Building and Scaling Brocade SAN Fabrics

Version 2.6

Publication Number 53-0000196-02

 Publication Number 53-0000196-02

Brocade Communications Systems, Incorporated
Corporate Headquarters
1745 Technology Drive
San Jose, CA 95110

European Headquarters
29, route de l-Aeroport
Case Postale 105
1211 Geneva 15,
Switzerland
T: +41 22 799 56 40
F: +41 22 799 56 41
europe-info@brocade.com

Asia-Pacific Headquarters
The Imperial Tower 15th Floor
1-1-1 Uchisaiwaicho
Chiyoda-ku, Tokyo 100-0011
Japan
T: +81 35219 1510
F: +81 33507 5900
apac-info@brocade.com

Contents

Chapter 3 Expanding the Fabric

Chapter 4 Maintenance

Preface

This User's Guide provides procedures and guidelines for bringing up and maintaining High Port Count Fabrics. This guide is intended for system administrators who are familiar with SAN technology and Brocade hardware and software products.

About This Guide

This guide provides the following information about High Port Count Fabrics:

Chapter 1 Introduction	Defines the terminology used in this document, and lists scalability guidelines and recommendations.
Chapter 2 Building the Fabric (Initial Bring Up)	Provides instructions for bringing up a High Port Count Fabric for the first time.
Chapter 3 Expanding the Fabric	Provides information about how to expand the fabric through adding switches or merging with other fabrics.
Chapter 4 Upgrading the Firmware	Provides procedures such as upgrading the firmware, updating zone configurations, replacing a switch, shutting down the fabric, and recovering from power failure.
Appendix A Example Topologies	Describes example topologies for High Port Count Fabrics.
Appendix B Bring Up Checklists	Provides printable checklists for use when bringing up High Port Count Fabrics.

Related Publications

Related product information can be found in the following Brocade publications:

- Fabric OS Reference
- Fabric Watch User's Guide
- Brocade Web Tools User's Guide
- Distributed Fabrics User's Guide
- QuickLoop User's Guide
- Brocade Zoning User's Guide
- SES User's Guide
- SilkWorm 6400 Product Guide
- SilkWorm 2800 Hardware Reference Manual
- SilkWorm 2400 Hardware Reference Manual

Information about fibre channel standards and the fibre channel industry in general can be found on the Fibre Channel Industry Association web site, located at:

`http://www.fibrechannel.com`

Getting Help

Contact your switch supplier for technical support. This includes hardware and software support, all product repairs, and ordering of spare components.

Be prepared to provide the following information to the support personnel:

- Switch serial number
- Switch World Wide Name
- Topology configuration
- Output from the `supportShow` telnet command
- Detailed description of the problem
- Troubleshooting steps already performed

Getting Software Updates

Contact your switch supplier for software updates and maintenance releases. New switch firmware can be installed from the following host operating systems:

- UNIX
- Windows NT
- Windows 2000
- Windows 98
- Windows 95

Utility programs to facilitate loading firmware from the listed operating systems, in addition to MIB files for switch management by SNMP, can be accessed on the Brocade Web site through the following steps:

1. Launch your web browser and enter `http://www.brocade.com`.
2. Click **Partner Login**.
3. Enter your Brocade Partner userid and password and click **Login**.
4. Scroll down to Technical Support (in the left margin).
5. Click **MIBs and RSH Utilities** or **Firmware**.

Introduction

Chapter 1

This chapter provides the following information:

This document applies to heterogeneous networks running Brocade 2000-series switches running Fabric OS 2.6.

Overview

High Port Count Fabrics (fabrics containing more than 200 ports) are the key to achieving enterprise-class scalability and flexibility from switched Fibre Channel Storage Area Networks (SANs). High Port Count Fabrics extend the benefits of SAN technology to the enterprise level and facilitate data sharing across the corporate campus, the Wide Area Network (WAN), and even the Internet. A High Port Count Fabric—comprising a well-designed network of highly intelligent SAN switches—enables a “pay-as-you-grow” strategy for expanding the reach of SANs.

High Port Count Fabrics, however, may have scalability requirements that are not seen in smaller configurations. This document describes the scalability requirements inherent in High Port Count Fabrics, and describes how to bring up and administer these fabrics most efficiently.

In particular, this document provides procedures for bringing up a High Port Count Fabric. The following ‘bring-up” scenarios are described:

Bring up scenario	See the following section:
First time bring-up	Chapter 2, *Building the Fabric (Initial Bring Up)*
One switch down	*Replacing a Switch* on page 4-3
All switches down	*Recovering from Power Failure (Disaster Recovery)* on page 4-4

The document also describes how to increase the size of the fabric, by adding additional switches and by merging Fabric islands (Chapter 3, *Expanding the Fabric*). Finally, the document lists maintenance procedures for High Port Count Fabrics (Chapter 4, *Maintenance*).

Terminology

This section defines terminology used in this document. Figure 1-1 illustrates the components of a High Port Count Fabric.

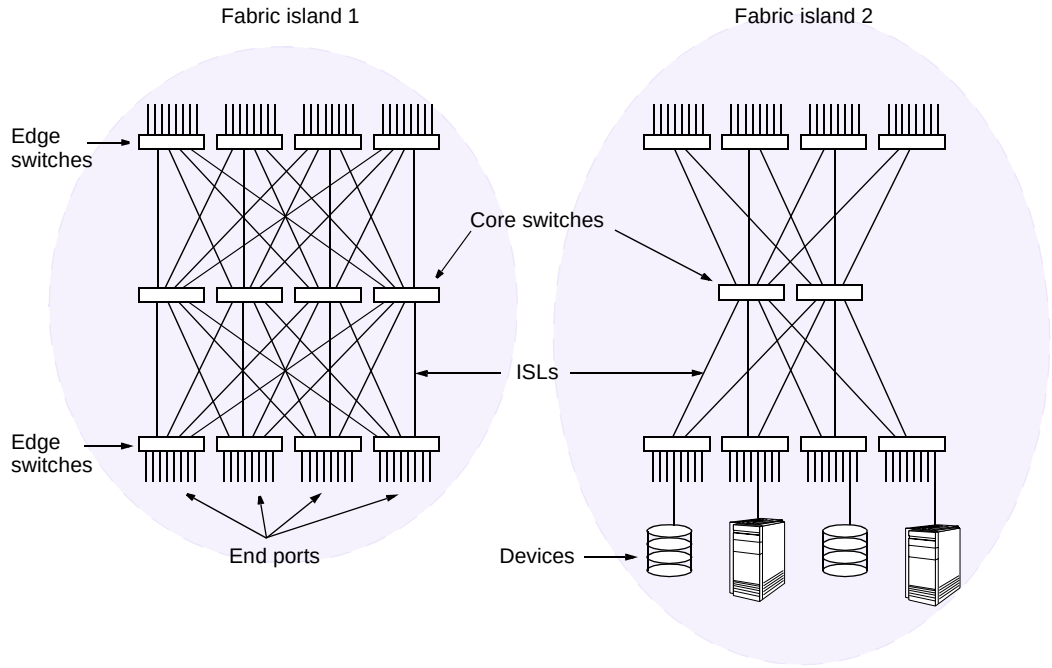

Figure 1-1 Components of a high port count fabric

Core switch	A switch used to interconnect other switches. Core switches are used to cascade edge switches, providing multiple paths to each edge switch. A core switch is also referred to as a *backbone* switch.
Node	Hosts and storage that connect to a switch. Example devices are servers, JBODs, RAID arrays, and tape subsystems.
Dual fabric	Two identical fabrics that allow redundancy in the event one fabric fails (see Figure 1-2 on page 1-3). Use a dual fabric for mission critical applications.
Edge switch	A switch used to attach nodes to the fabric.
End port	A port on an edge switch that connects a node to the fabric.
High Port Count Fabric	A fabric containing 200 or more ports. **Note:** The number of ports is time-relative. For example, a few years from now, a high port count fabric may be defined as a fabric containing 3000 or more ports.
ISL (Interswitch Link)	Link between two switches via an E-Port.
Fabric island	A group of storage devices and servers connected to switches in a fabric.

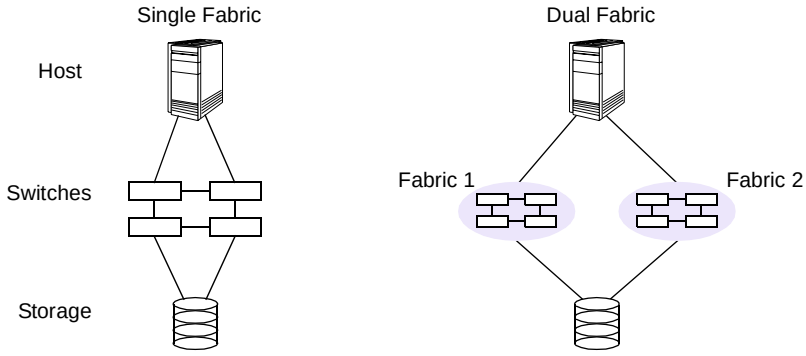

Figure 1-2 Single and dual fabrics

Scalability Guidelines

This section discusses configuration information and recommendations to consider when creating a High Port Count Fabric.

Hardware and Software Configurations

Dual Fabrics

For mission critical applications, Brocade strongly recommends that you install a dual fabric, which allows you to upgrade each fabric separately with no loss of service (provided that you have configured failover software).

For example, to upgrade the dual fabric shown in Figure 1-2, you first upgrade Fabric 1 by deactivating the link from the host to Fabric 1. The host continues to access the data through Fabric 2. After Fabric 1 is upgraded, reconnect the host to Fabric 1, disconnect the link from the host to Fabric 2, and upgrade Fabric 2.

OS Uniformity

Install the same version of Fabric OS on all of the switches when building a fabric. If you have multiple versions of the Fabric OS in the fabric, update the switches to the latest version. If different Fabric OS versions must be used in the same fabric, then check the list of compatible features supported in each version to prevent fabric segmentation.

Check with your switch provider to identify the recommended minimum Fabric OS version.

Configuration Uniformity

If you have multiple versions of zoning configurations and parameters, determine the version of the configuration that you need and update all switches to that version. A fabric can only have one zone configuration.

Hardware Metrics

Brocade switches require that you pay careful attention to the number of switches in a fabric and the number of ISLs between two switches.

Number of Switches

The ultimate limitation in fabric design is a maximum of 239 physical switches, be they 8- or 16-port versions. The practical limit and what has been tested is much fewer switches. Brocade extensively tests fabrics of up to 32 switches, with no more than 7 hops allowed from the source port to the destination port (in accordance with FC time out standards).

Brocade recommends an upper limit of seven hops between any beginning and end switch in the fabric. That is, a frame should cross no more than eight switches from any source to any destination. The latency between switches is 2 microseconds.

Number of ISLs

No more than eight ISLs between any two switches is supported. More than eight ports can be used on a switch for ISL traffic as long as no more than eight go to a single adjacent switch.

Recommendations

The following recommendations will help you build and scale your fabric easily and efficiently:

- Manually assign Domain IDs for each switch.

  Although the Brocade Fabric OS can automatically assign Domain IDs to switches, Brocade recommends that for ease of management you manually assign the Domain IDs. The advantages of manually assigning Domain IDs are as follows:

  - More control over what Domain ID goes with what switch in the fabric.
  - Ease of migration to future switch models that may have hard-assigned Domain IDs.
  - Fewer Domain ID clashes when merging fabrics. A switch with a Domain ID that matches an existing switch is not allowed to join into the fabric.
- Create a topology diagram to use as a reference guide when cabling the switches.
- Have a well thought out switch naming convention to enable easy identification of a physical switch should a problem arise.

  Use a switch naming convention that scales across the organization, keeping in mind that the SAN may start small but can extend to become enterprise-wide over time.

Consider using the following items when making up the switch name field:

- Incorporate an ID for the site or building where the switch is located.
- Add a component to identify the floor or room where the switch is located.
- Add a component that shows to which organization or project the switch belongs.
- Include the rack ID in the name to further detail switch location.
- If redundant fabrics are being used, select an ID for complementary fabrics.

  Example: FINANCE-A-BLDG55-RM15-RACK5 and
  FINANCE-B-BLDG55-RM15-RACK6

- Add a physical label to the switch that matches the switch name to ensure the proper switch is accessed if a problem is reported via a SAN monitoring agent.
- Whenever possible, devices that exchange the highest amount of data between each other should be connected to the same switch. If this in not possible, then configure multiple ISLs between switches, to increase the available bandwidth and increase fabric resiliency.
- Add additional ISLs only if there is a real need for the extra bandwidth.

  Design the fabric for the sustained bandwidth requirements, and then add safety margins. Planning bandwidth for peak utilization could be wasteful, and should be done only when a specific need exists.

  Also note the usage patterns of the devices when planning bandwidth. Hosts and storage communicate with each other. Storage does not normally communicate with other storage, and hosts do not normally communicate with other hosts.

- Try to keep the number of zones down to reduce the amount of interswitch traffic.
- Use an Uninterruptable Power Supply (UPS) to protect all storage and storage-related devices.

Chapter

2

Building the Fabric (Initial Bring Up)

This chapter contains procedures to help you configure new switches and bring up a High Port Count Fabric *for the first time*. The procedures in this section assume that the switches are being used for the first time, the entire fabric is down, and you are bringing the new fabric up from scratch.

Note: For detailed explanation and syntax of the commands in the following procedures, refer to the *Brocade Fabric OS Reference Manual*.

If you are adding switches or merging Fabric islands to a fabric that is already up and running, refer to the procedures in Chapter 3, *Expanding the Fabric*. If you are bringing up an entire fabric after a power failure, see *Recovering from Power Failure (Disaster Recovery)* on page 4-4.

Bring Up Overview

This section provides an overview of the "bring up" procedure. Refer to Appendix B, *Bring Up Checklists* for a bring up overview checklist.

Bringing up a High Port Count Fabric

1. Determine the fabric topology.
2. Power on each switch, and go through the Power-On Self-Test (POST).
3. Configure each switch:
    a. Configure each switch for network access.
    b. Run diagnostic tests to verify hardware.
    c. Upgrade the firmware and install software licenses.
    d. Configure the fabric parameters and software features.
4. Reboot each switch and then verify the switch configuration.
5. Connect ISLs to form a large fabric.
6. Verify the fabric configuration.
7. Load the desired zoning configuration onto the fabric.
8. Connect devices to the fabric.
9. Power on the devices:
    a. Power on or enable the storage devices.
    b. Power on or enable the host devices.
10. Verify the SAN.

The following sections describe each of these steps in more detail.

Bringing Up the Fabric (Detailed Steps)

This section describes in detail the steps for bringing up the fabric for the first time.

Note: For detailed information about the telnet commands used in this procedure, refer to the *Brocade Fabric OS Reference*.

Determine the Fabric Topology

Create a topology diagram to use as a reference guide when cabling the switches.

When you first set up a fabric, determine what topology best fits your needs. Consult with your switch supplier and refer to the Brocade publication *Brocade SAN Configuration and Design Guidelines* (part number 53-0000023-02) for guidance. Refer to Appendix A, *Example Topologies* in this document for some sample topologies.

For your topology, determine which are the edge switches and which are the core switches. Refer to *Terminology* on page 1-2 for definitions of core and edge switches.

Power On the Switches

Power on each switch. When the switch is powered on, it automatically runs the POST to guarantee switch stability. Errors that occur during POST are written to the system error log. Verify that the POST completes successfully. Refer to the appropriate SilkWorm product manual for more information about the POST.

Configure the Switches

You can configure the SilkWorm switch using the RS-232 serial port. If your switch has a front panel display, you can configure it locally using the front panel buttons. Refer to your switch reference manual or *Fabric OS Reference Manual* for more information on this option.

Connecting to the serial port requires use of a serial cable and a host system that allows for serial connection. The cable should be a DB9 connector type with female connector for the SilkWorm serial port. Upon switch power up, the switch is automatically logged in as admin. If you connect the switch after it is powered up, you must supply a user name and password.

Configure Each Switch for Network Access

To enable remote connection to the switch, the switch must have a valid IP address. Two IP addresses can be set: one for the external out-of-band ethernet port and one for in-band fibre channel network access.

To set the switch IP address using the front panel:

1. Select the “Configuration” menu using the right button.
2. Scroll down on configuration options until the option “Ethernet IP Address” appears, and select this option using the right button.
3. Use the left button to move from one IP address value to the next.
4. Use the scroll up/down keys to set each of the four numeric IP address values.
5. When all values are set, press the right button to finish.
6. Confirm the IP address is correct (select “Yes” option to store to flash). The switch stores the IP address in flash memory.

To set the switch IP address using the serial port:

As the admin user, enter `ipAddrSet` at the telnet prompt. This command prompts the user for the following:

- Ethernet IP Address
- Ethernet Subnetmask
- Fibre Channel IP Address
- Fibre Channel Subnetmask
- Gateway Address

If the current value is acceptable, press Enter, otherwise enter a new address.

Run Diagnostic Tests to Verify Hardware (Optional)

At this point you can optionally run diagnostic tests on each switch to verify the switch hardware. You can run the tests using either the front panel buttons or telnet commands.

If a test is started using the front panel, you can monitor the test progress, but cannot control the test through telnet commands. If you start a test using telnet commands, attempting to control the test via the front panel may lock up the switch and require a reboot. (For specifics on which commands to use, see *Reboot and Verify Each Switch* on page 2-4)

Note: Accessing the switch via telnet commands provides a more detailed response indicating the switch condition and allows the use of some commands that do not have an equivalent front panel command.

Upgrade the Firmware and Install Software Licenses

If you need to upgrade the firmware on each switch, do so now, using the `firmwareDownload` command. Refer to the *Fabric OS Reference* for information about this command.

Note: To prevent fabric segmentation, install software licenses on all switches now, before configuring the software features.

Determine which software features (for example, Zoning, Web Tools) you will use in your fabric and install the appropriate licenses on all switches now. Make sure that a Fabric license is pre-installed on each switch that requires such a license. Use the `licenseShow` telnet command to determine which licenses are installed. In the paper pack envelope that ships with the license, you can find instructions to help you install the licenses.

Configure the Fabric Parameters and Software Features

To save time when you configure the fabric parameters, configure one switch first, then use the `configUpload` and `configDownload` telnet commands to save the configuration information and download it onto each of the remaining switches.

Note: After you upload the configuration, but before you download it, make sure that you delete the line containing the license keys (the line begins with `licenseKey`).

- Use the `configure` telnet command to configure fabric parameters as required for each predetermined topology. (Refer to Appendix A, *Example Topologies* for some sample topologies.)

  To prevent fabric segmentation and for ease of fabric management, use the `configure` command to manually assign a unique Domain ID for each switch.

  Note: When you use the `configDownload` command to download the same configuration to each of your switches, you may overwrite your domain ID. To avoid this error, manually set your domain ID after you download the configuration, or remove the domain ID field from the configuration that you intend to download.

- Set a name for each switch using the `switchName` telnet command. For example, this command sets the switch name to `sw10`:

  ```
  switchName “sw10”
  ```

- Configure the software features (such as Fabric Watch and Zoning) for each switch. Refer to the User’s Guide for each software feature for configuration information. Configure the software feature on one switch, then use the `configUpload` and `configDownload` telnet commands to save the configuration information and download it onto each of the remaining switches.

Reboot and Verify Each Switch

Note: The switches are not cascaded at this point.

After switch configuration is complete, reboot each switch to ensure the configuration changes take effect. Use the following command:

```
fastboot
```

The `fastboot` command reboots the switch, bypassing POST, thus reducing boot time significantly. After the reboot completes, verify the switches using the following telnet commands:

- Use `configShow` to verify switch parameters and to verify that all Domain IDs are unique.
- Use the `version` command to check the firmware version.
- Use `licenseShow` to verify that the software licenses are installed and are the same for all switches.
- Use `cfgShow` or `zoneShow` to verify that each switch has the same zone information.

Connect ISLs to Form a Large Fabric

Before connecting the switches, label the exterior of each switch with the switch name and Domain ID. Also label the topology design and use it as a reference guide when cabling the switches.

Connect all of the switches, starting with the core switches, and then working outward to the edge switches, for ease of cable management.

Verify the Fabric Configuration

Verify the switch status and ISL port status for each switch using the `switchShow` telnet command (Figure 2-1). Confirm that each switch role is either “Principal” or “Subordinate.” Only one switch should be designated as the “Principal” switch. All others should be “Subordinate.”

The ISL ports should display as E-Ports.

```
dev189:admin> switchShow
switchName:     dev189
switchType:     4.1
switchState:    Online
switchRole:     Subordinate
switchDomain:   189
switchId:       fffcbd
switchWwn:      10:00:00:60:69:30:06:24
switchBeacon:   OFF
Zoning:         ON (tmp)
port  0: sw  No_Light
port  1: sw  No_Light
port  2: sw  Online        E-Port  10:00:00:60:69:10:1c:8c "dev184" (upstream)
port  3: sw  No_Light
port  4: sw  No_Light
port  5: sw  No_Light
port  6: sw  No_Light
port  7: --  No_Module
dev189:admin> _
```

Figure 2-1 switchShow command

Use the `fabricShow` telnet command (shown in Figure 2-2) to verify that the fabric has the correct number of switches. All of the switches that you have connected to the fabric should appear.

```
dev189:admin> fabricShow
Switch ID   Worldwide Name           Enet IP Addr    FC IP Addr      Name
-------------------------------------------------------------------------
101: fffc65 10:00:00:60:69:12:2b:8c  192.168.163.16  0.0.0.0          "switch1"
102: fffc66 10:00:00:60:69:12:2a:7b  192.168.163.15  0.0.0.0          "switch2"
103: fffc67 10:00:00:60:69:12:2a:4c  192.168.163.14  0.0.0.0          "switch3"
104: fffc68 10:00:00:60:69:12:2c:af  192.168.163.13  0.0.0.0          "switch4"
184: fffcb8 10:00:00:60:69:10:1c:8c  192.168.172.184 0.0.0.0         >"dev184"
189: fffcbd 10:00:00:60:69:30:06:24  192.168.172.189 0.0.0.0          "dev189"
193: fffcc1 10:00:00:60:69:30:1d:4f  192.168.172.193 0.0.0.0          "dev193"

The Fabric has 7 switches

dev189:admin> _
```

Figure 2-2 fabricShow command

Load Zoning Configuration

Before you add devices to the fabric, download the appropriate zoning configuration to all switches on the fabric. Be sure you have a zoning configuration that is uniform throughout the fabric to prevent errors once you connect devices. For more on downloading zoning configurations, see the *Brocade Zoning User's Guide*.

Connect Devices to the Fabric

Power off all devices (to minimize PLOGIs) and connect them to the fabric, according to the topology diagram you created earlier. (See *Determine the Fabric Topology* on page 2-2.)

For devices that cannot be powered off, connect the devices but use the `portDisable` telnet command to disable the port on switch.

Note: Brocade recommends powering off the devices before connecting them to the fabric because some devices are not capable of handling State Change Notifications (SCNs) issued from fabric switches. The devices that cannot handle SCNs are not able to detect subsequent targets that are added to the fabric, and should be turned on last.

Power On the Devices

1. Power on the storage devices, one at a time, waiting for each device to complete fabric login before powering on the next. (Use the `switchShow` command to verify that the device has successfully logged in.)

   For storage devices that are connected to disabled ports (because they could not be powered off), use the `portEnable` command to enable their ports on the switch.

2. After all storage devices are powered on, for each switch with storage devices connected to it:

   - Use the `switchShow` telnet command to verify that the storage devices are logged in.
   - Use the `nsShow` telnet command to verify that the storage devices have successfully registered with the Name Server.

   Alternatively, you can use the Brocade Web Tools feature if it is installed.

3. Power on the host devices, one at a time, waiting for each host to complete fabric login before powering on the next.

   Note: If zoning is enabled, power on the host devices that belong in the biggest zones first.

   For host devices that are connected to disabled ports (because they could not be powered off), use the `portEnable` command to enable their ports on the switch.

4. After all of the host devices are powered on, for each switch with host devices connected to it:

   - Use the `switchShow` telnet command to verify that the host devices are logged in.
   - Use the `nsShow` telnet command to verify that the host devices have successfully registered with the Name Server.

   Alternatively, you can use the Brocade Web Tools feature if it is installed.

5. Record the storage and host device counts. If you know the device count you can use the `nsAllShow` telnet command to quickly identify if devices were dropped off or added.

Verify the SAN

Check each switch one more time. For each switch in the fabric, do the following:

1. Reconfirm the switch and port status using the `switchShow` and `nsShow` telnet commands. Alternatively, you can use Web Tools to reconfirm this switch and port status, if you have the Web Tools feature installed.
2. Reconfirm fabric status using the `fabricShow` telnet command. The number of switches should be the same throughout.
3. Verify fabric routing using the `uRouteShow` telnet command to verify that every in port has an out port. (See Figure 2-3 for an example.)
4. Check for switch or fabric errors using the `errShow` telnet command.

This completes the initial fabric bring up procedure.

```
dev184:admin> uRouteShow

Local Domain ID: 184

In Port    Domain    Out Port    Metric    Hops    Flags    Next (Dom, Port)
-------------------------------------------------------------------------------
   2         101          6         3000       3       D          104,11
             102          6         2000       2       D          104,11
             103          6         2000       2       D          104,11
             104          6         1000       1       D          104,11
             189          4         1000       1       D          189,2

Type <CR> to continue, Q<CR> to stop:

   4         101          6         3000       3       D          104,11
             102          6         2000       2       D          104,11
             103          6         2000       2       D          104,11
             104          6         1000       1       D          104,11
             193          2         1000       1       D          193,1

Type <CR> to continue, Q<CR> to stop:
```

Figure 2-3 uRouteShow command

Chapter

3

Expanding the Fabric

This chapter describes procedures for expanding the fabric. You expand the fabric by adding additional switches. The switches you cascade can be new switches (that is, switches that are offline and have no devices attached), or online switches that are already part of another fabric or Fabric island.

Brocade switches are designed to expand automatically into a fabric environment. However, follow the guidelines in this chapter to maximize fabric performance and minimize disruption to the fabric.

This chapter lists general expanding considerations, and provides procedures for three types of cascading. This chapter contains the following sections:

Cascading Considerations

Adding additional switches to a fabric is minimally disruptive: just connect the new switch to the existing fabric and then power it up. The new switch cascades into the fabric automatically, and you do not need to suspend service to any other part of the fabric during the process, however the switch additon will cause a fabric reconfiguration which results in a disruption to I/O while the fabric converges.

Because SilkWorm 2000 series switches automatically select a port's mode of operation, you do not need to select a specific port in which to connect the switches together. Any port can be used.

If the new configuration creates shorter paths between source and destination nodes, the SilkWorm routing software automatically re-routes the traffic to these shorter paths.

Configuration Parameters

This section contains the unique switch settings and configuration parameters that must be identical for cascading to occur.

Switch Settings

The switch IP address and Domain ID must be unique to allow the cascading of switches.

Note: Brocade recommends that you manually assign the Domain ID for ease of management.

Configuration Parameters

The following fabric configuration parameters must be identical in all switches for cascading to occur:

- BB_Credit
- R_A_TOV
- E_D_TOV
- Data Field Size
- Device Probing
- VC Encoded Address Mode
- Translative Mode
- Per-Frame Route Priority
- Core Switch PID Format

Use the `configShow` command to display these parameters, and the `configure` command to change them. Refer to the *Brocade Fabric OS Reference* for information about these commands.

Cascading Guidelines

When cascading switches to a fabric, make sure that the switches entering the fabric follow all the rules that presently exist in the fabric. Use the following guidelines when cascading switches:

- If Brocade Zoning is licensed on the new switch, then when you add it to the fabric the switch automatically takes on the zone configuration information of the fabric. If the new switch has zone configuration information already defined on it, then
  - The alias names, zone names, and zone configuration names on the new switch and the fabric must be unique (the zone configurations must be completely different), or
  - The zone configurations on the new switch must exactly match the zone configurations of the fabric.

  If the name of a zone object on the new switch is the same as a different type of zone object in the fabric, then a segmentation error occurs.
- If you are using Brocade Zoning, you must disable the zoning configuration on the switch that you are joining into the fabric (using the `cfgDisable` command). The fabric may continue to have its zone configuration enabled, however. If the new switch has a different zone configuration enabled, a fabric segmentation error occurs.
- If a zone configuration is active in the existing fabric and you do not need to import any of the zone configuration that exists on the new switch, then perform a `cfgClear` and a `cfgSave` on the new switch before cascading it into the fabric, to delete the zone information on the new switch.

  Note: Be very careful—run these commands on the new switch only before it is cascaded into the fabric. Running these commands on the existing fabric will erase the configuration on the fabric. Back up all old zoning configurations before you remove them.
- Make sure the Domain ID and the IP address of the new switch are not the same as any other switch in the fabric. If they match another switch in the fabric, a segmentation error occurs.
- When adding or removing switches in a fabric, ensure that the fabric is in a quiescent state as possible. The process of adding a new switch that is already online or removing a switch causes a brief pause in I/O while the fabric reconfigures.

- Brocade recommends that all switches in a single fabric have the same firmware version to ensure a full feature set across all switches in the fabric.

Adding Additional Switches

This section assumes that you are cascading a single, offline switch. If your switch is already part of an existing fabric, See *Merging Fabric Islands* on page 3-4. Before adding the switch to the fabric, follow the guidelines listed in *Cascading Considerations* on page 3-1.

If the new switch has been previously configured for zoning, then clear the zoning information on the new switch by using the `cfgClear` and the `cfgSave` commands *before* connecting the switch to the fabric.

When the switch is connected to the fabric, all zone configuration data is immediately copied from the fabric into the new switch. If a zone configuration is enabled in the fabric, then the same configuration becomes enabled in the new switch. After cascading, the `cfgShow` command displays the same output on all switches in the fabric, including the new switch.

To Cascade the SilkWorm 2000 Switch

The following steps explain how to add a Brocade SilkWorm 2000 switch to your network:

1. Check the device count of the existing fabric. After you add a switch, check the device count again to see if the new switch caused any devices to go offline.
2. Power on the new switch, and check the following:
   - Check the Domain ID to prevent conflict before cascading to the fabric.
   - Check to see if the new switch has been previously configured for zoning; if it has, clear the zoning information on the new switch by using the `cfgClear` and the `cfgSave` commands *before* connecting the switch to the fabric.
   - Check for supported zoning parameters with an older Fabric OS in the fabric before cascading, to prevent fabric segmentation.
   - Make sure the new switch has the same feature licenses before cascading to the fabric, to prevent segmentation and multiple fabric initializations.
   - Verify all switch parameters are compatible with the fabric parameters before merging.
3. Power off or disable the switch.
4. Connect the switch to the existing fabric, using one ISL at a time. The first ISL cascades the switch into the fabric. Additional ISLs added are used for load balancing or redundant paths.
5. Power on or enable the switch.
6. Issue the `fabricShow` telnet command to verify that the new switch is in the fabric.
7. Check the device count again, noting any disparities.
8. Attach devices to the new switch.
9. Verify that the new devices are connected (switchShow, nsShow)
10. Verify that the new devices are part of the fabric by issuing the nsallshow command and validating the the name server count increased in line with the total number of devices added.

This completes the procedure for cascading a new switch into a fabric.

Merging Fabric Islands

This section contains guidelines for merging Fabric islands. The process must be planned carefully to minimize down time in both fabrics.

Note: Contact your switch supplier for assistance with merging SAN islands.

Merging Guidelines

Follow the following steps as you prepare to merge multiple SAN islands:

1. Check for conflicting Domain IDs on both fabrics before merging.
2. Check for conflicting zone definitions before merging.
3. Verify that the Fabric islands have the same feature licenses before merging.
4. Verify that all switch parameters are compatible with the fabric before merging.
5. Merge the fabrics using one ISL at a time.

   The first ISL merges the fabrics as one and causes a disruption on both fabrics. Additional ISLs are used for load balancing or redundant paths and will rarely cause a disruption to the fabric.

Zoning Considerations

If two fabrics that have zone configuration information are joined, the zoning software attempts to merge the two zone configurations.

The simplest case is where both fabrics have identical zone configuration data and the same configuration is enabled. In this case, the fabrics join to make one larger fabric with the same zone configuration in effect across the whole new fabric.

If the fabrics have different zone configuration data, then the two sets of information are merged if possible, or the ISL is segmented if a merge is not possible.

This merge does not take place under the following conditions:

- The zoning is enabled in both fabrics and the zone configuration that is enabled is different (configuration mismatch).
- The name of a zone object in one fabric is used for a different type of zone object in the other fabric (type mismatch).
- The definition of a zone object in one fabric is different from its definition in the other fabric (content mismatch).

When these conditions are detected by the switch, error messages are displayed on the LCD (SilkWorm 2800 only) or telnet console. During fabric segmentation the port lights blink green on the ISL link. One possible way to recover from this state is to disconnect the new switch, perform a `cfgClear` followed by a `cfgSave`, and then reconnect the new switch.

Domain ID Considerations

If any switch in either fabric has the same Domain ID, one of the Domain IDs must be changed to avoid fabric segmentation when merged.

Change one switch Domain ID at a time to minimize I/O interruption.

Perform the following steps to change the Domain ID:

1. Make sure the switch has redundant paths for devices attached to that switch. Force the I/O path on the devices to fail over to a neighboring switch using software provided on those devices.
2. Disable the switch using the `switchDisable` command.
3. Change the Domain ID using the `configure` command.
4. Enable the switch using the `switchEnable` command.
5. Restore the original I/O paths of the devices.

Fabric Parameters

Fabric parameters on both fabrics should be identical. See *Configuration Parameters* on page 3-1 for a list of these parameters.

Adding Additional or Redundant Core Switches

Adding additional core switches provides redundancy and increases bandwidth in the core. This section contains guidelines for adding additional or redundant core switches.

1. Power up the redundant or additional core switch as a separate fabric.
2. If you are adding a new switch, you must configure the switch, as described in Chapter 2:
   - *Configure Each Switch for Network Access* on page 2-2
   - *Run Diagnostic Tests to Verify Hardware (Optional)* on page 2-3
   - *Upgrade the Firmware and Install Software Licenses* on page 2-3
   - *Configure the Fabric Parameters and Software Features* on page 2-4
3. Check for conflicting zone definitions with the existing fabric before cascading the new core switch to the fabric.
4. Verify that the new core switch has the same feature licenses before cascading to the fabric.
5. Power off or disable the switch.
6. Merge the core into the fabric using one ISL at a time. The first ISL merges the core into the fabric. Additional ISLs added are used for load balancing or redundant paths.
7. Power on or enable the switch.
8. Verify the fabric configuration as described in *Verify the Fabric Configuration* on page 2-5 and *Verify the SAN* on page 2-8.

Maintenance

Chapter 4

This section describes maintenance procedures and guidelines for the following:

Upgrading the Firmware

Brocade recommends that all switches be upgraded to the same firmware level, to support all features in the current fabric.

If the configuration is designed correctly, the firmware upgrade should not require any fabric down time using the guidelines and procedure below.

Guidelines

- Plan to upgrade the firmware when there is the least amount of traffic in the fabric.
- Upgrade the core switches first, and work outward to the edge switches in the fabric.
- Configure any new software features and zoning parameters after all switches in the fabric are upgraded to the new firmware.

Procedure

1. Make sure the switch has redundant paths for devices attached to it. Force the I/O path on the devices to fail over to a neighboring switch or fabric using software provided on those devices.
2. Verify that there is no traffic on the switch, using the `perfShow` telnet command.
3. Download the new firmware onto the switch. Refer to the *Brocade Fabric OS Reference* for information about the `firmwareDownload` command.
4. Reboot the switch for the firmware to take effect, using the `fastBoot` command to bypass POST.

   Note: The switch reboot causes a fabric reconfiguration.
5. After the switch comes back online, verify the fabric configuration using the `switchShow` command. (See *Verify the Fabric Configuration* on page 2-5).
6. For firmware upgrades on subsequent switches, repeat step 1 through step 5 for each switch.

7. When all switches in the fabric have been upgraded, check each switch one more time, using the procedure in *Verify the SAN* on page 2-8.

This completes the procedure for upgrading the firmware.

Updating the Zone Configuration

Before making zone changes to the fabric, consider the amount of changes necessary to minimize the time and effort involved while maintaining fabric stability. Two scenarios (for minor and major zone updates) are described in detail below.

Guidelines

Follow the following guidelines when you make either a minor or major zone update:

- Plan to update the zone configuration when there is minimal traffic in the fabric.
- Verify that the new zoning parameters are supported with the current Fabric OS in the fabric.
- Update the zone configuration on one of the core switches, and allow the changes to automatically propagate to the other switches.

Minor Zone Updates

Perform the following steps to make a minor zone update:

1. Use the telnet command line interface or Web Tools to make zone changes or additions while the switch is online.
2. Save the zone updates into flash memory using the `cfgSave` command.

This completes the procedure for making minor zone updates.

Major Zone Updates

Perform the following steps to make a major zone update:

1. Use `uRouteShow` to find the routing paths that use the management switch for routing.
2. Direct the I/O path to redundant or neighbor core switches, using software on the hosts.
3. Verify that there is no traffic on the management switch, using the `perfShow` command.
4. Use `configUpload` to upload the current zoning configurations.
5. Modify the saved zoning configurations file to reflect the update.

   Note: If the new zoning configuration is a superset of the existing zoning configuration in the fabric, then you can skip steps 6 and 7. If you are unsure, then continue with steps 6 and 7.

6. Disable the current zone configuration in the fabric using the `cfgDisable` command.

7. Clear the current zone configuration in the fabric using the `cfgClear` command.
8. Disable the management switch using the `switchDisable` command.
9. Use the `configDownload` command to download the new zone configuration onto the management switch.
10. Disable the zone configuration on the management switch using the `cfgDisable` command.
11. Bring the switch online, and wait for the fabric to complete initialization before enabling the zone configuration.
12. Enable the zone configuration using the `cfgEnable` command. The zone configuration propagates to all switches in the fabric.
13. Save zone updates into flash memory using the `cfgSave` command.

    Note: Devices that do not respond to the State Change Notifications (SCNs) will not be aware of zone updates. These devices should be rebooted so they can log back into the fabric. For devices that can not be powered down, toggle the FC channel connections to force them to reinitialize login procedures and discover updates in the fabric.

Refer to the *Brocade Fabric OS Procedures Guide* and the *Brocade Zoning User's Guide* for information about these commands. Alternatively, you can update the zone configuration online, using the telnet console, Web Tools, or Fabric Manager.

Replacing a Switch

This section contains procedures for replacing two types of switches:

- A switch that has malfunctioned and needs replacement
- A switch that is still functional, but needs upgrading (for example, if you want to replace a switch with a higher port count switch)

To Replace a Malfunctioning Switch

1. Direct the traffic to a neighboring switch using software tools on each connected host, and shut down the malfunctioning switch to prevent interswitch traffic emigrating from the switch being swapped out.
2. Power on the replacement switch and verify that the POST completes successfully.
3. Prepare the replacement switch as a separate fabric by following the procedures in *Configure the Switches* on page 2-2.
4. Disconnect the Fibre Channel connections, one at a time, from the bad switch and connect them to the replacement switch, starting with the ISL connections.
5. Check the switch using the procedures in *Verify the SAN* on page 2-8.

This concludes the procedure for replacing a malfunctioning switch.

To upgrade a switch

1. Use the `configUpload` command to save switch configuration and zoning parameters.
2. Direct traffic to neighboring switches using software tools on each connected host. If you are replacing a core switch, redirect the traffic for each host that is routed across the switch that is being replaced. Verify that all traffic is redirected using the `perfShow` command.

3. Power off the switch. A fabric reconfiguration occurs to update the fabric.
4. Power on the replacement switch, and verify that the POST completes successfully.
5. Prepare the replacement switch as a separate fabric by following the procedures in *Configure the Switches* on page 2-2.
6. Use the `configDownload` command to duplicate the same configuration as the original switch.
7. Disconnect the fibre channel connections from the old switch and connect them to the replacement switch, one at a time, starting with the ISL connections.
8. Check the switch using the procedures in *Verify the SAN* on page 2-8.

This concludes the procedure for upgrading a switch.

Shutting Down the Fabric

Perform the following steps to successfully shut down the fabric:

1. Shut down all host devices.
2. Shut down all storage devices.
3. Shut down all edge switches.
4. Shut down all core switches.

Recovering from Power Failure (Disaster Recovery)

This section describes how to bring up a High Port Count Fabric when all of the switches are down, for example, as what happens when you recover from a power failure. The procedures in this section assume that the entire fabric is down, and that the switches in the fabric have been previously configured.

If you are bringing up a new fabric for the first time, where the switches have not been previously configured, refer to Chapter 2, *Building the Fabric (Initial Bring Up)*. If you are adding switches or merging Fabric islands to a fabric that is already up and running, refer to the procedures in Chapter 3, *Expanding the Fabric*.

Bring Up Overview

This section provides an overview of the bring up procedure. The following sections describe each step in more detail. Refer to Appendix B, *Bring Up Checklists* for a bring up overview checklist.

Bringing up a High Port Count Fabric when all of the switches are down involves the following general steps:

1. Make sure all switches and devices are powered off.
2. Power on the fabric:

a. Power on the core switches.

b. Power on the first edge switch to merge the core switches and the edge switch as one fabric.

c. Power on the remaining edge switches.

3. Verify the fabric configuration.
4. Power on the devices:

a. Power on or connect the storage devices.

b. Power on or connect the host devices.

5. Verify the SAN.

Power Off the Switches and Devices

Make sure all switches are powered off.

Power off all devices that can be powered off, to minimize fabric attachment until the fabric is up. Disconnect the ports of any devices that cannot be powered off.

Power On the Fabric

This section contains the generic procedure for powering on the switches in a High Port Count Fabric. The actual order of powering on switches may vary depending on your SAN topology.

Power On the Core Switches

Perform the following steps to power on the core switches:

Note: Make sure devices are powered off or disconnected before proceeding.

1. Power on the core switches. You can power on all of the core switches simultaneously. If the core switches are not cascaded, then each switch comes up as a separate fabric.
2. Check the fabric and switch status on each core, using the `switchShow` and `fabricShow` commands.

Power On the Edge Switches

Perform the following steps to power on the edge switches:

1. Power on the first edge switch to merge the edge switch and the core switches into one fabric. Wait for the fabric to complete initialization before proceeding to the next step.
2. Power on the remaining edge switches.

This completes the procedure for powering on the switches.

Verify the Fabric Configuration

Verify the switch status and ISL port status for each switch using the `switchShow` command.

Confirm that each switch role is either “Principal” or “Subordinate.” Only one switch should be designated as the “Principal” switch. All others should be “Subordinate.”

The ISL ports should display as E-Ports.

Use the `fabricShow` command to verify that the fabric has the correct number of switches.

Power On or Connect the Devices

Perform the following steps to power on devices or connect devices that you could not shut down:

1. Power on the storage devices, one at a time, waiting for each device to complete fabric login before powering on the next.

   For devices that could not be powered down, connect them into the fabric now.

2. After all storage devices are powered on or connected, verify that all storage devices have logged into the fabric and registered with the Name Server successfully. Use the `switchShow` and `nsShow` telnet commands on the switch to which the device is connected. Alternatively you can use Web Tools if the Web Tools feature is installed.

3. Power on the host devices, one at a time, waiting for each host to complete fabric login before powering on the next.

4. For hosts that cannot be powered down, connect them into the fabric now.

   Note: If zoning is enabled, power on the host devices that belong in the biggest zones first.

5. After all of the host devices are powered on, verify that all host devices have logged into the fabric and registered with the Name Server successfully. Use the `switchShow` and `nsShow` telnet commands on the switch to which the device is connected. Alternatively you can use Web Tools if the Web Tools feature is installed.

6. Record the storage and host device counts. If you know the device count you can use the `nsAllShow` telnet command to quickly identify if there is a change in the configuration.

This completes the procedure for powering on the devices.

Verify the SAN

For each switch in the fabric, do the following:

1. Reconfirm the switch and port status using `switchShow` and `nsShow`. Alternatively, you can use Web Tools to reconfirm this switch and port status, if you have the Web Tools feature installed.

2. Reconfirm fabric status using the `fabricShow` command. The number of switches should be the same throughout.

3. Verify fabric routing using `uRouteShow` to verify that there is an out port for every in port.

4. Check for switch or fabric errors using the `errShow` command.

This completes the fabric bring up procedure when all switches are down.

Example Topologies

Appendix A

You should consider a number of factors when designing a fabric, and know that no one answer or single topology addresses all problems. Each user has unique system elements and design needs that need to be factored into the fabric design. This appendix describes several example SAN topologies that you can use as templates for fabric designs.

18-Switch Star Configuration

Figure A-1 shows a SAN topology with 18 switches. This example topology has the following characteristics:

- 18 switches, 2 of which are core switches
- Each switch has 16 ports
- The core switches are fully meshed, meaning that each core switch is connected to every edge switch
- 96 ISL ports (one-way trunking)
- 192 end ports

Note: The core switches in Figure A-1 are enlarged for illustration purposes only.

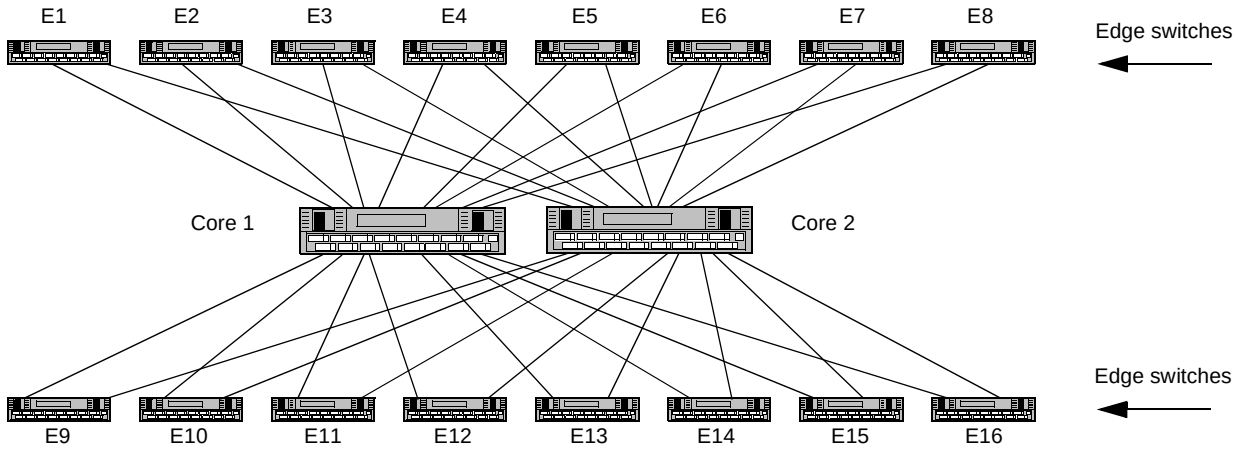

Figure A-1 18-switch star configuration

20-Switch Star Configuration

Figure A-2 shows a SAN topology with twenty switches. This example topology has the following characteristics:

- Four SilkWorm switches, used as core switches
- Each core contains two switches, for a total of 4 core switches
- Sixteen edge switches (E1 through E16)
- Each edge switch has sixteen ports
- Redundant ISLs from each edge switch to each core
- 192 end ports

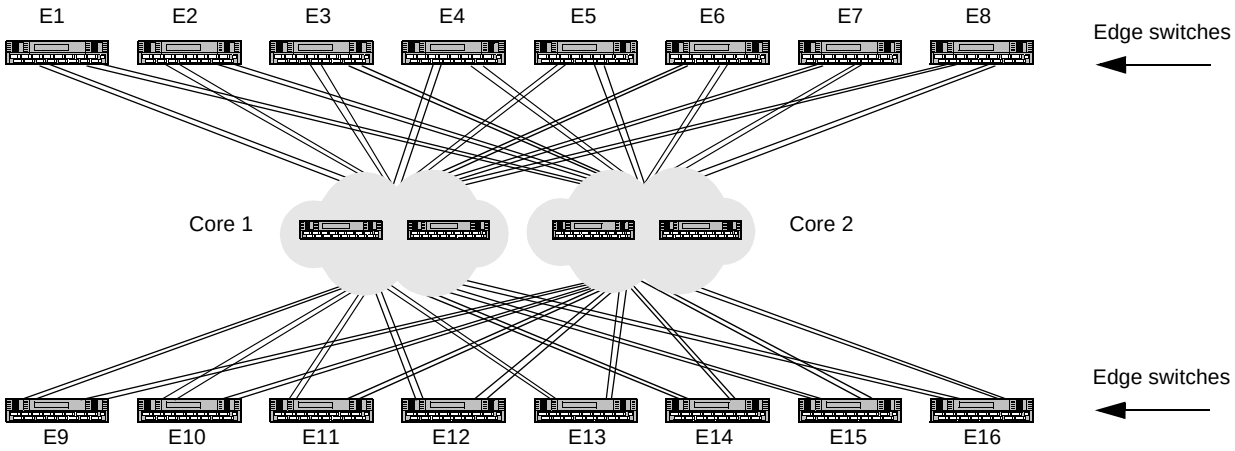

Figure A-2 20-Switch Star Configuration

Appendix

B

Bring Up Checklists

This Appendix contains checklists you can use when bringing up the fabric. The checklists are on separate pages, so you can print them and reference them easily.

This appendix contains the following checklists:

Checklist for Initial Bring Up

- ☐ Determine the topology of your system. Determine which are the core switches and which are the edge switches.
- ☐ Power on each switch and verify the POST completes successfully.
- ☐ Set the IP addresses on each switch.
- ☐ Run diagnostic tests on each switch to verify hardware (optional).
- ☐ Upgrade the firmware and install software licenses on each switch.
- ☐ Configure the fabric parameters and software features.
- ☐ Reboot and verify each switch.
- ☐ Connect ISLs to form a large fabric.
- ☐ Verify the fabric configuration.
- ☐ Power on the storage devices.
- ☐ Power on the host devices.
- ☐ Verify the SAN.

Checklist for Recovering from Power Failure

- ☐ Make sure all switches and devices are powered off.
- ☐ Power on the core switches.
- ☐ Power on the first edge switch.
- ☐ Power on the remaining edge switches.
- ☐ Verify the fabric configuration.
- ☐ Power on the storage devices.
- ☐ Power on the host devices.
- ☐ Verify the SAN.

Glossary

8b/10b encoding An encoding scheme that converts each 8-bit byte into 10 bits. Used to balance ones and zeros in high-speed transports.

address identifier A 24-bit or 8-bit value used to identify the source or destination of a frame.

AL_PA Arbitrated loop physical address. A unique 8-bit value assigned during loop initialization to a port in an arbitrated loop.

alias An alternate name for an element or group of elements in the fabric. Aliases can be used to simplify the entry of port numbers and WWNs when creating zones.

alias address identifier An address identifier recognized by a port in addition to its standard identifier. An alias address identifier may be shared by multiple ports. See also *alias.*

alias AL_PA An AL_PA value recognized by an L_Port in addition to the AL_PA assigned to the port. See also *AL_PA.*

alias server A fabric software facility that supports multicast group management.

ANSI American National Standards Institute. The governing body for fibre channel standards in the U.S.A.

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

arbitrated loop A shared 100 MBps fibre channel transport structured as a loop. Can support up to 126 devices and one fabric attachment. See also *topology*.

ASIC Application specific integrated circuit.

ATM Asynchronous transfer mode. A transport used for transmitting data over LANs or WANs that transmit fixed-length units of data. Provides any-to-any connectivity, and allows nodes to transmit simultaneously.

authentication The process of verifying that an entity (such as a switch) in a fabric is what it claims to be. See also *digital certificate, switch-to-switch authentication.*

AW_TOV Arbitration wait time-out value. The minimum time an arbitrating L_Port waits for a response before beginning loop initialization.

backup FCS switch Backup fabric configuration server switch. The switch or switches assigned as backup in case the primary FCS switch fails. See also *FCS switch, primary FCS switch.*

bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a link or system. See also *throughput.*

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. See also *buffer-to-buffer flow control, EE_Credit.*

beacon When all 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 telnet command or through Brocade Web Tools.

beginning running disparity The disparity at the transmitter or receiver when the special character associated with an ordered set is encoded or decoded. See also *disparity*.

BER Bit error rate. The rate at which bits are expected to be received in error. Expressed as the ratio of error bits to total bits transmitted. See also *error*.

block As applies to fibre channel, upper-level application data that is transferred in a single sequence.

broadcast The transmission of data from a single source to all devices in the fabric, regardless of zoning. See also *multicast, unicast.*

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

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

cascade Two or more interconnected fibre channel switches. 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*.

chassis The metal frame in which the switch and switch components are mounted.

circuit An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions. See also *link.*

Class 1 The class of frame switching service for a dedicated connection between two communicating ports (also called connection-oriented service), with acknowledgement of delivery or nondelivery of frames.

Class 2 A connectionless class of frame switching service that includes acknowledgement of delivery or nondelivery of frames.

Class 3 A connectionless class of frame switching service that does not include acknowledgement of delivery or nondelivery of frames. Can be used to provide a multicast connection between the frame originator and recipients, with acknowledgement of delivery or nondelivery of frames.

Class F The class of frame switching service for a direct connection between two switches, allowing communication of control traffic between the E_Ports, with notification of delivery or nondelivery of data.

class of service A specified set of delivery characteristics and attributes for frame delivery.

CLI Command line interface. Interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.

comma A unique pattern (either 1100000 or 0011111) used in 8B/10B encoding to specify character alignment within a data stream. See also *K28.5.*

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*.

CRC Cyclic redundancy check. A check for transmission errors that is included in every data frame.

credit As applies to fibre channel, the number of receive buffers available for transmission of frames between ports. See also *BB_Credit, EE_Credit.*

cut-through A switching technique that allows the route for a frame to be selected as soon as the destination address is received. See also *route.*

data word A type of transmission word that occurs within frames. The frame header, data field, and CRC all consist of data words. See also *frame, ordered set, transmission word.*

defined zone configuration The set of all zone objects defined in the fabric. May include multiple zone configurations. See also *enabled zone configuration, zone configuration.*

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

disparity The proportion of ones and zeros in an encoded character. “Neutral disparity” means an equal number of each, “positive disparity” means a majority of ones, and “negative disparity” means a majority of zeros.

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 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 SilkWorm switch can be any integer between| 1 and 239.

E_D_TOV Error detect time-out 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 condition is declared. See also *R_A_TOV, RR_TOV*.

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL. See also *ISL*.

EE_Credit End-to-end credit. The number of receive buffers allocated by a recipient port to an originating port. Used by Class 1 and 2 services to manage the exchange of frames across the fabric between source and destination. See also *BB_Credit, end-to-end flow control.*

EIA rack A storage rack that meets the standards set by the Electronics Industry Association.

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.*

end-to-end flow control Governs flow of class 1 and 2 frames between N_Ports. See also *EE_Credit.*

error As applies to fibre channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors). See also *loop failure.*

exchange The highest level fibre channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in either one or both directions.

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 fibre channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. See also *cascade, SAN, topology.*

fabric name The unique identifier assigned to a fabric and communicated during login and port discovery.

FC-AL-3 The Fibre Channel Arbitrated Loop standard defined by ANSI. Defined on top of the FC-PH standards.

FC-FLA The Fibre Channel Fabric Loop Attach standard defined by ANSI.

FCIA Fibre Channel Industry Association. An international organization of fibre channel industry professionals. Among other things, provides oversight of ANSI and industry developed standards.

FCP Fibre channel protocol. Mapping of protocols onto the fibre channel standard protocols. For example, SCSI FCP maps SCSI-3 onto fibre channel.

FC-PH-1, 2, 3 The Fibre Channel Physical and Signalling Interface standards defined by ANSI.

FC-PI The Fibre Channel Physical Interface standard defined by ANSI.

FC-PLDA The Fibre Channel Private Loop Direct Attach standard defined by ANSI. Applies to the operation of peripheral devices on a private loop.

FCS switch Fabric configuration server switch. One or more designated SilkWorm switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by WWN, and the list of designated switches is communicated fabric-wide. See also *backup FCS switch, primary FCS switch.*

FC-SW-2 The second generation of the Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of fibre channel switches in order to create a multi-switch fibre channel fabric.

fibre channel transport A protocol service that supports communication between fibre channel service providers. See also *FSP.*

Fill Word An IDLE or ARB ordered set that is transmitted during breaks between data frames to keep the fibre channel link active.

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.*

FLOGI Fabric login. The process by which an N_Port determines whether a fabric is present, and if so, exchanges service parameters with it. See also *PLOGI.*

frame The fibre channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, any optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: Link control frames (transmission acknowledgements, etc.) and data frames.

FRU Field-replaceable unit. A component that can be replaced on site.

FS	Fibre channel service. A service that is defined by fibre channel standards and exists at a well-known address. For example, the Simple Name Server is a fibre channel service. See also *FSP*.
FSP	Fibre channel service protocol. The common protocol for all fabric services, transparent to the fabric type or topology. See also *FS*.
FSPF	Fabric shortest path first. Brocade's routing protocol for fibre channel switches.
full-duplex	A mode of communication that allows the same port to simultaneously transmit and receive frames. See also *half-duplex*.
Fx_Port	A fabric port that can operate as either an F_Port or FL_Port. See also *F_Port, FL_Port*.
G_Port	Generic port. A port that can operate as either an E_Port or F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.
GBIC	Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for fibre channel and gigabit ethernet.
Gbps	Gigabits per second (1,062,500,000 bits/second).
GBps	GigaBytes per second (1,062,500,000 bytes/second).
half-duplex	A mode of communication that allows a port to either transmit or receive frames at any time, but not simultaneously (with the exception of link control frames, which can be transmitted at any time). See also *full-duplex*.
hard address	The AL_PA that an NL_Port attempts to acquire during loop initialization.
hardware translative mode	A method for achieving address translation. The following two hardware translative modes are available to a QuickLoop enabled switch: • Standard translative mode: Allows public devices to communicate with private devices that are directly connected to the fabric. • QuickLoop mode: Allows initiator devices to communicate with private or public devices that are not in the same loop.
HBA	Host bus adapter. The interface card between a server or workstation bus and the fibre channel network.
hub	A fibre channel wiring concentrator that collapses a loop topology into a physical star topology. Nodes are automatically added to the loop when active and removed when inactive.
idle	Continuous transmission of an ordered set over a fibre channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.
initiator	A server or workstation on a fibre channel network that initiates communications with storage devices. See also *target*.
Integrated Fabric	The fabric created by a SilkWorm 6400, consisting of six SilkWorm 2250 switches cabled together and configured to handle traffic as a seamless group.
IOD	In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.
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*.

isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). See also *E_Port.*

IU Information unit. A set of information as defined by either upper-level process protocol definition or upper-level protocol mapping.

JBOD Just a bunch of disks. Indicates a number of disks connected in a single chassis to one or more controllers. See also *RAID.*

K28.5 A special 10-bit character used to indicate the beginning of a transmission word that performs fibre channel control and signaling functions. The first seven bits of the character are the comma pattern. See also *comma*.

key A string of data (usually a number) shared between two entities and used to control a cryptographic algorithm. Usually selected from a large pool of possible keys to make unauthorized identification of the key difficult. See also *key pair.*

key pair In public key cryptography, a pair of keys consisting of an entity's public and private key. The public key can be publicized, but the private key must be kept secret. See also *public key cryptography.*

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 one of two modes:

- Fabric mode: Connected to a port that is not loop capable, and using fabric protocol.
- Loop mode: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or non-participating mode.

See also *non-participating mode, participating mode.*

latency The period of time required to transmit a frame, from the time it is sent until it arrives. Together, latency and bandwidth define the speed and capacity of a link or system.

LED Light emitting diode. Used to indicate status of elements on switch.

link As applies to fibre channel, a physical connection between two ports, consisting of both transmit and receive fibres. See also *circuit.*

link services A protocol for link-related actions.

LIP Loop initialization primitive. The signal used to begin initialization in a loop. Indicates either loop failure or resetting of a node.

LM_TOV Loop master time-out value. The minimum time that the loop master waits for a loop initialization sequence to return.

loop failure Loss of signal within a loop for any period of time, or loss of synchronization for longer than the time-out value.

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_ID A hex value representing one of the 127 possible AL_PA values in an arbitrated loop.

looplet A set of devices connected in a loop to a port that is a member of another loop.

LPSM Loop port state machine. The logical entity that performs arbitrated loop protocols and defines the behavior of L_Ports when they require access to an arbitrated loop.

LWL Long wavelength. A type of fiber optic cabling that is based on 1300mm lasers and supports link speeds of 1.0625 Gbps. May also refer to the type of GBIC or SFP. See also *SWL.*

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

multicast The transmission of data from a single source to multiple specified N_Ports (as opposed to all the ports on the network). See also *broadcast, unicast.*

multimode A fiber optic cabling specification that allows up to 500 meters between devices.

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 Frequently used to indicate Simple Name Server. See also *SNS.*

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.

non-participating mode A mode in which an L_Port in a loop is inactive and cannot arbitrate or send frames, but can retransmit any 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.*

Nx_Port A node port that can operate as either an N_Port or NL_Port.

ordered set A transmission word that uses 8B/10B mapping and begins with the K28.5 character. Ordered sets occur outside of frames, and include the following items:

- Frame delimiters: Mark frame boundaries and describe frame contents.
- Primitive signals: Indicate events.
- Primitive sequences: Indicate or initiate port states.

Ordered sets are used to differentiate fibre channel control information from data frames and to manage the transport of frames.

packet A set of information transmitted across a network. See also *frame.*

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, non-participating mode.*

path selection The selection of a transmission path through the fabric. Brocade switches use the FSPF protocol. See also *FSPF.*

phantom address An AL_PA value that is assigned to an device that is not physically in the loop. Also known as phantom AL_PA.

phantom device A device that is not physically in an arbitrated loop but is logically included through the use of a phantom address.

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

PKI certification utility	Public key infrastructure certification utility. A utility that makes it possible to collect certificate requests from switches and load certificates to switches. See also *digital certificate, PKI.*
PLOGI	Port login. The port-to-port login process by which initiators establish sessions with targets. See also *FLOGI.*
point-to-point	A fibre channel topology that employs direct links between each pair of communicating entities. See also *topology*.
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.
primary FCS switch	Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric. See also *backup FCS switch, FCS switch.*
private device	A device that supports arbitrated loop protocol and can interpret 8-bit addresses, but cannot log into the fabric.
private key	The secret half of a key pair. See also *key, key pair*.
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 into the fabric.
protocol	A defined method and set of standards for communication.
public device	A device that supports arbitrated loop protocol, can interpret 8-bit addresses, and can log into the fabric.
public key	The public half of a key pair. See also *key, key pair*.
public key cryptography	A type of cryptography which uses a key pair, with the two keys in the pair called at different points in the algorithm. The sender uses the recipient's public key to encrypt the message, and the recipient uses the recipient’s private key to decrypt it. See also *key pair, PKI.*
public loop	An arbitrated loop that includes a participating FL_Port, and may contain both public and private NL_Ports.
public NL_Port	An NL_Port that logs into the fabric, can function within either a public or a private loop, and can communicate with either private or public NL_Ports.
quad	A group of four adjacent ports that share a common pool of frame buffers.
R_A_TOV	Resource allocation time-out value. The maximum time a frame can be delayed in the fabric and still be delivered. See also *E_D_TOV, RR_TOV*.
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. See also *JBOD.*
request rate	The rate at which requests arrive at a servicing entity. See also *service rate.*
route	As applies to a fabric, the communication path between two switches. May 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.
RR_TOV	Resource recovery time-out value. The minimum time a target device in a loop waits after a LIP before logging out a SCSI initiator. See also *E_D_TOV, R_A_TOV.*
RSCN	Registered state change notification. A switch function that allows notification of fabric changes to be sent from the switch to specified nodes.
SAN	Storage area network. A network of systems and storage devices that communicate using fibre channel protocols. See also *fabric.*
sectelnet	A protocol similar to Telnet but with encrypted passwords for increased security.
security policy	A set of rules that determine how security is implemented in a fabric. Security policies can be customized.
sequence	A group of related frames transmitted in the same direction between two N_Ports.
service rate	The rate at which an entity can service requests. See also *request rate.*
SI	Sequence initiative.
SilkWorm	The brand name for the Brocade family of switches.
single mode	The fiber optic cabling standard that corresponds to distances of up to 10 km between devices.
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. 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. May also be referred to as directory service. See also *FS.*
switch	Hardware that routes frames according to fibre channel protocol and is controlled by software.
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. See also *authentication, digital certificate.*
SWL	Short wavelength. A type of fiber optic cabling that is based on 850mm lasers and supports 1.0625 Gbps link speeds. May also refer to the type of GBIC or SFP. See also *LWL.*
target	A storage device on a fibre channel network. See also *initiator.*
tenancy	The time from when a port wins arbitration in a loop until the same port returns to the monitoring state. Also referred to as loop tenancy.
throughput	The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). See also *bandwidth.*

topology As applies to fibre channel, 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.

translative mode A mode in which private devices can communicate with public devices across the fabric.

transmission character A 10-bit character encoded according to the rules of the 8B/10B algorithm.

transmission word A group of four transmission characters.

trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. See also *SNMP*.

tunneling A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network, but are connected by a different type of network.

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric.

UDP User datagram protocol. A protocol that runs on top of IP and provides port multiplexing for upper-level protocols.

ULP Upper-level protocol. The protocol that runs on top of fibre channel. Typical upper-level protocols are SCSI, IP, HIPPI, and IPI.

ULP_TOV Upper-level time-out value. The minimum time that a SCSI ULP process waits for SCSI status before initiating ULP recovery.

unicast The transmission of data from a single source to a single destination. See also *broadcast, multicast.*

well-known address As pertaining to fibre channel, a logical address defined by the fibre channel standards as assigned to a specific function, and stored on the switch.

workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN Worldwide name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

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 permission 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.*

Index

P

R

S

T

U

Z