whether a trace dump is available. If the **Trace Auto FTP Uploaded** box is checked, the trace dump has been automatically uploaded to the FTP host.
3. Click **Upload Trace**. If the **Upload Trace** button is inactivated, it means that a trace dump is not available.

   The Upload Trace dialog displays, along with the default trace dump file name.
4. *Optional*: Type a new trace dump file name if you want to change it from the default name.
5. **For the SilkWorm 12000 and 24000 only:** Click the CP (active or standby) from which the trace dump is to be uploaded.

   If the CP does not have a trace dump, that CP selection is disabled.
6. Click **OK**.

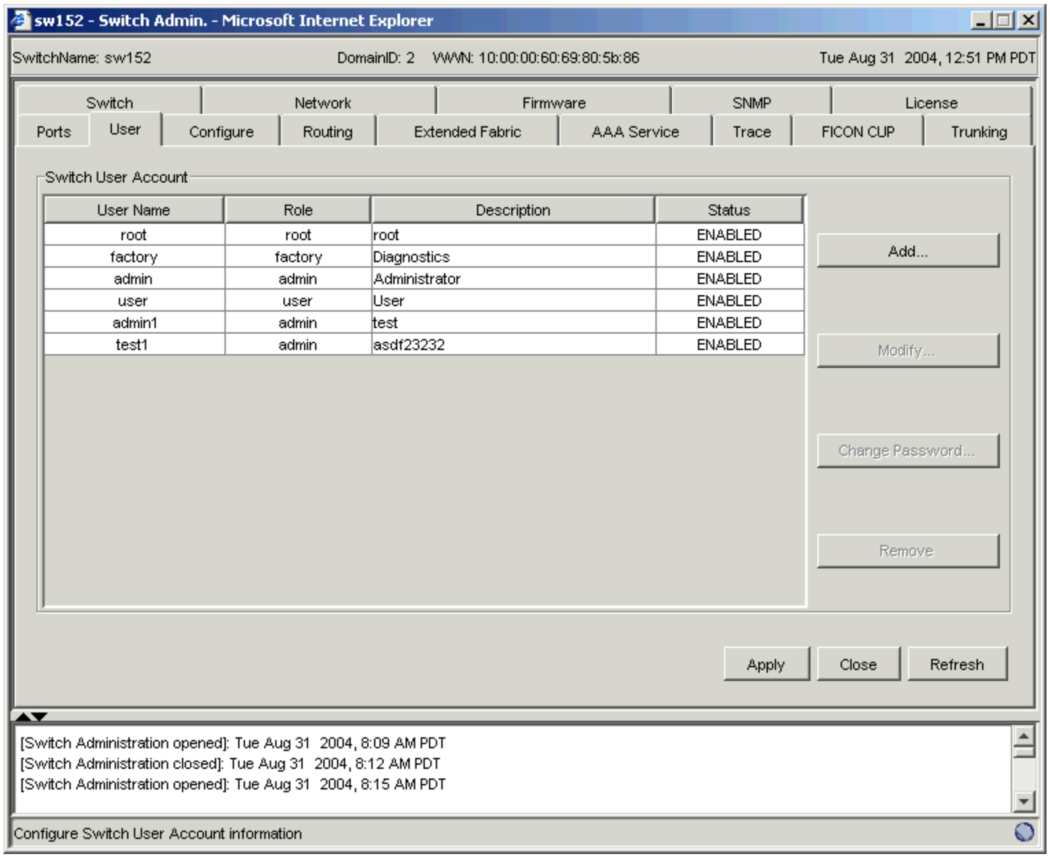
Creating and Maintaining User-Defined Accounts

In addition to the four default accounts—root, factory, admin, and user—Fabric OS supports up to 15 user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

The **User** tab of the Switch Admin module (see Figure 3-12) displays account information and enables you to create and manage user accounts.

Note
If you are operating in secure mode, you can perform these operations only on the primary FCS switch.

Figure 3-12 User Tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 12:51 PM PDT

User Name	Role	Description	Status
root	root	root	ENABLED
factory	factory	Diagnostics	ENABLED
admin	admin	Administrator	ENABLED
user	user	User	ENABLED
admin1	admin	test	ENABLED
test1	admin	asdf23232	ENABLED

```
[Switch Administration opened]: Tue Aug 31  2004, 8:09 AM PDT
[Switch Administration closed]: Tue Aug 31  2004, 8:12 AM PDT
[Switch Administration opened]: Tue Aug 31  2004, 8:15 AM PDT
```

Configure Switch User Account information

To display account information

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **User** tab.

   A list of the default and user-defined accounts displays.

   Note that for the SilkWorm 3016 switch, the default administrator account name is “USERID” and the default password is “PASSW0RD”. The “0” is the number zero and not the letter “O.”

To create a user-defined account

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **User** tab.
3. Click the **Add...** button.

   The Add User Account dialog displays.
4. Type the user name, which must begin with an alphabetic character. The name can be up to 40 characters long. It is case-sensitive and can contain alphabetic and numeric characters, the dot (.) and the underscore (_). It must be different from all other account names on the logical switch.
5. Select a role from the drop-down list: either admin or user in nonsecure mode; admin, user, or nonfcsadmin in secure mode.
6. *Optional*: Type a description of the account.

7. Click the **Enabled** or **Disabled** radio button to enable or disable the account.

8. Type the password for the account.

   Passwords can be from 8 through 40 characters long. They must begin with an alphabetic character. They can include numeric characters, the dot (.), and the underscore (_). They are case-sensitive, and they are not displayed when you enter them on the command line.

9. Retype the password in the **Confirm Password** field for confirmation.

10. Click **OK**.

11. Click **Apply** to save your changes.

To delete a user-defined account

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **User** tab.
3. Select the account to remove.
4. Click the **Remove** button.
5. Click **Apply** to save your changes.

You cannot delete the default accounts. An account cannot delete itself. All active command line interface (CLI) sessions for the deleted account are logged out.

To change account parameters

1. Launch the Switch Admin module as described on page 3-2.

2. Click the **User** tab.

3. Select the account to modify.

   You cannot modify the default root and factory accounts, even if you are logged in as root.

4. Click the **Modify** button.

   The Modify User Account dialog displays.

   Note that you cannot change the user name of the account. To change the user name, you must delete the account and create a new account.

5. Select a role from the drop-down list: either admin or user in nonsecure mode; admin, user, or nonfcsadmin in secure mode.

   You can change the role only on user-level accounts. You cannot change the role on the default accounts. You cannot change the role of your own account.

6. Type a new description.

   You can change the description only on user-level accounts. You cannot change the description of the default accounts. You cannot change the description of your own account.

7. Click the **Enabled** or **Disabled** radio button to enable or disable the account.

   You can enable and disable user- and admin-level accounts except for your own account. You cannot enable or disable your own account or the factory account. Only the root account can disable itself.

   If you disable an account, all active CLI sessions for that account are logged out.

8. Click **OK**.
9. Click **Apply** to save your changes.

To change the password for an admin or user level account

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **User** tab.
3. Select the account to modify.

   You can change the password of your own account, peer admin accounts, and user accounts. You cannot change the root or factory account passwords.
4. Click the **Change Password...** button.

   The Set User Account Password dialog displays.

   If you are changing the password of an admin account, you must also provide the current password. You do not need to provide the current password if you are changing the password of a lower-level user account.
5. Type the current password of the account. This step is required only if you are changing the password of your own or a peer admin account.
6. Type the new password of the account.

   The new password must have at least one character different from the old password.
7. Retype the new password in the **Confirm Password** field.
8. Click **OK**.
9. Click **Apply** to save your changes.

Configuring SNMP Information

This section describes how to manage the configuration of the SNMP agent in the switch. The configuration includes SNMPv1 and SNMPv3 configuration, accessControl, and systemGroup configuration parameters.

For more information, refer to the **snmpConfig** command in the *Brocade Fabric OS Command Reference Manual*.

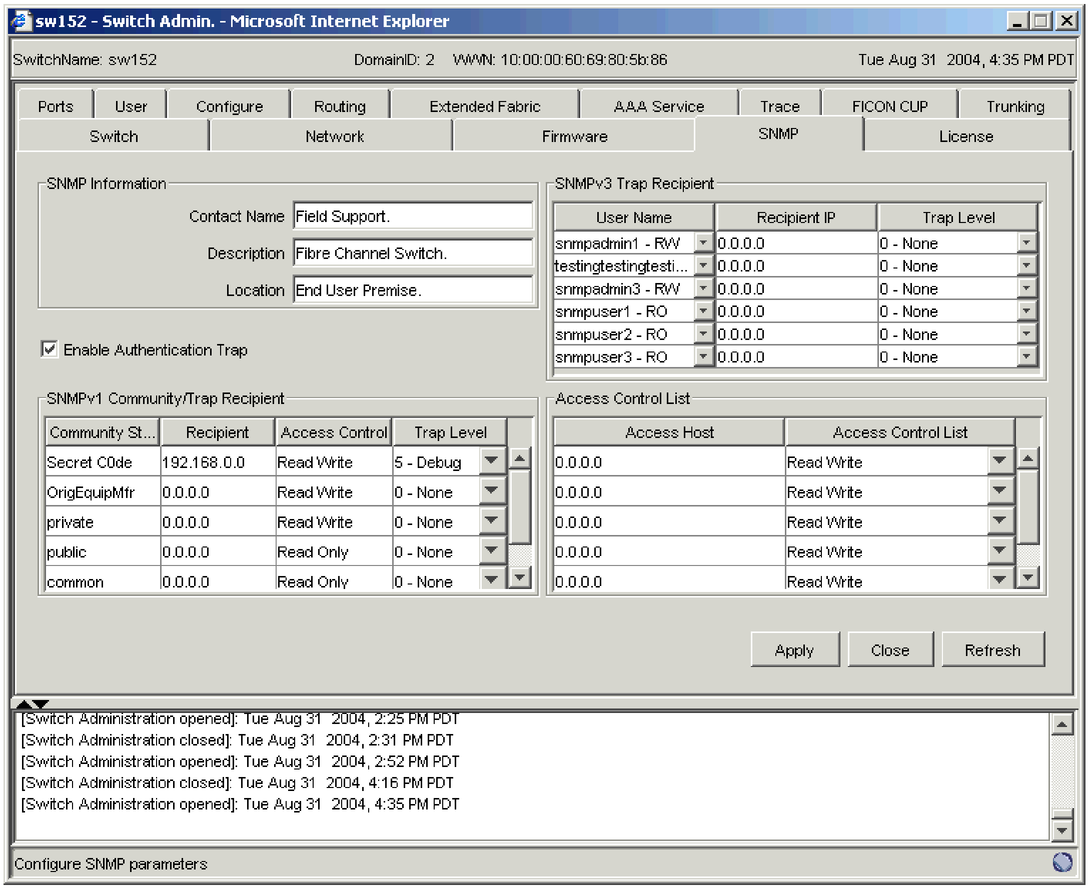
Setting SNMP Trap Levels

When you set trap levels for the SilkWorm 12000 director or for a SilkWorm 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must set trap levels individually.

To set trap levels

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **SNMP** tab (see Figure 3-13 on page 3-35).

Figure 3-13 SNMP Tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 4:35 PM PDT

SNMP Information

Contact Name: Field Support.

Description: Fibre Channel Switch.

Location: End User Premise.

☑ Enable Authentication Trap

SNMPv3 Trap Recipient

User Name	Recipient IP	Trap Level
snmpadmin1 - RW	0.0.0.0	0 - None
testingtestingtesti...	0.0.0.0	0 - None
snmpadmin3 - RW	0.0.0.0	0 - None
snmpuser1 - RO	0.0.0.0	0 - None
snmpuser2 - RO	0.0.0.0	0 - None
snmpuser3 - RO	0.0.0.0	0 - None

SNMPv1 Community/Trap Recipient

Community St...	Recipient	Access Control	Trap Level
Secret C0de	192.168.0.0	Read Write	5 - Debug
OrigEquipMfr	0.0.0.0	Read Write	0 - None
private	0.0.0.0	Read Write	0 - None
public	0.0.0.0	Read Only	0 - None
common	0.0.0.0	Read Only	0 - None

Access Control List

Access Host	Access Control List
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write

```
[Switch Administration opened]: Tue Aug 31  2004, 2:25 PM PDT
[Switch Administration closed]: Tue Aug 31  2004, 2:31 PM PDT
[Switch Administration opened]: Tue Aug 31  2004, 2:52 PM PDT
[Switch Administration closed]: Tue Aug 31  2004, 4:16 PM PDT
[Switch Administration opened]: Tue Aug 31  2004, 4:35 PM PDT
```

Configure SNMP parameters

3. Select a trap level for a recipient from the corresponding **Trap Level** drop-down list in the SNMPv1 and SNMPv3 sections.

   The level you select identifies the minimum event level that will prompt a trap.

4. Click **Apply**.

Configuring SNMP Information

When you configure SNMP information for the SilkWorm 12000 director or for a SilkWorm 24000 configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure SNMP information individually.

To change the systemGroup configuration parameters

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **SNMP** tab (see Figure 3-13).
3. Type a contact name, a description, and a location in the **SNMP Information** section.
4. *Optional*: Click the **Enable Authentication Trap** checkbox to allow authentication traps to be sent to the reception IP address.
5. Click **Apply**.

To set SNMPv1 configuration parameters

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **SNMP** tab (see Figure 3-13).
3. Double-click a community string in the **SNMPv1** section and type a new community string.
4. Double-click a recipient IP address in the **SNMPv1** section and type a new IP address.
5. Click **Apply**.

To set SNMPv3 configuration parameters

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **SNMP** tab (see Figure 3-13).
3. Select a user name from the User Name drop-down list in the **SNMPv3** section.
4. Double-click a recipient IP address in the **SNMPv3** section and type a new IP address.
5. Select a trap level from the Trap Level drop-down list.
6. Click **Apply**.

To change the accessControl configuration

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **SNMP** tab (see Figure 3-13).
3. Double-click an access host IP address in the **Access Control List** section and type a new host IP address.
4. Select a permission for the host from the **Access Control List** drop-down list. Options are **Read Only** and **Read Write**.
5. Click **Apply**.

Administering High Availability

The procedures in this section apply only to the SilkWorm 12000 and SilkWorm 24000 directors, because the High Availability module is available only on these switch types.

Launching the Hi Availability Module

The background color of the Hi Avail button indicates the overall status of the switch. The Hi Avail module displays information about the status of the High Availability (HA) feature on the SilkWorm 12000 and 24000 directors and each CP. It also enables you to perform tasks such as CP failover or to synchronize services on the CPs.

To launch the Hi Avail module

1. Select a SilkWorm 12000 or 24000 director from the Fabric Tree.

   The selected director appears in the Switch View.

2. Click the **Hi Avail** button Hi Avail from the Switch View.

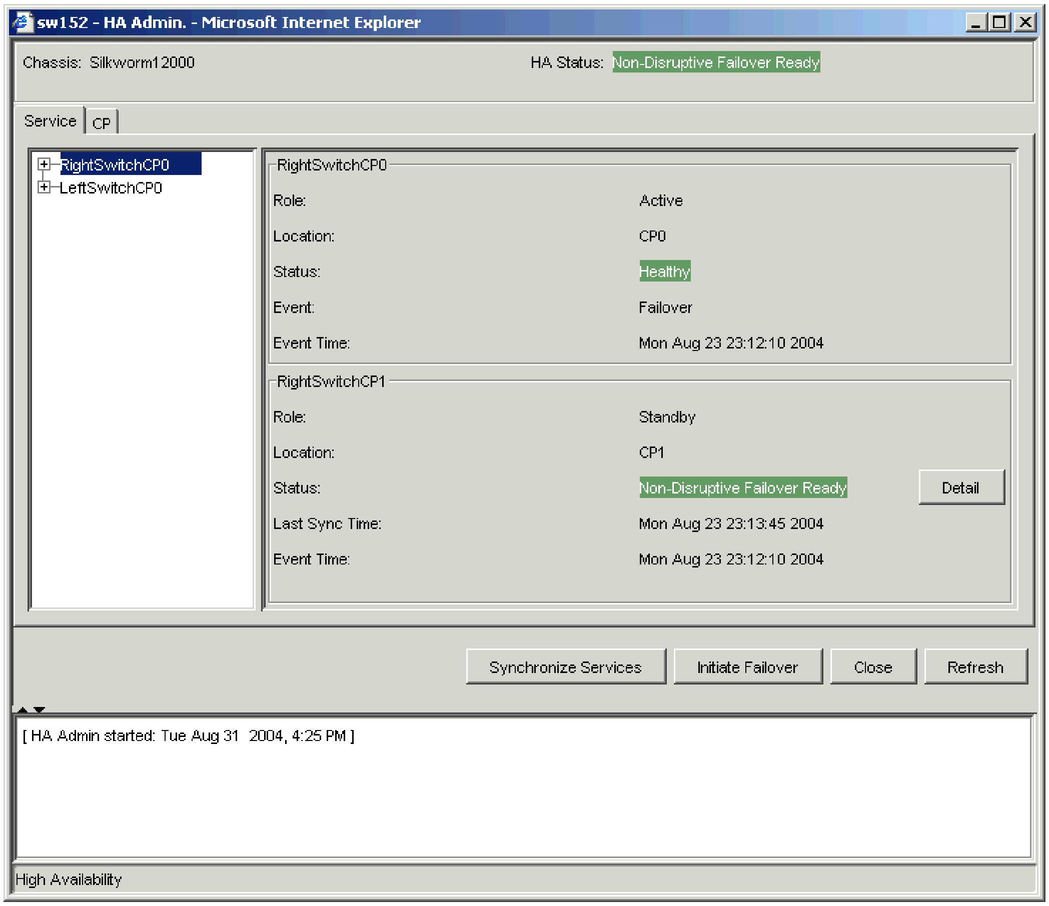
   The login dialog box displays.

3. Type the user name of an account with the admin role.

4. Type the password.

   The **HA Admin** module displays, as shown in Figure 3-14.

Figure 3-14 High Availability Module for the SilkWorm 12000



Chassis: Silkworm12000

HA Status: Non-Disruptive Failover Ready

RightSwitchCP0

Role:	Active
Location:	CP0
Status:	Healthy
Event:	Failover
Event Time:	Mon Aug 23 23:12:10 2004

RightSwitchCP1

Role:	Standby
Location:	CP1
Status:	Non-Disruptive Failover Ready
Last Sync Time:	Mon Aug 23 23:13:45 2004
Event Time:	Mon Aug 23 23:12:10 2004

```
[ HA Admin started: Tue Aug 31  2004, 4:25 PM ]
```

Note that there is a background color with the HA Status for each CP. The HA Admin module is not refreshed automatically. Click **Refresh** to update the information displayed in the HA Admin module.

Synchronizing Services on the CP

A nondisruptive CP failover is possible only when all the services on it have been synchronized.

To synchronize the services

1. Launch the Hi Avail module as described in "Launching the Hi Availability Module" on page 3-36.

2. If the HA Status field displays **Non-Disruptive Failover Ready**, you are done.

   If the HA Status field displays **Disruptive Failover Ready**, continue with step 3.

3. Click the **Synchronize Services** button.

   The Warning dialog box displays.

4. Click **Yes** and wait for the CPs to complete a synchronization of services, so that a nondisruptive failover is ready.
5. Click **Refresh** to update the HA Status field.

   When the HA Status field displays **Non-Disruptive Failover Ready**, a failover can be initiated without disrupting frame traffic on the fabric.

Initiating a CP Failover

A nondisruptive failover might take a few minutes to complete. You might lose connection to the switch for a few minutes during the failover; however, Web Tools automatically resumes the connection after the failover.

To initiate a CP failover

1. Launch the Hi Avail module as described in "Launching the Hi Availability Module" on page 3-36.
2. Verify that the HA Status field displays **Non-Disruptive Failover Ready** or **Disruptive Failover Ready**. Refer to "Synchronizing Services on the CP" on page 3-37 for more information.
3. Click **Initiate Failover**.

   The Warning dialog box displays.

4. Click **Yes** to initiate a non-disruptive failover.

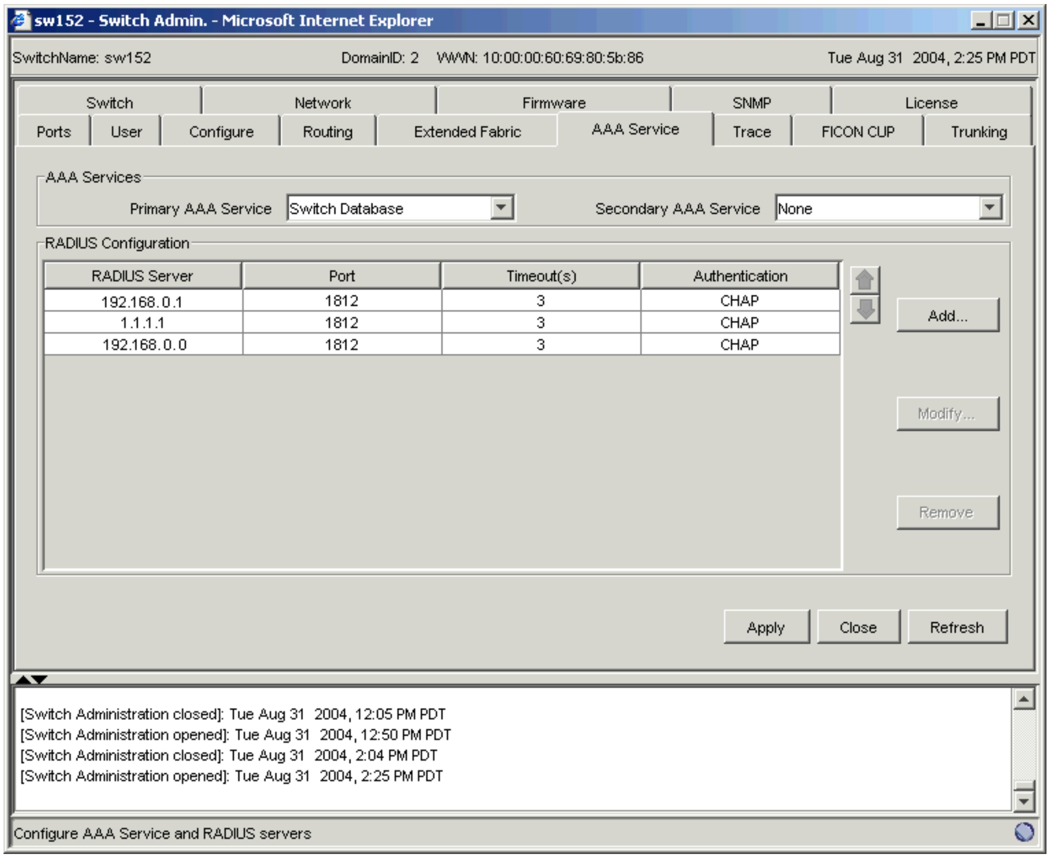
Managing RADIUS Server

Fabric OS supports RADIUS authentication, authorization, and accounting service (AAA). When configured for RADIUS, the switch becomes a Network Access Server (NAS) that acts as a RADIUS client. In this configuration, authentication records are stored in the RADIUS host server database. Login and logout account name, assigned role, and time accounting records are also stored on the RADIUS server.

You should set up RADIUS service through a secure connection such as SSH.

Use the AAA Service tab of the Switch Admin module to manage the RADIUS server (see Figure 3-15 on page 3-39)

Figure 3-15 AAA Service Tab



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 2:25 PM PDT

Primary AAA Service: Switch Database
Secondary AAA Service: None

RADIUS Server	Port	Timeout(s)	Authentication
192.168.0.1	1812	3	CHAP
1.1.1.1	1812	3	CHAP
192.168.0.0	1812	3	CHAP

```
[Switch Administration closed]: Tue Aug 31  2004, 12:05 PM PDT
[Switch Administration opened]: Tue Aug 31  2004, 12:50 PM PDT
[Switch Administration closed]: Tue Aug 31  2004, 2:04 PM PDT
[Switch Administration opened]: Tue Aug 31  2004, 2:25 PM PDT
```

Configure AAA Service and RADIUS servers

Enabling and Disabling RADIUS Service

At least one RADIUS server must be configured before you can enable RADIUS service.

To enable or disable RADIUS service

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **AAA Service** tab.
3. To enable RADIUS service, select a RADIUS service from the Primary AAA Service drop-down list. Select **None** or **Switch Database** from the Secondary AAA Service drop-down list.

   To disable RADIUS service, select **Switch Database** from the Primary AAA Service drop-down list and select **None** from the Secondary AAA Service drop-down list.
4. Click **Apply**.

Configuring the RADIUS Server

The configuration is chassis-based, so it applies to all logical switches (domains) on the switch and replicates itself on a standby CP, if one is present. It is saved in a configuration upload, and so it can be applied to other switches in a configuration download. You should configure at least two RADIUS servers so that if one fails, the other will assume service.

You can configure the RADIUS server even if it is disabled. You can configure up to five RADIUS servers. You must be logged in as admin to configure the RADIUS server.

To configure the RADIUS server

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **AAA Service** tab.
3. Click **Add**. You can configure up to five RADIUS servers. If five RADIUS servers are already configured, the **Add** button is disabled.

   The RADIUS Configuration dialog displays.
4. Type the RADIUS server name, which is a valid IP address or Dynamic Name Server (DNS) string. Each RADIUS server must have a unique IP address or DNS name for the RADIUS server.
5. *Optional*: Type the port number.
6. *Optional*: Type the secret string.
7. *Optional*: Type the timeout time in minutes.
8. *Optional*: Select an authentication protocol from CHAP or PAP. The default value is CHAP, and if you do not change it, CHAP will be the authentication protocol.
9. Click **OK** to return to the **AAA Service** tab.
10. Click **Apply**.

Modifying the RADIUS Server

Use the following procedure to change the parameters of a RADIUS server that is already configured.

To modify the RADIUS server

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the **RADIUS Configuration** list.
4. Click **Modify**.

   The RADIUS Configuration dialog displays.
5. Type new values for the port number, secret string, and timeout time (in minutes).
6. Select an authentication protocol from CHAP or PAP. The default value is CHAP, and if you do not change it, CHAP will be the authentication protocol.
7. Click **OK** to return to the **AAA Service** tab.
8. Click **Apply**.

Modifying the RADIUS Server Order

The RADIUS servers are contacted in the order they are listed, starting from the top of the list and moving to the bottom.

To modify the order in which the RADIUS servers are contacted

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the RADIUS Configuration list.
4. Click the up and down arrows to rearrange the order of the RADIUS servers.
5. Click **Apply**.

Removing a RADIUS Server

Use the following procedure to remove a RADIUS server.

To remove a RADIUS server

1. Launch the Switch Admin module as described on page 3-2.
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the RADIUS Configuration list.
4. Click **Remove**. If there is no RADIUS server configured, the **Remove** button is disabled. You cannot remove the only RADIUS server if the RADIUS service is the primary AAA service.

   The RADIUS server is not deleted until you apply the changes from the AAA Services tab.
5. Click **Apply** in the AAA Services tab.

   A confirmation displays, warning you that you are about to remove the selected RADIUS server.
6. Click **Yes** in the confirmation.

Chapter
4

Monitoring Your Fabrics, Switches, and Ports

This chapter contains the following sections:

Monitoring Events

Web Tools displays fabric-wide and switch-wide events. Event information includes sortable fields for the following:

- switch name
- message number
- time stamp
- indication of whether the event is from a logical switch or a chassis
- severity level
- unique message identifier (in the form *moduleID-messageType*)
- detailed error message for root cause analysis

There are four message severity levels: Critical, Error, Warning, and Info. Table 4-1 on page 4-2 lists the event message severity levels displayed in the Switch and Fabric Events windows, and explains what qualifies event messages to be certain levels.

In both the Switch Events view and the Fabric Events view, you can click the **Filter** button to launch the Filter Events dialog. The Filter Events dialog allows you to define which events should be displayed in the Switch Events view or Fabric Events view. For more information on filtering events, refer to "Filtering Fabric and Switch Events" on page 4-4.

Table 4-1 Event Severity Levels

Icon and Level	Description
❗ Critical (0)	Critical-level messages indicate that the software has detected serious problems that will eventually cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
△ Error (1)	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate timeouts on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
⚠ Warning (2)	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode and that the failed power supply needs to be replaced or fixed.
ℹ Info (4)	Information-level messages report the current nonerror status of the system components; for example, the online and offline status of a fabric port.

Displaying Fabric Events

Events are displayed for all switches in the fabric in the Fabric Events view (see Figure 4-1 on page 4-3). Fabric Events are not automatically polled. You must click **Refresh** from the Fabric Events view to poll fabric events. Switch events are automatically polled every 15 seconds.

Fabric Events can be collected only for switches that have the same security level (http or https) as the launch switch. For switches that have a different level of security from the launch switch, a message is displayed at the top of the window indicating how many switches have no events reported from the last polling. For detailed information on the switch names and reasons for not polling (if available), click **Details**.

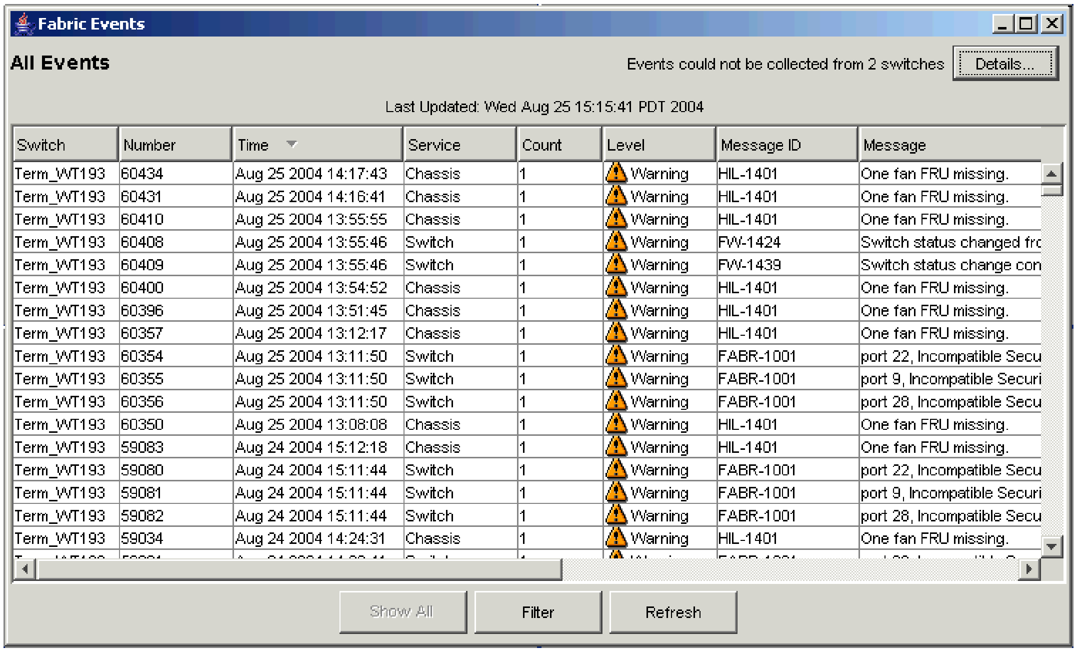
To display fabric events

1. Click a fabric from the Fabric Tree.
2. Click the **Fabric Events** icon on the Fabric Toolbar.

   The Fabric Events window displays (see Figure 4-1).
3. *Optional*: Click the column head to sort the events by a particular column.
   Drag the column divider to resize a column.

You can also filter switch events, as described in "Filtering Fabric and Switch Events" on page 4-4.

Figure 4-1 Fabric Events View



All Events

Events could not be collected from 2 switches

Last Updated: Wed Aug 25 15:15:41 PDT 2004

Switch	Number	Time	Service	Count	Level	Message ID	Message
Term_WT193	60434	Aug 25 2004 14:17:43	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60431	Aug 25 2004 14:16:41	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60410	Aug 25 2004 13:55:55	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60408	Aug 25 2004 13:55:46	Switch	1	⚠ Warning	FW-1424	Switch status changed frc
Term_WT193	60409	Aug 25 2004 13:55:46	Switch	1	⚠ Warning	FW-1439	Switch status change con
Term_WT193	60400	Aug 25 2004 13:54:52	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60396	Aug 25 2004 13:51:45	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60357	Aug 25 2004 13:12:17	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	60354	Aug 25 2004 13:11:50	Switch	1	⚠ Warning	FABR-1001	port 22, Incompatible Secu
Term_WT193	60355	Aug 25 2004 13:11:50	Switch	1	⚠ Warning	FABR-1001	port 9, Incompatible Securi
Term_WT193	60356	Aug 25 2004 13:11:50	Switch	1	⚠ Warning	FABR-1001	port 28, Incompatible Secu
Term_WT193	60350	Aug 25 2004 13:08:08	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	59083	Aug 24 2004 15:12:18	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.
Term_WT193	59080	Aug 24 2004 15:11:44	Switch	1	⚠ Warning	FABR-1001	port 22, Incompatible Secu
Term_WT193	59081	Aug 24 2004 15:11:44	Switch	1	⚠ Warning	FABR-1001	port 9, Incompatible Securi
Term_WT193	59082	Aug 24 2004 15:11:44	Switch	1	⚠ Warning	FABR-1001	port 28, Incompatible Secu
Term_WT193	59034	Aug 24 2004 14:24:31	Chassis	1	⚠ Warning	HIL-1401	One fan FRU missing.

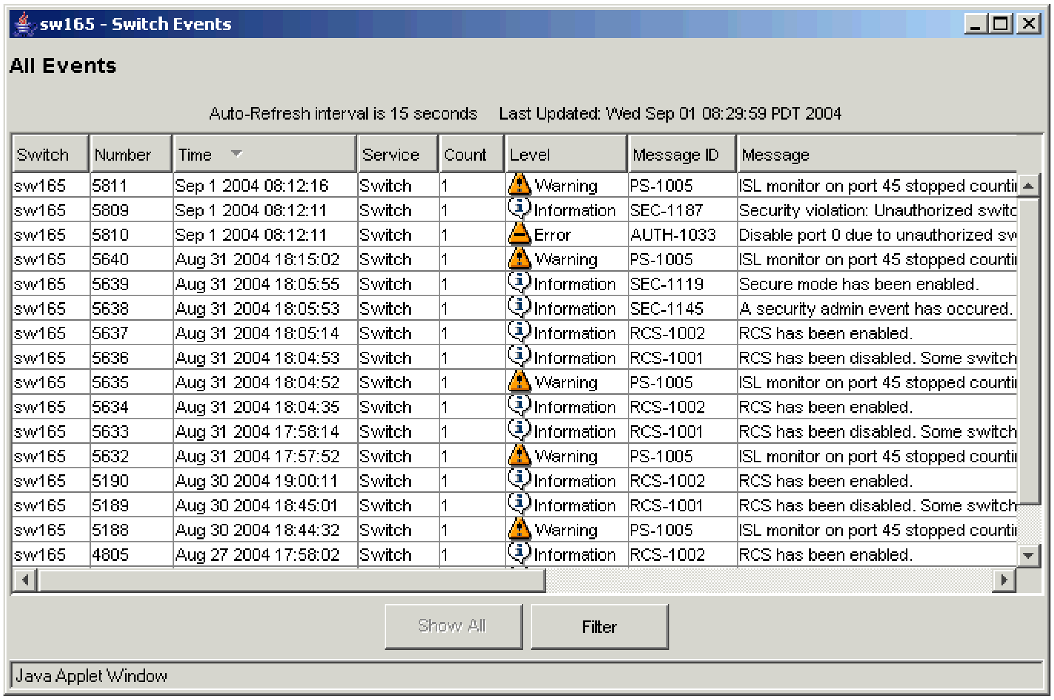
Displaying Switch Events

The Switch Events window displays a running log of events for the selected switch (see Figure 4-2). Switch events are polled and updated every 15 seconds, so there is no refresh-on-demand option for switch events, as there is for the fabric events.

Note

For two-switch configurations, all chassis-related events are displayed in the event list of each logical switch for convenience.

Figure 4-2 Switch Events View



sw165 - Switch Events

All Events

Auto-Refresh interval is 15 seconds Last Updated: Wed Sep 01 08:29:59 PDT 2004

Switch	Number	Time	Service	Count	Level	Message ID	Message
sw165	5811	Sep 1 2004 08:12:16	Switch	1	⚠ Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5809	Sep 1 2004 08:12:11	Switch	1	ⓘ Information	SEC-1187	Security violation: Unauthorized switc
sw165	5810	Sep 1 2004 08:12:11	Switch	1	⚠ Error	AUTH-1033	Disable port 0 due to unauthorized sw
sw165	5640	Aug 31 2004 18:15:02	Switch	1	⚠ Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5639	Aug 31 2004 18:05:55	Switch	1	ⓘ Information	SEC-1119	Secure mode has been enabled.
sw165	5638	Aug 31 2004 18:05:53	Switch	1	ⓘ Information	SEC-1145	A security admin event has occured.
sw165	5637	Aug 31 2004 18:05:14	Switch	1	ⓘ Information	RCS-1002	RCS has been enabled.
sw165	5636	Aug 31 2004 18:04:53	Switch	1	ⓘ Information	RCS-1001	RCS has been disabled. Some switch
sw165	5635	Aug 31 2004 18:04:52	Switch	1	⚠ Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5634	Aug 31 2004 18:04:35	Switch	1	ⓘ Information	RCS-1002	RCS has been enabled.
sw165	5633	Aug 31 2004 17:58:14	Switch	1	ⓘ Information	RCS-1001	RCS has been disabled. Some switch
sw165	5632	Aug 31 2004 17:57:52	Switch	1	⚠ Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	5190	Aug 30 2004 19:00:11	Switch	1	ⓘ Information	RCS-1002	RCS has been enabled.
sw165	5189	Aug 30 2004 18:45:01	Switch	1	ⓘ Information	RCS-1001	RCS has been disabled. Some switch
sw165	5188	Aug 30 2004 18:44:32	Switch	1	⚠ Warning	PS-1005	ISL monitor on port 45 stopped countii
sw165	4805	Aug 27 2004 17:58:02	Switch	1	ⓘ Information	RCS-1002	RCS has been enabled.

To display switch events

1. Click the switch from the Fabric Tree.

   The Switch View displays.

2. Click the **Events** button Events from the Switch View.

   The Switch Events window displays (see Figure 4-2).

3. *Optional*: Click the column head to sort the events by a particular column. Drag the column divider to resize a column.

You can also filter switch events, as described in “Filtering Fabric and Switch Events” on page 4-4.

Filtering Fabric and Switch Events

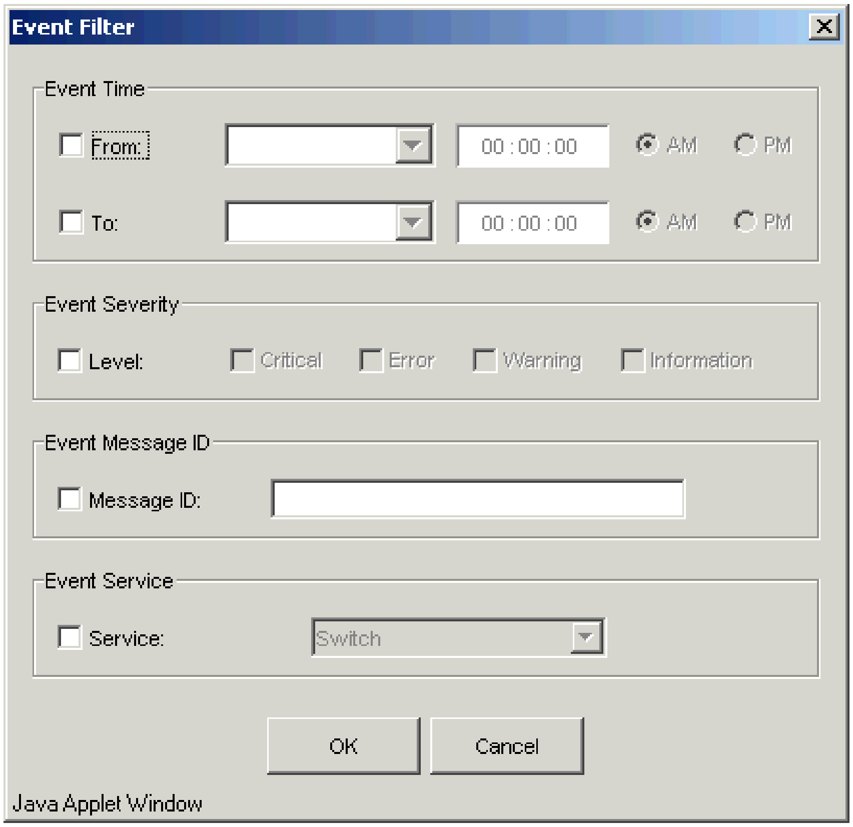
You can filter the events in the Fabric Events window and Switch Events window by time, severity, message ID, and service. You can apply either one type of filter at a time or multiple types of filters at the same time. The Switch and Fabric Events windows both have a **Filter** button. Click the **Filter** button to display the Filter Events dialog (see Figure 4-3 on page 4-5).

When a filter is applied, the **Show All** button is active in the events window and the type of filter applied is identified at the top of the events window (see Figure 4-2). To unapply a filter, click the **Show All** button in the events window.

Note

For two-switch configurations, clicking the Events button for a given switch automatically filters out switch service events from the other switch. Chassis service is shown in both events lists.

Figure 4-3 Event Filter Dialog



To filter events by time intervals

1. Launch the Fabric or Switch Events window as described in "Displaying Fabric Events" on page 4-2 or "Displaying Switch Events" on page 4-3.
2. Click **Filter**.

   The Event Filter dialog displays.
3. To filter events within a certain time period:
   a. Click **From** and enter the start time and date in the fields.
   b. Click **To** and enter the finish time and date in the fields.
4. To filter all events beginning at a certain date and time, click **From** and enter the start time and date in the fields.
5. To filter events up until a certain date and time, click **To** and enter the finish time and date in the fields.
6. Click **OK**.

The filter is enabled and the enabled filter type is displayed in the events window.

To filter events by event severity levels

1. Launch the Fabric or Switch Events window as described in "Displaying Fabric Events" on page 4-2 or "Displaying Switch Events" on page 4-3.
2. Click **Filter**.

   The Event Filter dialog displays.
3. Click **Level**.

   The event severity level checkboxes are enabled.
4. Click the event levels you want to display.
5. Click **OK**.

The filter is enabled and the enabled filter type is displayed in the events window.

To filter events by message ID

1. Launch the Fabric or Switch Events window as described in "Displaying Fabric Events" on page 4-2 or "Displaying Switch Events" on page 4-3.
2. Click **Filter**.

   The Event Filter dialog displays.
3. Click **Message ID**.
4. Type the message IDs in the associated field. You can enter multiple message IDs as long as you separate them by commas. You can type either the full message ID (moduleID-messageType) or a partial ID (moduleID only).
5. Click **OK**.

The filter is enabled and the enabled filter type is displayed in the events window.

To filter events by service component

1. Launch the Fabric or Switch Events window as described in "Displaying Fabric Events" on page 4-2 or "Displaying Switch Events" on page 4-3.
2. Click **Filter**.

   The Event Filter dialog displays.
3. Click **Event Service**.

   The event service drop-down list is enabled.
4. Select either "Switch" or "Chassis" from the drop-down list to show only those messages from the logical switch or from the chassis.
5. Click **OK**.

The filter is enabled and the enabled filter type is displayed in the events window.

Displaying a Fabric Topology Report

A fabric topology report lists all of the domains in the fabric and the active paths for each domain. A sample fabric topology report is shown in Figure 4-4 on page 4-7.

To view a fabric topology report

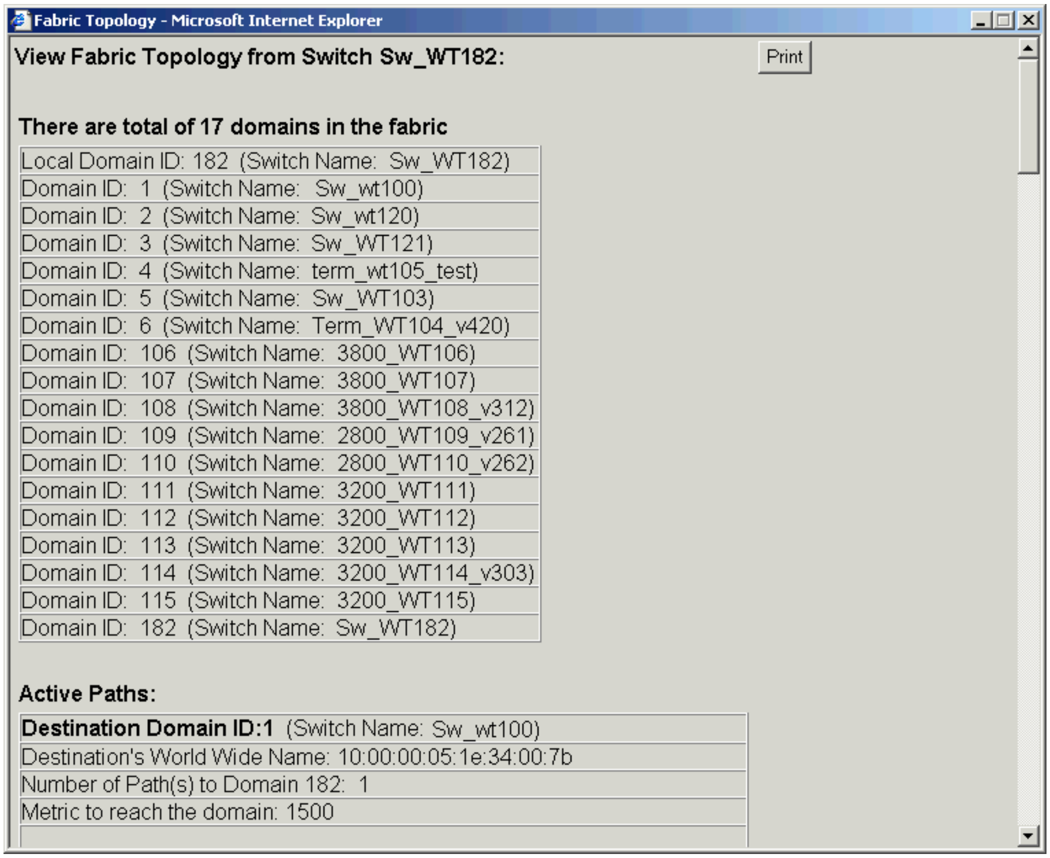
1. Click the **Fabric Topology** icon on the Fabric Toolbar.

   The Fabric Topology window displays.

2. Click the **Print** button to print a topology report.

   A **Print** button is located at the top and bottom of the report. Both **Print** buttons have the same function.

Figure 4-4 Fabric Topology Report



View Fabric Topology from Switch Sw_WT182:

There are total of 17 domains in the fabric

Local Domain ID: 182 (Switch Name: Sw_WT182)
Domain ID: 1 (Switch Name: Sw_wt100)
Domain ID: 2 (Switch Name: Sw_wt120)
Domain ID: 3 (Switch Name: Sw_WT121)
Domain ID: 4 (Switch Name: term_wt105_test)
Domain ID: 5 (Switch Name: Sw_WT103)
Domain ID: 6 (Switch Name: Term_WT104_v420)
Domain ID: 106 (Switch Name: 3800_WT106)
Domain ID: 107 (Switch Name: 3800_WT107)
Domain ID: 108 (Switch Name: 3800_WT108_v312)
Domain ID: 109 (Switch Name: 2800_WT109_v261)
Domain ID: 110 (Switch Name: 2800_WT110_v262)
Domain ID: 111 (Switch Name: 3200_WT111)
Domain ID: 112 (Switch Name: 3200_WT112)
Domain ID: 113 (Switch Name: 3200_WT113)
Domain ID: 114 (Switch Name: 3200_WT114_v303)
Domain ID: 115 (Switch Name: 3200_WT115)
Domain ID: 182 (Switch Name: Sw_WT182)

Active Paths:

Destination Domain ID:1 (Switch Name: Sw_wt100)
Destination's World Wide Name: 10:00:00:05:1e:34:00:7b
Number of Path(s) to Domain 182: 1
Metric to reach the domain: 1500

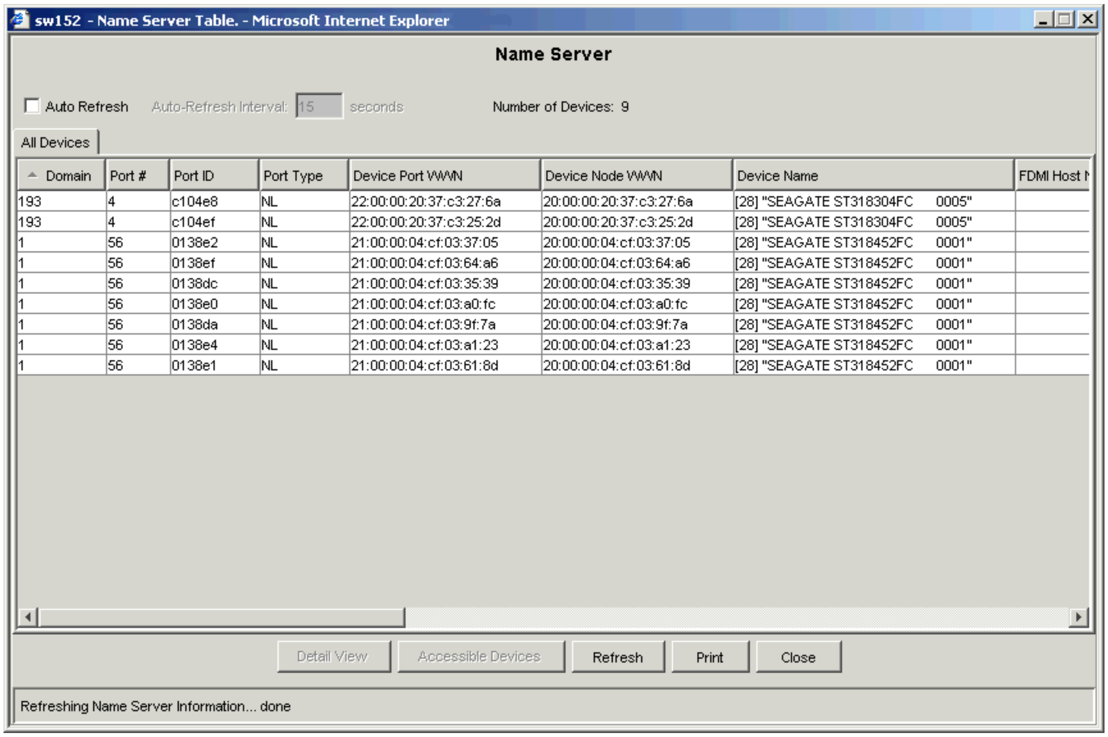
Displaying the Name Server Entries

Web Tools displays Name Server entries listed in the Simple Name Server database (see Figure 4-5). This includes all Name Server entries for the fabric, not only those related to the local domain. Each row in the table represents a different device.

Note
Name Server entries are not automatically polled by default. You must click **Refresh** from the Name Server view to poll Name Server entries.

You can also specify a time interval at which the Name Server entries will be automatically refreshed.

Figure 4-5 Name Server View



□ Auto Refresh   Auto-Refresh Interval: 15 seconds   Number of Devices: 9

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	FDMI Host N
193	4	c104e8	NL	22:00:00:20:37:c3:27:6a	20:00:00:20:37:c3:27:6a	[28] "SEAGATE ST318304FC 0005"	
193	4	c104ef	NL	22:00:00:20:37:c3:25:2d	20:00:00:20:37:c3:25:2d	[28] "SEAGATE ST318304FC 0005"	
1	56	0138e2	NL	21:00:00:04:cf:03:37:05	20:00:00:04:cf:03:37:05	[28] "SEAGATE ST318452FC 0001"	
1	56	0138ef	NL	21:00:00:04:cf:03:64:a6	20:00:00:04:cf:03:64:a6	[28] "SEAGATE ST318452FC 0001"	
1	56	0138dc	NL	21:00:00:04:cf:03:35:39	20:00:00:04:cf:03:35:39	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e0	NL	21:00:00:04:cf:03:a0:fc	20:00:00:04:cf:03:a0:fc	[28] "SEAGATE ST318452FC 0001"	
1	56	0138da	NL	21:00:00:04:cf:03:9f:7a	20:00:00:04:cf:03:9f:7a	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e4	NL	21:00:00:04:cf:03:a1:23	20:00:00:04:cf:03:a1:23	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e1	NL	21:00:00:04:cf:03:61:8d	20:00:00:04:cf:03:61:8d	[28] "SEAGATE ST318452FC 0001"	

Refreshing Name Server Information... done

To view a list of the switches in the Name Server

1. Click the **Name Server** icon from the Fabric Toolbar.

   The Name Server Table displays.

2. *Optional*: Check the **Auto Refresh** checkbox from the Name Server window.

3. *Optional*: Enter an autorefresh interval (in seconds), at a minimum of 15 seconds. The Name Server entries will refresh at the rate you set.

To print the Name Server entries

1. Click the **Name Server** icon from the Fabric Toolbar.

   The Name Server Table displays.

2. Click **Print**.
3. The Page Setup dialog displays. Make changes, as appropriate.
4. Click **OK** in the Page Setup dialog.

   The Print dialog displays.
5. Select a printer and click **OK** in the Print dialog.

To display detailed Name Server information for a particular device

1. Click the **Name Server** icon ▦ from the Fabric Toolbar.

   The Name Server Table displays.
2. Click a device from the Domain column.
3. Click **Detail View**.

The Name Server Information dialog displays information specific to that device.

To display the zone members of a particular device

1. Click the **Name Server** icon ▦ from the Fabric Toolbar.

   The Name Server Table displays.
2. Click a device from the Domain column.
3. Click **Accessible Devices**.

The Zone Accessible Devices window displays accessible zone member information specific to that device.

Displaying Switch Information

This section describes how to display information about the physical components of the switch (such as fan, temperature, and power supply) as well as how to display other detailed switch information (such as firmware and IP address).

Displaying Detailed Fan Hardware Status

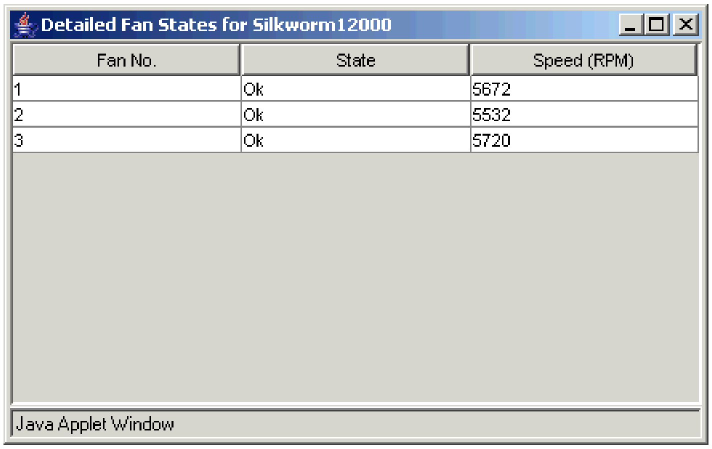
The background color of the **Fan** button indicates the overall status of the fans. For more information about the switch fan, refer to the appropriate hardware documentation.

Note

The SilkWorm 3016 Switch View does not have a **Fan** button as there are no fan FRUs in this embedded switch.

You can display status information about the fans, as shown in Figure 4-6 on page 4-10.

Figure 4-6 Fan Status Window



Detailed Fan States for Silkworm12000

Fan No.	State	Speed (RPM)
1	Ok	5672
2	Ok	5532
3	Ok	5720

Java Applet Window

Note that the **Fan No.** column indicates either the fan number or the fan FRU number, depending on the switch model. A fan FRU can contain one or more fans.

- For the SilkWorm 12000 and 24000 directors and the SilkWorm 4100 switch, the **Fan No.** column indicates the fan FRU number.
- For the SilkWorm 3900, the **Fan No.** column indicates the fan number.
- The SilkWorm 3250 and 3850 switches do not contain fan FRUs, so for these switch models, the **Fan No.** column indicates the fan number.

To display the fan status detail

1. Select a switch from the Fabric Toolbar.

   The selected switch appears in the Switch View. The background color of the **Fan** button indicates the overall status of the fan.

2. Click the **Fan** button Fan from the Switch View.

The detailed fan status for the switch is displayed, as shown in Figure 4-6.

Displaying the Temperature Status

The background color of the **Temp** button indicates the overall status of the temperature. For more information regarding switch temperature, refer to the appropriate hardware documentation.

To display the temperature status detail

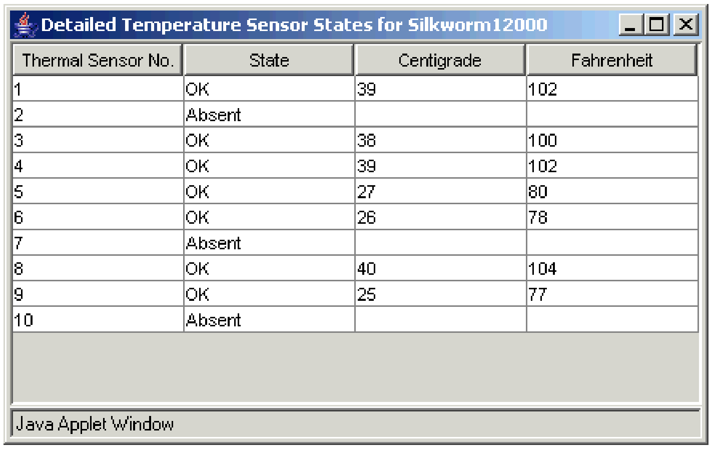
1. Select a switch from the Fabric Toolbar.

   The selected switch appears in the Switch View. The background color of the **Temp** button indicates the overall status of the temperature.

2. Click the **Temp** button Temp from the Switch View.

The detailed temperature sensor states for the switch are displayed, as shown in Figure 4-7 on page 4-11.

Figure 4-7 Temperature Status Window



Detailed Temperature Sensor States for Silkworm12000

Thermal Sensor No.	State	Centigrade	Fahrenheit
1	OK	39	102
2	Absent		
3	OK	38	100
4	OK	39	102
5	OK	27	80
6	OK	26	78
7	Absent		
8	OK	40	104
9	OK	25	77
10	Absent		

Java Applet Window

Displaying the Power Supply Status

The background color of the **Power** button indicates the overall status of the power supply status. For more information regarding switch power modules, refer to the appropriate hardware documentation.

Note
The SilkWorm 3016 Switch View does not have a **Power** button as there are no power supply FRUs in this embedded switch.

To display the power supply status detail

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View. The background color of the Power button indicates the overall status of the power supply.

2. Click the **Power** button Power from the Switch View.

The detailed power supply states are displayed for the switch.

Checking the Physical Health of a Switch

The **Status** button Status displays the operational state of the switch. The background color of the button displays the real-time status of the switch. Refer to the Status Legend for the meaning of the background colors.

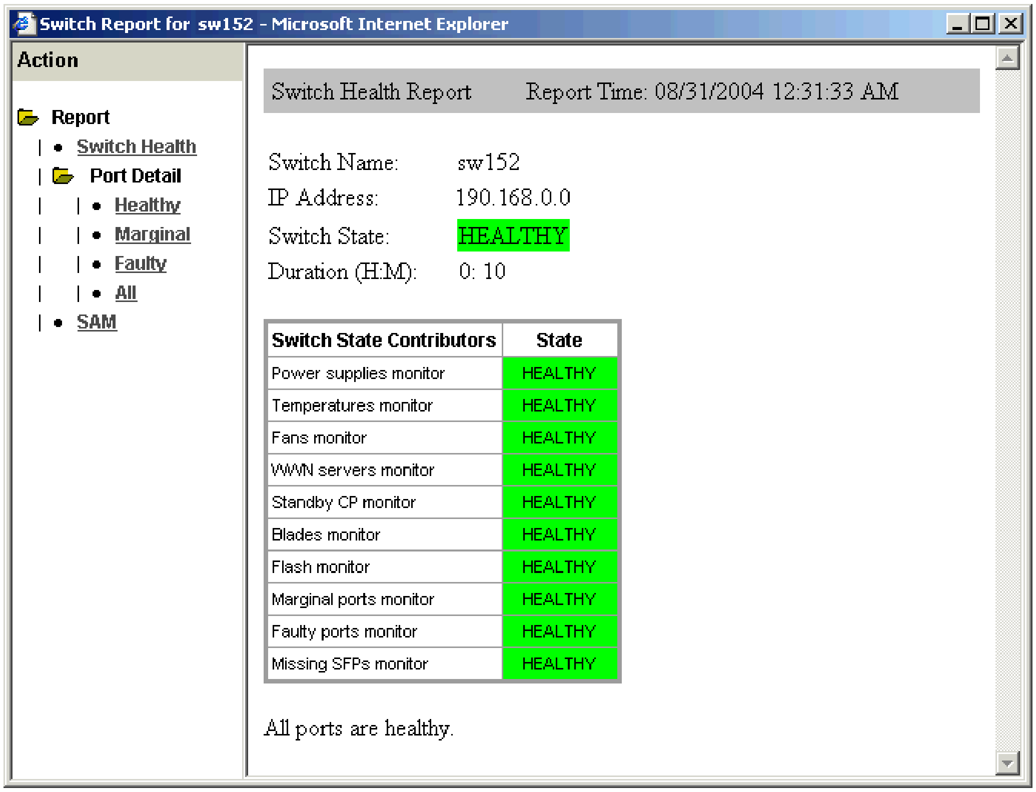
If no data is available from a switch, the most recent background color remains displayed.

For all statuses that are based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

If the switch status is marginal or critical, information on the trigger that caused that status is displayed in the Switch Information view.

Click the **Status** button to display a detailed, customizable switch status report, as shown in Figure 4-8 on page 4-12.

Figure 4-8 Switch Report



Switch Report for sw152 - Microsoft Internet Explorer

Action

- Report
  - Switch Health
  - Port Detail
    - Healthy
    - Marginal
    - Faulty
    - All
  - SAM

Switch Health Report Report Time: 08/31/2004 12:31:33 AM

Switch Name: sw152
IP Address: 190.168.0.0
Switch State: HEALTHY
Duration (H:M): 0: 10

Switch State Contributors	State
Power supplies monitor	HEALTHY
Temperatures monitor	HEALTHY
Fans monitor	HEALTHY
WWN servers monitor	HEALTHY
Standby CP monitor	HEALTHY
Blades monitor	HEALTHY
Flash monitor	HEALTHY
Marginal ports monitor	HEALTHY
Faulty ports monitor	HEALTHY
Missing SFPs monitor	HEALTHY

All ports are healthy.

To display a detailed switch status report

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View. The background color of the Status button indicates the overall status of the switch.

2. Click the **Status** button Status from the Switch View.

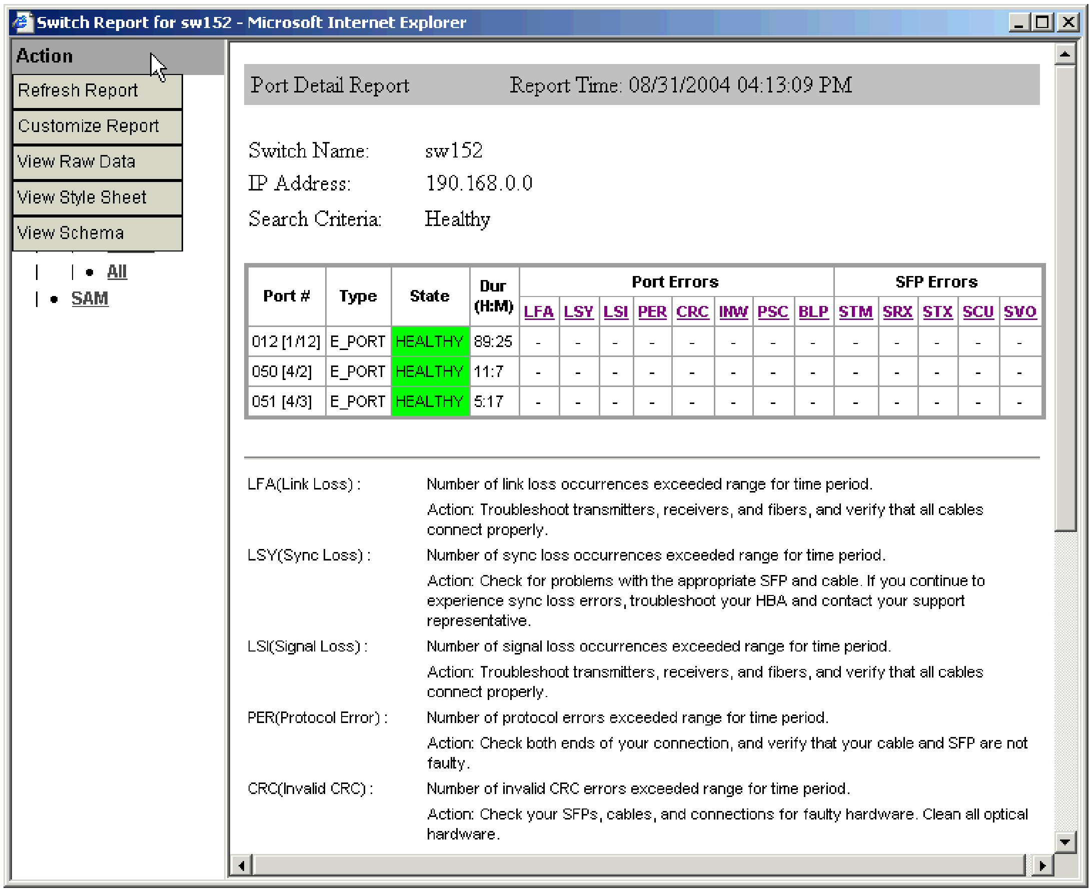
   The detailed switch health report is displayed, as shown in Figure 4-8.

3. *Optional*: Click the underlined links in the left panel to display detailed information about ports and Switch Availability Monitoring (SAM).

4. *Optional*: Mouse-over the Action field (see Figure 4-9 on page 4-13) and click an action to:

   - refresh the information displayed in the report
   - customize the report
   - view the data in raw XML format
   - view the style sheet for the report
   - view the XML schema for the report

Figure 4-9 Switch Report Action Menu



Port Detail Report Report Time: 08/31/2004 04:13:09 PM

Switch Name: sw152
IP Address: 190.168.0.0
Search Criteria: Healthy

Port #	Type	State	Dur (H:M)	Port Errors								SFP Errors				
				LFA	LSY	LSI	PER	CRC	INW	PSC	BLP	STM	SRX	STX	SCU	SVO
012 [1/12]	E_PORT	HEALTHY	89:25	-	-	-	-	-	-	-	-	-	-	-	-	-
050 [4/2]	E_PORT	HEALTHY	11:7	-	-	-	-	-	-	-	-	-	-	-	-	-
051 [4/3]	E_PORT	HEALTHY	5:17	-	-	-	-	-	-	-	-	-	-	-	-	-

LFA(Link Loss) : Number of link loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

LSY(Sync Loss) : Number of sync loss occurrences exceeded range for time period.
Action: Check for problems with the appropriate SFP and cable. If you continue to experience sync loss errors, troubleshoot your HBA and contact your support representative.

LSI(Signal Loss) : Number of signal loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

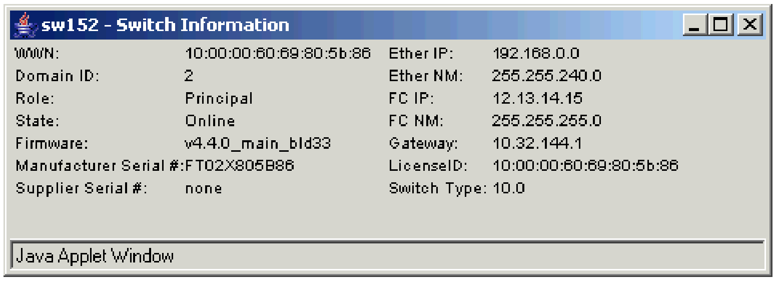
PER(Protocol Error) : Number of protocol errors exceeded range for time period.
Action: Check both ends of your connection, and verify that your cable and SFP are not faulty.

CRC(Invalid CRC) : Number of invalid CRC errors exceeded range for time period.
Action: Check your SFPs, cables, and connections for faulty hardware. Clean all optical hardware.

Displaying Detailed Switch Information

The **Info** button in the Switch View displays detailed switch information, as shown in Figure 4-10.

Figure 4-10 Switch Information View



WWN:	10:00:00:60:69:80:5b:86	Ether IP:	192.168.0.0
Domain ID:	2	Ether NM:	255.255.240.0
Role:	Principal	FC IP:	12.13.14.15
State:	Online	FC NM:	255.255.255.0
Firmware:	v4.4.0_main_bld33	Gateway:	10.32.144.1
Manufacturer Serial #:	FT02X805B86	LicenseID:	10:00:00:60:69:80:5b:86
Supplier Serial #:	none	Switch Type:	10.0

To display detailed switch information

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Info** button Info.

The Switch Information window is displayed.

Physically Locating a Switch Using Beaconing

Use the **Beacon** button to physically locate a switch in a fabric. The beaconing function helps to physically locate a switch by sending a signal to the specified switch, resulting in an LED light pattern that cycles through all ports for each switch (from left to right).

To enable beaconing

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Beacon** button Beacon on the Switch View.

   The LED lights on the actual switch (selected in the GUI) light up on the physical switch in a pattern running back and forth across the switch itself. The beaconing is not shown in the GUI.

3. Look at the physical switches in your installation location to identify the switch.

Displaying Port Information

The Switch View displays port graphics with blinking LEDs, simulating the physical appearance of the ports. One of the LEDs indicates port status; the other indicates port speed. For LED information, refer to the hardware documentation for the switch you are viewing.

The background color of the port icon indicates the port status, as follows:

- green (healthy)
- yellow (marginal)
- red (critical)
- gray (unmonitored)

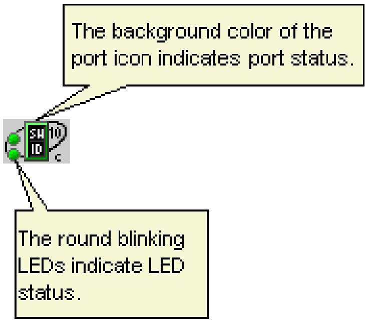
If the entire port icon is blue, the port is buffer-limited.

If a group of port icons is grayed out, those ports are not licensed.

The port status is also indicated in the Port Information screen in the Port Health field for the selected port.

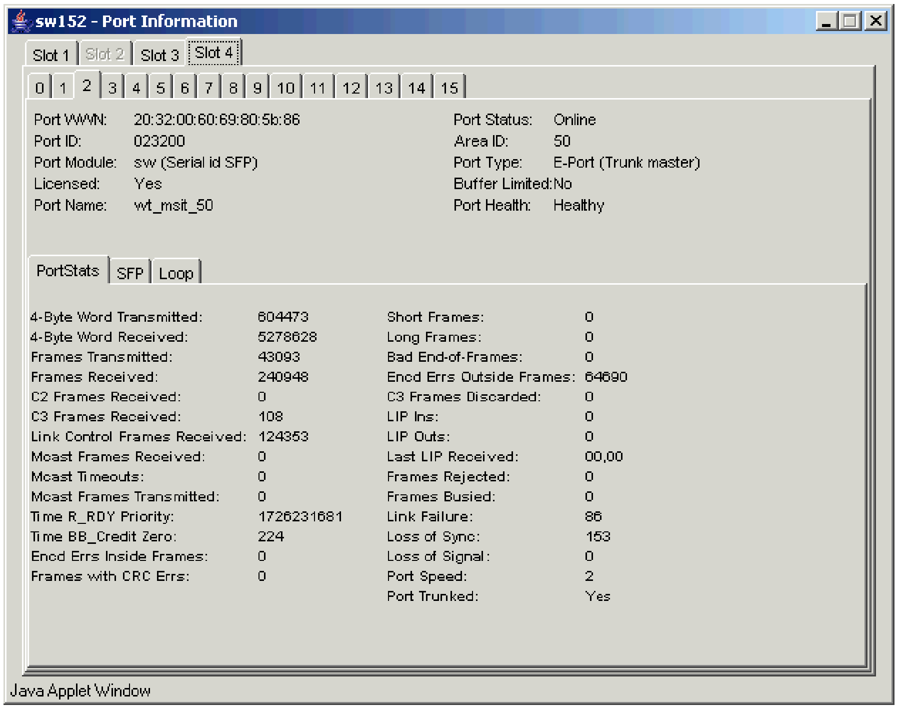
Figure 4-11 on page 4-15 shows a port icon and associated LEDs from a SilkWorm 12000 director.

Figure 4-11 Port and LED Status Color-Coded Information in the Port Icon in Switch View


The background color of the port icon indicates port status.
The round blinking LEDs indicate LED status.

The Port Information screen displays statistics and status for the selected port, SFP, or loop, as shown in Figure 4-12 on page 4-15. Access the Port Information screen by clicking any of the ports in the Switch View.

Figure 4-12 Port Information Screen



```
Port WWN:     20:32:00:60:69:80:5b:86          Port Status:    Online
Port ID:      023200                           Area ID:        50
Port Module:  sw (Serial id SFP)               Port Type:      E-Port (Trunk master)
Licensed:     Yes                              Buffer Limited:No
Port Name:    wt_msit_50                       Port Health:    Healthy

4-Byte Word Transmitted:      604473        Short Frames:               0
4-Byte Word Received:         5278628       Long Frames:                0
Frames Transmitted:           43093         Bad End-of-Frames:          0
Frames Received:              240948        Encd Errs Outside Frames:   64690
C2 Frames Received:           0             C3 Frames Discarded:        0
C3 Frames Received:           108           LIP Ins:                    0
Link Control Frames Received: 124353        LIP Outs:                   0
Mcast Frames Received:        0             Last LIP Received:          00,00
Mcast Timeouts:               0             Frames Rejected:            0
Mcast Frames Transmitted:     0             Frames Busied:              0
Time R_RDY Priority:          1726231681    Link Failure:               86
Time BB_Credit Zero:          224           Loss of Sync:               153
Encd Errs Inside Frames:      0             Loss of Signal:             0
Frames with CRC Errs:         0             Port Speed:                 2
                                            Port Trunked:               Yes
```

The number of slots displayed in the Port Information screen depends on the model of switch the port is on.

For example, each logical switch in the SilkWorm 12000 director (and the SilkWorm 24000 director, if it is configured for two logical switches) has four slots. For these switch types, a subtab is displayed for each physically inserted and powered on slot in the Port Information screen. You must first click the slot tab and then the port tab for that slot.

For the SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, there are no subtabs for the slots. There is just a port tab for each port.

To access the Port Information screen

1. Select a switch from the Fabric Tree.

   The selected switch displays in the Switch View.

2. Click the port icon for which you want to view information.

   The Port Information screen displays.

3. This step is switch-specific:

   For SilkWorm 12000 and 24000 directors, click the slot tab that corresponds to the correct slot for the logical switch.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed directly to the next step.

4. Click the port tab.
5. *Optional*: To view additional port information, click one of the subtabs for each port: **PortStats**, **SFP**, or **Loop**.

Displaying Swapped Port Area IDs

Use this procedure to *view* swapped ports on the switch. You cannot *swap* ports using Web Tools: you can swap ports using the Fabric OS CLI only.

To determine if a port area ID has been swapped with another switch port

1. Launch the Switch Admin module as described in "Launching the Switch Admin Module" on page 3-2.
2. Click the **Ports** tab.
3. View the Port (Area ID) column in the Port Settings tab. For ports that have been swapped, the port number is followed by the area ID, in parentheses.

Chapter

5

Zone Administration

This chapter briefly describes zoning and provides the procedures for managing zoning using Brocade Advanced Web Tools. It contains the following sections:

Introduction to Zoning

Zoning enables you to partition your storage area network (SAN) into logical groups of devices that can access each other. For example, you can partition your SAN into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage.

Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

When using a mixed fabric—that is, a fabric containing v4.x, v3.x and v2.x switches—you should use the most advanced switches to perform zoning tasks.

When zone or Fabric Assist (FA) zone members are specified by fabric location (domain, area) *only*, or by device name (node name or port WWN) *only*, then zone boundaries can be enforced at the hardware level, and the zone is referred to as a "hard zone."

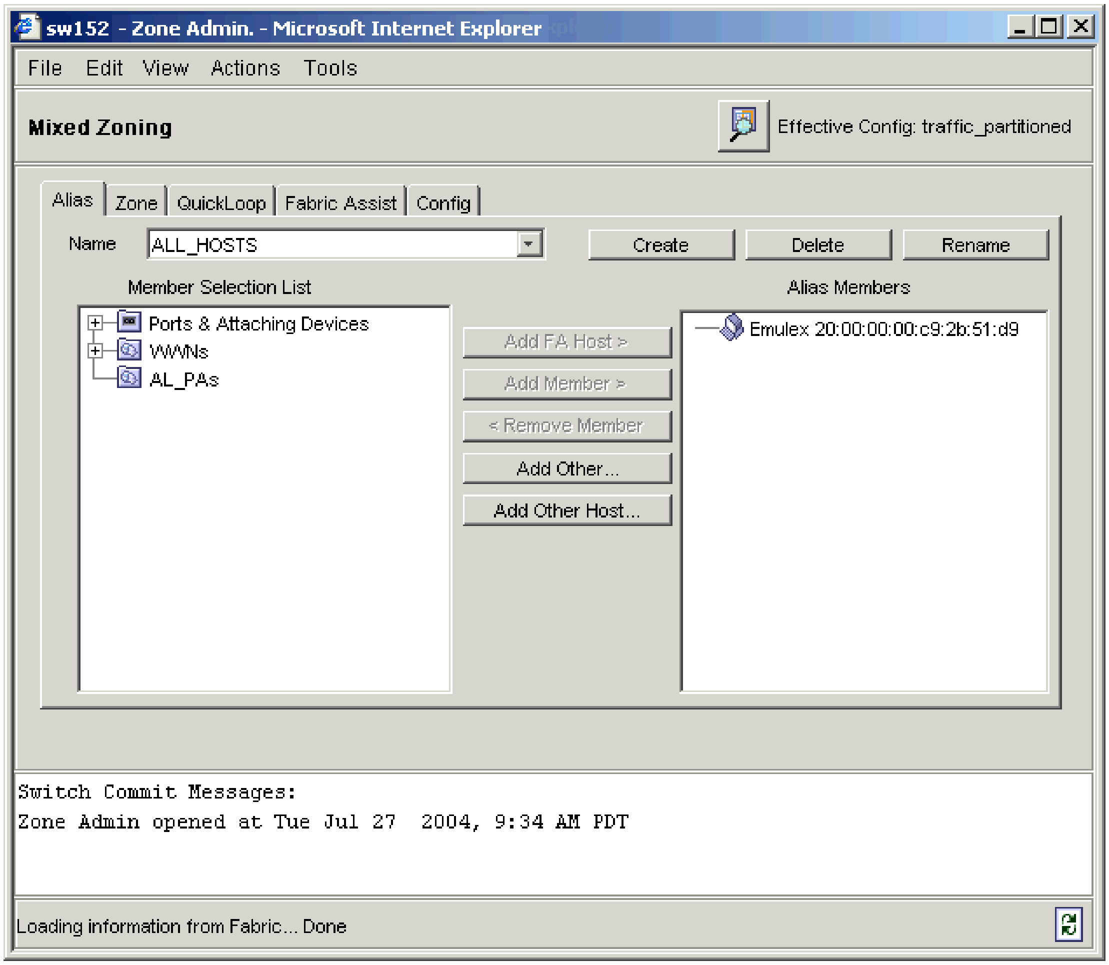
When zone elements are specified by fabric location (domain, area) *and other elements of the same zone* are specified by device name (node name or port WWN), zone enforcement depends on Name Server lookups, and the zone is referred to as a "soft zone."

For more specific information about zoning concepts, refer to the *Brocade Fabric OS Features Guide*.

Managing Zoning with Advanced Web Tools

You can monitor and manage zoning through the Web Tools Zone Admin module. Click the Zone Administration icon in the Fabric Toolbar to access the Zone Admin module, shown in Figure 5-1. The Zone Admin icon is displayed in the Fabric Toolbar only if an Advanced Zoning license is installed on the switch.

Figure 5-1 Zone Admin Module



sw152 - Zone Admin. - Microsoft Internet Explorer
File Edit View Actions Tools
Alias Zone QuickLoop Fabric Assist Config
Create
Delete
Rename
Member Selection List
Ports & Attaching Devices
WWNs
AL_PAs
Add FA Host >
Add Member >
< Remove Member
Add Other...
Add Other Host...
Alias Members

Mixed Zoning

Effective Config: traffic_partitioned

Name: ALL_HOSTS

Alias Members: Emulex 20:00:00:00:c9:2b:51:d9

```
Switch Commit Messages:
Zone Admin opened at Tue Jul 27  2004, 9:34 AM PDT
```

Loading information from Fabric... Done

The information in the Zone Admin module is collected from the selected switch.

If secure mode is enabled, zoning can be administered only from the primary FCS switch. If the selected switch has an Advanced Zoning license installed but is not the primary FCS switch, the Zone Admin icon is displayed in the Fabric Toolbar but not activated. For specific information regarding secure fabrics, refer to the *Brocade Secure Fabric OS User's Guide*.

When you click the Zone Admin icon from the Fabric Toolbar, you must log in as an admin to launch the Zone Admin module. A snapshot is taken of all the zoning configurations at the time you launch the Zone Admin module; this information is *not* updated automatically by Web Tools. To update this information, refer to "Refreshing the Zone Admin Module Information" on page 5-4.

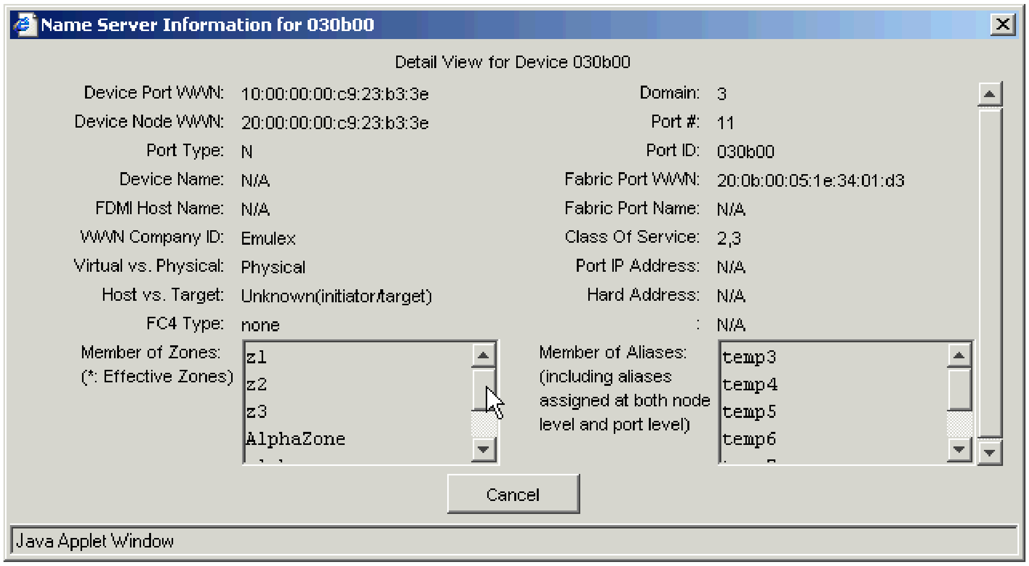
Caution

Any changes you make in the Zone Admin module are held in a buffered environment and do *not* update the zoning database until you save the changes. If you close the Zone Admin module without saving your changes, your changes are lost. To save the buffered changes you make in the Zone Admin module to the zoning database on the switch, refer to "Saving Local Zoning Changes" on page 5-5.

"Saving" means updating the zoning database on the switch with the local changes from the Web Tools buffer. "Refreshing" means copying the current state of the zoning database on the switch to the Web Tools buffer, overwriting its current contents.

In the Zone Admin module, all WWNs also display vendor names. In the Member Selection List panel (see Figure 5-1), you can right-click port and device nodes to display which aliases the port or device is a member of. In addition, you can right-click the device nodes and click **View Device Detail** to display detailed information about the selected device, as shown in Figure 5-2.

Figure 5-2 Device Detail View Example



Name Server Information for 030b00

Detail View for Device 030b00

Device Port WWN:	10:00:00:00:c9:23:b3:3e	Domain:	3
Device Node WWN:	20:00:00:00:c9:23:b3:3e	Port #:	11
Port Type:	N	Port ID:	030b00
Device Name:	N/A	Fabric Port WWN:	20:0b:00:05:1e:34:01:d3
FDMI Host Name:	N/A	Fabric Port Name:	N/A
WWN Company ID:	Emulex	Class Of Service:	2,3
Virtual vs. Physical:	Physical	Port IP Address:	N/A
Host vs. Target:	Unknown(initiator/target)	Hard Address:	N/A
FC4 Type:	none	:	N/A
Member of Zones: (*: Effective Zones)	z1 z2 z3 AlphaZone	Member of Aliases: (including aliases assigned at both node level and port level)	temp3 temp4 temp5 temp6

Note

In the Device Detail view, the scroll bars in the Member of Zones and Member of Aliases sections do not scroll unless you double-click them first.

The remainder of this section describes basic zoning procedures you can do in the Zone Admin module that are useful for all zoning operations.

Launching the Zone Admin Module

This section describes how to launch the Zone Admin module, from which all zoning procedures are performed.

To launch the Zone Administration module

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Zone Administration** icon in the Fabric Toolbar.

   The login dialog displays.

3. Type the user name of an account with the admin role.

4. Type the password.

   The Zone Admin module displays (see Figure 5-1).

Refreshing the Fabric Information

This function refreshes the display of *fabric* elements (switches, ports, devices, and AL_PAs) *only*. It does not affect any *zoning* element changes or update zone information in the Zone Admin module. To refresh the zone information displayed in the Zone Admin module, refer to “Refreshing the Zone Admin Module Information,” next.

This option allows you to refresh the fabric element information displayed at any time.

To refresh the fabric information

1. In the Zone Admin module, click **View** > **Refresh Fabric**.

   This refreshes the status for the fabric, including switches, ports, and devices.

Refreshing the Zone Admin Module Information

The information displayed in the Zone Admin module is initially a snapshot of the contents of the fabric zoning database at the time the module is launched. Any changes you make to this view are saved to a local buffer; they are not applied to the fabric zoning database until you invoke one of the transactional operations listed in the Actions menu.

Any local zoning changes are buffered by the Zone Admin module until explicitly saved to the fabric, if the fabric zoning database is independently changed by another user or from another interface (for example, the CLI) while Web Tools zoning changes are still pending, the refresh icon starts to blink (after a 15 second polling delay). You can then choose to refresh the current Web Tools zoning view to reflect the new, externally changed contents of the fabric zoning database, in which case any pending local changes are lost, or you can ignore the blinking refresh icon and save your local changes, overwriting the external changes that triggered the icon to blink.

Another reason to refresh zoning is to back out of current, unsaved work and start over.

You can refresh the zoning information at any time, either using the refresh icon (whether it is flashing or not) or from the View menu.

The following procedure updates the information in the Zone Admin module with the information saved in the zoning database on the switch.

Caution

When you refresh the buffered information in the Zone Admin module, any zoning configuration changes you have made *and not yet saved* are erased from the buffer and replaced with the currently enabled zone configuration information that is saved on the switch.

To refresh the local Zone Admin buffer from the fabric zoning database

1. Launch the Zone Admin module as described on page 5-3.
2. Click **View** > **Refresh Zoning** or click the zone refresh icon (located in the lower right corner of the Zone Admin module).

This refreshes the information in the Zone Admin module with the information in the switch's zoning database. This action also refreshes the fabric information as described in "Refreshing the Fabric Information" on page 5-4. Any unsaved zoning changes are deleted.

Saving Local Zoning Changes

All information displayed and all changes made in the Zone Admin module are buffered until you save the changes. That means that any other user looking at the zone information for the switch will not see the changes you have made until you save them. Saving the changes propagates any changes you have made in the Zone Admin module (buffered changes) to the zoning database on the switch. If another user has a zoning operation in progress at the time that you attempt to save changes, a warning is displayed that indicates that another zoning transaction is in progress on the fabric. You can select to abort the other transaction and override it with yours.

This action updates the entire contents of the Zone Admin module, not just the selected zone, alias, or configuration. You can save your changes at any time during the zone administration session.

To save Zone Admin module changes to the switch zoning database

1. Make your zoning changes in the Zone Admin module.
2. Click **Actions** > **Save Config Only**.

Note

If you have made changes to a configuration, you must enable the configuration before the changes will be effective. To enable the configuration, refer to "Enabling a Zone Configuration" on page 5-18.

Closing the Zone Admin Module

It is very important to remember that any changes you make in the Zone Admin module are not saved automatically. It is recommended that you always close the Zone Admin module from the **File** menu, as described in the procedure below.

Caution
If you click the X in the top right corner of the Zone Admin module, the Zone Admin session is closed immediately, and any changes you made without saving are lost. To avoid potential loss of data, use the following procedure to close the Zone Admin module. In this procedure, the Zone Admin session displays a warning if you have unsaved changes when you are trying to close the Zone Admin module.

To safely close the Zone Admin module

1. From the Zone Admin module, click **File** > **Close**.

   If any changes exist in the buffer that have not been saved, a warning dialog displays, asking you to confirm that you want to close the Zone Admin session without saving the changes.

2. Click **Yes** to close without saving changes, or click **No** to go back to the Zone Admin module to save the changes as described in "Saving Local Zoning Changes" on page 5-5.

Zoning Views

You can choose how zoning elements are displayed in the Zone Admin module. The zoning view you select determines how members are displayed in the Member Selection List panel (see Figure 5-1). The views filter the fabric and device information displayed in the Member Selection List for the selected view, making it easier for you to create and modify zones, especially when creating "hard zones."

Depending on the method you use to zone, certain tabs might or might not be available in the Zone Admin window.

There are four views of defining members for zoning:

Mixed zoning — This view displays the port area number, device WWNs, or QuickLoop AL_PAs, and is useful when creating a soft zone.

Port zoning — This view displays port area numbers *only*, and is useful when creating a hard zone.

WWN zoning — This view displays device WWNs *only*, and is useful when creating a hard zone.

AL_PA zoning — This view displays QuickLoop AL_PAs only, and is useful when creating a soft zone.

To select a zoning view

1. Launch the Zone Admin module as described on page 5-3.
2. From the View menu, select one of the following:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

Managing Zone Aliases

An alias is a logical group of port area numbers, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port area number pair: for example, "2, 20"
- Device node and device port WWNs
- QuickLoop AL_PAs

Creating and Populating a Zone Alias

Use the following procedure to create a zone alias.

To create an alias

1. Launch the Zone Admin module as described on page 5-3.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning Views" on page 5-6.
3. Click the **Alias** tab.
4. Click **Create**.

   The Create New Alias dialog displays.
5. Type a name for the new alias, and click **OK** in the Create New Alias dialog.

   The new alias displays in the Name list in the Alias tab.
6. Click "+" signs in the Member Selection List to view the nested elements.

   The choices available in the Member Selection List depend on the selection made in the View menu.
7. Click elements in the Member Selection List that you want to include in your alias.

   The **Add Member** button becomes active.
8. Click **Add Member** to add alias members.

   Selected members move to the Alias Members window.
9. *Optional*: Repeat steps 7 and 8 to add more elements to your alias.
10. *Optional*: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.

Adding and Removing Members of a Zone Alias

Use the following procedure to add or remove zone alias members.

To modify the members of an alias

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Alias** tab.
3. Select the alias you want to modify from the Name drop-down list.
4. Highlight an element in the **Member Selection List** that you want to add to your alias, or highlight an element in the **Alias Members** list that you want to delete.
5. Click **Add Member** to add the selected alias member.
   Click **Remove Member** to remove the selected alias member.

Renaming a Zone Alias

Use the following procedure to change the name of a zone alias.

To rename a zone alias

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Alias** tab.
3. Select the alias you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename an Alias dialog appears.
5. Type a new alias name and click **OK**.

The alias is renamed in the Zone Admin buffer.

Deleting a Zone Alias

You can remove a zone alias from the Zone Admin buffer. When a zone alias is deleted, it is no longer a member of the zones of which it was once a member.

To delete a zone alias

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Alias** tab.
3. Select the alias you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Alias dialog displays.
5. Click **Yes**.

The selected alias is deleted from the Zone Admin buffer.

Managing Zones

A zone is a region within the fabric in which specified switches and devices can communicate. A device can only communicate with other devices connected to the fabric within its specified zone. You can specify members of a zone using the following methods:

- Alias names
- Switch domain and port area number pair: for example, “2, 20”
- WWN (device)
- QuickLoop AL_PAs (device)

Creating and Populating a Zone

Use the following procedure to create a zone.

To create a zone

1. Launch the Zone Admin module as described on page 5-3.
2. Select a format to display zoning members in the Member Selection List as described in “Zoning Views” on page 5-6.
3. Click the **Zone** tab.
4. Click **Create**.

   The Create New Zone dialog displays.
5. Enter a name for the new zone in the Create New Zone dialog, and click **OK**.

   The new zone displays in the Name list.
6. Click “+” signs in the Member Selection List to view the nested elements.

   The choices available in the Member Selection List depend on the selection made in the View menu.
7. Select an element in the Member Selection List that you want to include in your zone.

   The **Add Member** button becomes active.
8. Click **Add Member** to add the zone member.

   The selected member is moved to the Zone Members window.
9. *Optional*: Repeat steps 7 and 8 to add more elements to your zone.
10. *Optional*: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.

Adding and Removing the Members of a Zone

Use the following procedure to add or remove zone members.

To modify the members of a zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Zone** tab.
3. Select the zone you want to modify from the Name drop-down list.

   The zone members for the selected zone are listed in the Zone Members list.
4. Highlight an element in the Member Selection List that you want to include in your zone, or highlight an element in the Zone Members list that you want to delete.
5. Click **Add Member** to add a zone member.
   Click **Remove Membe**r to remove a zone member.

Renaming a Zone

Use the following procedure to change the name of a zone.

To rename a zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Zone** tab.
3. Select the zone you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a Zone dialog displays.
5. Type a new zone name and click **OK**.

The zone is renamed in the Zone Admin buffer.

Deleting a Zone

Use the following procedure to delete a zone.

To delete a zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Zone** tab.
3. Select the zone you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Zone dialog displays.
5. Click **Yes**.

The selected zone is deleted from the Zone Admin buffer.

Managing QuickLoops

QuickLoop is a Brocade software product that allows multiple ports on a switch to create a logical loop. Devices connected via QuickLoop appear to each other as if they are on the same arbitrated loop.

QuickLoop can be administered using Fabric OS v4.x versions; however, switches or directors running Fabric OS v4.x cannot be members of a QuickLoop. SilkWorm 24000 and 12000 directors and 3016, 3250, 3850, 3900, and 4100 switches cannot be members of a QuickLoop.

Note
You must have a QuickLoop license installed to create or modify a QuickLoop.

Creating a QuickLoop

Use the following procedure to create a QuickLoop.

To create a QuickLoop

1. Launch the Zone Admin module as described on page 5-3.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning Views" on page 5-6.
3. Click the **QuickLoop** tab.
4. Click **Create**.

   The Create New QuickLoop dialog displays.
5. Type a name for the new QuickLoop.
6. Click **OK**.
7. Click an element in the Member Selection List that you want to include in your QuickLoop.

   The **Add Member** button becomes active.

   Note
   There is a limit of two members per QuickLoop. Only switches capable of running QuickLoop are displayed in the Member Selection List.
8. Click **Add Member** to add QuickLoop members.

   Selected members are moved to the QuickLoop Members area.
9. *Optional*: Repeat steps 7 and 8 to add a second element to your QuickLoop.

Adding and Removing Members of a QuickLoop

Use the following procedure to add or remove members of a QuickLoop.

To modify the members of a QuickLoop

1. Launch the Zone Administration module as described on page 5-3.
2. Click the **QuickLoop** tab.
3. Select the QuickLoop you want to modify from the Name drop-down list.
4. Highlight an element in the Member Selection List that you want to include in your QuickLoop, or highlight an element in the QuickLoop Members that you want to delete.

Note
There is a limit of two members per QuickLoop. Only switches capable of running QuickLoop are displayed in the Member Selection List.

5. Click **Add Member** to add a QuickLoop member.
   Click **Remove Member** to remove a QuickLoop member.

Renaming a QuickLoop

Use the following procedure to change the name of a QuickLoop.

To rename a QuickLoop

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **QuickLoop** tab.
3. Select the QuickLoop you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a QuickLoop dialog displays.
5. Type a new QuickLoop name and click **OK**.

The QuickLoop is renamed in the Zone Admin buffer.

Deleting a QuickLoop

Use the following procedure to delete a QuickLoop.

To delete a QuickLoop

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **QuickLoop** tab.
3. Select the QuickLoop you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting QuickLoop dialog opens.
5. Click **Yes**.

The selected QuickLoop is deleted from the Zone Admin buffer.

Managing Fabric Assist Zones

Fabric Assist is an extension to QuickLoop. A Fabric Assist (FA) zone allows private hosts to communicate with public or private targets across the fabric.

Fabric Assist zones can be administered using Fabric OS v4.x versions; however, switches or directors running Fabric OS v4.x cannot be members of a Fabric Assist zone. SilkWorm 24000 and 12000 directors and 3016, 3250, 3850, 3900, and 4100 switches cannot be members of a Fabric Assist zone.

Note
You must have a QuickLoop license installed to create or modify a Fabric Assist zone.

Creating a Fabric Assist Zone

Use the following procedure to create a Fabric Assist zone. For this example, the Mixed Zone level is used.

To create a Fabric Assist zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click **View** > **Mixed Zoning**. You can select any view except the AL_PA view.

   The Mixed View tab displays.
3. Click the **Fabric Assist** tab.
4. Click **Create**.

   The Create New FA dialog displays.
5. Type a name for the new Fabric Assist zone and click **OK**.

   A fabric host is required.
6. Click the Fabric Assist zone members from the Member Selection List.
7. Click **Add Member**.

The new members appear in the Fabric Assist Members area. The newly created Fabric Assist zone also displays in the **Config** tab.

Adding and Removing Fabric Assist Zone Members

Use the following procedure to add and remove Fabric Assist zone members.

To modify the members of a Fabric Assist zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Fabric Assist** tab.

3. Select the Fabric Assist zone you want to modify from the Name drop-down list.
4. Click an element in the Member Selection List that you want to include in your Fabric Assist zone, or click an element in the Fabric Assist Zone Members that you want to delete.
5. Click **Add Member** to add a Fabric Assist zone member.
   Click **Remove Member** to remove an Fabric Assist zone member.

Renaming a Fabric Assist Zone

Use the following procedure to change the name of a Fabric Assist zone.

To rename a Fabric Assist zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Fabric Assist** tab.
3. Select the Fabric Assist Zone you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a Fabric Assist Zone dialog displays.
5. Type a new Fabric Assist zone name and click **OK**.

The Fabric Assist zone is renamed in the Zone Admin buffer.

Deleting a Fabric Assist Zone

Use the following procedure to delete a Fabric Assist zone.

To delete a Fabric Assist Zone

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Fabric Assist Zone** tab.
3. Select the Fabric Assist zone you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Fabric Assist Zone dialog displays.
5. Click **Yes**.

The selected Fabric Assist zone is deleted from the Zone Admin buffer.

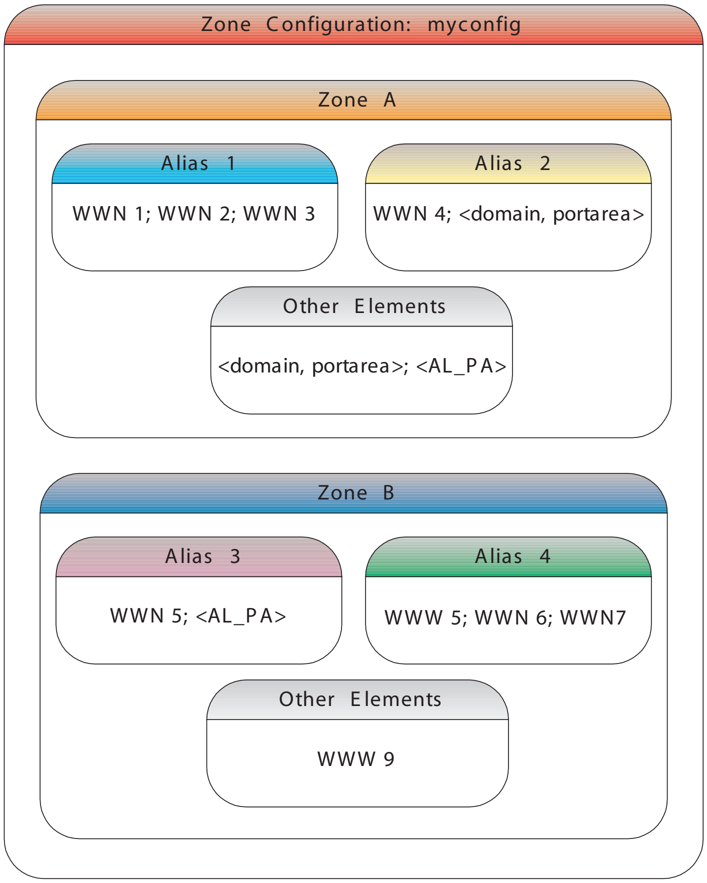
Managing Zoning Configurations

A zone configuration is a group of zones; zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration using the following methods:

- Zone names
- QuickLoop names
- FA (Fabric Assist) zone names

Figure 5-3 on page 5-15 shows a sample zoning database and the relationship between the zone aliases, zones, and zoning configuration. The database contains one zoning configuration, *myconfig*, which contains two zones: *Zone A* and *Zone B*. The database also contains four aliases, which are members of Zone A and Zone B. Zone A and Zone B also have additional members other than the aliases.

Figure 5-3 Sample Zoning Database



Creating a Zoning Configuration

Use the following procedure to create a zone configuration. After creating a zone configuration, you must explicitly enable it for it to take effect.

To create a zone configuration

1. Launch the Zone Admin module as described on page 5-3.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning Views" on page 5-6.
3. Click the **Config** tab.
4. Click **Create**.

   The Create New Config dialog box appears.
5. Type a name for the new configuration and click **OK**.

   The new configuration displays in the Name list.
6. Click "+" signs in the Member Selection List to view the nested elements.

   The choices available in the list depend on the selection made in the View menu.
7. Highlight an element in the Member Selection List that you want to include in your configuration.

   The **Add Member** button becomes active.
8. Click **Add Member** to add configuration members.

   Selected members are moved to the Config Members Window.
9. Repeat steps 7 and 8 to add more elements to your configuration.
10. Click **Actions** > **Save Config Only** to save the configuration changes.

    To enable the configuration, refer to "Enabling a Zone Configuration" on page 5-18.

Note
Any changes made to the currently enabled configuration will not appear until the configuration is reenabled.

Adding or Removing Zone Configuration Members

Use the following procedure to add or remove members of a zone configuration.

Note
You can make changes to a configuration that is currently enabled; however, changes will not appear until the configuration is reenabled.

To modify the members of a zone configuration

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Config** tab.
3. Select the configuration you want to modify from the Name drop-down list.
4. Click an element in the Member Selection List that you want to include in your configuration or click an element in the Config Members that you want to delete.

5. Click **Add Member** to add a configuration member.
   Click **Remove Member** to remove a configuration member.
6. Click **Actions** > **Save Config Only** to save the configuration changes.

   To enable the configuration, refer to "Enabling a Zone Configuration" on page 5-18.

Renaming a Zone Configuration

Use the following procedure to change the name of a zone configuration.

Note
You cannot rename the currently enabled configuration.

To rename a zone configuration

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Config** tab.
3. Click the configuration you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a Config dialog displays.
5. Type a new configuration name and click **OK**.

   The configuration is renamed in the configuration database.
6. Click **Actions** > **Save Config Only** to save the configuration changes.

To enable the configuration, refer to "Enabling a Zone Configuration" on page 5-18.

Deleting a Zone Configuration

Use the following procedure to delete a zone configuration.

Note
You cannot delete a currently enabled configuration.

To delete a disabled configuration

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Config** tab.
3. Select the configuration you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Config dialog displays.
5. Click **Yes**.

The selected configuration is deleted from the configuration database.

Enabling a Zone Configuration

Several zone configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during the business hours and another enabled overnight. However, only one zone configuration can be enabled at a time.

When you enable a zone configuration from Web Tools, keep in mind that the entire zoning database is automatically saved, and then the selected zone configuration is enabled.

To enable a zone configuration

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Actions** > **Enable Config**.

   The Enable Config dialog displays.
3. Select the configuration to be enabled from the menu.

   A warning displays.
4. Click **OK** to save and enable the selected configuration.

Disabling a Zone Configuration

When you disable the active configuration, the Advanced Zoning feature is disabled on the fabric, and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted, however, only that there is no configuration active on the fabric.

When you disable a zone configuration from Web Tools, keep in mind that the entire zoning database is automatically saved, and then the selected zone configuration is disabled.

To disable a zone configuration

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Actions** > **Disable Zoning**.

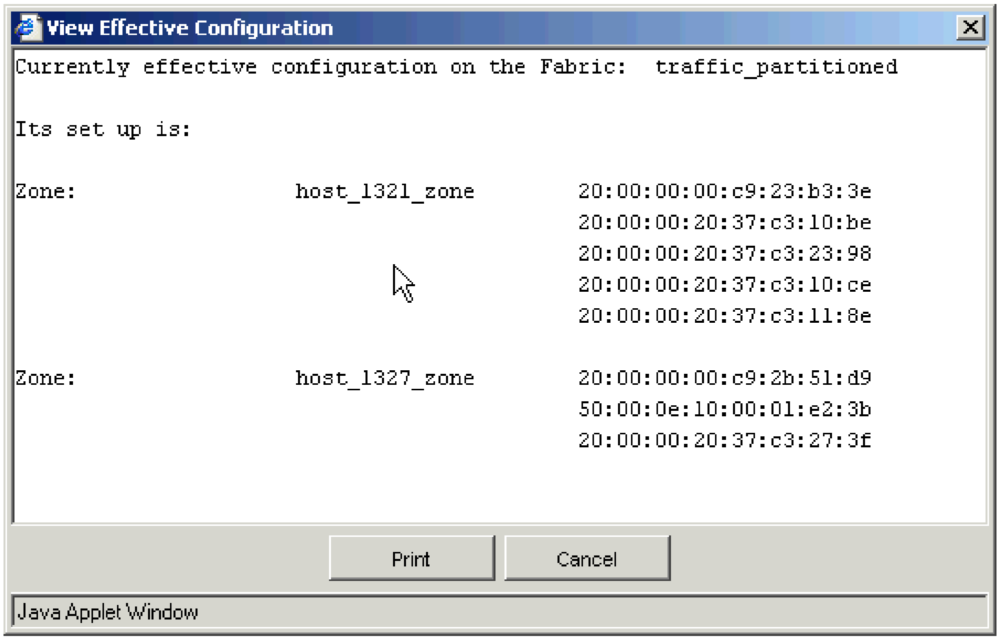
   The Disable Config warning displays.
3. Click **Yes** to save and disable the current configuration.

Displaying the Enabled Zone Configuration

The enabled zone configuration screen displays the actual content of the single zone configuration that is currently enabled on the fabric, whether or not it matches the configuration that was enabled when the current zone admin session was launched or last refreshed (see Figure 5-4). The zones, QuickLoops, and FA zones are displayed, and their contents (ports, WWNs, AL_PAs) are displayed next to them. Aliases are not displayed in the enabled zone configuration. If there is no active zoning configuration enabled on the switch, a message is displayed to that effect.

The enabled configuration is listed in the top right corner of the Zone Admin module.

Figure 5-4 Effective Configuration Window



```
Currently effective configuration on the Fabric:  traffic_partitioned

Its set up is:

Zone:                host_1321_zone        20:00:00:00:c9:23:b3:3e
                                           20:00:00:20:37:c3:10:be
                                           20:00:00:20:37:c3:23:98
                                           20:00:00:20:37:c3:10:ce
                                           20:00:00:20:37:c3:11:8e

Zone:                host_1327_zone        20:00:00:00:c9:2b:51:d9
                                           50:00:0e:10:00:01:e2:3b
                                           20:00:00:20:37:c3:27:3f
```

To view the enabled zone configuration name without launching the Zone Admin module

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View. The current zone configuration name (if one is enabled) is displayed in the lower portion of the Switch Information View. If no zone configuration is enabled, the field displays “none”.

To view detailed information about the enabled zone configuration

1. Launch the Zone Admin module, as described on page 5-3.

   The zone configuration in effect *at the time you launched the Zone Admin module* is identified in the top right corner. This information is automatically updated every 15 seconds. It is also updated if you manually refresh the Zone Admin module contents by clicking the refresh icon at the bottom right corner of the Zone Admin module, or when you enable a configuration through the Zone Admin module.

> **Caution**
> Clicking the refresh icon overwrites all local unsaved zoning changes. If anyone has made any changes to the zones outside of your Zone Admin session, those changes will be applied.

2. Use one of the following methods to identify the most recently effective zone configuration *without* saving or applying any changes you have made in the Zone Admin module:

   - Click **File > View Effective Configuration** in the Zone Admin module.
   - Click the enabled configuration button in the Zone Admin module.

   Both of these actions display the Effective Configuration window. If no zone is enabled, a message is displayed, indicating that there is no active zoning configuration on the switch.

3. *Optional*: Click **Print** to print the enabled zone configuration details. This launches the print dialog.

Displaying the Zone Configuration Summary

The zone configuration summary hierarchically lists all defined zoning elements known to the current Zone Admin session, whether or not any of the listed configurations has been enabled, and whether or not any of the lower level elements has been added as members of the higher level (aliases, zones, QuickLoops, FA zones) structures. The zone configuration summary displays the entire contents of the fabric zoning database as it was at the time the Zone Admin session was launched, or the most recently saved or refreshed information, and any unsaved changes you make since the time the Zone Admin session is launched. It provides the name of the zone configuration that was enabled at the time you launched the Zone Admin session; however, keep in mind that the enabled configuration might have changed since then and that this screen will not reflect those changes.

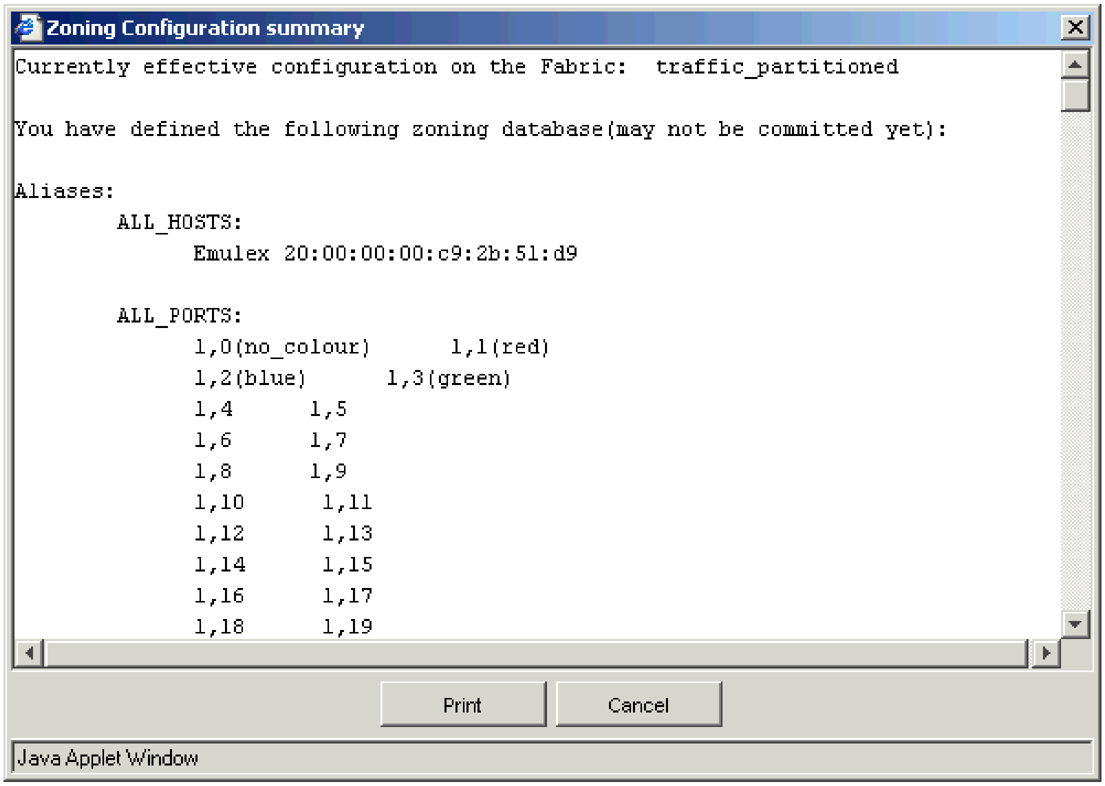
To view a zone configuration summary report

1. Launch the Zone Admin module as described on page 5-3.
2. Click **File** > **Print Summary**.

   The Zone Configuration Summary window displays, as shown in Figure 5-5 on page 5-20.

   It is important to note that the summary displays the information based on the changes just made. If current Zone Admin session changes have not yet been saved to the fabric, the information displayed here is different from what is seen from the switch.
3. *Optional*: Click **Print** to print the zone configuration summary. This launches the print dialog.

Figure 5-5 Zone Configuration Summary



```
Currently effective configuration on the Fabric:  traffic_partitioned

You have defined the following zoning database(may not be committed yet):

Aliases:
        ALL_HOSTS:
              Emulex 20:00:00:00:c9:2b:51:d9

        ALL_PORTS:
              1,0(no_colour)      1,1(red)
              1,2(blue)      1,3(green)
              1,4      1,5
              1,6      1,7
              1,8      1,9
              1,10      1,11
              1,12      1,13
              1,14      1,15
              1,16      1,17
              1,18      1,19
```

Creating a Configuration Analysis Report

The configuration analysis report lists the following:

- SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration.
- SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration but not in the fabric.

To create a configuration analysis report

1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Config** tab.
3. Select a configuration to be analyzed from the Name drop-down list.
4. Click **Analyze Config**.

   A dialog displays, asking if you want to refresh the fabric before running the analysis.
5. Click **Yes** or **No**.

The configuration analysis window displays.

Displaying Initiator/Target Accessibility

The Initiator/Target Accessibility Matrix shows a list of initiators and a list of targets and indicates which initiator can access which target.

To display an Initiator/Target Accessibility Matrix

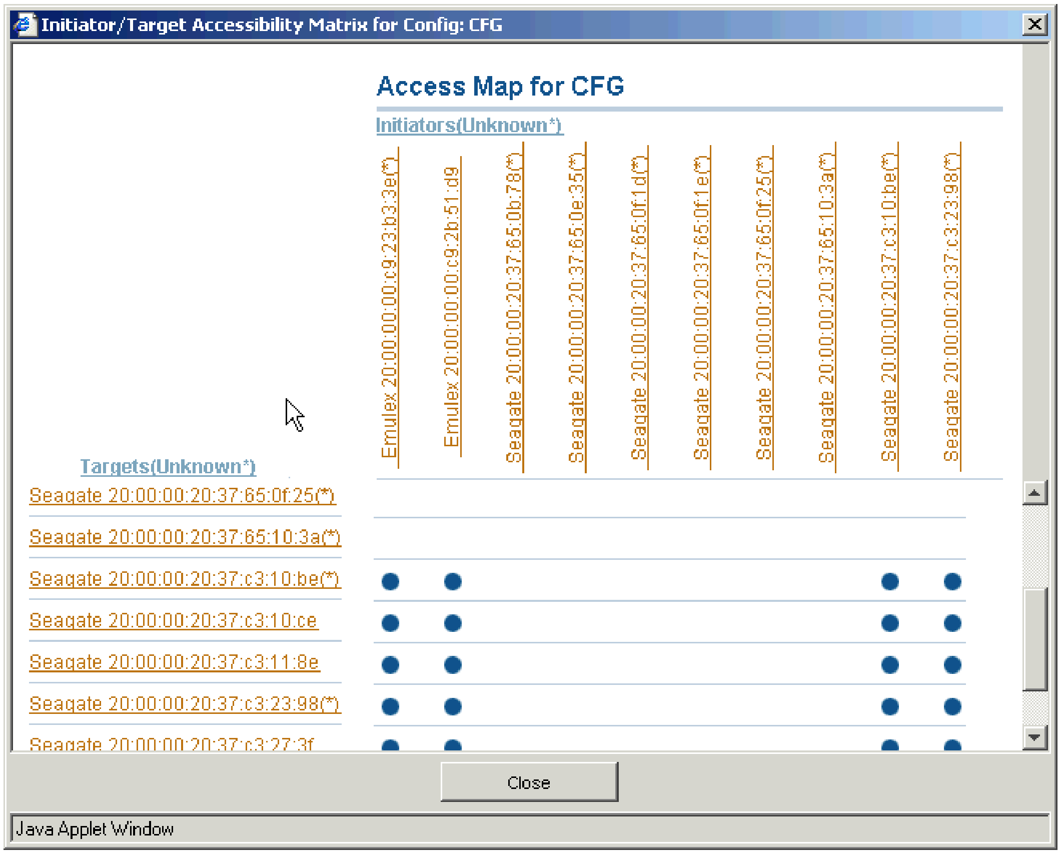
1. Launch the Zone Admin module as described on page 5-3.
2. Click the **Config** tab.
3. Select a configuration to be analyzed for device accessibility from the Name drop-down list.
4. Click **Device Accessibility**.

   The Initiator/Target Accessibility Matrix for Config- Device Selection dialog displays.
5. Select devices you want displayed in the accessibility matrix; click the radio button to select all devices in the fabric or to select a subset of the devices.

   If you select a subset, you must click the devices from the Select Devices list and click **Add** to move them to the Evaluate for Accessibility list.
6. Click **OK**.

The Initiator/Target Accessibility Matrix displays. You can “mouse over” a target to display the symbolic name of the device. You can click a WWN to launch the device view for that device. In addition, you can right-click the device nodes and click **View Device Detail** to display detailed information about the selected device.

Figure 5-6 Initiator/Target Accessibility Matrix



Initiator/Target Accessibility Matrix for Config: CFG

Access Map for CFG

	Initiators(Unknown*)									
Targets(Unknown*)	Emulex 20:00:00:00:c9:23:b3:3e(*)	Emulex 20:00:00:00:c9:2b:51:d9	Seagate 20:00:00:20:37:65:0b:78(*)	Seagate 20:00:00:20:37:65:0e:35(*)	Seagate 20:00:00:20:37:65:0f:1d(*)	Seagate 20:00:00:20:37:65:0f:1e(*)	Seagate 20:00:00:20:37:65:0f:25(*)	Seagate 20:00:00:20:37:65:10:3a(*)	Seagate 20:00:00:20:37:c3:10:be(*)	Seagate 20:00:00:20:37:c3:23:98(*)
Seagate 20:00:00:20:37:65:0f:25(*)										
Seagate 20:00:00:20:37:65:10:3a(*)										
Seagate 20:00:00:20:37:c3:10:be(*)	●	●							●	●
Seagate 20:00:00:20:37:c3:10:ce	●	●							●	●
Seagate 20:00:00:20:37:c3:11:8e	●	●							●	●
Seagate 20:00:00:20:37:c3:23:98(*)	●	●							●	●
Seagate 20:00:00:20:37:c3:27:3f	●	●							●	●

Managing the Zoning Database

This section contains the following procedures for managing the zoning database:

- "Adding a WWN to Multiple Aliases, Zones, and FA Zones," next
- "Removing a WWN from Multiple Aliases, Zones, and FA Zones" on page 5-23
- "Replacing a WWN in Multiple Aliases, FA Zones, and Zones" on page 5-24
- "Searching for a Zone Member" on page 5-24
- "Clearing the Zoning Database" on page 5-25
- "Adding Unzoned Online Devices to a Zone or Alias" on page 5-26
- "Removing Offline Devices from the Zoning Database" on page 5-26
- "Replacing Offline Devices" on page 5-27
- "Defining Device Aliases" on page 5-27

Adding a WWN to Multiple Aliases, Zones, and FA Zones

This procedure enables you to configure a WWN as a member in a zone configuration prior to adding that device to the fabric. Specifically, it is useful if you want to add a WWN to all or most zoning entities. The added WWN does not need to currently exist in the fabric.

To add a WWN to the Zone Admin buffer

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Edit** > **Add WWN**.

   The Add WWN dialog displays.
3. Type a WWN value in the WWN field.
4. Click **OK**.

   The Add WWN dialog displays all the zoning elements that will include the new WWN, including aliases, zones, and FA zones. All of the elements are selected by default.
5. Click items in the list to select or unselect, and click **Add** to add the new WWN to all the selected zoning elements.

The WWN is added to the Zone Admin buffer and can be used as a member.

Removing a WWN from Multiple Aliases, Zones, and FA Zones

This procedure is useful if you want to remove a WWN from all or most zoning entities.

To delete a WWN from the Zone Admin buffer

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Edit** > **Delete WWN**.

   The Delete WWN dialog displays.
3. Type a WWN value in the WWN field.
4. Click **OK**.

   The Delete WWN dialog displays all the zoning elements that include the WWN.
5. Click items in the list to select or unselect, and click **Delete** to delete the WWN from all the selected zoning elements.

The WWN is deleted from the selected items in the Zone Admin buffer.

Replacing a WWN in Multiple Aliases, FA Zones, and Zones

This procedure enables you to replace a WWN throughout the Zone Admin buffer. This is helpful when exchanging devices in your fabric and helps you to maintain your current configuration.

To replace a WWN in the Zone Admin buffer

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Edit** > **Replace WWN**.

   The Replace WWN dialog displays.
3. Type the WWN to be replaced in the **Replace** field.
4. Type the new WWN in the **By** field.
5. Click **OK**.

   The Replace WWN dialog is displayed. It lists all the zoning elements that include the WWN.
6. Click an item in the list to select or unselect, and click **Replace** to replace the WWN in all the selected zoning elements.

   The former WWN is replaced in the Zone Admin buffer by the new WWN, including within any alias or zone in which the old WWN was a member.

Searching for a Zone Member

You can search zone member selection lists for specified strings of text. If you know some identifying information about a possible member of a zoning entity, you can select the tab and view for that entity and then search through its member selection list using the Search for Zone Member option. If the target entity is an alias, zone, QuickLoop, or FA zone, then the search domain includes elements like switch names and domain numbers, port names and “domain, port” addresses, device WWNs and manufacturer names, and also any aliases that might already have been defined. If the target entity is a configuration, then zones, FA zones, and QuickLoops are also included, along with the elements they contain.

The search starts from the top of the list, and when the target element is found, it is also selected in the Member Selection List so it can be added or its parent or children can be found. By default, the Member Selection List is searched from beginning to end one time. If you select the wraparound option, the search will continue to loop from the beginning to the end of the Member Selection List.

To search for a zone member

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Edit** > **Search Member**.
3. Type the zone member name in the **Member Name** field.

   Optional: Narrow the search by checking one or more of the checkboxes, such as **Match Case**.
4. Click **Next** to begin the zone member search.

Clearing the Zoning Database

Use the following procedure to disable the active zoning configuration, if one exists, and delete the entire zoning database.

Caution
This action not only disables zoning on the fabric but also deletes the entire zoning database. This results in all devices being able to communicate with each other.

To disable any active configuration and delete the entire zoning database

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Actions** > **Clear All**.

   The Disable Config warning displays.
3. Click **Yes** to do *all* of the following:
   - Disable the current configuration.
   - Clear the entire contents of the current Web Tools Zone Admin buffer.
   - Delete the entire persistent contents of the fabric zoning database.

This action is *not* recoverable.

Using Zoning Wizards

The Zone Admin module contains the following wizards to help you perform the following zoning tasks:

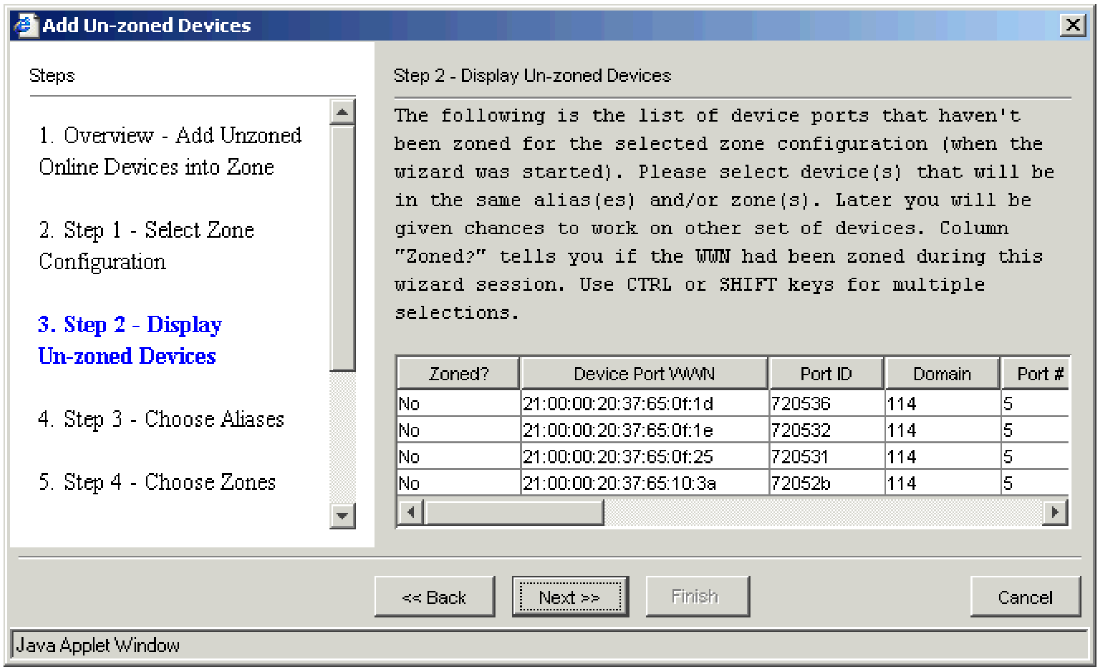
- Add Un-zoned Devices
- Remove Offline Devices
- Replace Offline Devices
- Define Device Alias

The wizards are accessed through the Tools menu in the Zone Admin module. The following sections describe the zoning tasks and the procedure for accessing the wizards for each task. The wizards are self-explanatory, so the specific steps are not documented here.

Note
The left side of each wizard window lists the steps you need to take to complete the task. The current step is in blue, as shown in Figure 5-7 on page 5-26. Some of the wizards allow you to loop and repeat the task multiple times; as a result, each step is listed in this panel, so that you not only see the steps that you still *need* to perform, but also the steps that you have *already* performed.

The step numbers do not necessarily match the overall numbering in this panel.

Figure 5-7 Add Un-zoned Devices Wizard


Add Un-zoned Devices
Steps
1. Overview - Add Unzoned Online Devices into Zone
2. Step 1 - Select Zone Configuration
3. Step 2 - Display Un-zoned Devices
4. Step 3 - Choose Aliases
5. Step 4 - Choose Zones
Step 2 - Display Un-zoned Devices
<< Back
Next >>
Finish
Cancel
Java Applet Window

The following is the list of device ports that haven't been zoned for the selected zone configuration (when the wizard was started). Please select device(s) that will be in the same alias(es) and/or zone(s). Later you will be given chances to work on other set of devices. Column "Zoned?" tells you if the WWN had been zoned during this wizard session. Use CTRL or SHIFT keys for multiple selections.

Zoned?	Device Port WWN	Port ID	Domain	Port #
No	21:00:00:20:37:65:0f:1d	720536	114	5
No	21:00:00:20:37:65:0f:1e	720532	114	5
No	21:00:00:20:37:65:0f:25	720531	114	5
No	21:00:00:20:37:65:10:3a	72052b	114	5

Adding Unzoned Online Devices to a Zone or Alias

When zoning is enabled, devices that are not included in a zone configuration are inaccessible to other devices in the fabric. Use the following procedure to identify online devices that are not zoned in any zone configuration and add them to a zone or alias.

To add unzoned online devices to a zone or alias

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Tools** > **Add Un-zoned Devices**.

   The Add Un-zoned Devices wizard starts.
3. Follow the steps outlined in the wizard.

The wizard displays unzoned devices and prompts you to select them and add them to an alias or a zone.

When you have finished the steps for adding a device to a zone or alias, if there are any more unzoned devices, you can either continue to add those unzoned devices or exit the wizard. If there are no more unzoned devices, you must exit the wizard.

Removing Offline Devices from the Zoning Database

Removing offline devices (WWNs) helps clean the zoning database to save more space for new entries. Use the following procedure to view all devices that are no longer online and remove all or selected offline devices from the zoning database.

To remove offline devices from the zoning database

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Tools** > **Remove Offline Devices**.

   The Remove Offline Devices wizard starts.
3. Follow the steps outlined in the wizard.

The wizard allows you to view all devices that are no longer online, and remove all or selected offline devices from the zoning database.

Replacing Offline Devices

Replacing an offline device replaces its WWN with a new given WWN in all of its containing aliases and zones. Use the following procedure to view offline devices and replace them with new ones in the zoning database.

To replace offline devices

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Tools** > **Replace Offline Devices**.

   The Replace Offline Devices wizard starts.
3. Follow the steps outlined in the wizard.

The wizard allows you to view all devices that are no longer online, and replace all or selected offline devices with new ones (WWNs) in the zoning database.

Defining Device Aliases

Use the following procedure to define zone alias names for devices in a single process. This procedure is especially useful if you use one unique zoning alias to name each device port.

The alias definitions of the devices are saved in the zoning database on the switch, which has a size limit. If database size becomes a concern, reconsider your use of alias definitions.

To assign aliases to devices

1. Launch the Zone Admin module as described on page 5-3.
2. Click **Tools** > **Remove Offline Devices**.

   The Define Device Alias wizard starts.
3. Follow the steps outlined in the wizard.

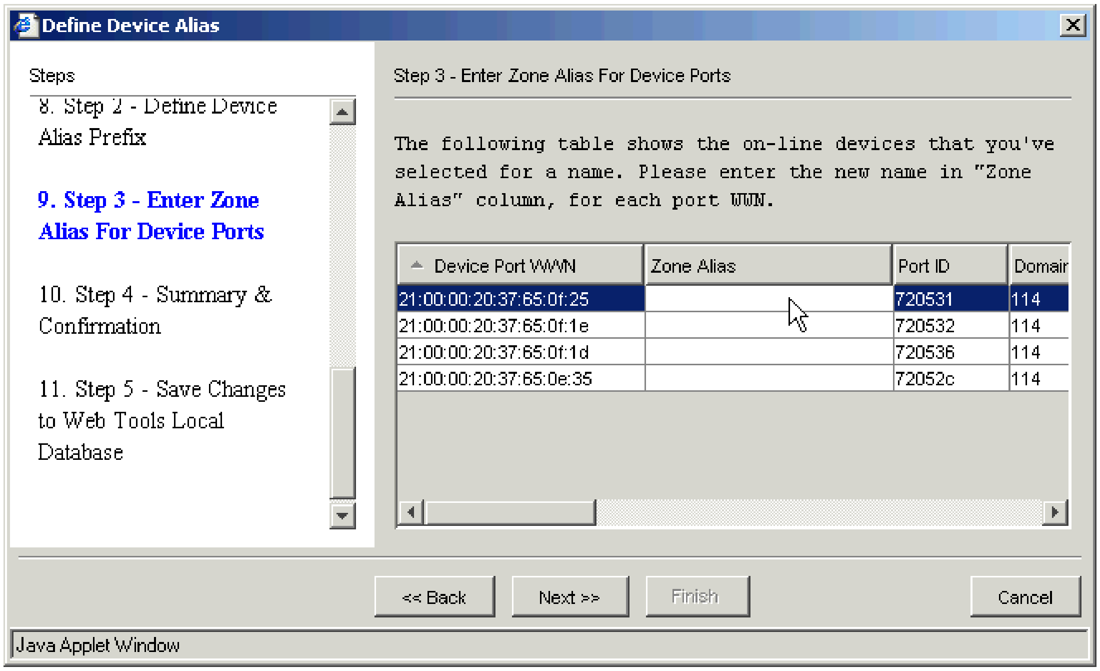
The wizard allows you to define one and only one name for each device port (WWN). Devices with one or more aliases are considered already named and are not displayed.

Note

To enter a zone alias name, double-click the Zone Alias field for each device, as shown in Figure 5-8 on page 5-28, and type the name.

After typing each alias name, you must press **Enter** or click another zone alias field, or the wizard does not accept the name.

Figure 5-8 Entering a Zone Alias in the Define Device Alias Wizard


Define Device Alias
Steps
8. Step 2 - Define Device Alias Prefix
9. Step 3 - Enter Zone Alias For Device Ports
10. Step 4 - Summary & Confirmation
11. Step 5 - Save Changes to Web Tools Local Database
<< Back
Next >>
Finish
Cancel
Java Applet Window

Step 3 - Enter Zone Alias For Device Ports

The following table shows the on-line devices that you've selected for a name. Please enter the new name in "Zone Alias" column, for each port WWN.

Device Port WWN	Zone Alias	Port ID	Domair
21:00:00:20:37:65:0f:25		720531	114
21:00:00:20:37:65:0f:1e		720532	114
21:00:00:20:37:65:0f:1d		720536	114
21:00:00:20:37:65:0e:35		72052c	114

Chapter
6

Performance Monitoring Administration

This chapter contains the following sections:

Monitoring Performance Using Web Tools

The Web Tools Performance Monitor module graphically displays throughput (in megabytes per second) for each port and for the entire switch.

The basic-mode Performance Monitor is standard in the Web Tools software. The Advanced Monitoring menu in Performance Monitor is an optionally licensed software.

Use the basic-mode Performance Monitor module to:

- Create user-definable reports.
- Display a performance canvas for application-level or fabric-level views.
- Save persistent graphs across reboots (saves parameter data across reboots).

Using Brocade Advanced Performance Monitoring, you can display predefined reports for AL_PA, end-to-end, and filter-based performance monitoring. You can track:

- The number of CRC errors for AL_PA devices.
- The number of words received and transmitted in Fibre Channel frames with a defined S_ID/ D_ID pair.
- The number of times a particular filter pattern in a frame is transmitted by a port.

For detailed information on these types of performance monitoring, refer to the *Brocade Fabric OS Features Guide*.

Each graph is displayed individually in a window, so it can be minimized, maximized, resized, and closed. Graphs within the Performance Monitor module are updated every 30 seconds.

When you have multiple graphs open in the Performance Monitor module, you can:

- Select **Tile** from the Window menu to view all graphs at once, tiled in the Performance Monitor module.
- Select **Cascade** from the Window menu to view one graph at a time.
- Select **Close All** to close all open Performance Monitor graphs in the Performance Monitor module.

In addition, the Window menu lists all open graphs. You can select a graph name from the Window menu to bring that graph to the front view when the graphs are cascaded, and to select the window for that graph when the graphs are tiled.

Predefined Performance Graphs

Web Tools predefines basic graph types, to simplify performance monitoring. A wide range of end-to-end fabric, LUN, device, and port metrics graphs are included. Table 6-1 lists the basic monitoring graphs available. Table 6-2 on page 6-3 lists the advanced monitoring graphs. The advanced monitoring graphs give more detailed performance information to help you manage your fabric. You can access the basic monitoring graphs on all switches; advanced monitoring graphs are available only on switches that have a Brocade Advanced Performance Monitoring license activated.

Table 6-1 Basic Performance Graphs

Graph Type	Description
Port Throughput	Displays the performance of a port, in bytes per second, for frames received and transmitted.
Switch Aggregate Throughput	Displays the aggregate performance of all ports on a switch.
Blade Aggregate Throughput	Displays the aggregate performance of all ports on a port card. This graph is available only for the SilkWorm 12000 and 24000 directors.
Switch Throughput Utilization	Displays the port throughput at the time the sample is taken. For the SilkWorm 12000 and 24000 directors, this graph displays the throughput for each slot. You can customize this graph to display information for particular ports.
Port Error	Displays a line of CRC errors for a given port.
Switch Percent Utilization	Displays the percentage utilization for each port in a switch. For the SilkWorm 12000 and 24000 directors, this graph displays the percent utilization for each slot. You can customize this graph to display information for particular ports.
Port Snapshot Error	Displays the CRC error count between sampling periods for all the ports on a switch. For the SilkWorm 12000 and 24000 directors, this graph displays the CRC error rate for each slot. You can customize this graph to display information for particular ports.

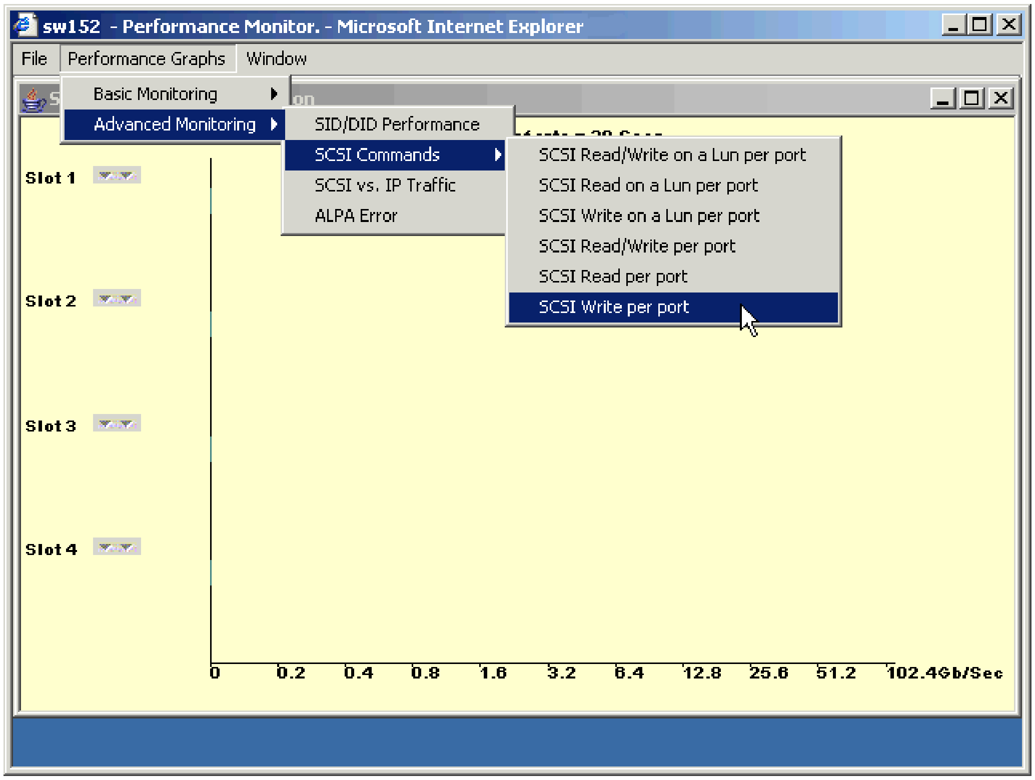
Table 6-2 Advanced Performance Monitoring Graphs

Graph Type	Description
SID/DID Performance	Displays the traffic between the SID-DID pair on the switch being managed. For more information, refer to "Creating an SID-DID Performance Graph" on page 6-7.
SCSI vs. IP Traffic	Displays percentage of SCSI versus IP frame traffic on each individual port. For more information, refer to "Creating a SCSI vs. IP Traffic Graph" on page 6-9.
AL_PA Errors	Displays CRC errors for a given port and a given AL_PA. For more information, refer to "Creating an AL_PA Error Graph" on page 6-10.
SCSI Commands by port and LUN (R, W, R/W)	Displays the total number of read/write commands on a given port to a specific LUN. For more information, refer to "Creating a SCSI Command Graph" on page 6-9.

The labeling of axes in the graphs depends on the switch type. For the SilkWorm 12000 and 24000 directors, slot numbers are displayed with expandable arrows next to them. Click the arrows to expand and contract the list of ports per slot. For the SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, slot numbers are not identified.

Figure 6-1 shows how to access the list of Advanced Performance Monitoring graphs using Web Tools. This example displays the graphs available in the Performance Monitor module for a SilkWorm 24000 director with the Advanced Performance Monitoring license installed. Note that the slot number is identified.

Figure 6-1 Accessing Performance Graphs



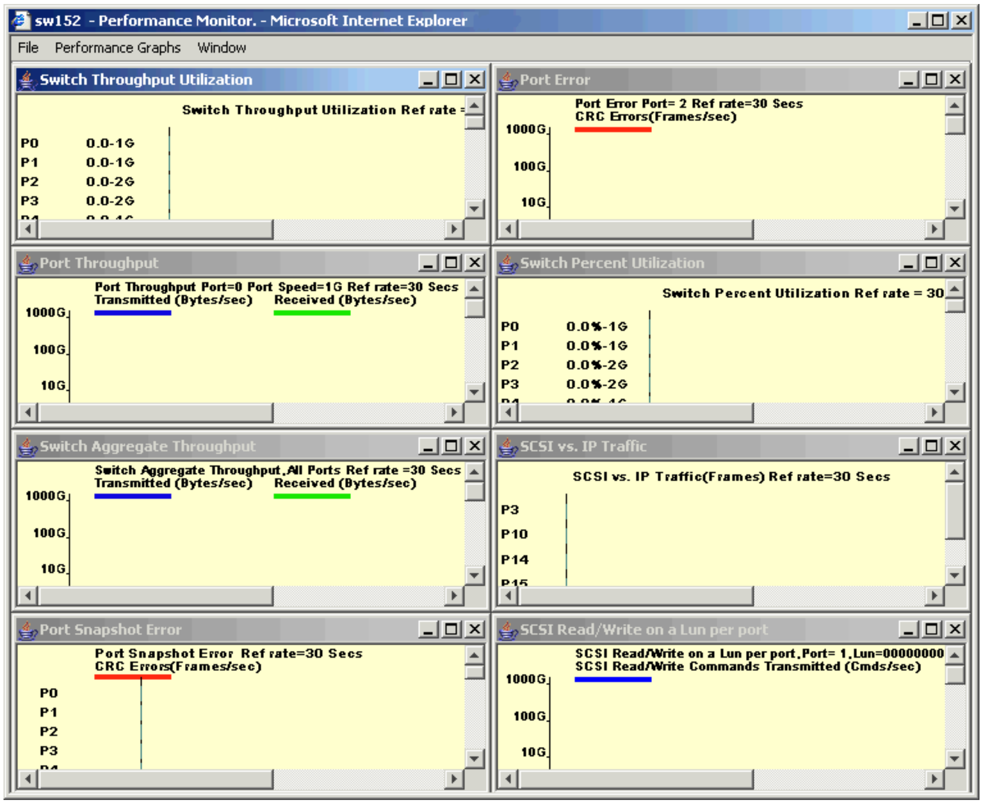
User-Defined Graphs

You can modify the predefined graphs to create your own customized graphs (refer to "Customizing Basic Monitoring Graphs" on page 6-5 for more information). These user-defined graphs can be added and saved to canvas configurations, described next.

Canvas Configurations

A *canvas* is a saved configuration of graphs. The graphs can be either the Web Tools predefined graphs or user-defined graphs. Each canvas can hold up to eight graphs per window, as shown in Figure 6-2. Up to 20 canvases can be set up for different users or different scenarios. Each canvas is saved with a name and an optional brief description.

Figure 6-2 Canvas of Eight Performance Monitoring Graphs


sw152 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Switch Throughput Utilization
Switch Throughput Utilization Ref rate =
P0 0.0-1G
P1 0.0-1G
P2 0.0-2G
P3 0.0-2G
Port Error
Port Error Port= 2 Ref rate=30 Secs
CRC Errors(Frames/sec)
1000G
100G
10G
Port Throughput
Port Throughput Port=0 Port Speed=1G Ref rate=30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
Switch Percent Utilization
Switch Percent Utilization Ref rate = 30
P0 0.0%-1G
P1 0.0%-1G
P2 0.0%-2G
P3 0.0%-2G
Switch Aggregate Throughput
Switch Aggregate Throughput,All Ports Ref rate =30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
SCSI vs. IP Traffic
SCSI vs. IP Traffic(Frames) Ref rate=30 Secs
P3
P10
P14
Port Snapshot Error
Port Snapshot Error Ref rate=30 Secs
CRC Errors(Frames/sec)
P0
P1
P2
P3
SCSI Read/Write on a Lun per port
SCSI Read/Write on a Lun per port,Port= 1,Lun=00000000
SCSI Read/Write Commands Transmitted (Cmds/sec)
1000G
100G
10G

Launching the Performance Monitor Module

Use the following procedure to launch the Web Tools Performance Monitor module.

To launch the Performance Monitor module

1. Select a switch from the Fabric Tree. The selected switch appears in the Switch View.
2. Click the **Perf** button Perf from the Switch View.

The Performance Monitor module displays.

Creating a Basic Performance Monitor Graph

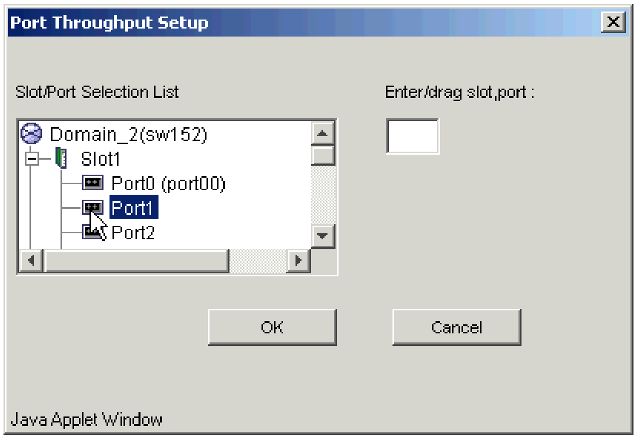
You can create the basic performance monitor graphs listed in Table 6-1 on page 6-2.

To create a basic performance monitor graph

1. Launch the Performance Monitor module as described earlier.
2. Click **Performance Graphs** > **Basic Monitoring** > ***Graph Type***.

   Depending on the type of graph you select, you might be prompted to select a slot or port for which to create a graph (see Figure 6-3).

   Figure 6-3 Creating a Port Throughput Graph

3. If prompted, drag the port into the **Enter/drag slot,port** field, or manually type the slot and port information in the field, in the format *slot,port*.

   For SilkWorm 12000 and 24000 directors, you must select first a slot number and then a port number.
   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, you need only type a port number.
4. Click **OK**.

   The graph is displayed in a window in the Performance Monitor module. The following section explains how you can customize some of these graphs.

Customizing Basic Monitoring Graphs

You can customize some of the basic performance monitoring graphs to display information for particular ports. For the SilkWorm 12000 and 24000 directors, you can also customize these graphs to display information for a slot.

You can customize the following graphs:

- Switch Throughput Utilization Graph
- Switch Percent Utilization Graph
- Port Snapshot Error Graph

The following procedure assumes that you have already created one of these customizable graphs.

To customize basic performance monitoring graphs

1. Create or access the graph you want to customize. Refer to "Creating a Basic Performance Monitor Graph" on page 6-5 for instructions on creating a graph.

2. **For SilkWorm 12000 and 24000 directors**, to display detailed port throughput utilization rates for each port in a slot, click the arrows next to a slot. Port information for that slot is displayed in the graph.

   For SilkWorm 3016, 3250, 3850, 3900, and 4100 switches, proceed to step 3.

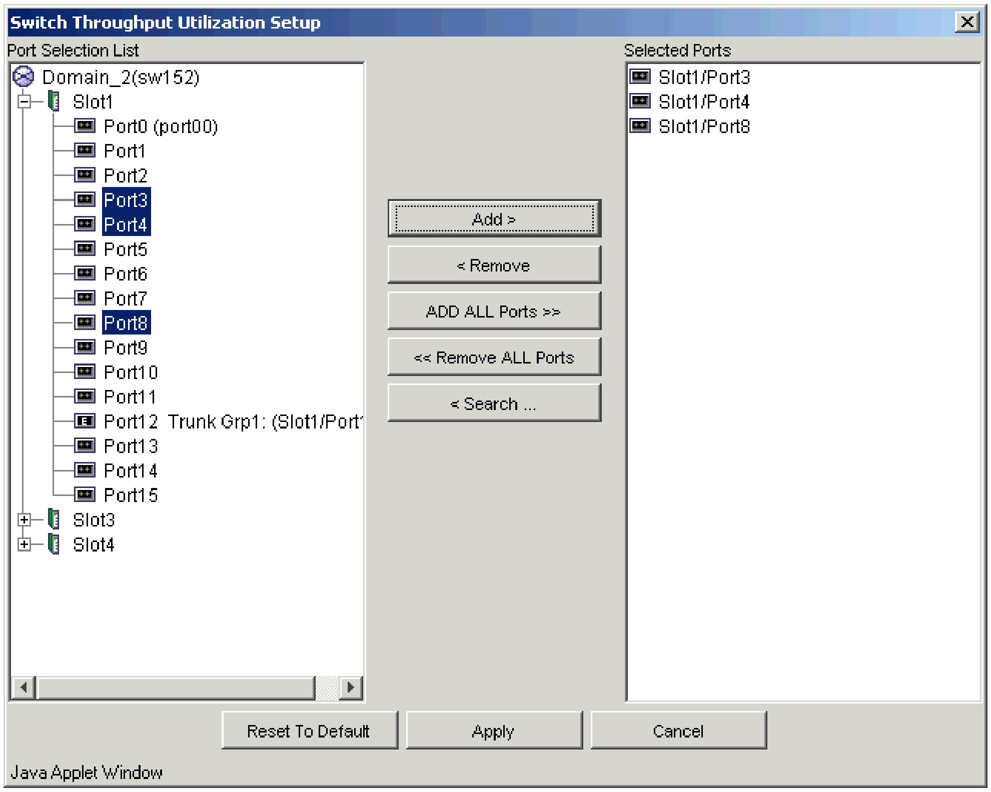
3. To display detailed port throughput utilization rates for particular ports only:

   a. Right-click anywhere in the graph.

   b. Click **Select Ports**.

   The setup dialog displays, as shown in Figure 6-4 on page 6-6. The title of the dialog varies, depending on the type of graph you are customizing, but the layout of the dialog is the same. Figure 6-4 shows an example of the setup dialog for the Switch Percent Utilization graph.

Figure 6-4 Switch Percent Utilization Setup Dialog



   c. Double-click the domain icon to expand the slot/port list.

   For the SilkWorm 12000 and 24000 directors, click the + signs to expand the ports under each slot, as shown in Figure 6-4.

   d. Click the particular port you want to monitor in the graph in the Port Selection List. Use Shift-click and Ctrl-click to select multiple ports.

   e. Click **Add** to move the selected ports to the Selected Ports list.

f. *Optional*: Click **ADD ALL Ports** to add all of the ports in the Port Selection List to the Selected Ports list.

g. *Optional*: Click **Search** to launch the Search Port Selection List dialog, from which you can search for all E_Ports, all F_Ports, or all port names with a defined string. Select the ports you want to add and click **Search** in the Search Port Selection List dialog.

h. Click **Apply** in the Switch Throughput Utilization Setup dialog.

Only the selected ports are displayed in the graph.

Creating Advanced Performance Monitoring Graphs

You can create the advanced performance monitor graphs listed in Table 6-2 on page 6-3. Because the procedure for creating these graphs differs depending on the type of graph, each type is described separately in the sections that follow.

Note
You must have an Advanced Performance Monitoring license installed to use the advance performance monitor features.

Creating an SID-DID Performance Graph

The SID/DID Performance graph displays the traffic between a SID-DID pair on the switch being managed.

To create an SID/DID performance graph

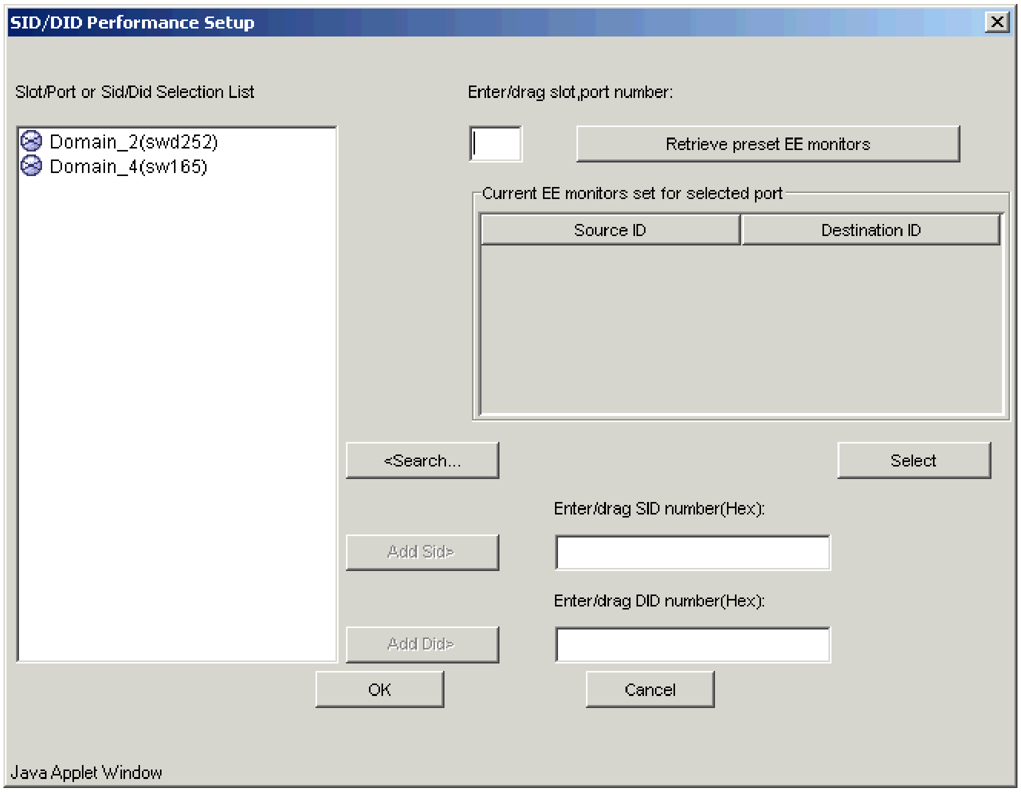
1. Launch the Performance Monitor module as described on page 6-4.
2. Click **Performance Graphs** > **Advanced Monitoring** > **SID/DID Performance**.

   The SID/DID Performance Setup dialog displays (refer to Figure 6-5 on page 6-8).

   If you want to see which end-to-end (EE) monitors are currently set up on a particular port, proceed to step 3.

   If you want to specify the port, source ID, and domain ID, skip to step 4.

Figure 6-5 Creating an SID/DID Performance Graph


SID/DID Performance Setup
Slot/Port or Sid/Did Selection List
Domain_2(swd252)
Domain_4(sw165)
Enter/drag slot,port number:
Retrieve preset EE monitors
Current EE monitors set for selected port
Source ID
Destination ID
<Search...
Select
Enter/drag SID number(Hex):
Add Sid>
Enter/drag DID number(Hex):
Add Did>
OK
Cancel
Java Applet Window

3. Click a port from the Slot/Port or Sid/Did Selection List.

    a. Drag the selected port into the Enter/drag port number field.

    b. Click **Retrieve preset EE monitors**.

    The current end-to-end monitors for that port are displayed in the “Current EE monitors set for selected port” table.

    c. *Optional*: To display a performance graph for the current EE monitors set for the selected port, click a SID-DID pair in the table. You can select multiple source ID and Destination IDs. Click **Select**. If you selected multiple SID/DID monitors, click **OK** in the confirmation dialog that appears. Skip to step 6.

    If you do not want to display a performance graph for the current EE monitors set for the selected port, continue with step 4.

4. Click a source ID from the “Port or Sid/Did Selection List,” and click **Add Sid**. You can also type a source ID in the “Enter/drag SID number” field.

5. Click a destination ID from the “Port or Sid/Did Selection List,” and click **Add Did**. You can also type a destination ID in the “Enter/drag DID number” field.

6. Click **OK**.

    If you selected multiple EE monitors, SIDs, or PIDs, a confirmation dialog displays, reminding you that one graph will be opened for each selection. Click **Yes** to display the graphs.

Creating a SCSI vs. IP Traffic Graph

The SCSI vs. IP Traffic graph displays the SCSI vs. IP traffic for selected ports. For SilkWorm 12000 and 24000 directors, the slot and port name is identified in the graph.

To create a SCSI vs. IP Traffic graph

1. Launch the Performance Monitor module as described on page 6-4.
2. Click **Performance Graphs** > **Advanced Monitoring** > **SCSI vs. IP Traffic**.

   The SCSI vs. IP Traffic Setup dialog displays. This dialog is similar to that shown in Figure 6-4 on page 6-6.
3. Double-click the domain icon to expand the slot/port list.

   For SilkWorm 12000 and 24000 directors, click the + signs to expand the ports under each slot, as shown in Figure 6-4.
4. Click the particular port you want to monitor in the graph in the Port Selection List. Use Shift-click and Ctrl-click to select multiple ports.
5. Click **Add** to move the selected ports to the Selected Ports list.
6. *Optional*: Click **ADD ALL Ports** to add all of the ports in the Port Selection List to the Selected Ports list.
7. *Optional*: Click **Search** to launch the Search Port Selection List dialog, from which you can search for all E_Ports, all F_Ports, or all port names with a defined string. Select the ports you want to add and click **Search** in the Search Port Selection List dialog.
8. Click **Apply** in the SCSI vs. IP Traffic Setup dialog.

   Only the selected ports are displayed in the SCSI vs. IP traffic graph.

Creating a SCSI Command Graph

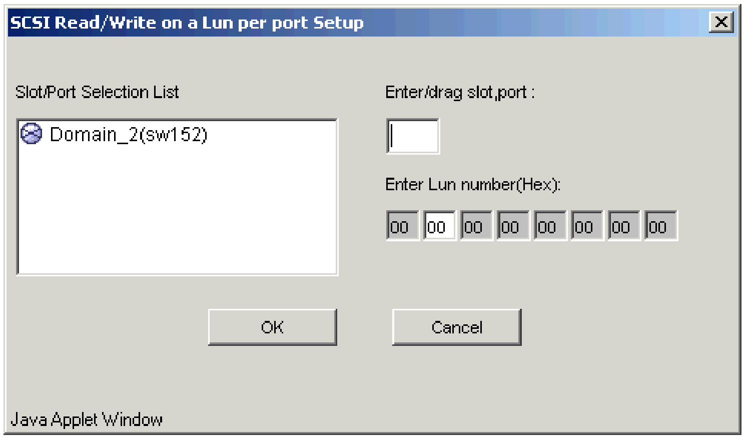
These graphs display the total number of read or write (or both) commands on a given port or to a specific LUN on a given port.

To create a SCSI command graph

1. Launch the Performance Monitor module as described on page 6-4.
2. Click **Performance Graphs** > **Advanced Monitoring** > **SCSI Commands > *Graph Type***.

   The applicable setup dialog displays. Figure 6-6 on page 6-10 shows the “SCSI Read/Write on a LUN per port Setup” dialog.

Figure 6-6 Creating a SCSI Command Graph



3. Navigate to a switch > slot > port in the Slot/Port Selection List.
4. Click the port from the Slot/Port Selection List and drag it into the Enter/drag slot,port field.
5. *Optional*: For the LUN per port graphs, type a LUN number, in hexadecimal.

   For the SilkWorm 4100 switch, you can enter up to eight LUN masks.
   For all other switches running Fabric OS v4.x, you can enter up to two LUN masks.
   For switches running Fabric OS v3.x, you can enter up to three LUN masks.
6. Click **OK**.

The selected graph is displayed in the canvas.

Creating an AL_PA Error Graph

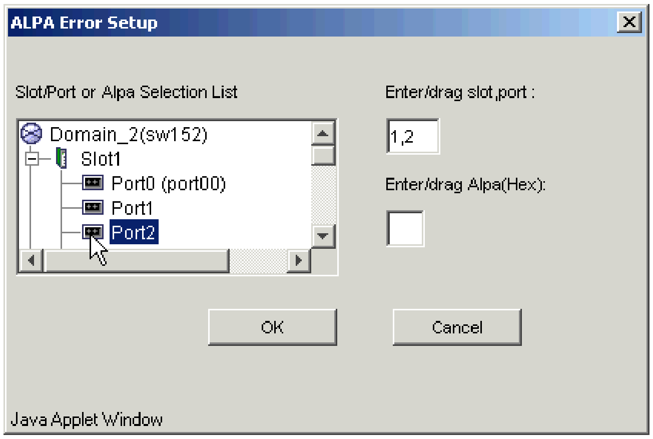
The AL_PA Error graph displays CRC errors for a given port and a given AL_PA. The AL_PA Error graph is not supported on the SilkWorm 4100 switch.

To create an AL_PA error graph

1. Launch the Performance Monitor module as described on page 6-4.
2. Click **Performance Graphs** > **Advanced Monitoring** > **ALPA Error**.

   The ALPA Error Setup dialog displays (see Figure 6-7).

Figure 6-7 Creating an ALPA Error Graph



Enter/drag slot,port : 1,2

3. Navigate to a switch > slot > port in the Slot/Port or Alpa Selection List.
4. Click the port from the Slot/Port Selection List or an AL_PA from the Slot/Port Selection List, and drag it into the "Enter/drag slot,port" field. You can also manually type the slot and port number, in the format *slot,port*.
5. Click **OK**.

The AL_PA Error graph displays on the canvas.

Managing Performance Graphs

This section provides the following procedures for managing performance graphs:

- Adding a Graph to an Existing Canvas
- Saving Graphs to a Canvas
- Printing Graphs
- Modifying an Existing Graph

Adding a Graph to an Existing Canvas

The following procedure assumes that a canvas is already created.

To create a new canvas, you must first create graphs, as described in "Creating a Basic Performance Monitor Graph" on page 6-5 and "Creating Advanced Performance Monitoring Graphs" on page 6-7, and then save those graphs to a canvas, as described in "Saving Graphs to a Canvas" on page 6-12.

To add a graph to an existing canvas

1. Click **File** > **Display Canvas Configurations**.

   The Canvas Configuration List displays. A message "No Canvas configuration to display" will display if there are no saved canvas configurations.

2. Click a canvas in the list.

3. Click **Edit**.

   The Edit Canvas dialog box displays.

4. Click **Add**.

   A list of graphs displays.

5. Click a graph to add it to the canvas.

6. Click **Save**.

Saving Graphs to a Canvas

Saving graphs is especially useful when you create customized graphs and do not want to re-create them every time you access the Performance Monitor module.

When you save graphs, you must save them to a canvas. The following procedure describes how to save graphs to a new canvas.

To save graphs

1. Launch the Performance Monitor module as described on page 6-4.

2. Create basic or advanced Performance Monitor graphs (refer to "Creating a Basic Performance Monitor Graph" on page 6-5 and "Creating Advanced Performance Monitoring Graphs" on page 6-7).

   The graphs are displayed in the in the Performance Monitor window.

3. Click **File > Save Current Canvas Configuration**.

   The Save Canvas Configuration dialog displays.

4. Type a name and description for the configuration and then click **Save Canvas**.

   A message displays, confirming that the configuration was successfully saved to the switch.

Printing Graphs

You can print a single graph or all the graphs displayed on the selected canvas configuration. Only one canvas configuration can be opened at a time.

To print a single graph

1. Launch the Performance Monitor module as described on page 6-4.

2. Create a basic or advanced Performance Monitor graph (refer to "Creating a Basic Performance Monitor Graph" on page 6-5 and "Creating Advanced Performance Monitoring Graphs" on page 6-7).

3. Right-click anywhere in the graph and click **Print**.

   The print dialog displays.

4. Click **OK**.

To print all graphs in a canvas

1. Launch the Performance Monitor module as described on page 6-4.
2. Click **File** > **Display Canvas Configurations**.

   The Canvas Configuration List displays. A message "No Canvas configuration to display" will display if there are no saved canvas configurations.
3. Select a canvas from the list and click **Load**.

   The graphs from that canvas are displayed in the Performance Monitor window.
4. Click **File** > **Print All Graphs**.

   The print dialog displays.
5. Click **OK**.

Modifying an Existing Graph

Use the following procedure to modify an existing graph that is saved in a canvas.

To modify an existing graph

1. Launch the Performance Monitor module as described on page 6-4.
2. Click **File** > **Display Canvas Configurations**.

   The Canvas Configuration List displays. A message "No Canvas configuration to display" displays if there are no saved canvas configurations.
3. Select a canvas from the list and click **Edit**.

   The **Performance Monitor Canvas: *Canvas Name*** dialog displays.
4. Select a graph from the list and click **Edit**.

Note
The **Edit** button is enabled only for the graphs that are configurable or editable.

5. Make changes in the Edit dialog, as necessary.
6. Click **OK** to close the Edit dialog.
7. Click **Save** to save the changes and close the Performance Monitor Canvas dialog.
8. Click **Close** to close the Canvas Configuration List.

Chapter

7

Fabric Watch Administration

This chapter contains the following sections:

Introduction to Fabric Watch

Fabric Watch is a Brocade optionally licensed feature that monitors the performance and status of switches and can automatically alert you when problems arise, before they become costly failures.

Fabric Watch tracks a variety of SAN fabric elements, events, and counters. For example, Fabric Watch monitors:

- Fabric resources, including fabric reconfigurations, zoning changes, and new logins.
- Switch environmental functions, such as temperature, power supply, and fan status, along with security violations.
- Port state transitions, errors, and traffic information for multiple port classes as well as operational values for supported models of Finisar "Smart" GBICs/SFPs.
- Performance information for AL_PA, end-to-end, and SCSI command metrics.

Fabric Watch lets you define how often to measure each switch and fabric element and allows you to specify notification thresholds. Whenever fabric elements exceed these thresholds, Fabric Watch automatically provides notification using several methods, including email messages, SNMP traps, and log entries.

Note

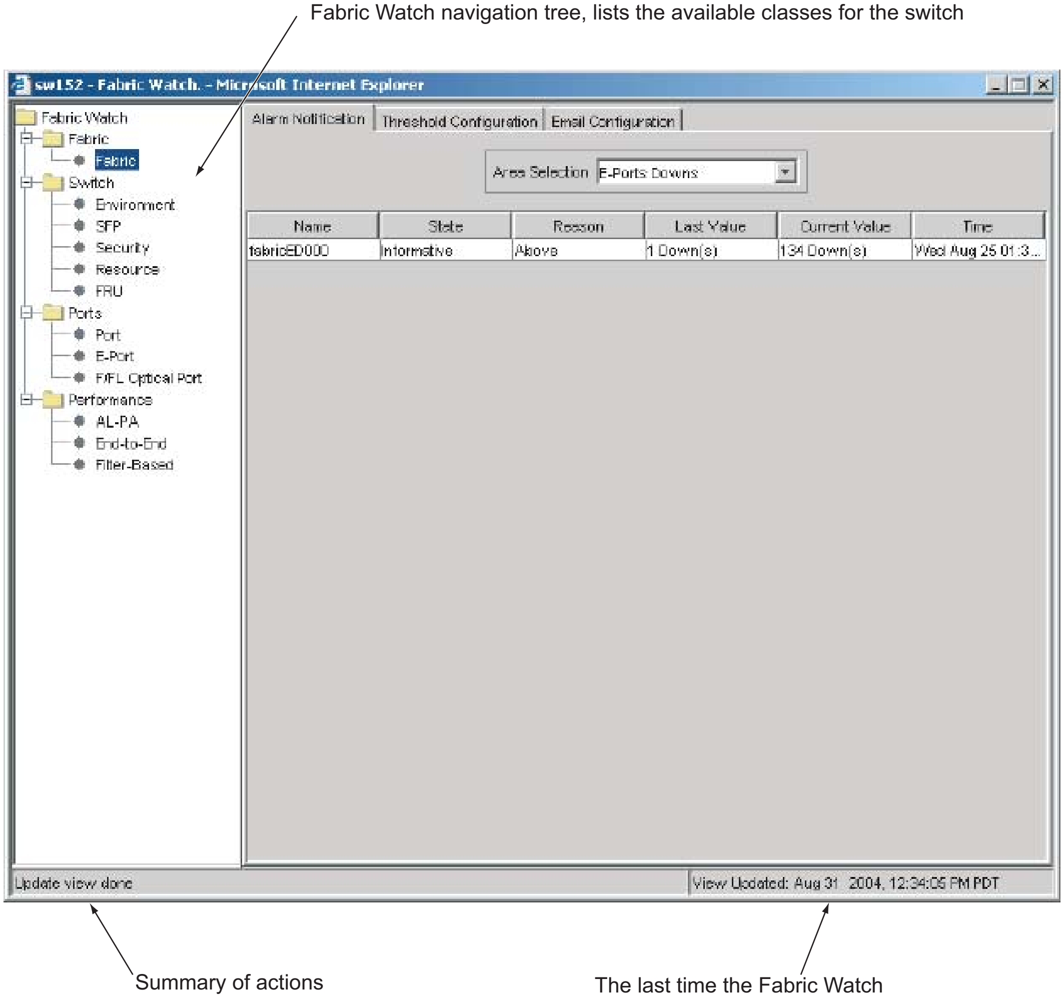
To use the Fabric Watch feature, you must have a Fabric Watch license installed on your switch.

For more detailed information regarding Fabric Watch, refer to the *Brocade Fabric Watch User's Guide*.

Using Fabric Watch with Advanced Web Tools

You can administer Fabric Watch operations through the Web Tools Fabric Watch module. Click the **Watch** button in the Switch View to access the Fabric Watch module, shown in Figure 7-1.

Figure 7-1 Fabric Watch Module



Area Selection: E-Ports Downs

Name	State	Reason	Last Value	Current Value	Time
fabricED000	Informative	Above	1 Down(s)	134 Down(s)	Wed Aug 25 01:3...

Update view done

View Updated: Aug 31 2004, 12:34:05 PM PDT

Fabric Watch navigation tree, lists the available classes for the switch

Summary of actions

The last time the Fabric Watch module was updated

The Fabric Watch navigation tree, on the left side of the module, displays the available classes. The classes are organized in a set of folders. Not all classes are available for all switches.

You should use the Fabric Watch module if you want to:

- Configure custom threshold values on particular elements.
- Place limits on the acceptable values of those elements and enable the custom limits (configure threshold boundaries).
- Choose if and how Fabric Watch alerts you to errant values (configure alarms).
- Choose if and how frequently Fabric Watch identifies unacceptable values (configure threshold traits).

To launch the Fabric Watch module

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Watch** button Watch from the Switch View.

   Note

   The **Watch** button displays in the Switch View only if the Fabric Watch license has been activated.

   The login dialog displays.

3. Type the user name of an account with the admin role.

4. Type the password.

   The Fabric Watch module displays (see Figure 7-1).

Configuring Fabric Watch Thresholds

The Threshold Configuration tab enables you to configure event conditions. From this tab, you configure threshold traits, alarms, and email configuration.

Use the following procedures to configure threshold traits for all classes except for the FRU class. Use the procedure described in "Configuring Alarms for FRUs" on page 7-6 for the FRU class.

Configuring Threshold Traits

Configure threshold traits to define a threshold for a particular class and area. Using the following procedure, you can configure the following traits for a threshold:

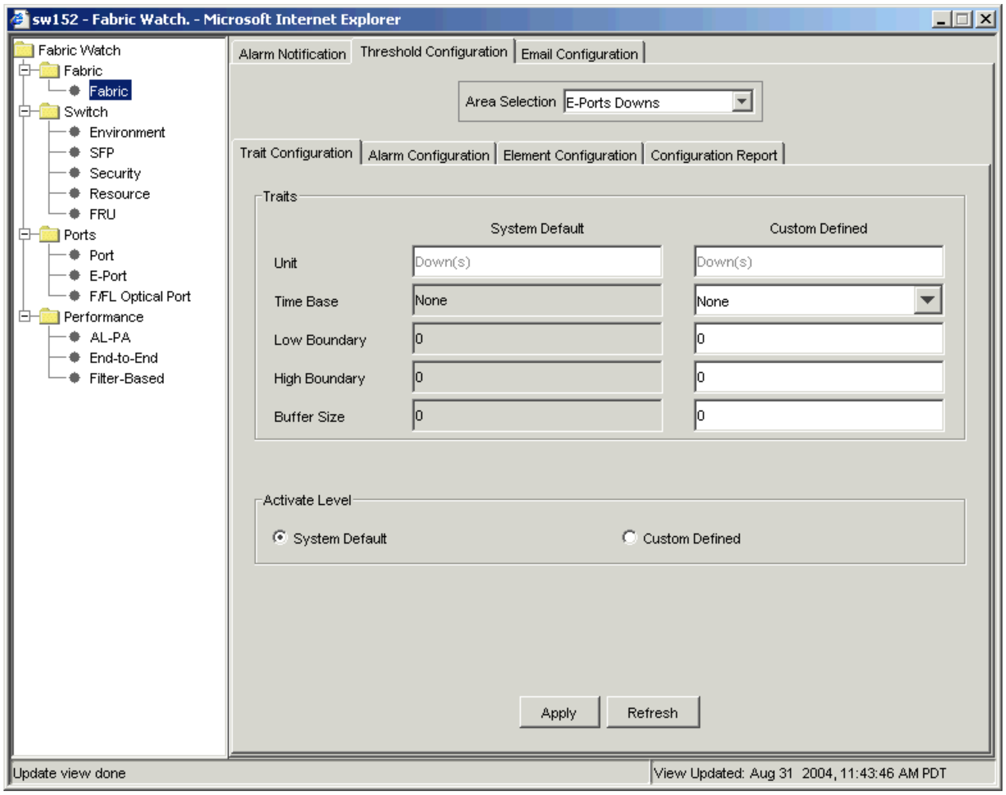
• Unit	The string used to define the units of measurement for the area.
• Time Base	The time base for the area.
• Low Boundary	The low threshold for the event-setting comparisons.
• High Boundary	The high threshold for the event-setting comparisons.
• Buffer Size	The size of the buffer zone used in event-setting comparisons.

To configure threshold traits

1. Launch the Fabric Watch module as described in "To launch the Fabric Watch module".

2. Click the **Threshold Configuration** tab (see Figure 7-2).

Figure 7-2 Threshold Configuration for Fabric Watch



Area Selection: E-Ports Downs

Traits

	System Default	Custom Defined
Unit	Down(s)	Down(s)
Time Base	None	None
Low Boundary	0	0
High Boundary	0	0
Buffer Size	0	0

Activate Level

● System Default ○ Custom Defined

Update view done

View Updated: Aug 31 2004, 11:43:46 AM PDT

3. Click the **Trait Configuration** subtab.
4. Click a class from the Fabric Watch navigation tree.

Note
If you select the FRU class from the Fabric Watch navigation tree, there is a separate set of instructions. Refer to "Configuring Alarms for FRUs" on page 7-6.

5. Select an area from the Area Selection menu in the Threshold Configuration tab.

   The module displays two columns of trait information, labeled **System Default** and **Custom Defined**. You cannot modify the information in the **System Default** column.

6. Click the **System Default** radio button to use the system default settings, and proceed to step 12.

   or

   Click the **Custom Defined** radio button to specify new settings and proceed to the next step.

7. Type a unit of threshold measurement in the Unit field.
8. Select a time to record the event in the Time Base field.
9. Type the lowest boundary of the normal zone in the Low Boundary field.
10. Type the highest boundary of the normal zone in the High Boundary field.
11. Type the size of the buffer zone in the Buffer Size field.
12. Click **Apply** to save your changes.

Configuring Threshold Alarms

After you update the threshold information, use the **Alarm Configuration** subtab (shown in Figure 7-1 on page 7-2) to customize the notification settings for each event setting.

To configure threshold alarms

1. Launch the Fabric Watch module as described in "To launch the Fabric Watch module".
2. Click the **Threshold Configuration** tab.
3. Click the **Alarm Configuration** subtab.
4. Click a class from the Fabric Watch tree.
5. Select an area from the Area Selection menu in the Threshold Configuration tab.

   The module displays two tables of alarm configuration information, labeled **System Default** and **Custom Defined**. You cannot modify the information in the **System Default** table.
6. Click the **System Default** radio button in the Activate Level section to use the system default settings, and proceed to step 8.

   or

   Click the **Custom Defined** radio button in the Activate Level section to specify new settings and proceed to the next step.
7. Click a checkbox to set the type of notification method for each event type (Changed, Below, Above, Inbetween). The available alarm actions are ERROR_LOG, SNMP_TRAP, RAPI_TRAP, and EMAIL_ALERT.
8. Click **Apply**.

Enabling or Disabling Threshold Alarms for Individual Elements

Use the **Element Configuration** subtab to configure element-specific alarm settings.

To enable or disable threshold alarms for an element

1. Launch the Fabric Watch module as described in "To launch the Fabric Watch module".
2. Click a class from the Fabric Watch navigation tree.

   You can set alarms for information on a switch only if that information is monitored by Fabric Watch for that switch; not all alarm options are available for all switches. For more information, refer to the *Brocade Fabric Watch User's Guide*.
3. Click the **Threshold Configuration** tab.
4. Click the area with the alarms that you want to enable or disable from the Area Selection menu.
5. Click the **Element Configuration** subtab.
6. Click an element from the Element Selection menu.

7. To disable threshold alarms, click **Disabled** in the Status area, and click **Apply**. The threshold alarms are disabled and you do not need to continue with this procedure.

   or

   To enable threshold alarms, click **Enabled** in the Status area, and continue with the next step.

8. Select a behavior type for the threshold alarms:

   - Click **Triggered** to receive threshold alarms only when they are triggered by events that you have defined.
   - Click **Continuous** to receive threshold alarms at a continuous interval. Select a time interval in which to receive the threshold alarms from the Time Interval menu.

9. Click **Apply**.

10. *Optional*: Apply the selections on this panel to multiple elements simultaneously.

    a. Click **Apply More**.

       This brings up the Multiple Selection Dialog.

    b. Click the boxes next to the indices of all applicable elements.

    c. Click **OK**.

Configuring Alarms for FRUs

Configuration for the FRU class is different than configuration for the other classes. Because FRUs are not monitored through a threshold-based system, they have a simpler interface for configuration. For FRUs, you configure the *states* for which an event occurs, as described in the following procedure.

To configure alarms for FRUs

1. Launch the Fabric Watch module as described in “To launch the Fabric Watch module”.
2. Click the **Threshold Configuration** tab.
3. Click the FRU class from the Fabric Watch navigation tree.
4. Select a FRU type from the Area Selection menu in the Threshold Configuration tab.
5. Click the alarm states for which you want an event to register. Whenever a FRU of the selected type is detected to be in one of the selected states, an event will occur.
6. Click the methods by which you want to be notified about the FRU alarms. For FRUs, the only options are error log and email alert.
7. Click **Apply** to apply the changes to the switch.

   A confirmation dialog displays, asking if you want to apply the changes to the switch.

8. Click **OK** in the confirmation dialog to save the changes to the switch.

Displaying Fabric Watch Alarm Information

From the Fabric Watch module, you can view two types of reports:

- Alarm notifications, which displays the alarms that have occurred for a selected class/area
- Alarm configuration, which displays threshold and alarm configurations for a selected class/area

Displaying an Alarm Configuration Report

Use the Threshold Configuration tab, Configuration Report subtab to display a report of the configuration for a selected class/area. The following information is displayed:

- Threshold settings (labeled **Threshold Configuration**)
- Notification settings (labeled **Action Configuration**)
- Element settings (not labeled)

You can scroll through this information but cannot make changes.

To view an alarm configuration report

1. Launch the Fabric Watch module as described in "To launch the Fabric Watch module".
2. Click the **Threshold Configuration** tab.
3. Click a previously configured element from the Fabric Watch navigation tree (refer to "Enabling or Disabling Threshold Alarms for Individual Elements" on page 7-5).
4. Click the alarm area report to be viewed from the Area Selection menu.
5. Click the **Configuration Report** subtab.

   This tab displays a report of the configuration for the selected area.

Displaying Alarms

Using the **Alarm Notification** tab, you can view a list of all alarms that have occurred for a selected class/area (see Figure 7-1 on page 7-2). Table 7-1 describes the columns in this report. (Note that for the FRU class, only the Name, State, and Time columns are displayed. In addition, if the FRU area is Fan, the Name column refers to either a fan or a fan FRU, depending on the switch model. Refer to "Displaying Detailed Fan Hardware Status" on page 4-9 for more information.)

Table 7-1 Alarm Notification Table Fields

Field	Description
Name	The string assigned to the element that had an event
State	The current state of the element
Reason	The event type that was triggered
Last Value	The data value of the element when the event was triggered
Current Value	The current data value of the element
Time	Time when the event occurred

To view alarms

1. Launch the Fabric Watch module as described in "To launch the Fabric Watch module".
2. Click the class that you want to check for alarms in the Fabric Watch navigation tree.
3. Click the **Alarm Notification** tab.
4. Click the area that you want to check for alarms from the Area Selection menu.

   All alarms for that area display.

For troubleshooting responses to alarms, refer to the *Brocade Fabric Watch User's Guide*.

Configuring Email Notifications

One of the ways that you can be notified of an alarm condition is through an email alert. If you have configured alarms to send an email notification, you must also configure the email server and the email recipient, as described in the following sections.

Configuring the Email Server on a Switch

You must set up the email notification recipient's DNS server and domain name on each switch for which email notification is enabled.

When you set up the email notification local network's DNS server and domain name for the SilkWorm 12000 and 24000 directors, it is on a logical-switch basis. This means that for each logical switch, you must set up the email notification recipient's DNS server and domain name individually.

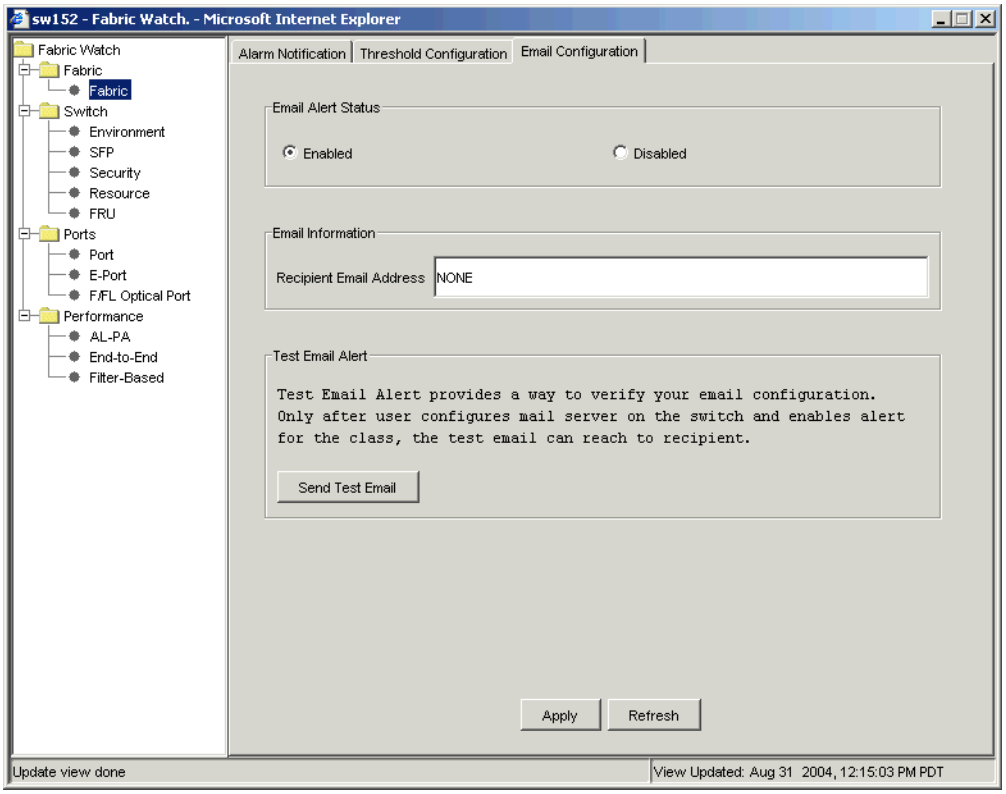
To configure the email server

1. Launch the Switch Admin module as described in "Launching the Switch Admin Module" on page 3-2.
2. Click the **Switch** tab.
3. Type your primary domain Name Server IP address in the DNS Server 1 field in the Email Configuration area.
4. Type your secondary domain server IP address in the DNS Server 2 field.
5. Type the domain name in the Domain Name field (between 4 and 32 characters).
6. Click **Apply** to save the changes.

Configuring the Email Alert Recipient

You can set a different email alert configuration for each class. For example, you can set one email notification for SFPs and another for E_Ports. Before configuring email alert recipients, you must set up the email notification recipient's DNS server and domain name. For more information, see "Configuring the Email Server on a Switch" on page 7-8.

Figure 7-3 Fabric Watch Email Configuration



Email Alert Status

● Enabled ○ Disabled

Email Information

Recipient Email Address: NONE

Test Email Alert

Test Email Alert provides a way to verify your email configuration. Only after user configures mail server on the switch and enables alert for the class, the test email can reach to recipient.

Update view done

View Updated: Aug 31 2004, 12:15:03 PM PDT

To configure the Email Alert alarm

1. Launch the Fabric Watch module as described in "To launch the Fabric Watch module".
2. Click the **Email Configuration** tab.
3. Click the **Enable** or **Disable** radio button to enable or disable the email alert status.

   When you disable email alerts, Fabric Watch does not send email notification even if the email notification method is assigned to monitored areas.
4. Type the email address of the recipient in the Recipient Email Address text box. Messages are sent to this address when email notification is enabled.

   Note

   Email addresses must not exceed 128 characters.
5. Click **Apply**.
6. *Optional*: Click **Send Test Email** to receive a test email so you can verify the email notification is working correctly. You can send a test email only after you have applied your settings.

Chapter

Administering and Managing FICON CUP Fabrics 8

This chapter contains the following sections:

- "Enabling or Disabling FMS Mode," next
- "Configuring FMS Parameters" on page 8-3
- "Displaying the Code Page Information" on page 8-4
- "Displaying the Control Device State" on page 8-5
- "Configuring CUP Port Connectivity" on page 8-6

Control Unit Port (CUP) is a protocol for managing FICON directors. Host-based management programs manage the switches using CUP protocol by sending commands to the emulated Control Device implemented by Fabric OS. A Brocade switch or director that supports CUP (SilkWorm 3900, 12000, or 24000) can be controlled by one or more host-based management programs or director consoles, such as Brocade Advanced Web Tools or Brocade Fabric Manager. (Refer to the *Brocade Fabric Manager User's Guide* for information about Fabric Manager.) The director allows control to be shared between host-based management programs and director consoles.

To use FICON CUP, you must:

- Install a FICON CUP license on a FICON director
- Enable FMS mode on the FICON director
- Configure CUP attributes (FMS parameters) for the FICON director

All of these things can be done using Web Tools. You can also use Web Tools to manage FICON directors (when FMS mode is enabled on those directors) to:

- Display the control device state
- Display a code page
- Manage port connectivity configuration

You do not need to install the FICON CUP license to perform FICON CUP management; you *must* install the FICON CUP license, however, if your switch is to enforce traffic between the FICON director and the host-based management program.

Enabling or Disabling FMS Mode

FICON Management Server (FMS) is used to support switch management using CUP. To be able to use the CUP functionality, all switches in the fabric must have FICON Management Server mode (FMS mode) enabled. FMS mode is a per-switch setting. After FMS mode is enabled, you can activate a CUP license without rebooting the director. You can use Web Tools to install a CUP license. For more information on installing licenses, refer to "Activating a License on a Switch" on page 3-25.

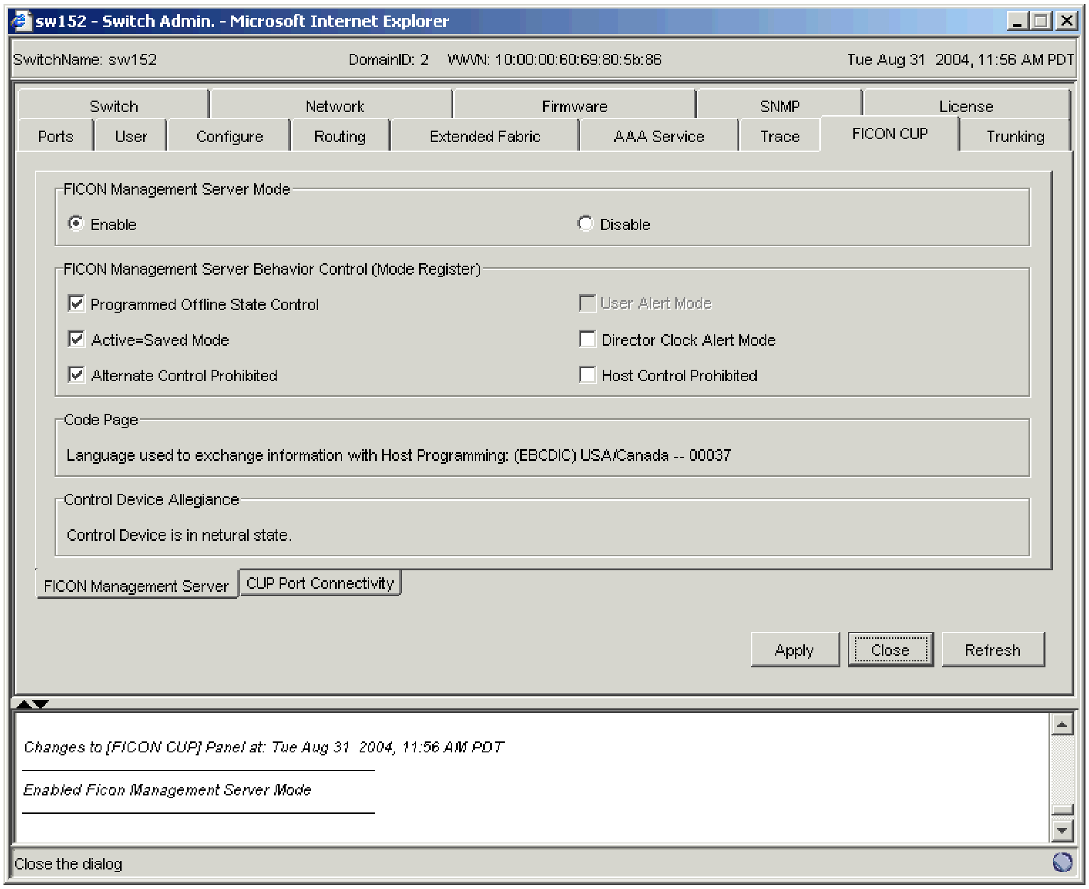
When FMS mode is disabled, mainframe management applications, director consoles, or alternate managers cannot communicate with a director with CUP. In addition, when FMS mode is disabled on a director, you cannot configure CUP attributes.

To enable or disable FMS mode

1. Click a FICON CUP-capable switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 3-2.
3. Click the FICON CUP tab.

   The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front, as shown in Figure 8-1. All attributes on this tab are disabled until FMS mode is enabled.
4. Click the **Enable** radio button to enable FMS mode.

Figure 8-1 FICON CUP Management



sw152 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 11:56 AM PDT

FICON Management Server Mode

● Enable ○ Disable

FICON Management Server Behavior Control (Mode Register)

☑ Programmed Offline State Control ☐ User Alert Mode

☑ Active=Saved Mode ☐ Director Clock Alert Mode

☑ Alternate Control Prohibited ☐ Host Control Prohibited

Code Page

Language used to exchange information with Host Programming: (EBCDIC) USA/Canada -- 00037

Control Device Allegiance

Control Device is in netural state.

Changes to [FICON CUP] Panel at: Tue Aug 31 2004, 11:56 AM PDT

Enabled Ficon Management Server Mode

Close the dialog

Configuring FMS Parameters

FMS parameters control the behavior of the switch with respect to CUP itself, as well as the behavior of other management interfaces (director console, Alternate Managers). You can configure FMS parameters for a switch *only* after FMS mode is enabled on the switch. All FMS parameters settings are persistent across switch power cycles. There are six FMS parameters, as described in Table 8-1.

Table 8-1 FMS Mode Parameter Descriptions

Parameter	Description
Programmed Offline State Control	This parameter controls whether host programming is allowed to set the switch offline or not. The parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.
Active=Saved Mode	This parameter controls the IPL file update. The IPL file saves port connectivity attributes and port names. After a switch reboot or power cycle, the switch reads the IPL file and actives its contents as default configuration. When this mode is enabled, activating a configuration saves a copy to the IPL configuration file. All changes made to the active connectivity attributes or port names by host programming or alternate managers are saved in this IPL file. It keeps the current active configuration persistent across switch reboots and power cycles. You cannot directly modify the IPL file or save a file as an IPL file. When this mode is disabled, the IPL file is not altered for a either new configuration activation or any changes made on the current active configuration. This parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools. NOTE: When FMS mode is enabled and the Active=Saved parameter is disabled, you can enable and disable ports, but the setting is not persistent. When the Active=Saved parameter is enabled, you can enable and disable ports and the setting is persistent.
Alternate Control Prohibited	This parameter determines whether alternate managers are allowed to modify port connectivity or not. Enabling this mode prohibits alternate manager control of port connectivity; otherwise, alternate managers can manage port connectivity. This parameter is set as enabled by the hardware after system installation, and can be reset by Web Tools.
User Alert Mode	This parameter controls director console behavior for alerts. Enabling this mode prompts the director consoles to display a warning whenever you attempt an action that will change switch parameters. When you disable this mode, no warning is displayed. In this case, in which Web Tools is the director console, warning messages are displayed by Web Tools regardless of the setting of the parameter, since Web Tools always displays warning messages when you apply a change to a switch that changes parameters. This parameter is always read-only in Web Tools. Each time that the switch is powered on, the parameter is reset to disabled.

Table 8-1 FMS Mode Parameter Descriptions (Continued)

Parameter	Description
Director Clock Alert Mode	This parameter controls behavior for attempts to set the switch timestamp clock through the director console When it is enabled, the director console (Web Tools, in this case) displays warning indications when the switch timestamp is changed by a user application. When it is disabled, you can activate a function to automatically set the timestamp clock. There is no indication for timestamp clock setting. This parameter is set as disabled by the hardware after system installation, and can be reset by Web Tools.
Host Control Prohibited	This parameter determines whether host programming allows modifying port connectivity. Enabling this mode prohibits host programming control of port connectivity; otherwise, host programming can manage port connectivity. This parameter is set as disabled by the hardware after system installation. and can be reset by Web Tools.

To configure FMS mode parameters

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 3-2.
3. Click the FICON CUP tab.

   The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see Figure 8-1 on page 8-2). All attributes on this tab are read-only until FMS mode is enabled.
4. To enable or disable an FMS mode parameter, click the checkbox next to the parameter. A marked checkbox means that the parameter is enabled. You cannot configure the User Alert Mode parameter in Web Tools, as it is read-only.

Displaying the Code Page Information

The Code Page field identifies the language used to exchange information between the FICON director with Host Programming. It is a read-only field in Web Tools, as it is set by Host Programming only. When FMS mode is disabled, the code page is displayed as unavailable.

To display the Code Page information:

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 3-2.
3. Click the FICON CUP tab.

   The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see Figure 8-1 on page 8-2). All attributes on this tab are read-only until FMS mode is enabled.

The code page format is displayed in the Code Page field.

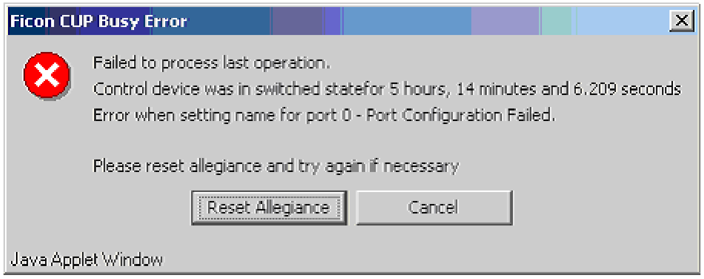
Example

```
Language used to exchange information with Host Programming: (EBCDIC) USA/Canada
-- 00037
```

Displaying the Control Device State

The Control Device is in either a neutral or a switched state. When it is neutral, the Control Device accepts commands from any channel that has established a logic path with it, and will accept commands from alternate managers. When the Control Device is switched, it establishes a logical path, and accepts commands only from that logical path ("device allegiance"). Commands from other paths cause a FICON CUP Busy Error (see Figure 8-2). Most "write" operations from alternate managers are also rejected.

Figure 8-2 FICON CUP Busy Error



Failed to process last operation.
Control device was in switched statefor 5 hours, 14 minutes and 6.209 seconds
Error when setting name for port 0 - Port Configuration Failed.

Please reset allegiance and try again if necessary

Device allegiance usually lasts for a very short time. However, under abnormal conditions, device allegiance can get "stuck" and fail to terminate. It might cause the switch to be unmanageable with CUP, and you will continue to receive the FICON CUP Busy Error. In this case, you should check the Control Device state and the last update time to identify if the device allegiance is stuck. The Web Tools Switch Admin displays the Control Device state and last update time (see Figure 8-1 on page 8-2). You can click **Refresh** to get most recent update.

You can manually reset allegiance to bring the Control Device back to the neutral state by clicking **Reset Allegiance** in the FICON CUP Busy Error display (see Figure 8-2).

The FICON CUP Busy Error can be caused by the following switch parameters being read or modified:

- Mode Register
- Port Names (also called Port Address Name)
- PDCM and Port Connectivity Attributes
- Switch enable/disable
- Switch name change

To display the Control Device state

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 3-2.
3. Click the FICON CUP tab.

The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see Figure 8-1 on page 8-2). All attributes on this tab are read-only until FMS Mode is enabled.

The Control Device state is displayed as neutral or switched in the Control Device Allegiance field.

If FMS mode is enabled, and the Control Device state is unavailable, the FICON CUP Busy Error is displayed. Click **Reset Allegiance** in the error message to reset the Control Device state to its correct state (see Figure 8-2).

Configuring CUP Port Connectivity

When initially installed, a switch allows any port to dynamically communicate with any other port. Two connectivity attributes are defined to restrict this any-to-any capability for external ports: *Block* and *Prohibit*.

Block is a port connectivity attribute that prevents all communication through a port. Prohibit is the port connectivity attribute that prohibits or allows dynamic communication between ports when a port is not blocked. Each port has a vector specifying its Prohibit attribute with respect to each of the other ports in the switch. This attribute is always set symmetrically in that a pair of ports is either prohibited or allowed to communicate dynamically.

The Port Connectivity table (shown in Figure 8-4 on page 8-9) displays the Port number (in physical-location format), Port Name (port address name), Block attribute, and Area Id (port address, displayed in hexadecimal) listed in fixed columns. The right side is Prohibit Port columns, which includes all prohibits ports identified by Area Id. Those columns are scrollable and swappable.

In the Port Connectivity subpanel, you can manage the configuration files and active configuration. All CUP configuration files and the active configuration are listed in a table. The active configuration is listed as “Active Configuration*” and the description in the table is “Current active configuration on switch.” The other special configuration file is the IPL. Any other files displayed are user-defined configurations and are stored on the switch.

You can create, activate, copy, or delete saved CUP port connectivity configurations; however, you can only edit or copy a configuration while it is active.You can also activate, edit, or copy the IPL configuration.You must have FMS mode enabled before you can make any changes to the configurations. Click **Refresh** to get the latest configuration file list from the switch.

When creating a new configuration or editing an existing configuration, keep in mind that Web Tools port name input is restricted to printable ASCII characters. Therefore, when Web Tools displays a port name, if there are characters beyond printable ASCII characters (which would have been created by the Host Program), those characters are displayed as dots (.).

Displaying the CUP Port Connectivity Configurations List

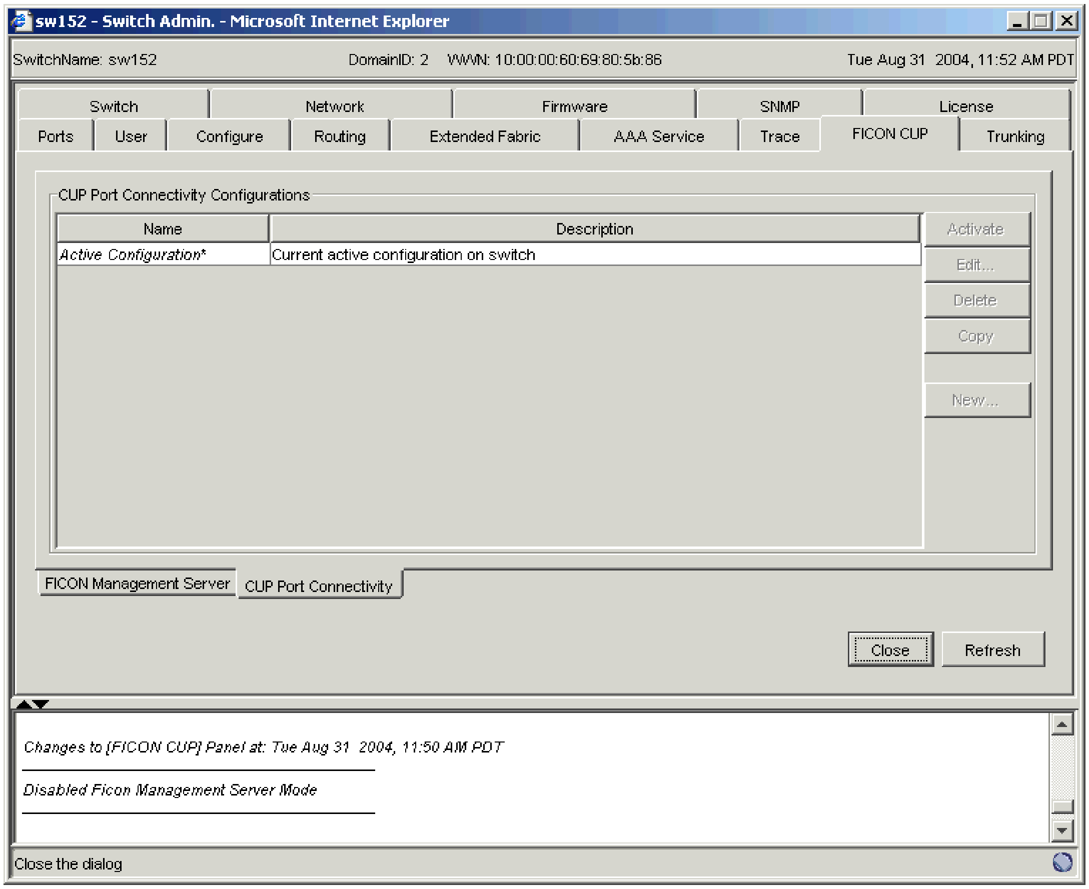
Use the following procedure to display a list of CUP port connectivity configurations, as shown in Figure 8-3 on page 8-7.

To display the CUP Port Connectivity Configurations list

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 3-2.
3. Click the FICON CUP tab.

   The FICON CUP tabbed page displays, with the FICON Management Server subtabbed page in front (see Figure 8-1 on page 8-2). All attributes on this tab are read-only until FMS mode is enabled.
4. Click the CUP Port Connectivity subtab.

Figure 8-3 Configuring CUP Port Connectivity



SwitchName: sw152 DomainID: 2 WWN: 10:00:00:60:69:80:5b:86 Tue Aug 31 2004, 11:52 AM PDT

CUP Port Connectivity Configurations

Name	Description
*Active Configuration**	Current active configuration on switch

Changes to [FICON CUP] Panel at: Tue Aug 31 2004, 11:50 AM PDT

Disabled Ficon Management Server Mode

Close the dialog

Creating or Editing CUP Port Connectivity Configurations

Use the following procedure to create a new CUP port connectivity configuration or to edit an existing configuration.

To create or edit CUP Port Connectivity Configurations

1. Display the CUP port connectivity configuration list, as described in "Displaying the CUP Port Connectivity Configurations List" on page 8-6.
2. You can either create a new configuration or edit an existing configuration. To create a new configuration, proceed to step 2a. To edit an existing configuration, proceed to step 2b.

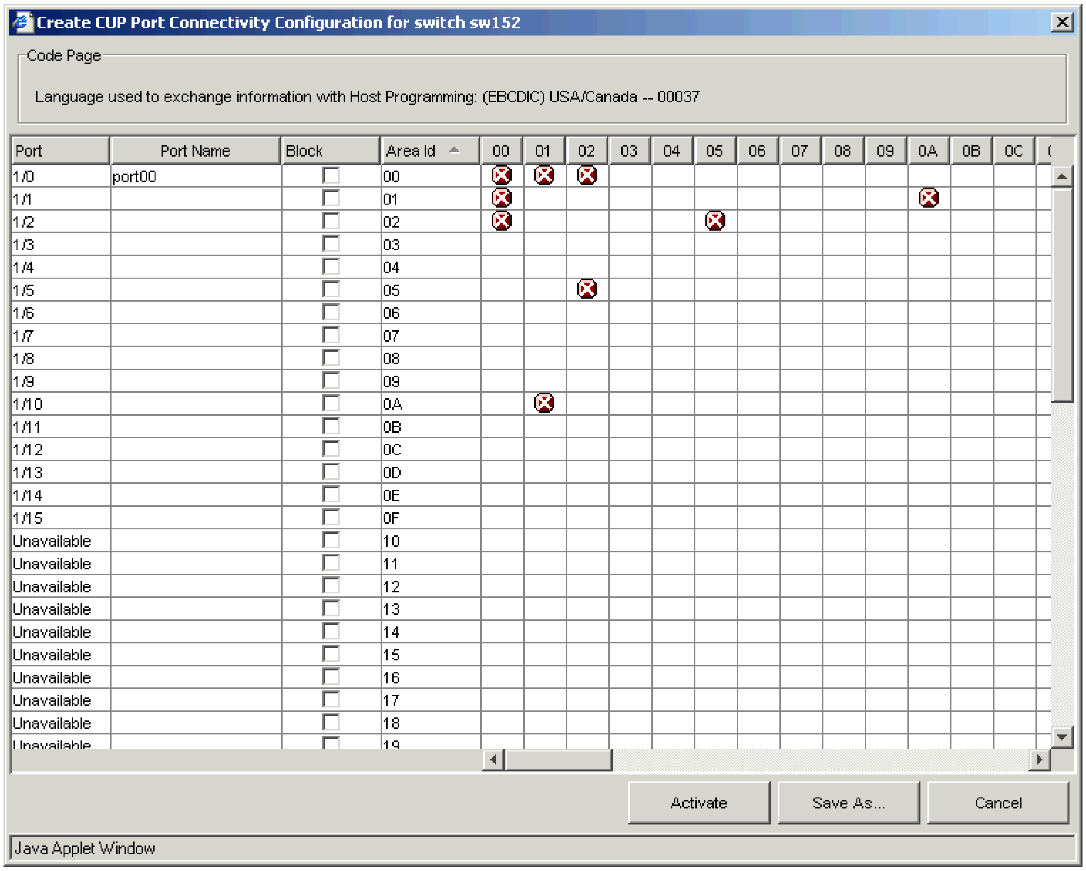
   a. To create a new configuration, click **New**.

      The Create Port CUP Connectivity Configuration dialog displays all ports and port names on the selected switch (similar to the dialog shown in Figure 8-4). The Block column and port prohibits matrix are displayed as empty for you to configure.

   b. To edit an existing configuration, click the configuration and then click **Edit**.

      The Edit Port CUP Connectivity Configuration dialog displays the content of the selected configuration from the switch in a table format (see Figure 8-4).
3. *Optional*: Click the checkbox corresponding to a port you want to block on the Block column. Repeat this step for all ports you want to block.
4. *Optional*: Click the individual cell corresponding to the combination of ports you want to prohibit. Repeat this step for all ports you want to prohibit. A red "x" icon identifies prohibited ports. You cannot prohibit a port to itself.
5. After you have finished making changes, do any of the following:
   - Click **Activate** to save the changes and make the configuration active immediately, as described in "Activating a Saved CUP Port Connectivity Configuration" on page 8-9.
   - Click **Save** to save the changes but not make the configuration active.
   - Click **Save As** to save the configuration to a new configuration file. When you click Save As, a dialog displays in which you should type a file name and description for the configuration file.
   - Click **Refresh** to refresh the information from the switch.
   - Click **Cancel** to cancel all changes without saving.

Figure 8-4 Port CUP Connectivity Configuration Dialog



Create CUP Port Connectivity Configuration for switch sw152

Code Page

Language used to exchange information with Host Programming: (EBCDIC) USA/Canada -- 00037

Port	Port Name	Block	Area Id	00	01	02	03	04	05	06	07	08	09	0A	0B	0C
1/0	port00	□	00	☒	☒	☒										
1/1		□	01	☒										☒		
1/2		□	02	☒					☒							
1/3		□	03													
1/4		□	04													
1/5		□	05			☒										
1/6		□	06													
1/7		□	07													
1/8		□	08													
1/9		□	09													
1/10		□	0A		☒											
1/11		□	0B													
1/12		□	0C													
1/13		□	0D													
1/14		□	0E													
1/15		□	0F													
Unavailable		□	10													
Unavailable		□	11													
Unavailable		□	12													
Unavailable		□	13													
Unavailable		□	14													
Unavailable		□	15													
Unavailable		□	16													
Unavailable		□	17													
Unavailable		□	18													
Unavailable		□	19													

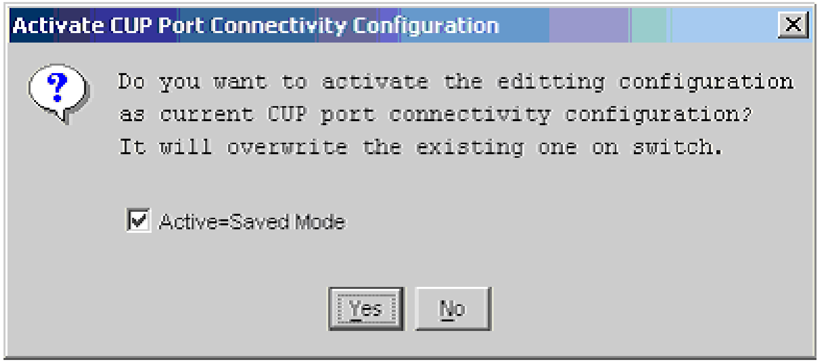
Activating a Saved CUP Port Connectivity Configuration

When you activate a CUP port connectivity configuration on the switch, the preceding configuration (currently activated) is overwritten.

To activate a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described in "Displaying the CUP Port Connectivity Configurations List" on page 8-6.
2. Click the saved configuration from the list.
3. Click **Activate**.

The Activate CUP Port Connectivity Configuration confirmation dialog displays.



Do you want to activate the editting configuration
as current CUP port connectivity configuration?
It will overwrite the existing one on switch.

☑ Active=Saved Mode

The dialog reminds you that the current configuration will be overwritten upon activation.

4. *Optional*: Click Active=Saved Mode to enable (checked) or disable (unchecked) the Active=Saved FMS parameter after the configuration is activated.

5. Click **Yes** in the confirmation dialog to activate the configuration, or click **No** to cancel the activation.

Copying a Saved CUP Port Connectivity Configuration

Use the following procedure to copy a CUP port connectivity configuration to a new configuration.

To copy a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described in "Displaying the CUP Port Connectivity Configurations List" on page 8-6.

2. Click a saved configuration or the active configuration from the list.

3. Click **Copy**.

   The Copy CUP Port Connectivity Configuration dialog displays.

4. In the dialog, type a name and description for the new configuration and click **OK** to save the configuration to the target file; click **Cancel** to cancel copying the configuration.

   The file name must be in alphanumeric characters and can contain only dashes or underscores as special characters.

Deleting a Saved CUP Port Connectivity Configuration

Use the following procedure to delete a CUP port connectivity configuration.

To delete a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described in "Displaying the CUP Port Connectivity Configurations List" on page 8-6.
2. Click the saved configuration from the list.
3. Click **Delete**.

   The Delete CUP Port Connectivity Configuration confirmation dialog displays.
4. Click **Yes** in the confirmation dialog to delete the selected configuration; click **No** to cancel the deletion.

Limitations

Chapter

9

This section provides the following information:

- "General Web Tools Limitations," next
- "Platform-Specific Limitations" on page 9-5
- "Limitations When Using the Mozilla Browser" on page 9-6

General Web Tools Limitations

Table 9-1 lists general Web Tools limitations that apply to all browsers and switch platforms.

Table 9-1 Web Tools Limitations

Problem Area	Details
Browser	The Fabric Watch, Switch Admin, HA, Name Server, and Zone Admin modules are separate applets embedded in HTML pages. The successful launch of the applet depends on whether the browser can successfully load the HTML page. Very occasionally, you will see a blank browser window with the message "loading pages..." that is stuck. This is likely caused by a sudden loss of switch Web server (either by normal HA failover, reboot, or other causes). **Workaround:** If the Fabric Watch, Switch Admin, HA, Name Server, or Zone Admin modules hang, close this window and relaunch the module.
Browser	A Web Tools browser window might stop responding following an HA failover immediately after a zoning configuration was enabled or disabled. It is likely that the Web daemon was terminated by the HA failover before the HTTP request was sent back. **Workaround:** If one of the Web Tools modules is hanging, close the window and relaunch the module. If the module is locked, shut down and relaunch the Web Tools application.

Table 9-1 Web Tools Limitations (Continued)

Problem Area	Details
Firmware download	There are multiple phases to firmware download and activation. When Web Tools reports that firmware download has completed successfully, this indicates that a basic sanity check, package retrieval, package unloading, and verification was successful. Web Tools forces a full package install. To perform an incremental upgrade, use the Fabric OS CLI. A reboot is required to activate the newly downloaded firmware. This reboot is done automatically; however, although Web Tools screens will continue to be visible during the reboot, they will not be available. Wait approximately 10 minutes to ensure that all of the application windows have been restored. If Web Tools fails to respond after 20 minutes, you might need to close all Web Tools applications windows and restart them, or to contact your system administrator for network assistance. The Web Tools loss of network connectivity during a failover or reboot (initiated though the **firmwaredownload**) varies for different configurations: • **SilkWorm 12000 and 24000 switches:** loss of network connectivity is up to 5 minutes if the power-on self-test (POST) is disabled. If POST is enabled, the loss of network connectivity can exceed 5 minutes. • **SilkWorm 3016, 3250, 3850, 3900, and 4100 switches:** loss of network connectivity is up to 1 minute if POST is disabled. If POST is enabled, the loss of network connectivity can exceed 1 minute.

HTTP timeout	Very occasionally, you might see the following message when you try to get data from a switch or to send a request to the switch:
	`Failed to get switch response. Please verify the status`
	`of your last operation and try again if necessary.`
	This indicates that an HTTP request did not get a response. The request was sent to the switch, but the connection was down, probably caused by a temporary loss of the Web server on the switch. Due to the nature of an HTTP connection, Web Tools will report this error after a 90-second default timeout.
	In this case, verify the status of your last request, using telnet to check related status, or click the **Refresh** button from the Web Tools application you were working on to retrieve related data. If your request did not get through to the switch, resubmit it. Executing a refresh from Web Tools retrieves a copy of switch data at that moment; the data you entered can be lost if it had not already committed to the switch.

Java Plug-in	When there is a dialog box opened for a module (for example, Switch Admin, Zone Admin, or Fabric Watch) and you try to open another module, the initial login dialog box receives an error and closes. This is a known defect in the Java 1.3.1_04 Plug-in and is documented in Bug Id 4763605 (available from *www.java.sun.com*). **Workaround:** Close and reopen the module.

Table 9-1 Web Tools Limitations (Continued)

Problem Area	Details
Licenses	If you remove the Web license after Web Tools application windows are opened, Web Tools displays the Web license missing dialog. From this point on, Web Tools behavior will be undefined if you continue with other operations after removing the license. **Workaround:** Close and relaunch the browser.

Loss of Connection	Occasionally, you might see the following message when you try to retrieve data from the switch or send a request to the switch:
	`Switch Status Checking`
	`The switch is not currently accessible.`
	The dialog title may vary, because it indicates which module is having the problem.
	This is caused by the loss of HTTP connection with the switch, due to a variety of possible problems. Web Tools will automatically try to regain the connection. While Web Tools is trying to regain the connection, check if your Ethernet connection is still functioning. If the problem is not with the Ethernet connection, wait for Web Tools to recover the connection and display the following message:
	`You will have to resubmit your request after closing this message.`
	If the temporary switch connection loss is caused by switch hot code load, or other similar operation, the Switch Explorer you are currently running can be downloaded from a different firmware version than the new one. In this case the following message displays:
	`Switch connection is restored. The firmware version you are running is not in sync with the version currently on switch. Close your browser and re-launch Webtools.`
	You need to close Switch Explorer and relaunch Web Tools to reopen the connection.

Performance Monitor	If the Web browser crashes or the Performance Monitor license is lost while the Performance Monitor module is running, some of the Performance Monitor resources owned by Web Tools might not be cleaned up correctly. **Workaround:** You might need to use the CLI to manually delete these counters. For example, if you detect Web Tools owned resources (using **perfshoweemonitor**), but you have verified that no Web users are actually using them, use the **perfdeleemonitor** or **perfcleareemonitor** command to free the resources.
Performance Monitor	For SCSI Read, Write, or Read/Write on a LUN per Port graphs, Fabric OS v4.1.0 (and later 4.x versions) allows you to enable only two bytes or less for the LUN value mask setting. Fabric OS v3.1 (and later 3.x versions) allows up to three bytes. Web Tools displays an error message if you exceed this limit. **Workaround:** There is no workaround.

Table 9-1 Web Tools Limitations (Continued)

Problem Area	Details
Refresh option in browsers	When a pop-up window requesting a user response is pushed into the background and a refresh is requested, a fatal Internet Explorer error may occur. **Workaround:** Restart the browser.
Refresh option in browsers	Web Tools must be restarted when the Ethernet IP address is changed using the NetworkConfig View command. Web Tools appears to hang if it is not restarted after this operation is executed. **Workaround:** Restart the browser.
Refresh option in browsers	If you change the switch name or domain ID using the CLI after the Web Tools Switch Admin module has started, the new switch name or domain ID will not be updated on the header of the Switch Admin page. Clicking the **Refresh** button will not fix the problem. **Workaround:** Click the **Switch** tab and the Switch Admin header will update.
Refresh option in browsers	If you change the switch name using the Web Tools Switch Admin page or SNMP and then open a telnet window to verify the name change, the CLI prompt (for example, **switch:admin>**) displays the previous name. The telnet prompt cannot pick up the new switch name until the switch is fastbooted. **Workaround:** In order to display the correct switch name in the CLI prompt after a switch name update using Web Tools or SNMP, **fastboot** the switch.
Refresh option in browsers	Following a switch enable or disable, you must wait at least 25–30 seconds for the fabric to reconfigure and for FSPF route calculations to complete before requesting routing information. If accessed too early, routing information will not be shown. **Workaround:** Following a switch enable or disable, wait at least 25–30 seconds before further action.
Refresh option in browsers	The Web Tools Switch Explorer might continue to display a switch from the Switch View, even when the switch has been removed from the fabric. **Workaround:** If this behavior is seen, relaunch the Switch Explorer. If the switch was removed from the fabric, the Fabric View window will list the switch as unavailable.
Refresh option in browsers	In the Switch Admin module, **Switch** tab, if you click the **Refresh** button, you might not be able to click the data entry fields to enter text. This behavior occasionally happens on a notebook or laptop computer; it rarely happens on a desktop computer. **Workaround:** If this happens, you should close the browser window and restart it.
Switch View	Occasionally, switches might display the port icons correctly, but be missing one or more control button icons. **Workaround:** Close the Switch View of the switch and reopen it.

Table 9-1 Web Tools Limitations (Continued)

Problem Area	Details
Windows Operating Systems	Occasionally, you will not see the “Lost connection to the switch” message on the Switch View even though the Ethernet connection has been lost. You might still be able to invoke various features from Switch View such as Status, Info, Fan Temp, Power and Beacon. This problem might be seen in the SilkWorm 12000, for example, when you see the “Lost connection to the switch” error for a single switch in the chassis, when a lost connection affects both logical switches. **Workaround:** Verify Ethernet connection to the switch by pinging the logical switch IP address.
Zone Admin	The accessibility matrix in the Zone Admin module does not show hosts and devices zoned by QuickLoop AL_PA as being accessible to each other.

Platform-Specific Limitations

Table 9-2 lists Web Tools limitations that are specific to the SilkWorm 12000 director and to the SilkWorm 24000 director when it is configured to have two domains.

Table 9-2 Platform-Specific Limitations

Problem Area	Details
Switch View	Neither CP is updated in the Switch View (refer to Figure 1-2 on page 1-4) when switch 0 is being rebooted. The CP data displayed on this Switch View is dependent on switch 0, and that data is not available when switch 0 is rebooting. **Workaround:** Wait until the reboot is finished and Switch View polling occurs; then, the CPs will be updated properly.
Java Plug-in	The Java Plug-in might sometimes have problems focusing on a particular field in an open applet if you have the same window open for both logical switches. **Workaround:** When this problem occurs, close and relaunch the affected applet.

Limitations When Using the Mozilla Browser

Table 9-3 lists limitations in Web Tools that occur when you use the Mozilla browser on a Linux system. These limitations do not occur when using Internet Explorer on Windows.

Table 9-3 Web Tools Limitations When Using the Mozilla Browser

Problem Area	Details
Mozilla Browser on Red Hat Operating System	On the Red Hat platform, the default system font size is larger than on other platforms. This can cause tabbed panes to not line up. There is no impact on functionality.
Mozilla Browser on Solaris Operating System	On a Solaris/Mozilla browser, some pop-up windows (for example, the firmware download completion message and performance monitor dialog boxes) display in the background, behind other windows. This can give the appearance of a session hang. **Workaround:** If you are apparently locked out of other windows in the Solaris/Mozilla environment, look for a pop-up window that needs to be dismissed before proceeding further.
Performance Monitor module	When creating performance graphs, you might not be able to drag and drop port numbers or AL_PAs in the graph setup dialog box. **Workaround:** Type the port numbers and AL_PAs in the appropriate fields.
Switch Admin, Routing tab	When you launch Web Tools and open the Switch Admin module for the first time, if you click the **Routing** tab, the FSPF route tree nodes do not display correctly. **Workaround:** Click another tab in the Switch Admin module; then click the **Routing** tab again.
Telnet	Mozilla browsers do not support the telnet application. **Workaround:** Launch an external telnet process.
Zone Admin	If you make changes in the Zone Admin module and then close the module without saving your changes, your changes are lost. If you have unsaved changes and you close the module by clicking **File > Close**, you receive a message warning that your changes are not saved and requesting confirmation before the module is closed. If you have unsaved changes and you close the module by clicking the X in the upper right corner of the window, you receive a warning message only if you are using Internet Explorer. If you are using the Mozilla browser, you do *not* receive this message and any unsaved changes are lost. **Workaround:** Always close the Zone Admin module by clicking **File > Close**. If you have not saved your changes, for all browsers, a warning message is displayed, requesting confirmation before the module is closed.

Glossary

#

A

address identifier A 24-bit or 8-bit value used to identify the source or destination of a frame. *See also* S_ID *and* D_ID.

Advanced Fabric Services, Brocade A Brocade proprietary feature.

Advanced Performance Monitoring, Brocade A Brocade proprietary feature.

Advanced Zoning, Brocade A Brocade proprietary feature.

AL_PA Arbitrated-loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop. Alternately, “arbitrated-loop parameters.”

alias A logical grouping of elements in a fabric. An alias is a collection of port numbers and connected devices, used to simplify the entry of port numbers and WWNs when creating zones.

arbitrated loop A shared 100-Mbit/sec Fibre Channel transport structured as a loop. Can support up to 126 devices and one fabric attachment. *See also* topology.

area number In Brocade Fabric OS v4.0 and above, ports on a switch are assigned a logical area number. Port area numbers can be viewed by entering the **switchShow** command. They are used to define the operative port for many Fabric OS commands: for example, area numbers can be used to define the ports within an alias or zone.

authentication The process of verifying that an entity in a fabric (such as a switch) is what it claims to be.

B

BB_Credit Buffer-to-buffer credit. The number of frames that can be transmitted to a directly connected recipient or within an arbitrated loop. Determined by the number of receive buffers available.

beacon A tool in which all of the port LEDs on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by a CLI command or through Brocade Advanced Web Tools.

C

CHAP Challenge-Handshake Authentication Protocol. Allows remote servers and clients to securely exchange authentication credentials. Both the server and client are configured with the same shared secret.

chassis The metal frame in which the switch and switch components are mounted.

CLI Command line interface. An interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.

client An entity that, using its common transport (CT), makes requests of a server.

community (SNMP) A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. *See also* SNMP.

compact flash Flash (temporary) memory that is used in a manner similar to hard disk storage. It is connected to a bridging component that connects to the PCI bus of the processor. Not visible within the processor's memory space.

configuration (1) A set of parameters that can be modified to fine-tune the operation of a switch. Use the **configShow** command to view the current configuration of your switch.

(2) In Brocade Zoning, a zoning element that contains a set of zones. The Configuration is the highest-level zoning element and is used to enable or disable a set of zones on the fabric. *See also* zone configuration.

CP Control processor.

credit As it applies to Fibre Channel technology, the number of receive buffers available to transmit frames between ports. *See also* BB_Credit.

D

D_ID Destination identifier. A 3-byte field in the frame header, used to indicate the address identifier of the N_Port to which the frame is headed.

defined zone configuration The complete set of all zone objects defined in the fabric. Can include multiple zone configurations. *See also* effective zone configuration, enabled zone configuration, zone configuration.

director A Brocade SilkWorm 12000 or 24000 switch.

DLS Dynamic load-sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

domain ID A unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch but can be assigned manually. The domain ID for a Brocade SilkWorm switch can be any integer from 1 through 239.

E

E_D_TOV Error-detect timeout value. The minimum amount of time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error is declared. *See also* R_A_TOV.

E_Port Expansion port. A standard Fibre Channel mechanism that enables switches to network with each other, creating an ISL. *See also* ISL.

effective zone configuration A subset of the defined zone configuration, containing only the zone configuration object that is currently enabled. Only one configuration can be active at a time, but since multiple configurations can be *defined* in the database, a new configuration can be easily switched. *See also* defined zone configuration.

enabled zone configuration The currently enabled configuration of zones. Only one configuration can be enabled at a time. *See also* defined zone configuration, zone configuration.

error As it applies to the Fibre Channel industry, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors).

Ethernet Popular protocols for LANs.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. *See also* FL_Port, Fx_Port.

fabric A collection of Fibre Channel switches and devices, such as hosts and storage. Also referred to as a “switched fabric.” *See also* SAN, topology.

Fabric Manager An optionally licensed Brocade software. Fabric Manager is a GUI that allows for fabric-wide administration and management. Switches can be treated as groups, and actions such as firmware downloads can be performed simultaneously.

Fabric Mode One of two possible modes for an L_Port, in which the L_Port is connected to another port that is not loop capable, using fabric protocol.

fabric services Codes that describe the communication to and from any well-known address.

fabric topology The arrangement of switches that form a fabric.

Fabric Watch An optionally licensed Brocade software. Fabric Watch can be accessed through either the command line or Advanced Web Tools, and it provides the ability to set thresholds for monitoring fabric conditions.

failover Describes the Brocade SilkWorm 12000 and 24000 process of one CP passing active status to another CP. A failover is nondisruptive.

FAN Fabric address notification. Retains the AL_PA and fabric address when a loop reinitializes, if the switch supports FAN.

FCS Fibre Channel switch; alternatively, Fabric Configuration Server.

FCS switch Relates to the Brocade Secure Fabric OS feature. One or more designated switches that store and manage security parameters and configuration data for all switches in the fabric. They also act as a set of backup switches to the primary FCS switch. *See also* primary FCS switch.

Fibre Channel The primary protocol used for building SANs to transmit data between servers, switches, and storage devices. Unlike IP and Ethernet, Fibre Channel was designed to support the needs of storage devices of all types. It is a high-speed, serial, bidirectional, topology-independent, multiprotocol, and highly scalable interconnection between computers, peripherals, and networks.

FICON® A protocol used on IBM mainframes. Brocade SilkWorm switch FICON support enables a SilkWorm fabric to transmit FICON format data between FICON-capable servers and storage.

firmware The basic operating system provided with the hardware.

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated-loop capabilities. Can be used to connect an NL_Port to a switch. *See also* F_Port, Fx_Port.

flash Programmable nonvolatile RAM (NVRAM) memory that maintains its contents without power.

frame The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements and so forth) and data frames.

FRU Field-replaceable unit. A component that can be replaced onsite.

FSPF Fabric shortest path first. The Brocade routing protocol for Fibre Channel switches.

FTP File Transfer Protocol.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. *See also* F_Port, FL_Port.

G

gateway Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

GBIC Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for Fibre Channel and gigabit Ethernet.

Gbit/sec Gigabits per second (1,062,500,000 bits/second).

GB/sec Gigabytes per second (1,062,500,000 bytes/second).

GUI A graphic user interface, such as Brocade Advanced Web Tools arbitrated-loop topology and Brocade Fabric Manager.

H

HA High availability. A set of features in Brocade SilkWorm switches that is designed to provide maximum reliability and nondisruptive replacement of key hardware and software modules.

header A Fibre Channel frame has a header and a payload. The header contains control and addressing information associated with the frame.

host A computer system that provides end users with services like computation and storage access.

HTTP Hypertext Transfer Protocol. The standard TCP/IP transfer protocol used on the World Wide Web.

I

initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices. *See also* target.

Insistent Domain ID Mode Sets the domain ID of a switch as insistent, so that it remains the same over reboots, power cycles, failovers, and fabric reconfigurations. This mode is required to support FICON® traffic.

interswitch link *See* ISL.

IOD In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

IP Internet Protocol. The addressing part of TCP.

ISL Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. *See also* E_Port.

J

K

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated-loop capabilities. An L_Port can be in either Fabric Mode or Loop Mode.

LAN Local area network. A network in which transmissions typically take place over fewer than 5 kilometers (3.4 miles).

LED Light-emitting diode. Used to indicate the status of elements on a switch.

loop initialization The logical procedure used by an L_Port to discover its environment. Can be used to assign AL_PA addresses, detect loop failure, or reset a node.

Loop Mode One of two possible modes for an L_Port, in which the L_Port is in an arbitrated loop, using loop protocol. An L_Port in Loop Mode can also be in Participating Mode or Nonparticipating Mode.

LUN Logical unit number.

M

Mbit/sec Megabits per second.

N

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. *See also* NL_Port, Nx_Port.

Name Server Simple Name Server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as "directory service."

NL_Port Node loop port. A node port that has arbitrated-loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. *See also* N_Port, Nx_Port.

node A Fibre Channel device that contains an N_Port or NL_Port.

node name The unique identifier for a node, communicated during login and port discovery.

Nonparticipating Mode A mode in which an L_Port in a loop is inactive and cannot arbitrate or send frames but can retransmit received transmissions. This mode is entered if there are more than 127 devices in a loop and an AL_PA cannot be acquired. *See also* L_Port, Participating Mode.

NS Name Server. The service provided by a fabric switch that stores names, addresses, and attributes related to Fibre Channel objects. Can cache information for up to 15 minutes. Also known as "Simple Name Server" or as a "directory service." *See also* Simple Name Server (SNS).

Nx_Port A node port that can operate as either an N_Port or NL_Port.

O

P

Participating Mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. *See also* L_Port, Nonparticipating Mode.

path selection The selection of a transmission path through the fabric. Brocade switches use the FSPF protocol. *See also* FSPF.

payload A Fibre Channel frame has a header and a payload. The payload contains the information being transported by the frame; it is determined by the higher-level service or FC_4 upper-level protocol. There are many different payload formats, based on protocol.

Performance Monitoring A Brocade SilkWorm switch feature that monitors port traffic and includes frame counters, SCSI read monitors, SCSI write monitors, and other types of monitors.

PID Port identifier.

PLOGI Port login. The port-to-port login process by which initiators establish sessions with targets.

point-to-point A Fibre Channel topology that employs direct links between each pair of communicating entities. *See also* topology.

port In a Brocade SilkWorm switch environment, an SFP or GBIC receptacle on a switch to which an optic cable for another device is attached.

port address In Fibre Channel technology, the port address is defined in hexadecimal. In the Brocade Fabric OS, a port address can be defined by a domain and port number combination or by area number. In an ESCON Director, an address used to specify port connectivity parameters and to assign link addresses for attached channels and control units.

port card A hardware component that provides a platform for field-replaceable, hot swappable ports.

port group A group of adjacent ports that share a common pool of frame buffers for long distance connections.

port-level zoning Defines a zone member by “domain,port”, which is the physical port to which the member is connected. *See also* zone member, WWN-level zoning.

port log A record of all activity on a switch, kept in volatile memory.

port name A user-defined alphanumeric name for a port.

port swapping Port swapping is the ability to redirect a failed port to another port. This feature is available in Fabric OS v4.1.0 and higher.

POST Power-on self-test. A series of tests run by a switch after it is turned on.

primary FCS switch Relates to the Brocade Secure Fabric OS feature. The primary fabric configuration server switch actively manages security and configurations for all switches in the fabric. *See also* FCS switch.

principal switch The first switch to boot up in a fabric. Ensures unique domain IDs among roles.

private device A device that supports arbitrated-loop protocol and can interpret 8-bit addresses but cannot log in to the fabric.

private loop An arbitrated loop that does not include a participating FL_Port.

private NL_Port An NL_Port that communicates only with other private NL_Ports in the same loop and does not log in to the fabric.

protocol A defined method and set of standards for communication. Determines the type of error-checking, the data-compression method, how sending devices indicate an end of message, and how receiving devices indicate receipt of a message.

public device A device that supports arbitrated-loop protocol, can interpret 8-bit addresses, and can log in to the fabric.

public loop An arbitrated loop that includes a participating FL_Port and can contain both public and private NL_Ports.

Q

QuickLoop A Brocade software product that allows multiple ports on a switch to create a logical loop. Devices connected via QuickLoop appear to each other as if they are on the same arbitrated loop.

R

R_A_TOV Resource allocation timeout value. The maximum time a frame can be delayed in the fabric and still be delivered. *See also* E_D_TOV.

route As it applies to a fabric, the communication path between two switches. Might also apply to the specific path taken by an individual frame, from source to destination. *See also* FSPF.

routing The assignment of frames to specific switch ports, according to frame destination.

S

S_ID Source ID. Refers to the native port address (24 bit address).

SAN Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. *See also* fabric.

SCSI Small Computer Systems Interface. A parallel bus architecture and a protocol for transmitting large data blocks to a distance of 15 to 25 meters.

sectelnet A protocol similar to telnet but with encrypted passwords for increased security.

Secure Fabric OS An optionally licensed Brocade feature that provides advanced, centralized security for a fabric.

security policy Rules that determine how security is implemented in a fabric. Security policies can be customized through Brocade Secure Fabric OS or Brocade Fabric Manager.

sequence A group of related frames transmitted in the same direction between two N_Ports.

serial The transmission of data bits in sequential order over a single line.

server A computer that processes end-user applications or requests.

SFP Small-form-factor pluggable. A transceiver used on 2 GB/sec and 4 GB/sec switches that replaces the GBIC.

SilkWorm The brand name for the Brocade family of switches.

Simple Name Server (SNS) A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also referred to as "directory service" or "name server."

SNMP Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. *See also* community (SNMP).

SNS Simple Name Server.

soft zone A zone consisting of zone members that are made visible to each other through client service requests. Typically, soft zones contain zone members that are visible to devices using Name Server exposure of zone members. The fabric does not enforce a soft zone. Note that well-known addresses are implicitly included in every zone.

SSH Secure shell. Used starting in Brocade Fabric OS v4.1 to support encrypted telnet sessions to the switch. SSH encrypts all messages, including the client sending the password at login.

switch A fabric device providing bandwidth and high-speed routing of data via link-level addressing.

switch name The arbitrary name assigned to a switch.

switch port A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.

syslog Syslog daemon. Used to forward error messages.

T

T11 A standards committee chartered with creating standards for Fibre Channel.

target A storage device on a Fibre Channel network. *See also* initiator.

TCP/IP Transmission Control Protocol Internet Protocol.

telnet A virtual terminal emulation used with TCP/IP. "Telnet" is sometimes used as a synonym for the Brocade Fabric OS CLI.

throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second or b/sec).

Time Server A Fibre Channel service that allows for the management of all timers.

topology As it applies to Fibre Channel technology, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

> **Point to point.** A direct link between two communication ports.
>
> **Switched fabric.** Multiple N_Ports linked to a switch by F_Ports.
>
> **Arbitrated loop.** Multiple NL_Ports connected in a loop.

transceiver A device that converts one form of signaling to another for transmission and reception; in fiber optics, optical to electrical.

trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. *See also* SNMP.

trunking In Fibre Channel technology, a feature that enables distribution of traffic over the combined bandwidth of up to four ISLs between adjacent switches, while preserving in-order delivery.

trunking group A set of up to four trunked ISLs for SilkWorm 3016, 3200, 3250, 3800, 3850, 3900, 12000, and 24000; up to eight for SilkWorm 4100.

U

V

W

watchdog A software daemon that monitors Fabric OS modules on the kernel.

well-known address As it pertains to Fibre Channel technology, a logical address defined by Fibre Channel standards as assigned to a specific function and stored on the switch.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

WWN-level zoning Defines a zone member using WWW port or WWN node. Defining a zone member as WWN allows the member (device) to be attached without regard to its physical location.

X

Y

Z

zone A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access to others in the zone but are not visible to any outside the zone.

zone configuration A specified set of zones. Enabling a configuration enables all zones in that configuration. *See also* defined zone configuration, enabled zone configuration, and effective zone configuration.

zone member Defines a device. A zone member can belong to more than one zone at a time.A zone member can be defined by either port-level zoning (domain,port: the physical port to which it is connected) or WWN-level zoning (using WWW port or WWN node).

zoning, port-level *See* port-level zoning.

zoning, WWN-level *See* WWN-level zoning.

Index