BROCADE®

Brocade® Secure Fabric OS

User's Guide

Version 2.6

Publication Number 53-0000195-02

Publication Number 53-0000195-02

Notice: This book was designed and written to provide information about storage area networking architectures. Every effort has been made to make this book as complete and accurate as possible. However, the information in this book is provided to you “AS IS,” without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

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

Security Notice

Secure Fabric OS includes security features that you can use, along with other security tools, to design and implement a more secure storage area network (“SAN”), as part of your overall network and information security infrastructure. However, simply installing Secure Fabric OS does not guarantee the security of your SAN or your overall network. There are numerous factors that affect the security of a SAN, including, without limitation, proper security policies and procedures, hardware and software selection (including network security tools), proper installation, configuration, and maintenance of the hardware and software, the interoperability of the various components of your SAN and your network, and a proper, secure operating environment. In addition, Secure Fabric OS utilizes digital certificates in connection with its access control features. Although digital certificates are a useful authentication security measure that improves overall security, they do not guarantee authenticity or security. To help you evaluate the digital certificate functionality of Secure Fabric OS, you can obtain details in the Certificate Practices Statement, which is included with the documentation you received with this product. In designing the security of your SAN, it is your responsibility to evaluate all of these factors to ensure your SAN will meet your security needs. Your experience may vary based on these and other factors. Your use of Secure Fabric OS, including the digital certificates, is subject to and governed by the terms of the applicable license agreement and to your compliance with the policies and procedures for the use of Secure

Fabric OS and digital certificates made available to you by Brocade from time to time. If Brocade becomes aware of a breach of the security of its digital certificate infrastructure, Brocade reserves the right to re-issue digital certificates. In that event, you will be required to submit new certificate signing requests and install reissued certificates across your SAN. You should plan for any network disruption that this may cause.

YOU ACKNOWLEDGE THAT YOU HAVE ACCESS TO SUFFICIENT INFORMATION TO ENSURE THAT YOU CAN MAKE AN INFORMED DECISION AS TO THE EXTENT TO WHICH YOU CHOOSE TO RELY ON DIGITAL CERTIFICATES AND OTHER SECURITY FEATURES IN SECURE FABRIC OS ("SECURITY"). THE SECURITY IS PROVIDED "AS IS," WITHOUT WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. BROCADE SHALL HAVE NO LIABITY WITH RESPECT TO YOUR USE OF AND RELIANCE ON THE SECURITY.

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

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

Preface

Chapter 1 Introducing Secure Fabric OS

Chapter 2 Licensing for Secure Fabric OS

Chapter 3 Setting Up Secure Fabric OS

Chapter 4 Using Secure Fabric OS

Preface

Brocade Secure Fabric OS is an optionally licensed product that requires a valid license key to function. It is supported for the SilkWorm® 2000 series of switches, using the Fabric OS v2.6.

About This Guide

This guide provides the following information about Brocade Security:

Chapter 1 Introducing Secure Fabric OS	Overview of the Brocade Security features.
Chapter 2 Prerequisites for Secure Fabric OS	Information on prerequisites for the Brocade Security features.
Chapter 3 Setting up Secure Fabric OS	Information on setting up the Brocade Security features.
Chapter 4 Using Secure Fabric OS	Information for using the Brocade Security features.

Related Publications

Related product information can be found in the following publications:

- *Brocade Fabric OS Reference*
- *Brocade Web Tools User's Guide*
- *Brocade Zoning User's Guide*
- *Brocade QuickLoop User's Guide*
- *Brocade Fabric Watch User's Guide*
- *Brocade Distributed Fabrics User's Guide*
- *Brocade SES User's Guide*

Information about fibre channel standards and fibre channel 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. Be prepared to provide the following information to support personnel:

- Switch serial number
- Switch worldwide 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 2000
- Windows NT
- 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 website as follows:

1. Open your web browser and enter:

   ```
   http://www.brocade.com
   ```

2. Click **Technical Support**.
3. Click **MIBs and RSH Utilities**.
4. Click the download link for the desired product.

Chapter

1

Introducing Secure Fabric OS

This chapter provides the following information:

- *Overview* on page 1-1
- *Key Security Elements* on page 1-2

Overview

Brocade Secure Fabric OS is an optionally licensed product, based on Brocade's Fabric OS v2.6, that manages the Brocade SilkWorm family of fibre channel fabric devices in both new and existing SANs (Storage Area Networks).

Note: Brocade's Fabric OS v2.6 alone does not provide Secure Fabric OS. To create security, you must:

- Install Brocade Fabric OS v2.6
- Purchase the optionally licensed Secure Fabric OS product

Why Secure a SAN?

Security is a fundamental requirement for enterprise SANs. As SANs increase in size and are internetworked over a metropolitan area network (MAN) or wide area network (WAN), physical monitoring and management are no longer feasible or cost-effective. If you have an environment with more than one customer, security:

- Enables sharing of SAN infrastructure resources among multiple customers securely
- Increases cost savings by eliminating the need for multiple fabrics to separate resources

SAN Security Features

Table 1-1 New Security Requirements for SANs

What Security Provides	How It Works
New levels of access control	SAN fabrics require more controls to prevent unauthorized access to a switched fabric, to SAN fabric switches through unprotected connections such as serial ports, or through the front panel of fabric switches and other SAN devices. SAN fabrics require more granularity in access controls for the following reasons: Spoofing Hosts can sign on with a phony world wide name (WWN) and get access to devices that they should not be able to Denial of service attack Unauthorized host application can send out dummy management messages or inputs/outputs to a logical unit device that it does not own Unauthorized devices could be added to the fabric
Strong authentication	Switch-to-switch authentication is key to security. Without authentication, SANs are susceptible to switches connected to fabric either accidentally or maliciously that compromise the security of the fabric.
More controls in SAN fabric management	You have the ability to turn certain management access to the fabric on or off. You also have control of end points accessing management facilities within the fabric. Remote management access can be secured. Configuration (security) parameters are now centralized.
Confidentiality (privacy with data)	Passwords are now encrypted so that they remain private.

Key Security Elements

The main security elements associated with Secure Fabric OS are:

1. Access control policies:
   - Fabric Configuration Server (FCS) Policy
   - Options Policy
   - Device Connection Control (DCC) Policies
   - Switch Connection Control (SCC) Policy
   - Management Access Control (MAC) Policies

2. Switch-to-switch authentication.

   The switches are identified by their WWNs (World Wide Names). Each switch's Digital Certificate contains its WWN.

3. Secure Management channels.

   Passwords are encrypted for Web Tools, telnet, and API.

Chapter

2

Licensing for Secure Fabric OS

This chapter provides the following information:

- *Overview* on page 2-1
- *Secure Fabric OS Licensing* on page 2-1
- *Getting License Keys* on page 2-3

Overview

To enable secure mode, all switches in the fabric must have:

- Fabric OS v2.6
- A certificate and public/private key pair
- A zoning license
- A security license

Secure Fabric OS Licensing

If you are using Secure Fabric OS v2.6, either with a new switch or field upgrade, you need to follow the licensing information on this page and the *Verifying a Security License* section on page 2-2.

Security is licensed separately and is not included in existing or new proposed software bundles.

Licenses for Secure Fabric OS

The Secure Fabric OS is licensed in the field by using License Paper Packs. Customers who have a base already installed and wish to deploy the Secure Fabric OS must first upgrade to Fabric OS 2.6. You are required to purchase and activate zoning and security licenses for the Secure Fabric OS on a per-switch basis.

Verifying a Security License

To verify that a security license is installed on a switch, do the following:

1. From a command prompt screen, use the `telnet` command to log onto the switch, using an account that has administrative privileges.

   Example:

   ```
   Z:\/telnet <System_name>|<IP address>
   ```

   where `System_name|IP address` is replaced with an assigned `System_name` or `IP address`.

2. Enter the `licenseShow` telnet command on the command line.

   A list displays all of the licenses currently installed on the switch.

   Example:

   ```
   admin> licenseShow

   1A1AaAaaaAAAA1a:

    Release v2.6
    Web license
    Zoning license
    SES license
    Security license
   ```

If the security license is not included in the list, or is incorrect, do the following:

1. Enter the following on the command line:

   ```
   licenseAdd “key”
   ```

   where “`key`” is the license key provided to you, through licensed Paper Packs, enclosed in double quotes.

   Note: The license key is case sensitive and must be entered exactly as given.

2. Verify the license was added by entering the following telnet command on the command line:

   ```
   licenseShow
   ```

   If the Secure Fabric OS license is listed, the feature is installed and immediately available.

   If the license is not listed, repeat step 1.

Repeat all the steps in the *Verifying a Security License* section on page 2-2 for obtaining a zoning license.

Note: An alternate method to getting license keys is by accessing the Brocade web site. Refer to the *Getting License Keys* section on page 2-3.

Getting License Keys

When generating a license key you have the option of generating either a:

- Single license key
- Batch of licenses

Generating a Single License Key

To generate a single license key perform the following:

1. Go to the Brocade web site at:

   `www.brocade.com.`

2. At the Brocade web site, click on **Products**.
3. Click on **Software Products** on the Products screen.
4. Click on **Software License Keys**.

   The Software License Keys instruction page appears.

5. If you want one license key, click on **Generate License Key**.

   The Software License Keys page appears.

6. Enter the required fields:
   - Email address
   - Switch world-wide name
   - Transaction key
7. Click the **Next** button.

   A verification screen appears. Press **Submit** if the information displayed is correct.

   If the information is incorrect, press **Previous** and change the information.

   An information screen appears that displays the license key.

8. You will receive an email from Brocade with a license key number and installation instructions for the license key.
9. Enter the license key number on your switch and follow the installation instructions.

Generating a Batch of Licenses

To generate a batch of licenses perform the following:

1. Go to the Brocade web site at:

   `www.brocade.com`

2. At the Brocade web site, click on **Products**.
3. Click on **Software Products** on the Products screen.
4. Click on **Software License Keys**.

   The Software License Keys process page appears.

5. If you want multiple license keys, click on **Batch Generation of Licenses**.

   The Software License Key instruction page appears.

6. Enter the required fields:

   - Email address
   - World-wide names
   - Transaction keys

   Note: Enter the world-wide names and transaction keys in the table at the bottom of the screen. If you need additional rows in the table, click on **Add More Rows**.

7. Click the **Next** button.

   A verification screen appears. Press **Submit** if the information displayed is correct.

   If the information is incorrect, press **Previous** and change the information.

8. Press **Submit**.

   An information screen that displays error messages or warnings appears.

9. If the information is incorrect, press **Previous** and change the information. You will cycle back to the information screen by pressing **Submit**.

   An information screen appears that displays the license keys.

10. You will receive an email from Brocade with license key numbers and installation instructions for the license keys.

    Enter the license key numbers on your switch and follow the installation instructions.

Chapter

3

Setting Up Secure Fabric OS

This chapter provides the following information:

Overview

This chapter explains how to set up secure Fabric OS v2.6:

- Initial setup, page 3-2

  Check to ensure that the security feature is installed on the switch. Refer to *Downloading Secure Fabric OS v2.6 Firmware onto a Switch* on page 3-5.

- On field upgrades, page 3-4

  On field upgrades, you need to upgrade the OS to Fabric OS v2.6 and load the security option.

Security Notice

Secure Fabric OS includes security features that you can use, along with other security tools, to design and implement a more secure storage area network ("SAN"), as part of your overall network and information security infrastructure. However, simply installing Secure Fabric OS does not guarantee the security of your SAN or your overall network. There are numerous factors that affect the security of a SAN, including, without limitation, proper security policies and procedures, hardware and software selection (including network security tools), proper installation, configuration, and maintenance of the hardware and software, the interoperability of the various components of your SAN and your network, and a proper, secure operating environment. In addition, Secure Fabric OS utilizes digital certificates in connection with its access control features. Although digital certificates are a useful authentication security measure that improves overall security, they do not guarantee authenticity or security. To help you evaluate the digital certificate functionality of Secure Fabric OS, you can obtain details in the Certificate Practices Statement, which is included with the documentation you received with this product. In designing the security of your SAN, it is your responsibility to evaluate all of these factors to ensure your SAN will meet your security needs. Your experience may vary based on these and other factors. Your use of Secure Fabric OS, including the digital certificates, is subject to and governed by the terms of the applicable license agreement and to your compliance with the policies and procedures for the use of Secure Fabric OS and digital certificates made available to you by Brocade from time to time. If Brocade becomes aware of a breach of the security of its digital certificate infrastructure, Brocade reserves the right to re-issue digital certificates. In that event, you will be required to submit new certificate signing requests and install reissued certificates across your SAN. You should plan for any network disruption that this may cause.

YOU ACKNOWLEDGE THAT YOU HAVE ACCESS TO SUFFICIENT INFORMATION TO ENSURE THAT YOU CAN MAKE AN INFORMED DECISION AS TO THE EXTENT TO WHICH YOU CHOOSE TO RELY ON DIGITAL CERTIFICATES AND OTHER SECURITY FEATURES IN SECURE FABRIC OS (“SECURITY”). THE SECURITY IS PROVIDED “AS IS,” WITHOUT WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. BROCADE SHALL HAVE NO LIABITY WITH RESPECT TO YOUR USE OF AND RELIANCE ON THE SECURITY.

Initial Setup

Perform the steps in this section, if you are initially setting up the secure Fabric OS v2.6:

1. *Getting Your Licenses* on page 3-2
2. *Completing Your First Login* on page 3-2
3. *Downloading sectelnet* on page 3-3

Getting Your Licenses

You need to ensure that you have licenses for security and zoning. To get the needed licenses, follow the steps in the *Secure Fabric OS Licensing* section on page 2-1. Digital certificates that come from the factory with v2.6 installed are already embedded in the switch.

Completing Your First Login

Initiate a telnet or sectelnet session to the switch.

To enter your first login, do the following:

1. Enter a login name at the login prompt.
2. Enter a password at the password prompt.
3. At the command line prompt, start using the security commands to manage security. Refer to the *Brocade Secure Fabric OS Telnet Commands* section on page 4-14.

The version 2.6 firmware increases password security such that the very first time you log in, you will be prompted to change all passwords. These new passwords must be different from the factory defaults.

Note: Remember your passwords. Forgotten passwords will require significant effort from which to recover and will result in fabric downtime.

Note: Until you change all passwords, you will be prompted at login time and the `passwd` Fabric OS command is disabled.

To enable security, refer to the *Enabling Security Mode on a Fabric* section on page 4-23.

Downloading sectelnet

To download sectelnet, perform the following steps:

1. Go to the Brocade web site at:

   `www.brocade.com`.

2. At the Brocade web site, click on **partners**.

   The Brocade Partner Network screen appears.

3. Click the **Brocade Partner Network** link in the first paragraph.

   The login screen appears.

   Note: If you do not have a login and password, email the following information to `partnerweb@brocade.com`:

   - First name
   - Last name
   - Company name
   - Name of Brocade partner program in which your company participates
   - Email address

4. Enter your login and password.

   The title page appears.

5. Under Services and Support, click on the **firmware** link.

6. Click on the **v2.6.x Firmware** link.

   The version 2.6.x Firmware screen appears.

7. Click on the **Version 2.6.0** link.

   The version 2.6.0 screen appears.

8. Click on **Obtain secure telnet client** (step 7).

9. Depending on whether you are using a PC or Solaris, click on one of the following:

   - Secure Telnet Client - PC
   - Secure Telnet Client - Solaris

   If you click on Secure Telnet Client - PC, a screen appears where you need to save the file.

If you click on Secure Telnet Client - Solaris, skip to step 13.

Note: The download is complete when you save the file.

In the above process, the file is saved as a Zip file in the location of your choice.

Example:

> The Secure Telnet Client - PC file could be saved in `c:\security`.

10. Unzip the file.
11. Invoke `setup.exe`.
12. Follow the prompts.

    After accepting the Finish prompt, `sectelnet.exe` is now available to access your secure fabric.
13. If you click on Secure Telnet Client - Solaris, the Save As screen appears and a default path is displayed. You may change the default path, if you'd like.

    Note: In order to enable security, you must use `sectelnet`.

Field Upgrades

Customers who already have switches installed and wish to deploy the Secure Fabric OS are required to first download Secure Fabric OS v2.6 onto all switches in each fabric. A secure fabric requires all switches to license and implement the security feature. Therefore, the firmware version itself is a prerequisite to deployment.

Perform the steps in the following sections to perform a field upgrade:

1. *Downloading Fabric OS v2.6 Firmware from Brocade's Web Site* on page 3-5
2. *Downloading Secure Fabric OS v2.6 Firmware onto a Switch* on page 3-5
3. *Secure Fabric OS Licensing* on page 2-1
4. *Downloading the PKICert Utility* on page 3-6
5. *Installing the PKICert Utility* on page 3-8
6. *Generating a Certificate Request* on page 3-8
7. *Requesting a Certificate* on page 3-12
8. *Loading Certificates onto the Switches* on page 3-14
9. *First Login* on page 3-17
10. *Downloading sectelnet* on page 3-17

Downloading Fabric OS v2.6 Firmware from Brocade’s Web Site

To download the firmware from Brocade’s web site, perform the following steps:

1. Go to the Brocade web site at:

   `www.brocade.com`.

2. At the Brocade web site, click on **partners**.

   The Brocade Partner Network screen appears.

3. Click the **Brocade Partner Network** link in the first paragraph.

   The login screen appears.

   Note: If you do not have a login and password, email the following information to `partnerweb@brocade.com`:

   - First name
   - Last name
   - Company name
   - Name of Brocade partner program in which your company participates
   - Email address

4. Enter your login and password.

   The title page appears.

5. Under Services and Support, click on the **firmware** link.

6. Click on the **v2.6.x Firmware** link.

   The version 2.6.x Firmware screen appears.

7. Click on the **Version 2.6.0** link.

   The version 2.6.0 screen appears.

8. Click on the firmware that you want. Then download the firmware to a location on your hard drive.

   Example:

   ```
   c:\security\v2.6.0 Firmware
   ```

   A message appears when the download is complete.

Downloading Secure Fabric OS v2.6 Firmware onto a Switch

If you have not downloaded the firmware from Brocade’s web site, follow the steps in the *Downloading Fabric OS v2.6 Firmware from Brocade’s Web Site* section on page 3-5. This section details downloading the Secure Fabric OS v2.6 onto a switch:

1. At the switch command prompt, enter:

   ```
   firmwaredownload
   ```

2. Enter the Server Name or IP Address of the server where Fabric OS v2.6 resides when prompted.

   Note: If you enter the IP address, you do not have to enter the server name.

3. Enter the user name of your account on the server when prompted.
4. Enter the file name and path on the server when prompted.
5. Enter the protocol to be used for the download. The options are:

   - ftp
   - rsh

   Several messages then appear.

   A typical example:

   ```
   107584+5788+131208, csum 991a
   loading to ram..................
   writing flash 0.................
   writing flash 1.................
   download complete
   value = 0
   ```

   The firmware is downloaded.

Enter the `reboot` command at the command line to reboot the switch. The message “Rebooting” appears on the screen.

Note: A key pair and Certificate Signing Request (CSR) are automatically created for each switch in the fabric upon its very first boot into the Fabric OS v2.6.

Note: It is necessary to install license keys to enable security. Refer to the *Getting License Keys* section on page 2-3.

Licensing

Information about licensing is covered in the *Secure Fabric OS Licensing* section on page 2-1. Complete the steps.

Downloading the PKICert Utility

To download the PKICert utility, perform the following steps:

1. Go to the Brocade web site at:

   `www.brocade.com`.

2. At the Brocade web site, click on **partners**.

The Brocade Partner Network screen appears.

3. Click the **Brocade Partner Network** link in the first paragraph.

   The login screen appears.

Note: If you do not have a login and password, email the following information to `partnerweb@brocade.com`:

- First name
- Last name
- Company name
- Name of Brocade partner program in which your company participates
- Email address

4. Enter your login and password.

   The title page appears.

5. Under Services and Support, click on the **firmware** link.

6. Click on the **v2.6.x Firmware** link.

   The version 2.6.x Firmware screen appears.

7. Click on the **Version 2.6.0** link.

   The version 2.6.0 screen appears.

8. Click on **Obtain and download PKICert utility** (step 2).

9. Depending on whether you are using a PC or Solaris, click on one of the following:

   - PKICert Utility - PC
   - PKICert Utility - Solaris

   If you click on PKICert Utility - PC, the FTP process automatically begins. Continue with step 10.

   If you click on PKICert Utility - Solaris, skip step 10 and go to step 11.

10. A screen appears requesting you to save the file.

    Note: The download is complete when you save the file.

    In the above process, the file is saved as a Zip file in the location of your choice.

    Example:

    The file could be saved in `c:\security`.

11. If you click on PKICert Utility - Solaris, a Save As screen appears and you are given a default path. You can change the default path, if you’d like.

    Note: When using Solaris, PKI is downloading when a Netscape Download screen appears.

Installing the PKICert Utility

You need to install the PKICert utility after you have downloaded the Zip file. If you are working on Solaris, follow the instructions in the readme file included in the download.

To install the PKICert utility on a PC, perform the following steps:

1. Click on the zipped file that you have saved in the downloading process.

   The WinZip menu appears.

2. Click on **Extract**.

   A screen appears where you are asked to give a location for the file.

   Example:

   The file could be placed in `c:\security`.

   A folder, called nt_pki, is created and the installation is complete.

3. Review the readme file for PKICert usage.

Generating a Certificate Request

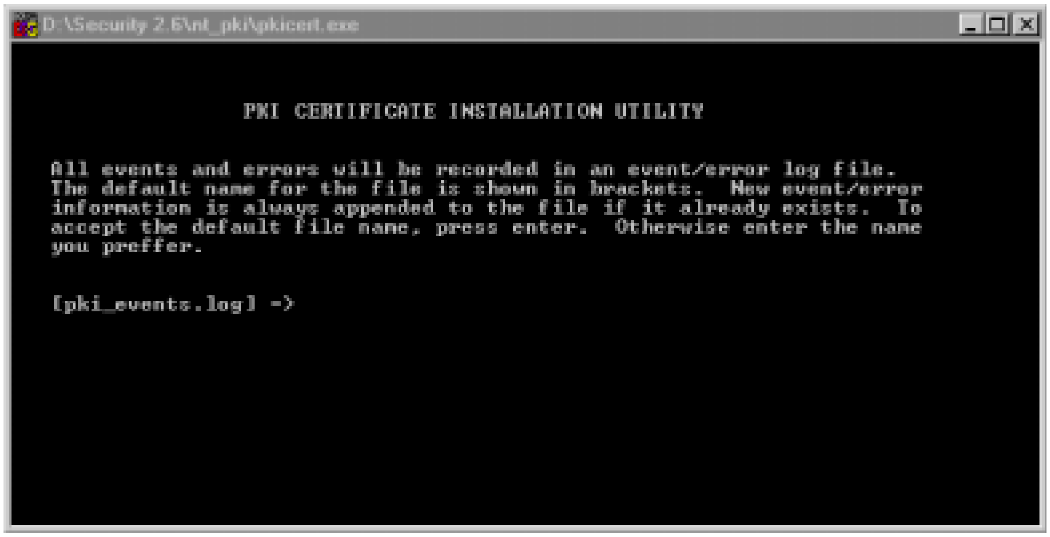
You will be using the PKICert utility to generate a certificate request in a Windows OS. Perform the following steps:

1. Click **Start/Run** at the lower left of your screen to open an NT command prompt.

2. Enter:

   `c:\security\nt_pki\pkicert` and press **Enter**.

   Note: When PKICert is opened, an event/error log is created. Enter a valid path/file name or press **Enter** to create a default file called pki_events.log in the current directory.



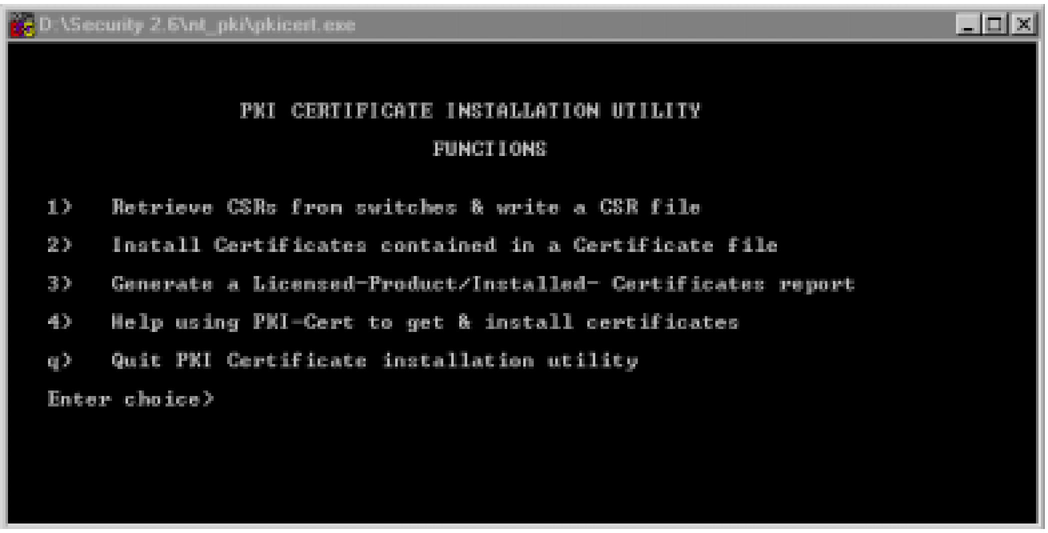
```
                  PKI CERTIFICATE INSTALLATION UTILITY

All events and errors will be recorded in an event/error log file.
The default name for the file is shown in brackets.  New event/error
information is always appended to the file if it already exists.  To
accept the default file name, press enter.  Otherwise enter the name
you preffer.


[pki_events.log] ->
```

Figure 3-1 PKI Event/Error Log

a. Enter:

`c:\security\nt_pki\security.log` and press **Enter**.

The PKI Certificate Installation Utility - Functions screen appears.



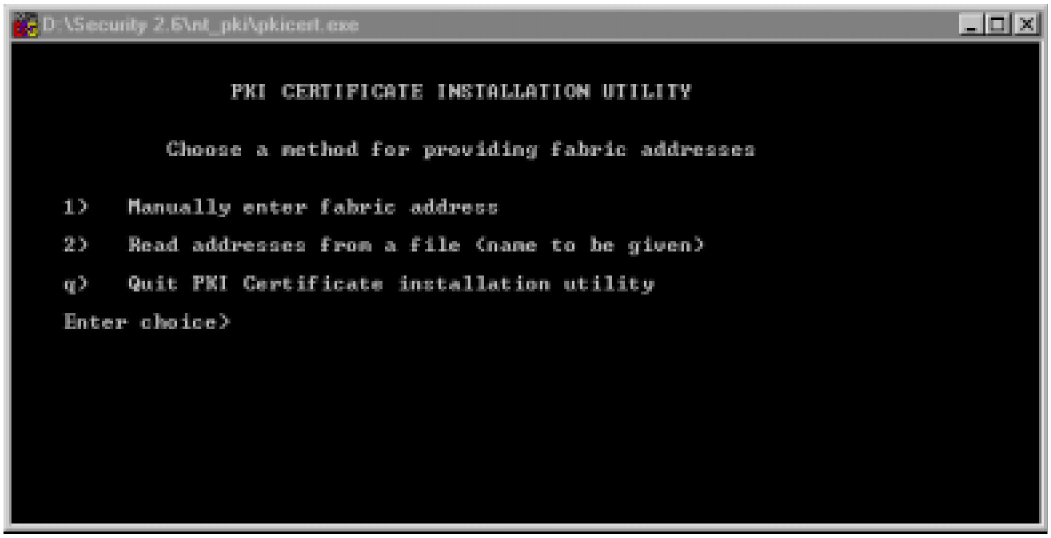
```
                PKI CERTIFICATE INSTALLATION UTILITY
                             FUNCTIONS

1)   Retrieve CSRs from switches & write a CSR file
2)   Install Certificates contained in a Certificate file
3)   Generate a Licensed-Product/Installed- Certificates report
4)   Help using PKI-Cert to get & install certificates
q)   Quit PKI Certificate installation utility
Enter choice>
```

Figure 3-2 PKI Certificate Installation Utility—Functions

b. Select option 1 (Retrieve CSRs from switches and write a CSR file).

c. Press **Enter**.

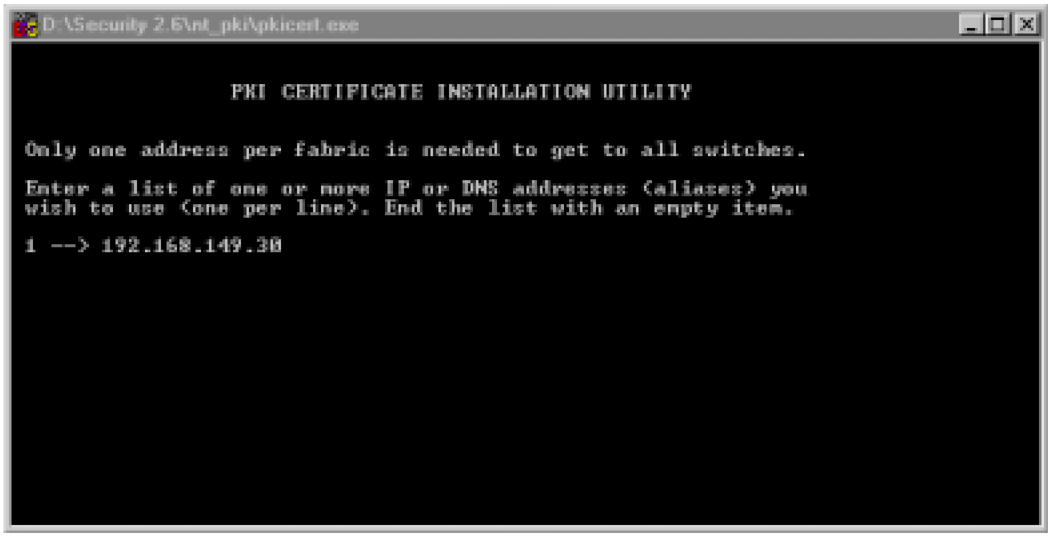
d. Select Manually enter fabric address (option 1) and press **Enter**.



```
              PKI CERTIFICATE INSTALLATION UTILITY

          Choose a method for providing fabric addresses

1)   Manually enter fabric address
2)   Read addresses from a file (name to be given)
q)   Quit PKI Certificate installation utility
Enter choice>
```

Figure 3-3 PKI Certificate Installation Utility—Option 1

Manually enter the IP address or switch name of one of the switches in the fabric.



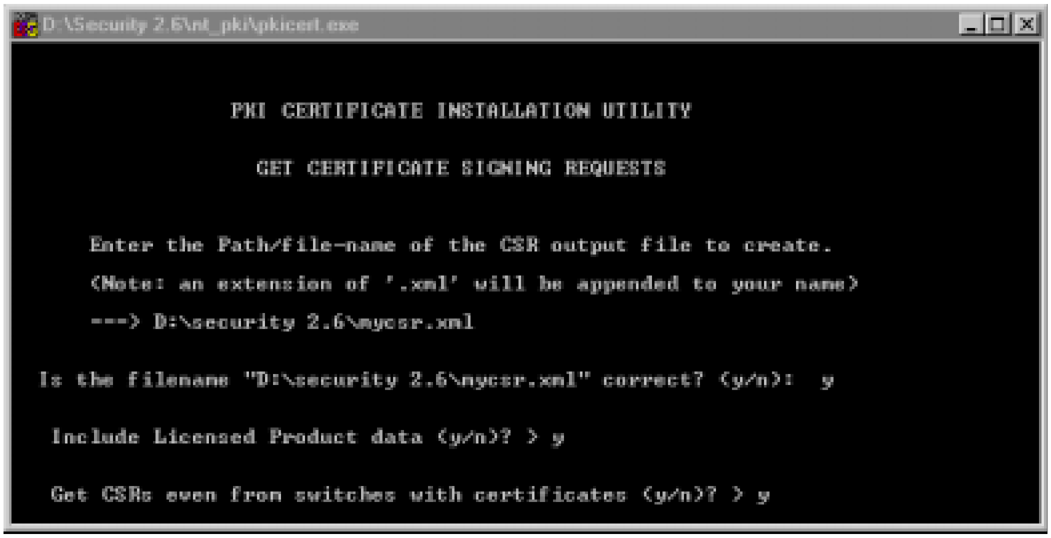
```
               PKI CERTIFICATE INSTALLATION UTILITY

Only one address per fabric is needed to get to all switches.

Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 --> 192.168.149.30
```

Figure 3-4 IP Entry for PKI Certificate Installation Utility

Note: You need only input one switch name or IP address for each fabric.

e. After entering the last entry, press **Enter** twice.

The screen titled PKI Certificate Installation Utility - Get Certificate Signing Requests appears.



```
               PKI CERTIFICATE INSTALLATION UTILITY

                 GET CERTIFICATE SIGNING REQUESTS


     Enter the Path/file-name of the CSR output file to create.

     (Note: an extension of '.xml' will be appended to your name)

     ---> D:\security 2.6\mycsr.xml

 Is the filename "D:\security 2.6\mycsr.xml" correct? (y/n):  y

  Include Licensed Product data (y/n)? > y

  Get CSRs even from switches with certificates (y/n)? > y
```

Figure 3-5 PKI Certificate Installation Utility—Get Certificate Signing Requests

f. Enter the path/file name for the CSR output file. The file name must end with an .xml extension.

Example:

```
c:\security\nt_pki\fab1.xml
```

g. Press **Enter**.

h. Press the y key if the file name is correct, or press the n key if the file name is incorrect.

i. Press **Enter**.

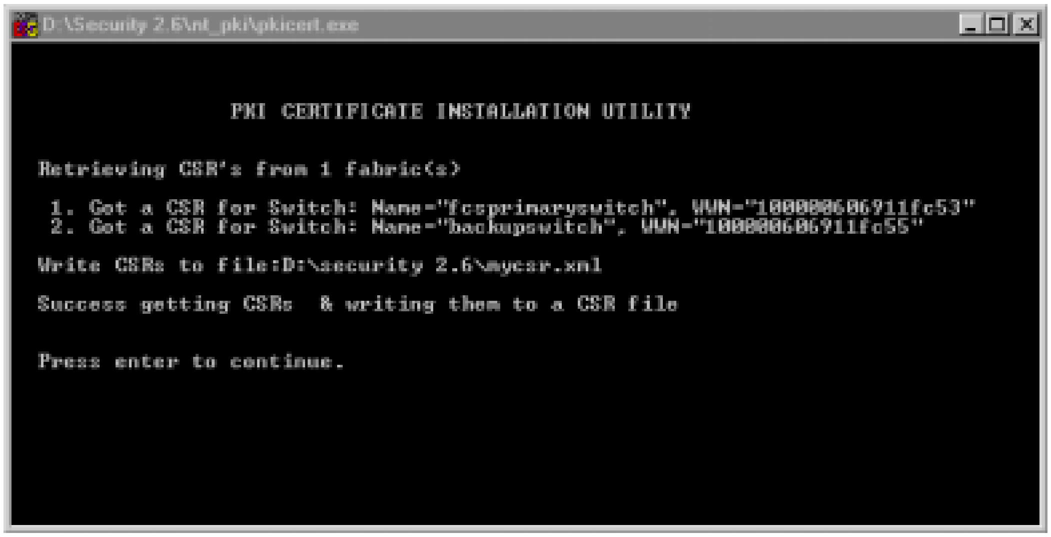
j. Press the y key (suggested) if you want to include the licensed product data, or press the n key if you do not want to include the licensed product data.

k. Press **Enter**.

l. Press the y key to get the CSR from switches that already have certificates or press the n key to not get the CSR from switches.

If you press the y key, CSRs are collected for all the switches; if you press the n key, CSRs are collected only for switches that do not already have certificates.

A message indicates successful or not successful if the CSRs are collected from the switch.



```
                 PKI CERTIFICATE INSTALLATION UTILITY

Retrieving CSR's from 1 fabric(s)

 1. Got a CSR for Switch: Name="fcsprimaryswitch", WWN="100000606911fc53"
 2. Got a CSR for Switch: Name="backupswitch", WWN="100000606911fc55"

Write CSRs to file:D:\security 2.6\mycsr.xml

Success getting CSRs  & writing them to a CSR file


Press enter to continue.
```

Figure 3-6 CSR Retrieval from PKI Certificate Installation Utility

3. Go to the Brocade web site to submit the CSR file. To download the firmware from Brocade's web site, perform the following steps:

a. Go to the Brocade web site at:

`www.brocade.com`.

b. At the Brocade web site, click on **partners**.

The Brocade Partner Network screen appears.

c. Click the **Brocade Partner Network** link in the first paragraph.

The login screen appears.

Note: If you do not have a login and password, email the following information to `partnerweb@brocade.com`:

- First name
- Last name
- Company name
- Name of Brocade partner program in which your company participates
- Email address

d. Enter your login and password.

The title page appears.

e. Under Services and Support, click on the **firmware** link.

f. Click on the **v2.6.x Firmware** link.

The version 2.6.x Firmware screen appears.

g. Click on the **Version 2.6.0** link.

The version 2.6.0 screen appears.

h. Click on **Request Certificate for all your switches** (step 3).

Note: If the host, from which the PKICert is executed, is not connected to the internet, transfer the CSR (fab1.xml) file to a host from which the Brocade web site can be accessed. Use a floppy disk or other method such as FTP to perform the transfer.

Requesting a Certificate

To request a certificate, perform the following steps:

1. Go to the Brocade web site at:

   `www.brocade.com`.

2. At the Brocade web site, click on **partners**.

   The Brocade Partner Network screen appears.

3. Click the **Brocade Partner Network** link in the first paragraph.

   The login screen appears.

   Note: If you do not have a login and password, email the following information to `partnerweb@brocade.com`:

   - First name
   - Last name
   - Company name
   - Name of Brocade partner program in which your company participates
   - Email address

4. Enter your login and password.

   The title page appears.

5. Under Services and Support, click on the **firmware** link.
6. Click on the **v2.6.x Firmware** link.

   The version 2.6.x Firmware screen appears.

7. Click on the **Version 2.6.0** link.

   The version 2.6.0 screen appears.

8. Click on **Request certificate for all your switches** (step 3).

   The Secure Fabric OS - Request Certificate screen appears.

9. Enter the following required fields:
   - Email address
   - Technical contact
   - Phone
   - Country
   - File name
10. Browse and upload the CSR file (fab1.xml) to the Brocade web site by pressing the **Browse** button (to locate the file) and then pressing the **Upload** button.

    Note: It is necessary to upload the file before pressing the **Submit** button.

11. Click **Submit** when the form is complete.

    A verification screen appears. If the information is incorrect, press **Previous** and change the information; click **Submit** if the information displayed is correct. After **Submit** is selected, the message “Request Accepted” appears along with the switch names, WWNs, and a confirmation number. The confirmation number will be the name of the certificate file, with an .xml extension, that Brocade returns, by email.

    If the information is incorrect, a screen appears that indicates “Error Notification.”

12. Save the digital certificate file that you receive from Brocade on your hard drive.

    Example:

    ```
    c:\security\nt_pki\<confirmation number>.xml
    ```

    The digital certificate file contains the certificates for each of the switches in the fabric.

13. Make a backup copy of the digital certificate file on a floppy and store in a secure place.

Loading Certificates onto the Switches

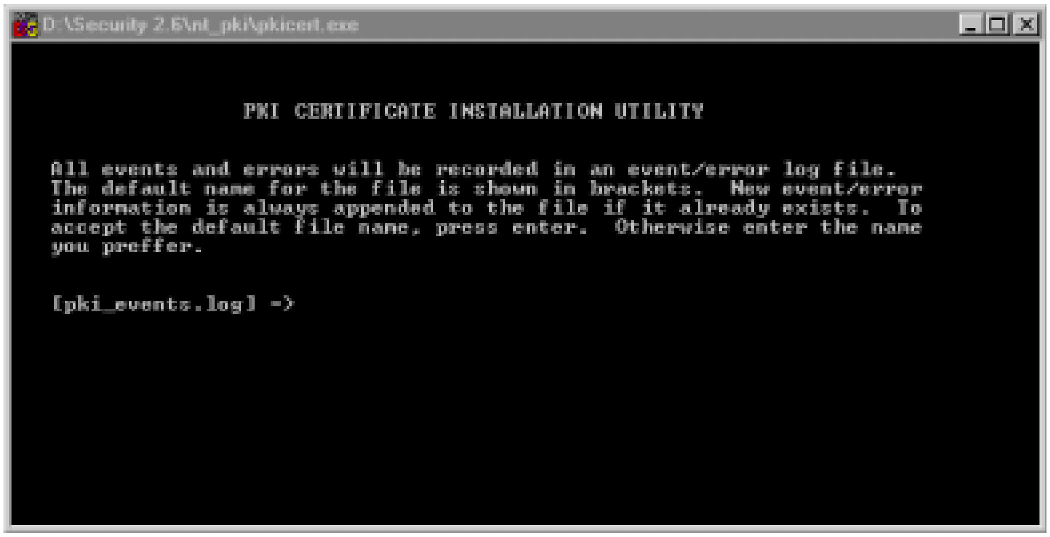
To load the certificate onto the switches, perform the following steps:

1. Start the `pkicert.exe` by double-clicking on it.

   The PKI Certificate Installation Utility screen appears.

2. On the screen, provide a path for an error log.

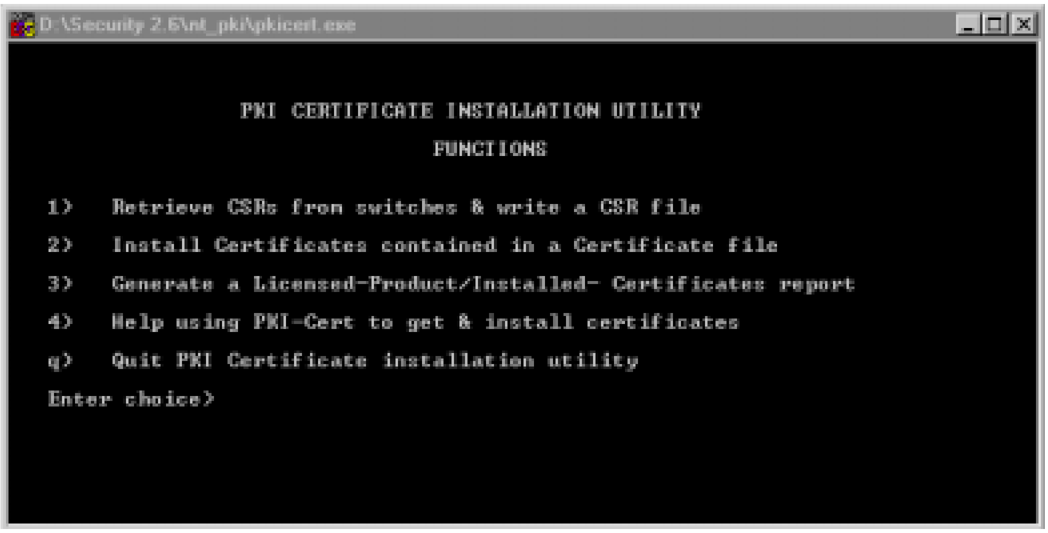
   If you do not provide a path, a default path is given.



```
                 PKI CERTIFICATE INSTALLATION UTILITY

   All events and errors will be recorded in an event/error log file.
   The default name for the file is shown in brackets.  New event/error
   information is always appended to the file if it already exists.  To
   accept the default file name, press enter.  Otherwise enter the name
   you preffer.

   [pki_events.log] ->
```

Figure 3-7 PKI Event/Error Log

3. Press the **Enter** key.
4. Select option 2 (Install Certificates contained in a Certificate file) to install the certificates.



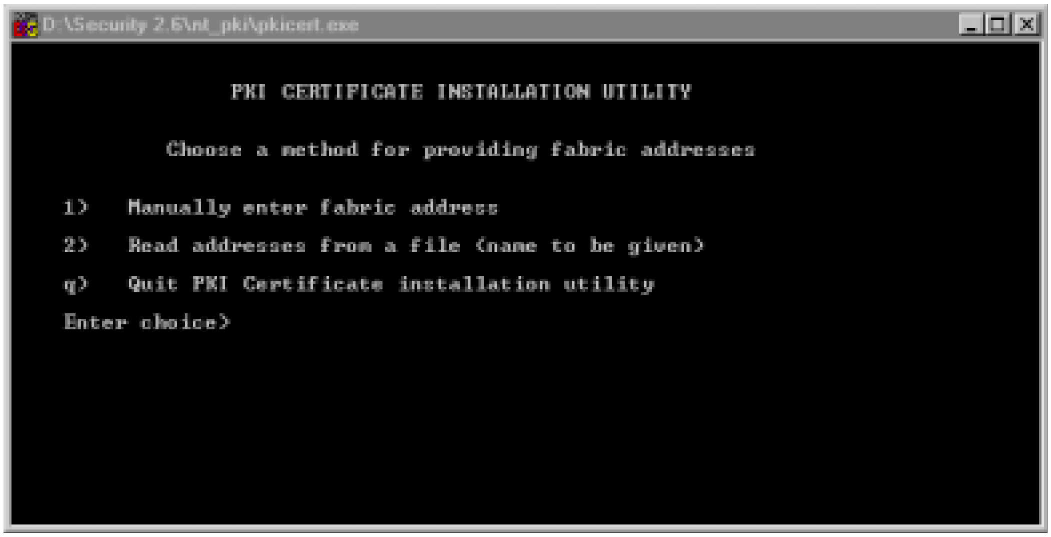
```
                 PKI CERTIFICATE INSTALLATION UTILITY
                              FUNCTIONS

   1)   Retrieve CSRs from switches & write a CSR file
   2)   Install Certificates contained in a Certificate file
   3)   Generate a Licensed-Product/Installed- Certificates report
   4)   Help using PKI-Cert to get & install certificates
   q)   Quit PKI Certificate installation utility
   Enter choice>
```

Figure 3-8 PKI Certificate Installation Utility—Functions

5. Press the **Enter** key.

   A screen titled Choose a method for providing fabric addresses appears.

6. Select option 1 (Manually enter fabric address) to connect to the switch.

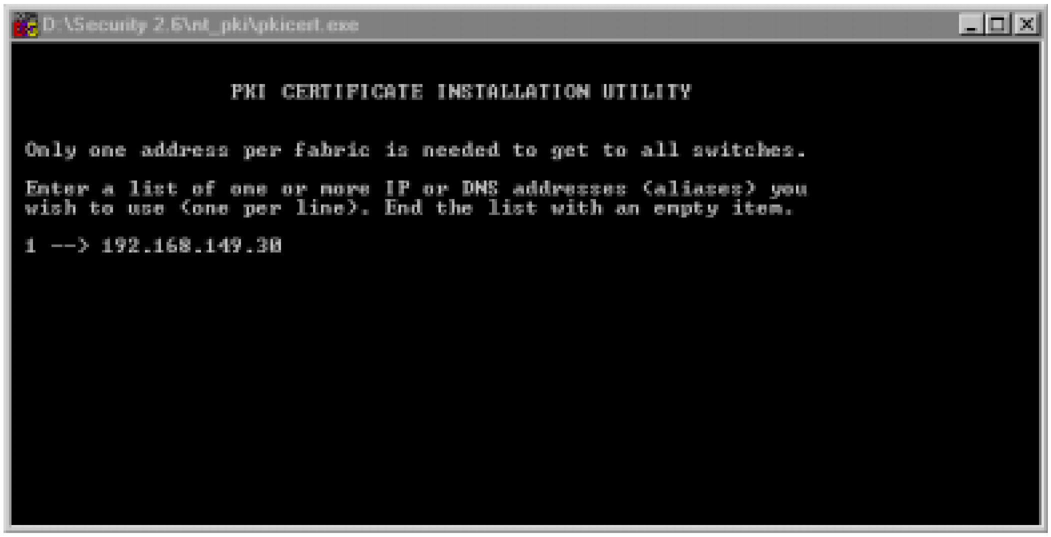


```
                PKI CERTIFICATE INSTALLATION UTILITY

            Choose a method for providing fabric addresses

    1)   Manually enter fabric address

    2)   Read addresses from a file (name to be given)

    q)   Quit PKI Certificate installation utility

    Enter choice>
```

   Another PKI Certificate Installation Utility screen appears.

Figure 3-9 PKI Certificate Installation Utility—Option 1

7. Enter the IP address or name of one switch in each fabric.

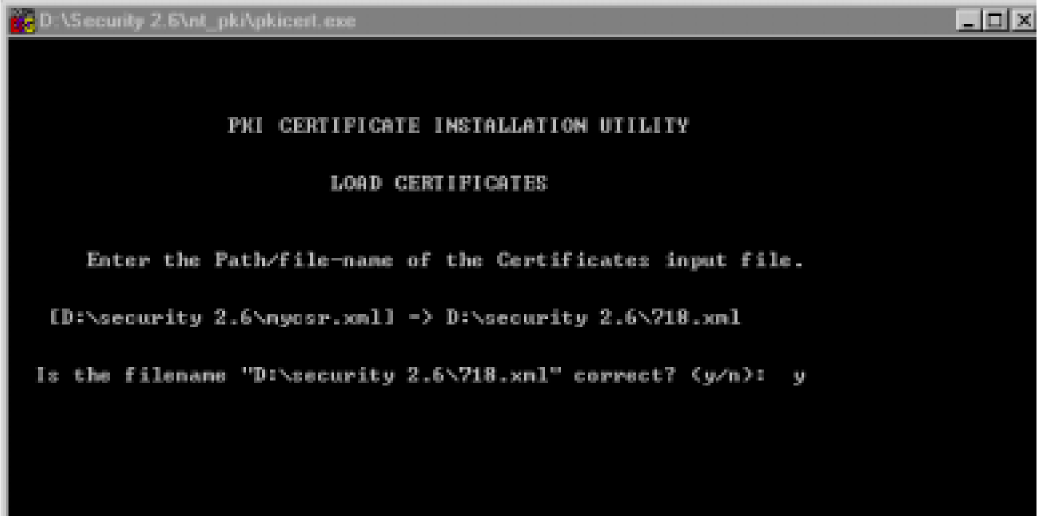


```
                PKI CERTIFICATE INSTALLATION UTILITY

Only one address per fabric is needed to get to all switches.

Enter a list of one or more IP or DNS addresses (aliases) you
wish to use (one per line). End the list with an empty item.

1 --> 192.168.149.30
```

Figure 3-10 IP Entry for PKI Certificate Installation Utility

8. Press the **Enter** key twice when you have completed entering the IP address or name.

   Note: If the switch default password is not changed, the Load Certificates screen appears. Otherwise, you are prompted for a user name and password for the switch. The Load Certificate screen appears.

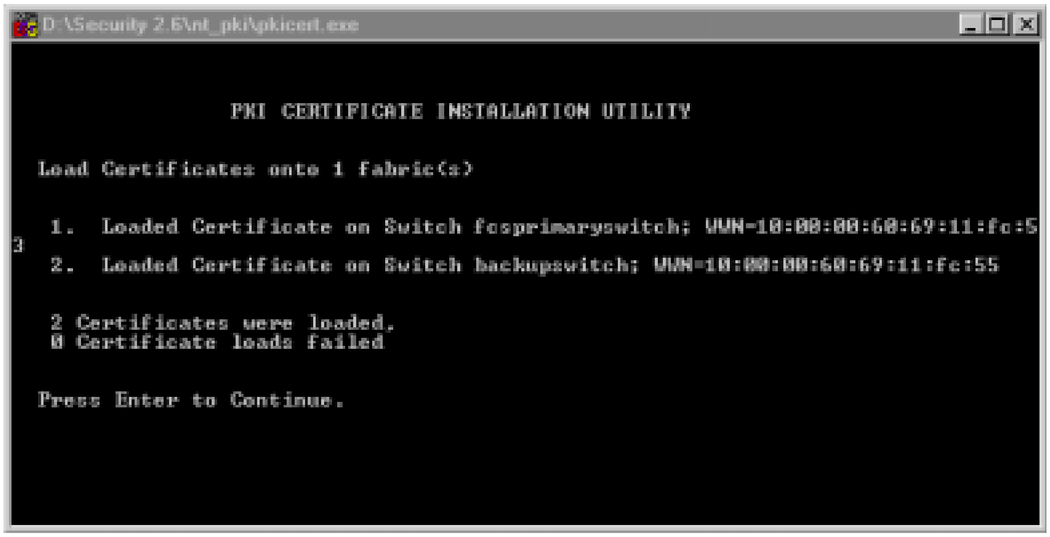


```
                PKI CERTIFICATE INSTALLATION UTILITY

                        LOAD CERTIFICATES


     Enter the Path/file-name of the Certificates input file.

  [D:\security 2.6\nycsr.xml] -> D:\security 2.6\718.xml

 Is the filename "D:\security 2.6\718.xml" correct? (y/n):   y
```

Figure 3-11 Certificate Loading onto Fabric

9. Provide a path and file name for the certificate file received from Brocade by email.
10. Press the **Enter** key.

    A confirmation screen appears asking if the file name is correct. Enter `y` (yes) if the file name is correct or `n` (no) if the file name is incorrect.



```
                PKI CERTIFICATE INSTALLATION UTILITY

 Load Certificates onto 1 fabric(s)


  1.  Loaded Certificate on Switch fosprimaryswitch; WWN-10:00:00:60:69:11:fc:5
3
  2.  Loaded Certificate on Switch backupswitch; WWN=10:00:00:60:69:11:fc:55


  2 Certificates were loaded.
  0 Certificate loads failed


 Press Enter to Continue.
```

Figure 3-12 PKI Certificate Installation Utility—Load Certificates

11. The loading certificates message appears.

    The new certificates are loaded onto the switches.
12. Exit `pkicert.exe` by entering the `q` (quit) command.
13. Press the **Enter** key.

    Note: You may have already completed steps for installing the zoning and security licenses. If not refer to the *Verifying a Security License* section on page 2-2, beginning at step 3.

First Login

Perform the steps described in the *Completing Your First Login* section on page 3-2.

Downloading sectelnet

Perform the steps described in the *Downloading sectelnet* section on page 3-3.

Chapter

4

Using Secure Fabric OS

This chapter provides the following information:

Overview

The Secure Fabric OS introduces the Fabric Management Policy Set (FMPS). This policy set is focused on specifying and controlling the access to fabric management capabilities and on controlling the physical components within the fabric as well as their connections within the fabric. Although it appears very similar to zoning, the FMPS is an independent facility with independent management methods. This includes new commands to maintain the FMPS database and to activate the policy set.

The FMPS is a set of security policies, each addressing a different piece of the overall FMPS. Each policy has a name, a type (implied by the name), and a member list. The nature of the member list varies with the type of policy and is described in this chapter.

These security policies must be enforced fabric-wide to be effective. If even one of the switches in the fabric does not enforce a specific security policy, the policy is compromised. Therefore, enabling of security can only be done if all of the switches in the fabric are capable of enforcing it (such as all switches must be at an appropriate minimum firmware level and have the appropriate license keys installed). Since zoning is an important part of the overall fabric security mechanisms, all switches in the fabric must have a zoning license installed before security can be enabled.

Fabric Security Components

The components of the Secure Fabric OS are described in Table 4-1:

Table 4-1 Secure Fabric OS Components

Component	What Component Does
Fabric Configuration Servers (FCS)	One or more switches capable of acting as trusted switches in charge of zoning changes and other security-related functions.
Management Access Controls (MAC)	Allow management services to be restricted to a specific set of endpoints: • IP addresses (for SNMP, telnet, HTTP or API access) • Device ports (for in-band methods such as SES or Management Server) • Switch WWNs (for serial port or front panel access)
Device Connection Controls (DCC)	Port-level Access Control Lists (ACLs) bind particular device ports to a set of one or more switch ports.
Switch Connection Controls (SCC)	SCCs authorize which switches are allowed to join the fabric.
Secure Management Channels	Encrypt certain sensitive data elements, such as passwords, in order to secure the management communications interface to the fabric.

Together, these items provide a new level of SAN security.

Fabric Configuration Servers

Fabric configuration servers (FCSs) provide for one or more switches to be configured as trusted switches in charge of controlling fabric management functions or parameters. These “trusted” switches are identified by their WWNs. These switches should be stored in a locked room.

The Brocade Secure Fabric OS permits definition of a fabric configuration server policy that defines a list of switches, by WWN, and are designated as FCS switches. The list designates a primary FCS switch (the first WWN in the list) followed by one or more backup FCS switches. If the designated primary switch is not a member of the fabric, the first backup FCS switch in the list will become the primary FCS switch, and so forth. Once secure mode is enabled, only the primary switch in a fabric can propagate any fabric-wide management changes. This type of management is termed policy-based asymmetric fabric management.

Activities that are exclusive to the primary FCS switch include:

- Zoning changes
- Changes to security policies
- Password changes
- SNMP community string changes
- Date changes

Password and SNMP Community String Management

When the secure fabric feature is either initially enabled or when the secure fabric feature is already enabled and a change is made, a change in password or SNMP community string on the primary FCS is reflected on all the other switches in the fabric or the affected switches in the fabric, as appropriate.

When a new switch joins the secure fabric, the new switch inherits the existing fabric's configuration.

For information about the Fabric Configuration Server Policy refer to the *Fabric Configuration Server (FCS) Policy* section on page 4-7.

The Primary FCS Server

The primary FCS server is responsible for distributing zoning, the Fabric Management policy set (FMPS,) the fabric password database, and SNMP community strings to switches that are "new" to the fabric. The primary FCS switch maintains a list of switches (by WWN) that are known to have up-to-date policy sets. When new switches join the fabric and become "reachable," the primary FCS switch pushes the zoning, FMPS policy sets, passwords, and SNMP community strings out to that switch. In no case will any policy set (zoning or FMPS) be accepted from any switch other than the primary FCS switch as described here.

FCS Redundancy

The use of a primary FCS insures that all switches in the fabric have a consistent view of zoning and FMPS.

If a primary server fails, the next switch on the FCS list assumes the role of primary. The new primary would then distribute the policy set to the entire fabric. Therefore, it is critical to have more than one FCS switch. This redundancy is used to insure that there is always a primary FCS for management operations and consistency of zoning and security databases.

Management Access Controls

Access control lists (ACLs) control access to the switch from different management sources. The major value of Management Access Controls (MACs) is that management access has many privileges and its misuse is a major threat to security. MACs allow access to management services to be restricted to the following endpoints:

- IP addresses (for SNMP, telnet access, HTTP or API)
- Device ports (for in-band methods such as SCSI Enclosure Services (SES) or Management Server)
- Switch WWNs (for serial port and front panel access).

Note: Device ports are specified by WWN and typically represent distribution devices such as HBAs.

For information about the Management Access Control Policies refer to the *Management Access Controls* section on page 4-7.

Caution!

Brocade strongly recommends that you do not allow Proxy servers access to your secure fabric.

When a Proxy server is included in a security MAC policy for IP based management, such as HTTP_POLICY, all IP packets that leave the Proxy server will appear to originate from the Proxy server. This could allow unwanted hosts with access to that Proxy server to access the secure fabric.

Device Connection Controls (DCC)

DCCs are used to manage which edge devices (specified by WWNs) can be connected to specific switch ports. (Typically, the devices are initiators and targets, but may be intermediate devices such as SCSI routers and Loop Hubs.) DCCs allow an individual device port to be bound to one or more switch ports.

DCC policies allow for the specification of the rules for binding of device ports (typically HBA ports) to specific switch ports. If DCC policies are in effect (such as one or more DCC policies have been activated), then whenever a device performs a FLOGI (fabric login) request, the WWN specified in the FLOGI is validated to insure that the device is connected to an authorized port. This process minimizes the risk of WWN “spoofing” (as an attack against access control mechanisms, including zoning). If the validation fails, the FLOGI is rejected and the device is denied access to the fabric. If a port WWN is specified in a DCC policy, that WWN will only be allowed access to the fabric if it is connected to one of the designated switch ports. Similarly, a switch port that has been designated in a DCC policy will allow connections from one of the specified WWNs. WWNs that are not specified in a DCC policy will be allowed to connect to the fabric at any switch port that has not been specified in a DCC policy. Switch ports and/or WWNs may exist in multiple DCC policies.

Note: You can create multiple DCC policies, each with a unique name.

For information about the Device Connection Control Policy refer to the *Device Connection Control (DCC) Policies* section on page 4-11.

Switch Connection Controls

The main business benefit of Switch Connection Controls is the enhanced physical and logical security, particularly for service providers and enterprise customers engaged in SAN island merging.

Each E-port (also known as ISL) connection between switches invokes a mutual authentication process either when:

- Secure mode is enabled.
- The fabric is initialized with secure mode already enabled.
- An E-port to E-port connection is made.

The authentication process uses the Switch Link Authentication Protocol (SLAP) to authenticate each switch that attempts to join the fabric.

When a new switch is connected to a switch that is part of the secure fabric, the two switches must be mutually authenticated, and the new switch must be on the list of authorized switches before it is allowed to join the fabric.

Switch Connection Controls occur at the following levels:

- No switch without a Brocade-issued digital certificate, based on the switch's factory-set identity, is permitted to join a secure fabric.
- A Switch Connection Control Policy list contains only the switches, by WWNs, that are permitted to join the fabric.

For information about the Switch Connection Control Policy refer to the *Switch Connection Control (SCC) Policy* section on page 4-12.

Secure Management Channels

Secure Management Channels are as stated in Table 4-1 on page 4-2 for sectelnet, Web Tools, and API. Refer to the *Web Tools User's Guide v2.6* for more information.

Fabric Management Policy Set (FMPS)

Secure Fabric Management Policies use the concept of a defined policy set (which is equivalent to the defined config in Brocade Zoning), as well as an active policy set, (which is equivalent to an effective config in Brocade Zoning). Like Brocade Zoning, both policy sets are saved in flash memory on all switches in the fabric once they are distributed.

The Fabric Management Policy Set (FMPS) consists of the following policies:

- Fabric Configuration Server (FCS) Policy
- Management Access Control (MAC) Policies
- Options Policy
- Device Connection Control (DCC) Policies
- Switch Connection Control (SCC) Policy

Secure mode is enabled on a fabric-wide basis. When secure mode is enabled, a list of one or more switches (that will become FCS switches) is specified, and the primary FCS switch is the first one on the list that is part of the fabric.

Enabling secure mode:

- Creates a default FMPS using the FCS policy containing the WWNs that are specified in the list.
- Distributes the FMPS to all switches in the fabric.
- Activates the FMPS.
- Reboots all switches

Fabric Configuration Server (FCS) Policy

The FCS Policy is FCS_POLICY. This policy contains a list of WWNs of the switches that are designated to be FCSs. The primary FCS switch will be the first one on the list that is in the fabric. The primary switch controls fabric management functions. The FCS policy is applied fabric-wide.

If secure mode is enabled, the FCS policy must exist and cannot be empty. You can have a policy with one or more entries meaning that there is one primary FCS switch with a varied number of backup FCS switches. It is advisable to have at least one backup FCS.

Management Access Control (MAC) Policies

MAC policies are applied fabric-wide. If a MAC policy does not exist, then no access controls are in effect for that access method. If a MAC policy exists but is empty, then that access method is disabled on all switches in the fabric.

The default for all MAC policies is “does not exist.” When secure mode is enabled, the default is in effect for all MAC policies until they are specifically changed. The management access policies are:

- SNMP MAC Policies
- Telnet MAC Policy
- HTTP MAC Policy
- API MAC Policy
- SES MAC Policy
- Management Server MAC Policy
- Serial Port MAC Policy
- Front Panel MAC Policy

SNMP MAC Policies

The SNMP MAC Policies are:

- RSNMP_POLICY (read access)
- WSNMP_POLICY (write access)

These policies contain lists of the hosts’ IP addresses from which connections or messages are accepted by any switch in the fabric.

The SNMP MAC Policies can be used to limit access to specific, trusted workstations in the customers' environment, and is done so with differing read/write access levels. The SNMP host must send its request to the Primary FCS switch to perform write operations.

The SNMP MAC policy states are shown in Table 4-2.

Table 4-2 SNMP MAC Policy States

Policy State	Description
No policy (does not exist)	Any host can access the fabric.
Policy with no entries (empty policy)	No host can access the fabric.
Policy with entries	Only the specified host(s) can access the switches in the fabric.

Telnet MAC Policy

The telnet MAC Policy is TELNET _POLICY. The TELNET_POLICY contains a list of IP addresses that are allowed to establish telnet connections to any of the switches in the fabric.

This policy limits access so that using telnet can only be granted (restricted) to specific, trusted workstations in the customers' environment.

The telnet MAC policy states are shown in Table 4-3.

Table 4-3 Telnet MAC Policy States

Policy State	Description
No policy	Any host can telnet to a switch in the fabric.
Policy with no entries	No host can telnet to the switches in the fabric.
Policy with entries	Only specified hosts can telnet to the switches in the fabric.

HTTP MAC Policy

The HTTP MAC Policy is HTTP_POLICY. This policy contains a list of IP addresses for devices that are allowed to establish HTTP connections to any of the switches in the fabric.

The HTTP_POLICY is used to limit access to specific, trusted workstations in the customers' environment.

The HTTP MAC policy states are shown in Table 4-4.

Table 4-4 HTTP MAC Policy States

Policy State	Characteristics
No policy	All hosts can establish an HTTP connection to any switch in the fabric.
Policy with no entries	No host can establish an HTTP connection to any switch in the fabric.
Policy with entries	Only specified hosts can establish an HTTP connection to any switch in the fabric.

API MAC Policy

The API MAC Policy is API_POLICY. This policy contains a list of IP addresses allowed to establish an API connection to switches in the fabric.

API connections can be made to any switch in the fabric, but only those connections to the primary FCS switch can be used for write operations.

The API MAC policy states are shown in Table 4-5.

Table 4-5 API MAC Policy States

Policy State	Characteristics
No policy	All hosts can establish an API connection to any switch in the fabric.
Policy with no entries	No host can establish an API connection to any switch in the fabric.
Policy with entries	Only specified hosts can establish an API connection to any switch in the fabric.

SES MAC Policy

The SES MAC Policy is SES_POLICY. This policy contains a list of device port WWNs that are allowed to access SES, and for which SES commands are accepted and acted upon.

The SES policy permits only specific, trusted fabric-connected devices to use SES commands.

In a fabric where security is turned on, the SES client must be directly attached to the primary FCS. Then, the SES client can be used to manage all of the switches in the fabric through the Brocade SES (refer to the *Brocade SES User's Guide* for more information).

The current Brocade SES implementation does not support the `Read Buffer/Write Buffer` commands issued for remote switches. If users want to direct these commands to a switch that is not the primary FCS switch, then that switch must be made the primary FCS switch and the SES client must be directly attached to it.

The SES MAC policy states are shown in Table 4-6.

Table 4-6 SES MAC Policy States

Policy State	Characteristics
No policy	All device ports can access SES.
Policy with no entries	No device port can access SES.
Policy with entries	The specified devices can access SES.

Management Server MAC Policy

The Management Server Policy is MS_POLICY. This policy contains a list of device port WWNs for which the FC-GS-3 management server implementation in Fabric OS accepts and acts on requests.

The MS_POLICY permits only specific, trusted fabric-connected devices to access the management server. Operations that perform fabric configuration and/or control functions will be allowed only to requestors that are directly connected to the primary FCS server switch.

The Management Server MAC policy states are shown in Table 4-7:

Table 4-7 Management Server MAC Policy States

Policy State	Characteristics
No policy	All devices can access the management server.
Policy with no entries	No devices can access the management server.
Policy with entries	Specified devices can access the management server.

Serial Port MAC Policy

The Serial Port MAC Policy is SERIAL_POLICY. This policy contains a list of switch WWNs for which serial port access is enabled. Once a serial port MAC policy is defined, any switch not identified in the policy is disabled for serial port access.

The serial port MAC policy states are shown in Table 4-8:

Table 4-8 Serial Port MAC Policy States

Policy State	**Characteristics**
No policy	All serial ports of the switches in the fabric are enabled.
Policy with no entries	All serial ports of the switches in the fabric are disabled.
Policy with entries	Only specified switches can be accessed through the serial ports.

Front Panel MAC Policy

The Front Panel Policy is FRONTPANEL_POLICY. This policy is specific to the SilkWorm® 2800 and contains a list of switch WWNs for which front panel access is enabled. Once a front panel MAC policy is defined, any switch not identified in the policy is disabled for front panel access.

This policy enhances physical security for Brocade switches equipped with front panels.

The front panel MAC policy states are shown in Table 4-9:

Table 4-9 Front Panel MAC Policy States

Policy State	**Characteristics**
No policy	All the switches in the fabric have front panel access enabled.
Policy with no entries	All the switches in the fabric have front panel access disabled.
Policy with entries	Only specified switches in the fabric have front panel access enabled.

Options Policy

The options policy is OPTIONS_POLICY. The options policy controls whether to allow the use of Node WWNs for WWN-based zoning.

When secure mode is enabled, the OPTIONS_POLICY defaults to “does not exist,” which means that Node WWW Zoning is allowed. The default “does not exist” means the same as an empty policy. Only when the option is specified within the policy does anything change.

Device Connection Control (DCC) Policies

There can be multiple Device Connection Control Policies: DCC_POLICY_nnn where nnn represents a policy name. These policies contain lists of WWNs of one or more device ports that are allowed to access designated switch port(s). DCC policies allow for the specification of the rules for binding of device ports (typically HBA ports) to specific switch ports.

When secure mode is enabled, the Device Connection Control policies default to “does not exist,” allowing any devices to connect to any switch port.

The states associated with DCC policies are shown in Table 4-10:

Table 4-10 DCC Policies States

Policy State	Characteristics
No policy	Any device can connect to any switch port on the fabric.
Policy with no entries	Any device can connect to any switch port on the fabric. An empty policy is the same as no policy.
Policy with entries	If a device WWN is specified in a DCC policy, that device will only be allowed access to the fabric if it is connected to one of the specified switch ports. Likewise, a switch port that has been specified in a DCC policy will only allow connections from a device having one of the specified WWNs. WWNs that are not specified in a DCC policy will be allowed to connect to the fabric at any switch port that has not been specified in a DCC policy. Switch ports and/or WWNs may exist in multiple DCC policies.

Note: The use of DCC policies minimizes the risk of WWN spoofing as an attack against access control mechanisms, including zoning.

Switch Connection Control (SCC) Policy

The Switch Connection Control Policy is SCC_POLICY. The SCC Policy is to prevent unauthorized switches from joining the fabric. This policy contains a list of WWNs of switches that are allowed to be members of the secure fabric.

When secure mode is enabled, the SCC_POLICY defaults to “does not exist,” allowing any authenticated switch to join the fabric. Switches are authenticated using the switches’ certificates and unique private keys provided to the Switch Link Authentication Protocol (SLAP).

Switch Connection Controls are used to restrict connection into a fabric by specifying a set of authorized switches.

The SCC policy states are shown in Table 4-11:

Table 4-11 SCC Policy States

Policy State	**Characteristics**
No policy	All switches can be in the fabric.
Policy with no entries	The SCC Policy cannot be empty. The Policy must contain all the FCS switches and non-FCS switches that are part of the fabric.
Policy with entries	The SCC Policy must contain all the FCS switches but it can also contain additional switches

Note: When creating an SCC_POLICY, do not exclude switches already present in the fabric because doing so will segment the excluded switches. See Table 4-15 on page 4-37 (number 4) for further information.

Enabling Security in the Fabric

The following items need to be completed before you enable security in a fabric:

- Identify the FCS switches and the primary FCS. Refer to the *Fabric Configuration Servers* section on page 4-2 and FCS_POLICY on page 4-7.
- Identify the telnet commands to be used. The `secModeEnable` command is used to enable security. This command and the other Fabric OS commands used to manage security are described on page 4-15.

After enabling security, the following items need to be completed to enhance the security policy settings:

- Identify all the switches in the secure fabric. Refer to SCC_POLICY on page 4-12.
- Identify the minimum group of policies that must be used. Refer to the policy descriptions starting on page 4-5.

To enable security perform the following:

1. Build the fabric.

   The administrator builds the fabric with switches that are identified to be in the secure fabric.

   Note: These switches may later be included in the SCC_POLICY if the policy is implemented.

   The administrator also determines which switches are FCS including the primary FCS switch. These switches will be included in the FCS_POLICY. The FCS switch with the highest priority position (the first one in the list) in the FCS policy list becomes the primary FCS switch.

2. Connect to the switch that will become the primary FCS switch usint `sectelnet`. (Refer to the *Downloading sectelnet* section on page 3-3.)

3. Run the `secModeEnable` command. (Refer to the *Enabling Security Mode on a Fabric* section on *page 4-23).* As part of issuing this command, you will specify the FCS switches.

4. The primary FCS switch distributes the default policy sets (refer to the *Management Access Control (MAC) Policies* section on page 4-7) to all switches in the fabric, activates the local zoning configurations and applies the policy set. In order to activate security, all switches in the fabric are automatically rebooted.

   To run the `secModeEnable` command, you must use `sectelnet` or the console. The sectelnet client encrypts sensitive data such as your password.

Brocade Secure Fabric OS Telnet Commands

Table 4-12 on page 4-15 shows the switch security telnet commands used to manage the Brocade Security feature. The commands in the table follow the order in which the commands are presented in this chapter.

Table 4-12 Security Commands

Command	**Description**
secModeEnable	Enable security mode.
secModeShow	Show current mode of security.
secPolicyCreate	Create a policy.
secPolicyDelete	Delete a policy.
secPolicyAdd	Add members to a policy.
secPolicyRemove	Remove members from a policy.
secPolicyShow	Show members of one or more policies.
secPolicyFCSMove	Move an FCS member in the FCS list.
secFCSFailover	Change the primary FCS switch.
secPolicySave	Save all policy sets and distribute to switches.
secPolicyActivate	Activate all policy sets.
secPolicyAbort	Abort policy changes.
secTransAbort	Abort the current security transaction.
secModeDisable	Disable security mode.
secPolicyDump	Display all policy information.
secVersionReset	Reset version stamp.
secStatsShow	Display security statistic.
secStatsReset	Reset security statistic.
secNonFCSPasswd	Set non-FCS password.
secTempPasswdSet	Set a temporary password for a switch.
secTempPasswdReset	Reset temporary password to default value.
secHelp	Display a list of Security commands.

For more detailed information on telnet commands, refer to *Fabric OS Reference*.

Describing Secure Telnet Commands

The secure telnet commands operate using a transaction model, with changes becoming permanent only when saved or activated.

The Brocade Security features are administered using Command Line Interface (CLI) (both serial and secure telnet) commands.

The `secModeEnable` telnet command is used to enable security on a fabric-wide basis. This command will fail if any switch in the fabric is not capable of enforcing security policies (including the ability to run Brocade Zoning). This command requires the specification of a list of one or more switches (by WWN) that will become the Fabric Configuration Server (FCS) switches. The `secModeEnable` command will create a default FMPS policy set with the FCS policy containing the FCS switch WWNs, will distribute the policy set to all of the switches in the fabric, and will activate the policy set. Refer to the *Enabling Security Mode on a Fabric* section on page 4-23 for information on the `secModeEnable` command.

The secure telnet commands are used to:

- View and reset version stamp information
- View and display statistics information
- Set and change password information
- View and modify FMPS
- Enable and disable security

Note: If a backup or non-FCS switch has its telnet output on hold when the primary switch does a fabric-wide operation, the switch with its output on hold is not updated from the primary FCS switch. Therefore, do not put telnet output on hold (`Ctrl-S`).

Version Stamp

When any kind of change is made to the aggregate policy set (zoning, FMPS, passwords, or SNMP), a random version number is generated; then the version number, along with the current time stamp, is attached to the aggregate policy set database.

From a policy perspective, the version stamp is used to distinguish different secure fabrics. The time stamp is used by the administrator to determine when the last change was made to the configuration of the fabric.

This versioning information is included when the policy sets are distributed by the primary FCS server to the other switches in the fabric.

Resetting the version stamp to zero allows security fabrics to merge and is covered below.

The `secVersionReset` command enables the version stamp on the fabric switches to be reset to zero.

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

    ```
    secVersionReset
    ```

    Note: The `secVersionReset` command may be issued on any switch if there is no active FCS in the fabric. This enables joining and recovery operations. For more information, refer to *Joining Secure Fabrics* on page 4-35 and *Recovery Operations* on page 4-36.

Statistics

Security Policy statistics can be displayed and reset.

Displaying Security Violation Statistics for a Security Policy

To display security violation statistics for a specific policy:

1. Log into any switch as the admin user using `sectelnet`.
2. At the command line enter the following command:

   ```
   secStatsShow "policy_name"
   ```

   Where policy_name is the security policy type for which you wish to display the violation statistics. If no security policy type is specified, all statistics for all security policy types are displayed. Valid values for policy_name include:

   - TELNET_POLICY
   - HTTP_POLICY
   - API_POLICY
   - RSNMP_POLICY
   - WSNMP_POLICY
   - SES_POLICY
   - MS_POLICY
   - SERIAL_POLICY
   - FRONTPANEL_POLICY
   - SCC_POLICY
   - DCC_POLICY
3. The security policy type and number of security violations associated with that policy are displayed.

Resetting Statistics for a Security Policy

To reset the violation counter to zero for a specific security policy:

1. Log into any switch as the admin user using `sectelnet`.
2. At the command line enter the following command:

   ```
   secStatsReset "policy_name"
   ```

   Where policy_name is the security policy type you wish to reset. If a security policy type is not specified, all statistics for all security policy types are reset to zero (0). Valid values for policy_name include:

   - TELNET_POLICY
   - HTTP_POLICY
   - API_POLICY
   - RSNMP_POLICY
   - WSNMP_POLICY
   - SES_POLICY
   - MS_POLICY
   - SERIAL_POLICY
   - FRONTPANEL_POLICY
   - SCC_POLICY
   - DCC_POLICY

Passwords

In secure mode, you can manage passwords by:

- *Setting the Admin Password for All non-FCS Switches* on page 4-18
- *Creating a Temporary Password on a Specific Switch* on page 4-18
- *Removing Temporary Passwords from a Fabric* on page 4-19
- *Entering Password Command* on page 4-19
- *Recovering from a Forgotten Password on Switch* on page 4-20

Note: Remember your passwords. Forgotten passwords will require significant effort from which to recover.

Setting the Admin Password for All non-FCS Switches

To set the admin password on all non-FCS switches:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secNonFCSPasswd
   ```

3. You are prompted to enter the non-FCS admin password. Enter a password between 8 and 40 alphanumeric characters in length. This password will become the administrator password for all non-FCS switches in a fabric.
4. You are prompted to re-enter the non-FCS admin password. Make sure to enter the password exactly as it was entered the first time.
5. The password is distributed to all switches in the fabric and saved in the security databases. All non-FCS switches now use the defined admin password. Any previously existing telnet connections to these non-FCS switches via the admin account will be terminated.

Creating a Temporary Password on a Specific Switch

To create a temporary admin password on a specific non-FCS switch:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secTempPasswdSet domain, login_ID
   ```

   where `domain` is the domain ID of the switch for which you want to change the password and `login_ID` is the login ID for which you want to set the temporary password.

3. For security reasons, if you are setting a `secTempPasswdSet` for a root or factory account, you will be prompted for the root password of the primary FCS switch.
4. You are prompted to enter a password. Enter an alphanumeric password between 8 and 40 characters in length.

   This password is only for the switch specified by domain ID and only for the account name specified.

5. You are prompted to re-enter the password. Make sure to enter the password exactly as it was entered the first time.
6. To revert the temporary password change, use the `secTempPasswdReset` command.

   Note: Passwords set by `secTempPasswdSet` are lost after a reboot.

Removing Temporary Passwords from a Fabric

To remove the temporary password on a specific switch:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secTempPasswdReset domain, login_ID
   ```

   where `domain` is the domain ID of the switch for which you want to revert a temporary password and `login_ID` is the login ID that owns the temporary password.

   Use the `secTempPasswdReset` command with no parameters to reset all temporary passwords for the entire fabric.

Entering Password Command

This explanation only applies to the secure mode.

Note: You cannot change login names in secure mode.

Four levels of passwords within security are:

1. Root - the highest level of security
2. Factory
3. Admin
4. User - the lowest level of security

Note: At whatever level you are logged in, you are asked not only for the password for that account but also for the passwords that have lesser privileges. For example, if you are logged in as admin, you will be asked for the password for admin and user because user has lesser privileges than that of admin.

Example:

For username - admin

Old password:

New password:

Re-enter new password:

For username - user

Old password:

New password:

Re-enter new password:

When you are in secure mode, the `password` command can only be executed on the primary FCS switch. The password is saved and distributed to all switches.

To cancel the operation, enter:

`Ctrl—C`.

Recovering from a Forgotten Password on Switch

If you forget your password on a switch, perform the following:

1. Contact Brocade's Customer Support to acquire the Password Recovery firmware version. The contacts are:

   - Telephone: 1-888-283-4273
   - Web site: www.brocade.com
   - Email address: support@brocade.com

   You will need to provide the WWN of your primary FCS switch.

   To perform password recovery, you must set up boot parameters on your switch, using a serial connection, to perform a netboot. The Password Recovery firmware is used only to reset the passwords to their defaults, change the firmware to boot from the flash again, and freeze the switch until it's manually rebooted. No other switch functions can be performed by the password recovery firmware.

   If you do not have a serial connection, contact Brocade's Customer Support.

2. Open a serial connection with the switch.

   Use Windows HyperTerminal in Windows OS or the Kermit program in Unix.

3. Power cycle the switch.

   If your switch is on, turn it off and on. If your switch is off, turn it on.

4. From the serial prompt window, press any key when you see the message:

   ```
   Press any key to stop autoboot....
   ```

   This process gives you access to the boot prompt.

5. When you see the prompt:

   ```
   [VxWorks Boot]
   ```

   Enter `c` to start changing the boot parameters to boot from the network.

   At each question, the default answer will be displayed. To change it, enter the new value next to the default.

The following example shows a typical message that appears from the console.

Example:

Prompt	Default	Entry
[VxWorks Boot]:c		
boot device	:fei	
processor number	:0	
host name	:host	MyHostMachine
file name	:/usr/switch/firmware	/brocade/resetPasswd
inet on ethernet (e)	:123.456.789.123	
inet on backplane (b):		
host inet (h)	:	123.456.789.234
gateway inet (g)	:255.255.255.1	123.456.789.1
user (u)	:user	jsmith
ftp password (pw) (blank = use rsh)	:	

Fields that you must specify are shown in Table 4-13.

Table 4-13 Required Fields

Field	Meaning
host name	name of the machine on which the recovery firmware can be found
file name	full path where the Password Recovery firmware is located
inet on Ethernet	the switch’s IP address
host inet	host’s IP address
gateway inet	IP gateway’s IP address
user	the user with an account on the host machine

6. Enter @ at the [VxWorks Boot] prompt to start booting the Password Recovery version of the firmware from the network.

   The firmware will reset the passwords to defaults.

   The following example shows a typical message that appears from the console.

Example:

```
  boot device                    :fei
  processor number               :0
  host name                      :MyHostMachine
  file name                      :/brocade/resetPasswd
  inet on ethernet (e)           :123.456.789.123
  host inet (h)                  :123.456.789.234
  gateway inet (g)               :123.456.789.1
  user (u)                       :jsmith
  flags (f)                      :0x8
  target name (tn)               :switch
Attaching network interface fei0...done.
Attaching network interface lo0...done.
MyHostMachine is alive.
Loading...4173912 + 339516 + 423108
Starting at 0x10400000...
Attaching network interface fei0...Committing configuration...done.
done.
Attached TCP/IP interface to fei unit 0
Attaching network interface lo0...done.
telnetlnit: telnetd initialized.
NFS client support not included.
Adding 9313 symbols for standalone.
Model: 9
moving passwd info from config DB
Saving passwd...done.
setting passwd to defaults
Saving passwd...done.
```

Passwords have been reset.

7. You need to reset your boot parameters back to their default settings so that the switch will boot from flash. Repeat steps 3 and 4.

8. When you see the prompt:

   ```
   [VxWorks Boot]
   ```

   Enter `c` to start resetting the boot parameters back to their default settings.

9. Remove the fields that you added in step 5 by entering a dot (.) to clear the fields and pressing **Enter**.

   The boot parameters have returned to their original settings.

10. Power cycle the switch so that the original firmware is re-loaded from flash and normal operations resume.

Security Commands

The security commands are used for:

- *Enabling Security Mode on a Fabric* on page 4-23
- *Displaying the Current Security Mode* on page 4-25
- *Creating a Security Policy* on page 4-26
- *Deleting a Security Policy* on page 4-30
- *Adding Members to an Existing Security Policy* on page 4-30
- *Removing a Member from a Security Policy* on page 4-31
- *Modifying the Order of FCS Switches* on page 4-32
- *Changing the Primary FCS Switch* on page 4-32
- *Saving a Security Policy to Flash Memory* on page 4-33
- *Activating a Security Policy* on page 4-33
- *Aborting Uncommitted Changes to Security* on page 4-33
- *Aborting Current Security Transaction* on page 4-33
- *Disabling Security Mode on a Fabric* on page 4-34
- *Viewing the Security Policy Database* on page 4-34
- *Displaying the Members of a Security Policy* on page 4-35

Enabling Security Mode on a Fabric

The `secModeEnable` command is used to manage the FCS and turn on security as well as creating an FCS policy. This section covers enabling security.

To enable security on a switch:

1. Verify that all switches in the fabric are capable of supporting the Security feature and that the switches are running Fabric OS v2.6. Ensure that the zoning and security licenses are installed as well as the digital certificates.
2. Open a `sectelnet` connection (refer to the *Downloading sectelnet* section on page 3-3) to the switch you intend to be the primary FCS. The login prompt is displayed if the `sectelnet` connection successfully found the switch in the network.

   Note: Most security commands must be executed on the primary FCS switch.
3. At the login prompt enter your user ID:

   Example:

   ```
   login: admin
   ```
4. Enter your password:

   ```
   password: xxxxxx
   ```

   Note: You can only run the `secModeEnable` command when you are logged in using a `sectelnet` connection. When running the `secModeEnable` command, no other sectelnet/telnet sessions should be active in the fabric. Passwords are always encrypted when using `sectelnet` and connecting to a secure fabric. `Sectelnet` will not work unless a certificate exists on the switch. Non-secure telnet connections will no longer work once security is enabled.
5. At the command line enter:

   ```
   secModeEnable "fcsmember;...;fcsmember"
   ```

   Where fcsmember is the domain ID, WWN, or switch name of the primary FCS and backup FCS switches. The first switch defined in this list is the primary FCS switch.

   Note: You may also use the interactive mode by entering `secModeEnable` and pressing the **Enter** key.

   Note: After invoking the `secMode Enable` command, your session will be immediately terminated, which allows for reconnecting with encrypted passwords.
6. Enter the FCS switch root password.
7. Re-enter the FCS switch root password.

   Note: Make sure to enter the password exactly as it was entered the first time.
8. Enter the FCS switch factory password.
9. Re-enter the FCS switch factory password.

   Note: Make sure to enter the password exactly as it was entered the first time.
10. Enter the FCS switch admin password.
11. Re-enter the FCS switch admin password.

    Note: Enter the password exactly as it was entered the first time.
12. Enter the new fabric-wide user password.
13. Re-enter the fabric-wide user password.

    Note: Make sure to enter the password exactly as it was entered the first time.

14. Enter the non-FCS switch admin password.
15. Re-enter the non-FCS switch admin password.

    Note: Make sure to enter the password exactly as it was entered the first time.

    Note: All the passwords are saved. The FCS list and passwords are distributed to the switches in the fabric.

16. Open a `sectelnet` connection to log into the secure fabric:

    Example:

    ```
    sectelnet <switchname>|<switch_IP>
    ```

    When using the `sectelnet` command, the password is encrypted.

    Note: All the switches are rebooted.

Displaying the Current Security Mode

To display if security mode is enabled or disabled:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

    ```
    secModeShow
    ```

The following example shows typical output when you enter the `secModeShow` command.

Example:

```
primaryfcs:admin> secmodeshow
Secure Mode: ENABLED.
Version Stamp: 10354, Thu Oct  4 10:23:32 2001.
Pos   Primary WWN                     DId swName.
=================================================
  1   Yes     10:00:00:60:69:11:fc:53   2 primaryfcs.
  2   No      10:00:00:60:69:11:fc:55   1 backupswitch.
```

This command displays whether the fabric has security mode enabled. It also displays a version stamp stating the current version, build date and time of the security database.

Table 4-14 identifies the type of information that displays. If security mode is enabled the following information appears:

Table 4-14 Security Mode Information

Information	**What is Displayed**
Pos	Displays the position (1, 2, 3) of the switches in the FCS list
Primary	Displays whether the switch is the primary FCS or not
WWN	Displays the WWN of each FCS switch
DId	Displays the domain ID of each FCS switch
swName	Displays the switch name of each FCS switch

Note: The `secModeShow` command can be issued on any switch if there is no active FCS in the fabric.

Creating a Security Policy

A security policy is a list of IP addresses or WWNs that can use a particular administrative access method. There is a security policy for each of the administrative methods.

You can create the following types of security policies:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- DCC_POLICY_nnn
- OPTIONS_POLICY

Note: The FCS_POLICY can only be created when enabling security mode. It may be modified after security is enabled using the `secModeEnable` command.

Each type of security policy (other than DCC_POLICY_nnn) can be created only once. When security mode is first enabled only the FCS_POLICY exists. For MAC policies, once you add either an IP address or WWN access to a member list of a policy, that policy is closed to all access except those members listed for each policy. If you then remove all members from a policy, that policy becomes closed to all access.

IP Address Member Policy Types

The following policy types require members be specified by IP address:

- TELNET_POLICY
- HTTP_POLICY
- API_POLICY
- RSNMP_POLICY
- WSNMP_POLICY

These policy types require member IDs in dot-decimal notation.

Example:

```
124.23.56.122
```

If (0)zero is specified in one of the octets, it means any number can be matched.

To create an IP Address member policy:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   `secPolicyCreate` "policy_name", "member;...;member"

   where:

   policy_name must be either `TELNET_POLICY, HTTP_POLICY, API_POLICY, RSNMP_POLICY`, or `WSNMP_POLICY`.

   Note: The policy_name value must be entered in all capitals.

   member must be a single or set of IP addresses in dot-decimal notation.

   Note: The member list must be enclosed in quotation marks and each member must be separated by a semicolon.

WWN Member Policy Types

The following policy types require that members be specified by WWN address:

- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY

These policy types require member IDs to be specified as WWN strings, domain IDs, or switch names. If domain IDs or switch names are used, the switches associated must be present in the fabric or the command fails.

Note: SES_POLICY and MS_POLICY use device WWNs while SERIAL_POLICY, FRONTPANEL_POLICY, and SCC_POLICY use switch WWNs.

To create a WWN member policy:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   `secPolicyCreate` "policy_name", "member;...;member"

   where:

   policy_name must be either `SES_POLICY, MS_POLICY, SERIAL_POLICY, FRONTPANEL_POLICY`, or `SCC_POLICY`.

   Note: The policy_name value must be entered in all capitals.

   member must be a single or set of WWNs, domains, or switch names.

   Note: The member and policy type must be enclosed in quotation marks and each member must be separated by a semicolon (;).

DCC_POLICY Members

The DCC policy is a list of member devices associated with a specific switch and port combination. A violation is registered if an unknown WWN device tries to access the fabric through the switch (port) combination defined in the policy.

You can create multiple DCC_POLICY_nnn values, although the violation statistics for all DCC policies are counted together.

To create a DCC_POLICY:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line:

   `secPolicyCreate` "DCC_POLICY_nnn", "member"

   where:

   DCC_POLICY_nnn must be named using the prefix DCC_POLICY_ followed by any alphanumeric or underscore value up to a total of 30 characters. Each DCC_POLICY must have a unique name.

   member must be a single or set of device and switch (port) combinations. The members of a DCC_POLICY must be specified:

   ```
   deviceWWN;switch(port)
   ```

   The attached device must be specified using the WWN. You can specify multiple devices. The switch value can be specified using WWN, domain ID, or switch name.

   The port values must be specified by port number separated by commas, and enclosed in either brackets or parentheses. Ports enclosed in brackets will include the devices currently attached to those ports.

   There are several ways to specify the port values:

   Examples:

   ```
   (1-6) = selects ports 1 through 6.

   (*) = selects all ports on the switch.

   [*] = selects all ports and all devices attached to those
   ports.
   ```

```
[3, 9] = selects ports 3 and 9 and all devices attached to
those ports.
```

```
[1-3, 9] = selects ports 1 through 3 and port 9 and all
devices attached to those ports.
```

A DCC_POLICY can be defined in several ways:

Examples:

1. `primaryfcs:admin> secPolicyCreate "DCC_POLICY_server", "11:22:33:44:55:66:77:aa;1(1,3)"`

   means that device “11:22:33:44:55:66:77:aa” and port 1 and port 3 of switch domain 1 will be included in the DCC_POLICY_server.

2. `primaryfcs:admin> secPolicyCreate "DCC_POLICY_storage", "22:33:44:55:66:77:11:bb;2[*]"`

   means that device WWN “22:33:44:55:66:77:11:bb,” all ports of switch domain 2, and all currently connected devices of switch domain 2 will be included in the DCC_POLICY_storage.

3. `primaryfcs:admin> secPolicyCreate "DCC_POLICY_abc", "33:44:55:66:77:11:22:cc;3(1-6,9)"`

   means that device “33:44:55:66:77:11:22:cc” and ports 1-6 and port 9 of switch domain 3 will be included in the DCC_POLICY_abc.

4. `primaryfcs:admin> secPolicyCreate "DCC_POLICY_example", "44:55:66:77:22:33:44:dd;33:44:55:66:77:11:22:cc;4[1-4]"`

   means that devices 44:55:66:77:22:33:44:dd and 33:44:55:66:77:11:22:cc, ports 1-4 of switch domain 4, and all devices currently connected to ports 1-4 of switch domain 4 will be included in the DCC_POLICY_example.

OPTIONS_POLICY members

The OPTIONS_POLICY has only one valid value for a member list "NoNodeWWNZoning."

To create an OPTIONS _POLICY:

1. You must be logged into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secPolicyCreate "OPTIONS_POLICY", "NoNodeWWNZoning"
   ```

   NoNodeWWNZoning disables the use of Node WWNs for WWN-based zoning. The use of node WWNs can introduce ambiguity when used with certain HBAs that use the same WWN for the node as for one of the ports on the HBA.

Deleting a Security Policy

If you delete a policy type, that policy becomes open to all access.

To delete a security policy:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   `secPolicyDelete` "policy_name"

   where policy_name is one of the following:

   - TELNET_POLICY
   - HTTP_POLICY
   - API_POLICY
   - RSNMP_POLICY
   - WSNMP_POLICY
   - SES_POLICY
   - MS_POLICY
   - SERIAL_POLICY
   - FRONTPANEL_POLICY
   - SCC_POLICY
   - DCC_POLICY_nnnn
   - OPTIONS_POLICY

   Note: The FCS_POLICY cannot be deleted by using the `secPolicyDelete` command. Instead refer to the *Disabling Security Mode on a Fabric* section on page 4-34 to delete an FCS_POLICY.

Adding Members to an Existing Security Policy

Each security policy type has a defined member list. When security mode is first enabled all policy types are empty and open (except the FCS_POLICY). Once you add either the IP address or WWN access to the member list of a policy type, the MAC policy type is closed to all access except those members listed.

To add a member to an existing security policy, perform the following:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   `secPolicyAdd` "policy_name", "member;...;member"

Where policy_name is the security policy name and member is the device IP address, switch domain, switch WWN, or switch alias name to be added. The valid security policy names are:

- FCS_POLICY
- TELNET_POLICY
- API_POLICY
- HTTP_POLICY
- RSNMP_POLICY
- WSNMP_POLICY
- SES_POLICY
- MS_POLICY
- SERIAL_POLICY
- FRONTPANEL_POLICY
- SCC_POLICY
- DCC_POLICY_nnn
- OPTIONS_POLICY

Removing a Member from a Security Policy

Each security policy type has a defined member list. When security mode is first enabled all policy types are empty and open (except the FCS_POLICY). Once you add either an IP address or WWN access to the member list of a policy type, that policy type is closed to all access except those members listed. If you then remove all the members of a policy type, that policy becomes closed to all access.

To remove a member from a security policy, perform the following:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secPolicyRemove "policy_name", "member;...;member"
   ```

   Where policy_name is the security policy name and member is the device IP address, switch domain, switch WWN, or switch alias name to be removed. The valid security policy names are:

   - FCS_POLICY
   - TELNET_POLICY
   - API_POLICY
   - HTTP_POLICY
   - RSNMP_POLICY
   - WSNMP_POLICY
   - SES_POLICY
   - MS_POLICY
   - SERIAL_POLICY
   - FRONTPANEL_POLICY
   - SCC_POLICY
   - OPTIONS_POLICY
   - DCC_POLICY_nnn

Modifying the Order of FCS Switches

The list of FCS switches is created when security mode is enabled on a switch and is maintained in the security database. The first switch in the list is the primary FCS switch. The other switches are backup FCS switches. The order of the backup FCS switches determines the order these switches are used if there is a problem with the primary FCS switch. For instance, the first backup switch would be used followed by the second backup switch and so forth.

You may need to rearrange the order of FCS backup switches in the security database or move a backup switch to the primary FCS position.

To modify the order of FCS switches:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secpolicyshow "Defined", "FCS_POLICY"
   ```

   This command displays the position and WWN of the primary FCS and backup FCS switches. Decide which switch you want to move and to where you want to move it in the list of FCS switches.
3. At the command line enter:

   ```
   secPolicyFCSMove pos_from, pos_to
   ```

   where `pos_from` (current table position number such as 1) and `pos_to` (new table position number such as 2) are exchanged in the FCS_POLICY list.

   Note: You may also use the interactive mode by entering the `secPolicyFCSMove` command and pressing the **Enter** key.

Changing the Primary FCS Switch

The `secFCSFailover` command is used to move the primary FCS role from the primary FCS switch to a backup FCS switch for recovery such as the primary FCS switch loses its Ethernet connection.

To change the primary FCS switch:

1. Log into the backup FCS switch (the switch that you want to become the primary FCS switch) as the admin user using the `sectelnet` command.
2. At the command line enter:

   ```
   secFCSFailover
   ```

The command will cause failover to your current session automatically changing the FCS list to match the failover.

Saving a Security Policy to Flash Memory

To save the changes made to any policy under the defined policy set and to propagate the changes to all the switches in the fabric, perform the following:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

```
secPolicySave
```

Note: Until a `secPolicySave` or `secPolicyActivate` command is issued, all policy changes are in volatile memory and will be lost upon rebooting.

Activating a Security Policy

If you have made any changes to the security policy and these changes are either saved or not saved in the defined security database, you must enter the `secPolicyActivate` command to make the policy changes effective. To activate the current defined security policy:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

```
secPolicyActivate
```

Aborting Uncommitted Changes to Security

The `secPolicyAbort` command is used to abort changes to security that have not been committed. To abort any uncommitted changes to security:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

```
secPolicyAbort
```

Note: All changes since entering the last `secPolicySave` or `secPolicyActivate` command are aborted.

Aborting Current Security Transaction

To abort the current security transaction on a fabric:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

```
secTransAbort
```

The current security transaction session will be aborted.

Disabling Security Mode on a Fabric

To disable Security Mode on a fabric:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   ```
   secModeDisable
   ```

3. Press the `y` key to verify that you want to disable security mode on the fabric.

Note: This entry deletes all information from the defined and active security database.

All `sectelnet` sessions will be terminated.

To log into the FCS switch after disabling security, the passwords remain the same as in secure mode. For the non-FCS switches, the root and factory passwords are the same as the secure mode administrator password for non-FCS switches.

Viewing the Security Policy Database

The security policy database contains the active policy set and the defined policy set.

To view the security policy database:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   `secPolicyDump <listtype>`, "policy_name"

   where

   listtype is either `active, defined, or` asterisk `(*)` meaning both active and defined; policy_name is one of the following:

   - TELNET_POLICY
   - FCS_POLICY
   - HTTP_POLICY
   - API_POLICY
   - RSNMP_POLICY
   - WSNMP_POLICY
   - SES_POLICY
   - MS_POLICY
   - SERIAL_POLICY
   - FRONTPANEL_POLICY
   - SCC_POLICY
   - DCC_POLICY_nnn
   - OPTIONS_POLICY

   If you do not specify the active or defined or the policy type, the `secPolicyDump` command will display both policy sets and all policy types.

   Note: The `secPolicyDump` command displays information without page breaks.

Displaying the Members of a Security Policy

The policy sets in the security policy databases are:

- Active
- Defined

To view the members of a specific security policy type:

1. Log into the primary FCS switch as the admin user using `sectelnet`.
2. At the command line enter:

   `secPolicyShow` <listtype>, "policy_name"

   where:

   listtype is `defined, active, or` asterisk `(*)` meaning both active and defined. This policy name value must be enclosed in quotation marks.

   Note: The `secPolicyShow` command displays information with page breaks.

   policy_name is one of the following:

   - FCS_POLICY
   - TELNET_POLICY
   - HTTP_POLICY
   - API_POLICY
   - RSNMP_POLICY
   - WSNMP_POLICY
   - SES_POLICY
   - MS_POLICY
   - SERIAL_POLICY
   - FRONTPANEL_POLICY
   - SCC_POLICY
   - DCC_POLICY_nnn
   - OPTIONS_POLICY

Joining Secure Fabrics

You can join secure production fabrics using the following methods:

1. Join two secure fabrics if they have the same FCS list and the same version stamp. Nothing needs to be done because these two join automatically after they are connected.

   Note: You should avoid merging two secure fabrics with zero version stamps if there is no FCS in the fabric. By doing this kind of merge, the fabric has no policy manager so you could end up with a fabric that has inconsistent policies.

2. Join two secure fabrics with the same FCS (both FCSs must match in content and order) and different version stamps. To do so you must:

   a. Determine which database to keep.

   b. Zero out the other version stamp by using the `secVersionReset` command.

c. Connect the two fabrics together.

The two fabrics will join and the databases become identical. The database that is kept is the one associated with the non-zero stamp.

3. To join two secure fabrics with different FCS and different version stamps, you must:

   a. Determine which switches will be FCS for the final fabric and use the appropriate commands to manipulate FCS_POLICY in both fabrics. These commands are:

      - secPolicyAdd
      - secPolicyRemove
      - secPolicyFCSMove

   b. Use the `secPolicyActivate` command to apply changes to both fabrics.

   c. Determine which fabric's database you want to keep.

   d. Zero out the version stamp of the other fabric by using the `secVersionReset` command.

   e. Connect the two fabrics together by plugging one into the other.

   The two fabrics will join and the databases become identical. The database that is kept is the one associated with the non-zero stamp.

4. To join a secure fabric with no FCS switch to a secure fabric with FCS switches:

   a. On any switch in the secure fabric with no FCS switch, issue the `secModeEnable` command and enter the FCS list from the secure fabric with FCS switches.

      The version stamp is set to zero automatically on the secure fabric with no FCS switch.

   b. Connect the two fabrics together by plugging one into the other.

   The two fabrics will join and the databases become identical. The database that is kept is the one that is associated with the non-zero stamp (the secure fabric with FCS switches).

5. To join a non-secure fabric to a secure fabric:

   a. Enable secure mode on a non-secure fabric using the FCS list from the secure fabric. To do this, use the `secModeEnable` command.

      The version stamp is automatically set to zero when there is no FCS in the secure fabric.

   b. Connect the two fabrics together by plugging one into the other.

      The two fabrics will join and the databases become identical. The database that is kept is the one associated with the non-zero stamp.

Recovery Operations

This section covers actions you can take when you are having problems with security operations.

Note: Ensure that the SCC_Policy (if it exists) does not exclude the switches you intend to merge. If the switches are excluded, they will be segmented. See Table 4-15 on page 4-37 (number 4) for recovery.

Table 4-15 covers what you can do when you need to recover.

Table 4-15 Recovery Processes

No.	Problem	Symptom	What To Do
1.	The fabric has no FCS.	The security, zoning, and password commands cannot be executed.	Select a new primary FCS switch in the fabric by using the `secModeEnable` command on the switch that you want to become the primary FCS switch.
2.	The telnet sessions are accidentally blocked.	You cannot telnet to any/primary switch.	Use a serial cable to connect to the primary FCS switch; delete or modify the telnet policy.
3.	The primary FCS switch loses all connections.	The switch cannot be accessed by any management method.	Move the primary FCS role to backup by using the `secFCSFailover` command on the switch that you want to become the primary FCS switch.
4.	SCC_POLICY excludes switches existing in the fabric. Even after modifying the SCC_POLICY to include these switches, the fabric is still segmented.	The excluded switches become segmented and cannot join any fabric because the switches have the original SCC_POLICY.	Run `secModeEnable` on the excluded switch making the excluded switch the primary FCS switch. You will automatically be logged out. Log in again to the excluded switch and run `secPolicyDelete` “SCC_POLICY” to remove the SCC_POLICY which was restricting the switch from joining the fabric. Run the `secPolicyActivate` command on the excluded switch so that you save and activate the changes to the policy set. Run the `switchDisable` and `switchEnable commands` (assuming that the FCS list and stamp match and that the only inaccuracy is the SCC policy limits). Under the *Joining Secure Fabrics* section, follow step 3 on page 4-36 to join the excluded switches back into the fabric.

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