Fabric OS

Features Guide

Supporting Fabric OS v4.4.0

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

Publication Number: 53-0000395-02
Publication Date: 9/15/2004

 Publication Number: 53-0000395-02

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 Fabric OS Features Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
Fabric OS Features Guide	53-0000395-01	First edition.	December 2003
Fabric OS Features Guide	53-0000395-02	Revised for Fabric OS v4.4.0.	September 2004

Contents

About This Document

This document provides a brief, high-level overview of Brocade Fabric OS standard features and licensed products.

How This Document Is Organized

The document contains the following topics:

- "Standard Features" on page 1-1 outlines the standard features of Fabric OS.
- "Management Features" on page 2-1 outlines licensed features that are available for managing Brocade SilkWorm models.
- "Brocade Extended Fabrics" on page 3-1 describes the Extended Fabrics licensed feature.
- "Brocade ISL Trunking" on page 4-1 describes the ISL Trunking licensed feature.
- "Brocade Advanced Zoning" on page 5-1 describes the Advanced Zoning licensed feature.
- "Brocade Advanced Performance Monitoring" on page 6-1 describes the Advanced Performance Monitoring licensed feature.
- "Brocade Support for FICON CUP Fabrics" on page 7-1 describes the Brocade licensed feature for FICON® CUP technology.
- 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 applies to Fabric OS v4.4.0 running on the following Brocade SilkWorm product models:

- 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

What's New in This Document

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

- The entire document was streamlined. Duplicated information from other Brocade documents and obsolete graphics were deleted.
- Fabric OS v4.4.0 features were added. These features are more fully described in the *Brocade Fabric OS Procedures Guide* and the documentation for the various Brocade licensed products.

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 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 Advanced Web Tools Administrator's Guide*
- *Brocade Fabric Watch User's Guide*
- *Brocade Secure Fabric OS User's Guide*
- *Brocade Secure Fabric OS QuickStart Guide*

SilkWorm 24000

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

SilkWorm 12000

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

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

Document Feedback

Brocade Communications Systems, Inc. makes 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.

Standard Features

Chapter 1

This chapter describes features that are standard with Fabric OS.

Configurable Accounts

Fabric OS provides different levels of authorization—called *roles*—for using the system:

- *admin* level for administrative use
- *user* level for nonadministrative use, such as monitoring system activity

The system provides default user and admin accounts. You can create up to 15 additional accounts per logical switch and designate their roles as either admin or user.

Table 1-1 shows the number of simultaneous login sessions allowed for each role.

Table 1-1 Maximum Number of Simultaneous Sessions

User Name	Maximum Sessions
admin	2
user	4

High Availability Features

Fabric OS High Availability (HA) features ensure stable fabric operations through the use of redundancy, hot-swapping, and nondisruptive operations. Table 1-2 summarizes the HA features available on various SilkWorm models.

Table 1-2 Fabric OS High Availability

Feature	24000	12000	4100	3900	3850	3250	3016
Redundant AC cables	Yes	Yes	Yes	Yes	Yes		
Redundant, hot-swappable power supplies	Yes	Yes	Yes	Yes			
Redundant, hot-swappable fans	Yes	Yes	Yes	Yes			
Hot-swappable port cards	Yes	Yes					
Hot-swappable control processor (CP) cards	Yes	Yes					
Hot-swappable WWN card	Yes	Yes					

Table 1-2 Fabric OS High Availability (Continued)

Feature	24000	12000	4100	3900	3850	3250	3016
Nondisruptive CP failover	Yes	Yes					
Background CP health monitor	Yes	Yes					
Nondisruptive firmware download	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Nondisruptive code activation	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Secure Protocols

Fabric OS supports the secure protocols shown in Table 1-3.

Table 1-3 Secure Protocol Support

Protocol	Description
SSL	Supports SSLv3, 128-bit encryption by default. Fabric OS uses SSL to support HTTPS. To enable SSL, a certificate must be generated and installed to each switch.
HTTPS	Graphical user interfaces (GUIs) support HTTPS.
Secure File Copy (scp)	Configuration upload and download support the use of scp. Firmware download does not use scp.
SNMPv3	SNMPv1 is also supported.

SSL and HTTPS support secure operations through GUIs such as Advanced Web Tools.

Secure file copy (scp) supports secure configuration maintenance.

Simple Network Management Protocol (SNMP) is a standard method for monitoring and managing network devices. Using SNMP components, you can program tools to view, browse, and manipulate Brocade switch variables and set up enterprise-level management processes.

Every Brocade switch carries an SNMP agent and management information base (MIB). The agent accesses MIB information about a device and makes it available to a network manager station. You can manipulate information of your choice by *trapping* MIB elements using the Fabric OS CLI, Advanced Web Tools, or Fabric Manager.

The SNMP Access Control List (ACL) provides a way for the administrator to restrict SNMP get/set operations to certain hosts/IP addresses. This would be used for enhanced management security in the storage area network.

For details on the Brocade MIB files, naming conventions, loading instructions, and information about using Brocade's SNMP agent, refer to the *Brocade MIB Reference Manual*.

Table 1-4 describes additional software or certificates that you must obtain to deploy secure protocols.

Table 1-4 Items Needed to Deploy Secure Protocols

Protocol	Host Side	Switch Side
Secure telnet	Secure telnet client	License for Brocade Secure Fabric OS
SSH	SSH client	None
HTTPS	Certificate Authority	Switch IP certificate for SSL
Secure file copy (scp)	SSH daemon, scp server	None
SNMPv3, SNMPv1	None	None

The security protocols are designed with the four main usage cases described in Table 1-5.

Table 1-5 Main Security Scenarios

Fabric	Traffic Management	Configuration via Policy	Comments
Nonsecure	Nonsecure	No	No special setup is needed.
Nonsecure	Secure/ nonsecure	No	Allows secure fabric management without the use of Secure Fabric OS. SSL certificates must be installed.
Secure	Secure	Yes	Encrypted protocols are supported on Fabric OS v4.4.0 (and later) switches. Fabric OS v3.2.0 switches support telnet and secure telnet only. Switches running earlier Fabric OS versions can be part of the secure fabric, but they do not support secure management. Secure management must be enabled on each participating switch. Nonsecure management can be disabled on nonparticipating switches. If SSL is used, then certificates must be installed.
Secure	Nonsecure/ secure	Yes	Nonsecure traffic management is necessary under these circumstances: • The fabric contains switches running Fabric OS 3.2.0. • The presence of software tools that do not support secure protocols; for example, Fabric Manager v4.0.0. • The fabric contains switches running Fabric OS versions earlier than v4.4.0. Nonsecure management is enabled by default.

RADIUS AAA Service

For large enterprises, 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.

Director CP Card Management

SilkWorm directors support these CP card management features:

- SilkWorm 24000, which is configured by default with one domain, can be configured with two domains.
- Mixed card support

  Systems with SilkWorm 24000 CP cards installed can support various combinations of 12000 and 24000 port cards:

  - one domain of 128 ports, 24000 port cards only
  - two domains, 64 ports per domain, 24000 port cards only
  - two domains, 24000 port cards on one domain and 12000 port cards in the other

Routing Policies

All SilkWorm models support *port-based* routing, in which the routing path chosen for an incoming frame is based only on the incoming port and the destination domain. 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.

The SilkWorm 4100 model allows you to tune routing performance with these additional routing policies:

- *device-based* routing, in which the choice of routing path is based on the Fibre Channel addresses of the source device (S_ID) and the destination device (D_ID), improving path utilization for better performance
- *exchange-based* routing, in which the choice of routing path is based on the S_ID, D_ID, and Fibre Channel originator exchange ID (OXID), optimizing path utilization for the best performance

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*.

Message Logging

Standard features allow you to display system, port, and specific hardware messages. You can set up system logging mapping (**syslogd**) and you can specify that the system offload diagnostic messages to a server automatically.

SilkWorm director models provide a unique error log on each CP.

Fabric OS also maintains a separate, internal port log of all port activity, which can be used to troubleshoot device connections.

Fabric OS Command Line Interface

The Fabric OS command line interface (CLI) lets you monitor and manage entire fabrics, individual switches, and ports from a standard workstation. The entire suite of Fabric OS features and capabilities is available across an entire fabric from a single access point.

Access is controlled by a switch-level password for each account. CLI commands are based on the account role and activated license keys. All configuration and management tasks are available using the admin or user role.

Distributed Management Server

The Brocade Fabric OS Distributed Management Server allows a SAN management application to retrieve information and administer interconnected switches, servers, and storage devices. The management server assists in the autodiscovery of switch-based fabrics and their associated topologies.

A client of the management server can find basic information about the switches in the fabric and use this information to construct topology relationships. The management server also allows you to obtain certain switch attributes and, in some cases, modify them. For example, logical names identifying switches can be registered with the management server.

The management server provides several advantages for managing a Fibre Channel fabric:

- It is accessed by an external Fibre Channel node at the well-known address FFFFFAh, so an application can access information about the entire fabric management with minimal knowledge of the existing configuration.
- It is replicated on every SilkWorm switch within a fabric (Fabric OS v2.3.0 and later).

- It provides an unzoned view of the overall fabric configuration. This fabric topology view exposes the internal configuration of a fabric for management purposes; it contains interconnect information about switches and devices connected to the fabric. Under normal circumstances, a device (typically an FCP initiator) queries the Name Server for storage devices within its member zones. Because this limited view is not always sufficient, the management server provides the application with a list of the entire Name Server database.

Note

Management server platform service is available only with Fabric OS v2.3.0 and later. If the management server platform service is started on a fabric that contains any switches running earlier Fabric OS versions, services are not enabled.

Brocade Support for FICON

IBM Fibre Connections (FICON®) is an industry-standard, high-speed input/output (I/O) interface for mainframe connections to storage devices. Fabric OS supports *intermix mode* operations, in which FICON and Fibre Channel technology work together. For specific information about intermix mode and other aspects of FICON, refer to the IBM Redbook, *FICON® Native Implementation and Reference Guide*.

Fabric OS provides standard support for FICON single-switch operation.

Multiple-switch cascaded FICON operation requires a Brocade Secure Fabric OS license.

Control Unit Port (CUP) operation requires a Brocade FICON CUP license. For information on CUP, refer to "Brocade Support for FICON CUP Fabrics" on page 7-1.

The following Fabric OS standard features support FICON fabrics:

- Port swapping redirects resources from a failed port to a healthy port without changing the FICON host configuration. Port swapping is available for both FICON and open system environments. Port swapping resolves situations in which the hardware has failed and the channel configurations cannot be changed quickly. Port swapping has minimal or no impact on other switch features.
- Insistent domain ID (IDID) allows the switch to insist on a specific domain ID before joining a fabric. This feature guarantees that a switch operates only with its preassigned domain ID.
- The FICON MIB module addresses link incident data for FICON hosts and devices connected to a switch. It supplements other MIBs used to manage switches and should be used in conjunction with those other MIBs. For more information, refer to the *Brocade MIB Command Reference Manual*.
- Link incident detection, registration, and reporting provide administrative and diagnostic information.

These optional features provide further support:

- The Secure Fabric OS optional license includes fabric binding, switch binding, and port binding security methods that prevent unauthorized devices from joining a fabric.
- A Fabric Manager optional license can be used to manage a fabric that supports FICON and FCP devices and traffic. This is the recommended GUI management tool for FICON environments.
- Advanced Web Tools can be used to manage a fabric that supports FICON and Fibre Channel Protocol (FCP) devices and traffic.

To incorporate and manage FICON on a switch or fabric, your system must have Fabric OS v4.1.2 or later installed. If you are implementing FICON in a single-switch *noncascaded environment*, there are no additional software requirements. The Secure Fabric OS and Advanced Zoning optional Brocade licensed features are required on all switches participating in a FICON multiple-switch *cascaded* environment:

Note

Some licenses are installed and activated on the switch at the factory. Use a Brocade management interface to verify that the required licenses are installed and activated on the switch. Refer to the *Brocade Fabric OS Procedures Guide* for detailed instructions.

The optional Secure Fabric OS license provides these fabric, switch, and port binding features:

- *Fabric binding* is a security method for restricting switches within a multiple-switch fabric. The Switch Connection Control (SCC) policy prevents unauthorized switches from joining a fabric. Switches are authenticated using digital certificates and unique private keys provided to the Switch Link Authentication Protocol (SLAP).
- *Switch binding* is a security method for restricting devices that connect to a particular switch. If the device is another switch, this is handled by the SCC policy. If the device is a host or storage device, the Device Connection Control (DCC) policy binds those devices to a particular switch. Powerful policies provide a range from completely restrictive to reasonably flexible policies, based upon customer needs.
- *Port binding* is a security method for restricting host or storage devices that connect to particular switch ports. The DCC policy also binds device ports to switch ports. Powerful policies provide a range from completely restrictive to reasonably flexible policies, based upon customer needs.

For more information, refer to the *Brocade Secure Fabric OS User's Guide*.

Chapter
2

Management Features

This chapter describes optional features that can be used to manage Brocade SilkWorm models.

Brocade Advanced Web Tools

Brocade Advanced 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.

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.

Brocade Fabric Manager

Fabric Manager is a complete storage area network (SAN) management tool for Brocade-based SANs. You can use Fabric Manager to configure multiple switches simultaneously from one location, view the status of multiple devices in one window, and perform SAN-level maintenance without having to access each switch in your fabric or SAN. Fabric Manager is tightly integrated with additional SAN management products (including Advanced Web Tools and Fabric Watch), and can be used in conjunction with other SAN and storage resource management applications as the tool to drill down into single or multiple Brocade fabrics.

Fabric Manager includes the following basic features to manage multiple SANs:

- Manages multiple Brocade switch elements across multiple fabrics.
- Discovers and collects SAN data, and provides multiple views of that data (including topology maps and detailed views in a tabular format).
- Displays the status of critical fabric elements and key discovery data at varying levels of detail, such as high-level “At-A-Glance” views, and detailed tables that display information about switches, ports, devices, and events.
- Presents data and management console views designed for effective management of a FICON environment.

Fabric Manager includes the following advanced features for additional management capabilities:

- Fabric, switch, and port naming
- Data storage (persistent files)

- Change management
- License key management
- HBA management
- Scalable firmware download
- Call home support
- End-to-end performance monitoring
- Secure Fabric OS management

Brocade Fabric Watch

Brocade Fabric Watch is a SAN health monitor for Brocade SilkWorm switches running Fabric OS v2.2 or later. It enables each switch to constantly watch its SAN fabric for potential faults and to automatically alert you to problems long before they become costly failures.

Fabric Watch tracks a variety of SAN fabric elements, events, and counters. Monitoring fabric-wide events, ports, GBICs, and environmental parameters enables early fault detection and isolation as well as performance measurement. You can select custom fabric elements and alert thresholds or choose from a selection of preconfigured settings. You can also easily integrate Fabric Watch with enterprise systems management solutions.

By implementing Fabric Watch, you can rapidly improve SAN availability and performance without installing new software or system administration tools.

Brocade Fabric Access

Brocade Fabric Access is an application programming interface (API) that enables software applications to interact with Brocade SilkWorm switches. Fabric Access gives third-party software the ability to retrieve detailed information about fabrics, such as properties, statistics, and states of fabric elements. Fabric Access also gives applications the ability to control and configure many fabric functions and properties, including zoning.

Brocade Secure Fabric OS

Brocade Secure Fabric OS provides customizable security restrictions through local and remote management channels on a SilkWorm fabric. Secure Fabric OS provides the ability to:

- Create policies to customize fabric management access.
- Specify which switches and devices can join the fabric.
- View statistics related to attempted policy violations.
- Manage the fabric-wide Secure Fabric OS parameters through a single switch.
- Create temporary passwords specific to a login account and switch.
- Enable and disable Secure Fabric OS as desired.

Secure Fabric OS uses digital certificates based on PKI or Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) shared secrets to provide switch-to-switch authentication.

Ports on Demand

The Brocade Ports on Demand feature is available on the SilkWorm 4100 model.

Ports on Demand enables you to scale your fabric as necessary. You can buy a switch with a subset of the ports activated. If you need more ports in your fabric, you can upgrade by purchasing a license key.

Chapter

3

Brocade Extended Fabrics

The Brocade Extended Fabrics optional feature extends the distance that interswitch links (ISLs) can reach.

As the distance between switches and the link speed increase, additional *buffer-to-buffer credits* are required to maintain maximum performance. The number of credits reserved for a port depends on the switch model and on the extended ISL mode for which it is configured.

For SilkWorm 3016, 3250, 3850, 3900, 12000, and 24000 models, each *port group* (called a *quad* on these models) contains four ports and shares a common pool of credits. Because the number of credits available for use within each port group is limited, configuring ports for extended links on these models might cause other ports to become disabled if there are not enough buffer credits available.

For the SilkWorm 4100 model, each port group contains eight ports and buffer credits are shared among all ports on the switch. *Buffer-limited* port technology allows all ports to remain operational, even when extended links are in use. A buffer-limited port can come online with fewer buffer credits allocated than its configuration specifies, allowing it to operate at a reduced bandwidth instead of being disabled for lack of buffers. Buffer-limited operation is persistent across switch reboots or power cycles.

Long-distance connections can participate in trunking if the Brocade ISL Trunking license is installed. For more information, refer to "Brocade ISL Trunking" on page 4-1.

Brocade ISL Trunking

Chapter 4

The Brocade ISL Trunking optional feature allows interswitch links between two SilkWorm models to merge logically into a group link. ISL Trunking reduces or eliminates situations that require static traffic routes and individual ISL management to achieve optimal performance.

Trunking optimizes fabric performance by distributing traffic across the shared bandwidth of all the interswitch links in a trunking group, allowing traffic to flow through any available link in a group rather than restricting it to a specific, potentially congested link. The use of trunking results in simplified fabric design and management, lowered cost of ownership, and increased data availability.

A trunking license is required on each switch that participates in trunking.

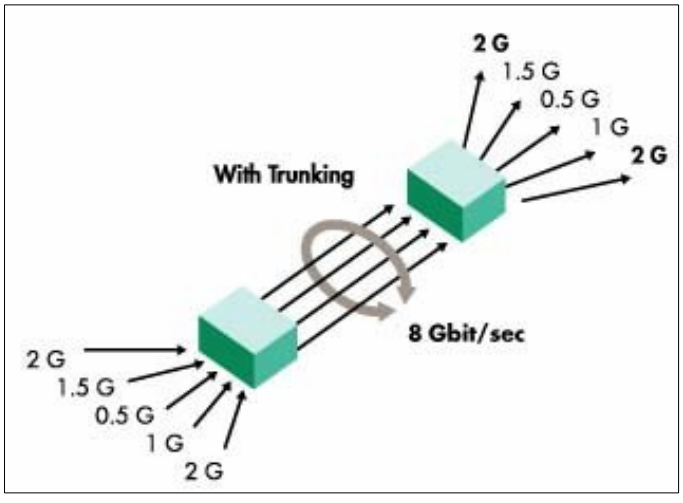
Trunks distribute traffic dynamically and in order at the frame level, achieving greater performance with fewer interswitch links.

Trunks are compatible with both short wavelength (SWL) and long wavelength (LWL) fiber optic cables and transceivers.

Trunking is enabled automatically when the ISL Trunking license is activated and ports are reinitialized, and trunks are easily managed using either Fabric OS CLI commands or Brocade Advanced Web Tools. You can enable and disable trunking and set trunk port speeds for entire switches or for individual ports.

Figure 4-1 illustrates how trunking can result in more throughput by distributing data over four ISLs with no congestion. In a fabric that does not have trunking capability, some paths would be congested and other paths underutilized.

Figure 4-1 Distribution of Traffic Over an ISL Trunking Group



Trunks operate best when the cable length of each trunked link is roughly equal to the others in the trunk. Cable lengths for participating links should differ by no more than 30 meters.

Connections between SilkWorm 4100 models support these advanced features:

- Up to eight ports in one trunk group
- ISL Trunking over longer distances than other models
- Dynamic trunk master reassignment if a trunk master is disabled (on other platforms, all ports on a trunk must be disabled temporarily to reassign a master)
- 4 Gbit/sec trunk links

The maximum number of ports per trunk and trunks per switch depends on the SilkWorm model.

Brocade Advanced Zoning

Chapter 5

Brocade Advanced Zoning is a licensed feature that allows you to partition a SAN into logical groupings—called *zones*—of devices that have access to each other.

Through the use of zoning, you can customize environments and optimize resources. All devices connected to a fabric can be configured into one or more zones. After you enable zoning, devices that are not explicitly defined in a zone are isolated and other devices in the fabric cannot access them.

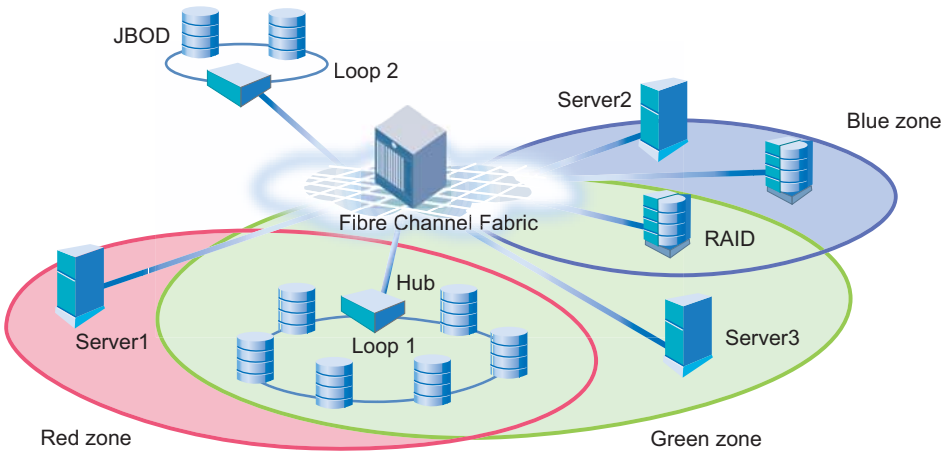
You can use zones to create logical subsets of the fabric to accommodate environments such as closed user groups or functional areas within the fabric. For example, you can identify selected devices within a zone for the exclusive use of zone members, or you can define a zone to create separate test or maintenance areas within the fabric.

You can use zones to logically consolidate equipment for efficiency or to facilitate time-sensitive functions; for example, to create a temporary zone to back up nonmember devices.

Any zone object connected to the fabric can be included in one or more zones. Zone objects can communicate only with other objects in the same zone. For example, consider Figure 5-1, which shows:

- Three zones are configured, named Red, Green, and Blue.
- Server 1 can communicate only with the Loop 1 devices.
- Server 2 can communicate only with the RAID and Blue zone devices.
- Server 3 can communicate with the RAID device and the Loop1 device.
- The Loop 2 JBODs are not assigned to a zone; no other zoned fabric device can access them.

Figure 5-1 Zoning Example



Zones can be configured dynamically and can vary in size, depending on the number of fabric-connected devices.

Zoning can be disabled at any time. When zoning is disabled, devices can freely access other devices in the fabric.

Zone configurations persist across reboots and power cycles. If two switches are connected in a fabric, they can become isolated (for example, due to an ISL failure); however, when rejoined, they maintain the same fabric configuration unless one of the switches has had a configuration change.

Zoning can be enabled in most storage units, in the switch fabric, and on the host. Zone administration is simplified when you use the Brocade Advanced Web Tools wizard.

Chapter

6

Brocade Advanced Performance Monitoring

Advanced Performance Monitoring is an optionally licensed product used for monitoring the performance of networked storage resources. This tool helps reduce overprovisioning and enables SAN performance tuning.

Advanced Performance Monitoring provides SAN performance monitoring through an end-to-end monitoring system that provides:

- Increased end-to-end visibility into the fabric.
- More accurate reporting for service-level agreements and charged access applications.
- Shortened troubleshooting time.
- Better capacity planning.
- Increased productivity through preformatted and customized screens and reports.

You can administer APM through the Fabric OS CLI, Brocade Advanced Web Tools, or Brocade Fabric Manager.

Using APM, you can monitor the following statistics:

- Measure the bandwidth consumed by individual routes (host-target pairs).
- Provide device performance measurements by port, AL_PA, and LUN.
- Report CRC error measurement statistics.
- Compare IP versus SCSI traffic on each port.
- Produce a wide range of predefined reports.
- Create customized user-defined reports.
- Provide a performance history for each port.
- With the Brocade Fabric Manager, you can store performance data persistently off the switch and maintain historical data for the performance of the switches in your fabric.

ISL monitoring is set up on E_ports automatically in Fabric OS v4.4.0 and later.

Using the Brocade Fabric Manager software application version 4.4.0 (or later), you can store Advanced Performance Monitoring data persistently off the switch.

Chapter

7

Brocade Support for FICON CUP Fabrics

Brocade FICON CUP is an optionally licensed product for managing FICON fabrics.

Control Unit Port (CUP) protocol enables IBM host-based management programs to manage switches in-band by sending commands to the Fabric OS emulated control device.

These Brocade platforms support FICON CUP:

- SilkWorm 3900
- SilkWorm 12000
- SilkWorm 24000

You can use CUP on a single-switch configuration or on a cascaded switch configuration.

You can manage CUP using Brocade Advanced Web Tools or Brocade Fabric Manager. Limited support for CUP is provided through the Fabric OS CLI.

CUP provides the following advantages:

- Single point of control and monitoring for channel, director (switch), and control unit.
- Automated tools on the mainframe can take advantage of the statistics to move channels where they are needed. This cannot be done from the switch alone.
- Seamless integration into existing management tools that are also used to manage ESCON Directors (switches). This makes migration from ESCON to FICON smoother.

You can monitor the FICON director (switch) using CUP to obtain the following information:

- Port statistics
  - Number of words transmitted
  - Number of words received
  - Frame Pacing Time, which is the number of 2.5-microsecond units that frame transmission is blocked due to 0 credit.

  Refer to the IBM document *FICON Director Programming Interface with Cascading Support.*
- Switch node identifier

  You can find switch node information, such as the serial number and the manufacturer name. This information is the same as the Switch Node ID in the RNID ELS (support in Fabric OS v4.1.2).
- Configuration file information

  You can get a list of configuration files on the switch. You can also obtain the actual file content, including port address name and port connectivity.
- History summary (director history buffer)

The history buffer logs each change in status or configuration of the ports. You can retrieve the history buffer using CUP.

- Switch configuration data

  You can get switch configuration data such as timeout values and number of ports per card.

For information on CUP functions and commands, refer to the IBM-proprietary document *FICON Director Programming Interface With Cascading Support.*

Glossary

A

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.

B

buffer-to-buffer flow control Management of the frame transmission rate in either a point-to-point topology or in an arbitrated loop.

bypass circuitry Circuits that automatically remove a device from the data path when valid signals are dropped.

C

CA Certificate authority. A trusted organization that issues digital certificates. *See also* digital certificate.

cascade Two or more interconnected Fibre Channel switches. Brocade SilkWorm 2000 and later switches can be cascaded up to 239 switches, with a recommended maximum of seven interswitch links (no path longer than eight switches). *See also* fabric, ISL.

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.

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.

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.

D

deskew Related to the Brocade Trunking feature. The time difference between traffic traveling over each ISL other than the shortest ISL in the group and traffic traveling over that shortest ISL. The deskew number corresponds to nanoseconds divided by 10. The firmware automatically sets the minimum deskew value of the shortest ISL to 15.

DH-CHAP Diffie-Hellman Challenge-Handshake Authentication Protocol. An implementation of CHAP using Diffie-Hellman encryption. *See also* CHAP.

digital certificate An electronic document issued by a CA (certificate authority) to an entity, containing the public key and identity of the entity. Entities in a secure fabric are authenticated based on these certificates.

director A Brocade SilkWorm 12000, 24000, or 48000 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 between 1 and 239.

E

E_Port Expansion port. A standard Fibre Channel mechanism that enables switches to network with each other, creating an ISL. *See also* ISL.

embedded port An embedded port (or domain controller) communicates and get updates from other switches' embedded ports. The well-known address is *fffcdd*, where *dd* = domain number.

enabled zone configuration The currently enabled configuration of zones. Only one configuration can be enabled at a time.

Ethernet Popular protocols for LANs.

EX_Port A type of E_Port that connects an FC router to an edge fabric. EX_Ports limit the scope of fabric services scope but provide device connectivity using FC-NAT.

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.

fabric A collection of Fibre Channel switches and devices, such as hosts and storage. Also referred to as a "switched fabric."

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 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 process of one CP passing active status to another CP. A failover is nondisruptive.

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.

FFFFFA Well-known Fibre Channel address for a management server.

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.

Fibre Channel transport A protocol service that supports communication between Fibre Channel service providers.

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.

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.

FTP File Transfer Protocol.

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.

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 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.

host A computer system that provides end users with services like computation and storage access.

hot swappable A hot swappable component can be replaced under power.

HTTP Hypertext Transfer Protocol. The standard TCP/IP transfer protocol used on the World Wide Web.

I

ID_ID Insistent domain ID. A parameter of the **configure** command in the Brocade Fabric OS.

in-band Transmission of management protocol over the Fibre Channel.

initiator A server or workstation on a Fibre Channel network that initiates communications with storage devices.

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* cascade, E_Port.

ISP Internet service provider.

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).

latency The time required to transmit a frame. Together, latency and bandwidth define the speed and capacity of a link or system.

login server The unit that responds to login requests.

M

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

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.

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."

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).

O

out-of-band Transmission of management protocol outside of the Fibre Channel network, usually over Ethernet.

oversub-scription A situation in which more nodes could potentially contend for a resource than the resource could simultaneously support (typically an ISL). Oversubscription could be a desirable attribute in fabric topology, as long as it does not produce unacceptable levels of congestion.

P

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.

PKI Public key infrastructure. An infrastructure that is based on public key cryptography and CA (certificate authority) and that uses digital certificates.

PKI certification utility Public key infrastructure certification utility. A utility that makes it possible to collect certificate requests from switches and to load certificates to switches. *See also* digital certificate, PKI.

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 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.

port_name The unique identifier assigned to a Fibre Channel port. Communicated during login and port discovery.

POST Power-on self-test. A series of tests run by a switch after it is turned on.

PPP Point-to-Point Protocol.

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.

principal switch The first switch to boot up in a fabric. Ensures unique domain IDs among roles.

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.

Q

QLA A type of Fibre Channel controller.

QoS Quality of service.

quad A group of four adjacent ports that share a common pool of frame buffers.

queue A mechanism for each AL_PA address that allows for collecting frames prior to sending them to the loop.

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.

QuickLoop Mode Allows initiator devices to communicate with private or public devices that are not in the same loop.

R

radius The greatest “distance” between any edge switch and the center of a fabric. A low-radius network is better than a high-radius network.

RAID Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking.

redundancy Having multiple occurrences of a component to maintain high availability (HA).

remote switch An optional product for long-distance fabrics, requiring a Fibre Channel-to-ATM or SONET gateway.

.

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.

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.

scalability One of the properties of a SAN: the size to which a SAN topology can grow port and switch counts with ease.

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.

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.

SSL Secure sockets layer.

storage A device used to store data, such as a disk or tape.

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.

switch-to-switch authentication The process of authenticating both switches in a switch-to-switch connection using digital certificates.

syslog Syslog daemon. Used to forward error messages.

T

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.

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 ports The ports in a set of trunked ISLs.

W

WAN Wide area network.

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.

workstation A computer used to access and manage the fabric. Also referred to as a “management station” or “host.”

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

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.

zoning A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address.

Index