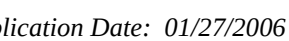
Firmware Download

Best Practice Notes

Supporting Fabric OS v5.1.0

Supporting SilkWorm 200E, 3250, 3850, 3900, 4100, 4900, 7500, 24000, and 48000

Publication Number: 53-1000039-03



Publication Date: 01/27/2006

 Publication Number: 53-1000039-03

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

Brocade Communications Systems, Incorporated

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

Asia-Pacific Headquarters
Brocade Communications Singapore Pte. Ltd.
9 Raffles Place
#59-02 Republic Plaza 1
Singapore 048619
Tel: +65-6538-4700
Fax: +65-6538-0302
Email: apac-info@brocade.com

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

Document History

The following table lists all versions of the *Firmware Download Best Practice Notes.*

Document Title	Publication Number	Summary of Changes	Publication Date
Firmware Download Best Practice Notes	53-0000039-01	New document.	June 2005
Firmware Download Best Practice Notes	53-0000039-02	Updated content.	September 2005
Firmware Download Best Practice Notes	53-0000039-03	Major revisions in content and structure. Includes content for Fabric OS v5.1.0.	January 2006

Installing and Maintaining Firmware

These notes contain procedures for installing and maintaining firmware. Fabric OS v5.1.0 provides nondisruptive firmware installation.

In most cases, you will be *upgrading* firmware; that is, installing a newer firmware version than the one you are currently running. However, some circumstances might require installing an older version; that is, *downgrading* the firmware. The procedures in this section assume that you are upgrading firmware, but they work for downgrading as well, provided the old and new firmware versions are compatible. Also, always reference the latest release notes for updates that may exist regarding downgrades under particular circumstances.

Using the CLI (or Web Tools), you can upgrade the firmware on one switch at a time. You can use the optionally licensed Brocade Fabric Manager software tool to upgrade firmware simultaneously on multiple switches. For more details on Fabric Manager and other licensed software tools, go to the Brocade Web site at *http://www.brocade.com*.

About the Firmware Download Process

The **firmwareDownload** command downloads uncompressed switch firmware from an FTP server to the switch's nonvolatile storage area.

In the SilkWorm 24000 and 48000 directors, this command (when not using any options flags) by default downloads the firmware image to a standby CP, if there is one, to prevent disruption to application services. This operation depends on high-availability (HA) support. If HA is not available, you can upgrade the CPs one at a time, using the **-s** option.

Caution
To ensure non-disruptive downloads on non-director-class switches, please ensure that the **firmwareDownload** is completed successfully on each switch in a serial fashion. Enter the **firmwareDownloadStatus** command on the switch before moving on to the next switch.

SilkWorm fixed-port models and each CP blade of the SilkWorm 24000 and 48000 models have two partitions of nonvolatile storage areas (a primary and a secondary) to store two firmware images. The **firmwareDownload** command always loads the new image into the secondary partition and swaps the secondary partition to be the primary. It then reboots the partition and activates the new image. Finally, it performs the **firmwareCommit** procedure automatically, to copy the new image to the other partition.

If you are using a SilkWorm 48000 with an FR4-18i blade: The Fabric OS automatically detects mismatches between the active CP firmware and the FR4-18i blade firmware. By the end of the firmware download process the active CP and the FR4-18i blade will be running the same version of firmware.

Effects of Firmware Changes on Accounts and Passwords

The following table describes what happens to accounts and passwords when you replace the switch firmware with a different version. *Upgrading* means installing a newer version of firmware. *Downgrading* means installing an older version of firmware.

Table 1 Effects of Firmware Changes on Accounts and Passwords

Change	First Time	Subsequent Times (After upgrade, then downgrade, then upgrade)
Upgrading	Default accounts and their passwords are preserved.	User-defined and default accounts and their passwords are preserved.
Downgrading	User-defined accounts are no longer valid. Default accounts and their passwords are preserved. If a default account was disabled, it is reenabled after the downgrade.	User-defined and default accounts and their passwords are preserved, including accounts added after the first upgrade.
Upgrading to v3.2.0	(You might upgrade a switch in the fabric as part of "Checking Connected Switches" on page 7.) Earlier versions allowed you to change the default account names. You cannot add user-defined accounts until you change the names back to default with the **passwdDefault** command.	

For more details on older releases of Fabric OS, refer to "Understanding Legacy Password Behavior" on page D-1 of the *Fabric OS Administrator's Guide*.

See Also: For details about downgrading and restoring firmware, refer to "Testing and Restoring Firmware: SilkWorm Directors" on page 17.

Considerations for FICON CUP Environments

To prevent channel errors during nondisruptive firmware installation, the switch CUP port must be taken offline from all host systems.

Preparing for a Firmware Download

Before executing a firmware download, it is recommended that you perform the tasks mentioned in this section. In the unlikely event of a failure or time-out, the preparation tasks that are described in this section will enable you to provide Brocade Support all the information required to perform advanced troubleshooting.

To prepare for a firmware download

1. Read the release notes for the new firmware to find out if there are any issues related to firmware download.
2. Establish a telnet session and log in as admin. Enter the **firmwareShow** command to verify the current version of Fabric OS. Brocade does not support upgrades from more than two previous releases. For example, upgrading from Fabric OS v4.4.0 to v5.1.x is supported, but upgrading from Fabric OS v4.2.0 or a previous release directly to v5.1.x is not. In other words, upgrading a switch from Fabric OS v4.2.0 or a previous release to v5.1.0 is a two-step process: first upgrade to v4.4.0 or v5.0.1, and then upgrade to v5.1.0. Following are the major upgrade versions for the Fabric OS:
   - v4.0
   - v4.1
   - v4.2
   - v4.4.0
   - v5.0.1
   - v5.1.0

   Note

   Newer Fabric OS versions (v4.4.x and v5.0.x) can support large zone databases. However, you should exercise caution when downgrading to v4.2.0 and earlier Fabric OS versions that do not support the large zone databases. If the zone database is too large, then you may be required to disable all ports in earlier versions of the Fabric OS to avoid data corruption; this would require a manual reactivation of all ports.

   Fabric OS v4.4.0 and later supports zone databases up to 256k in size.
3. Upon initial setup of a factory-delivered switch, make sure that all IP address have been set and the switch has been rebooted prior to running a firmware download.Establish a telnet session and log in to the SilkWorm switch.
4. (Optional) For enhanced support, connect the switch with a serial console cable to a computer. Ensure that all serial consoles (both CPs for bladed products) and all telnet sessions are logged and included with any trouble reports.
5. Establish a telnet session and log in to the switch as admin. Issue the **saveCore** command to remove all extra core files prior to executing the firmware download. This helps free up some disk space. If you are upgrading a director, log in to both the active and standby CPs and enter the **saveCore** command on each CP.

   Note

   If you do not know the CP address, use the **ipAddrShow** command to view a list of all CP IP addresses associated with the switch.
6. (Optional) Enter the **supportSave** command to capture a snapshot of your configuration and provide baseline information in case there is a need to troubleshoot or seek advanced support. Make sure that you enter this command on the standby CP as well.

   After you run **supportSave**, locate the compact flash usage information in the **supportSave** output files named *XXX_SUPPORTSHOW* (where *XXX* is a switch, date, or time prefix). Open the *XXX_SUPPORTSHOW* file in any text editor and search for the following information:

```
/bin/df:
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/root               120112     61128     58984  51% /
/dev/hda2               120128     72356     47772  60% /mnt
```

Verify that the compact flash usage is not above 90%. If the compact flash usage is above 90%, contact your switch service provider.

Note

If using Fabric OS v4.2.0 or earlier, enter the **supportShow** command and verify the above compact flash information by searching the output of the **supportShow** command.

7. (Optional) Enter the **errClear** command to erase all existing messages in addition to internal messages.

Checking Connected Switches

If the switch to be upgraded is running v4.1.0 firmware (or later), it is recommended that all switches directly connected to it be running versions no earlier than v2.6.1, v3.1.0, or v4.1.0. If some connected switches are running older firmware, upgrade them to *at least* the earliest recommended version (shown in Table 2) before upgrading firmware on your switch.

Note

Please go to *http://www.brocade.com* to view end-of-life policies for Brocade products. Navigate to the **Services and Support** tab, then select **End of Life Information**. End-of-life products are not supported.

Table 2 Recommended Firmware

SilkWorm Model[a]	**Earliest Recommended Fabric OS Version**
200E	v5.0.1
2000 series	v2.6.1
3200, 3600, 3800	v3.1.0
3016, 3250, 3850	v4.2.0
3900	v4.1.0
4012	v5.0.0
4100	v4.4.0
4900	v5.1.0
7500	v5.1.0
24000	v4.2.0
48000	v5.0.1
48000 with FR4-18i blade	v5.1.0

a. During code activation on SilkWorm 3016, 3250, 3850, or 3900 running Fabric OS v4.1.0 or later, data continues to flow between hosts and storage devices; however, fabric services are unavailable for a period of approximately 50-55 seconds. Possible disruption of the fabric can be minimized by ensuring that switches logically adjacent to these models (directly connected via an ISL) are running at the minimum Fabric OS v2.6.1 or later, v3.1.0 or later, or v4.1.0 or later.

If SilkWorm 3016, 3250, 3850, 3900, 4012, 4100, 4900 or 7500 models are adjacent and you start firmware downloads on them at same time, there might be I/O disruption.

To determine whether you need to upgrade connected switches before upgrading your switch, use the following procedure on each connected switch to display firmware information and build dates.

1. Connect to the switch and log in as admin.
2. Enter the **version** command.

   The following information is displayed:

Kernel:	Displays the version of switch kernel operating system.
Fabric OS:	Displays the version of switch Fabric OS.
Made on:	Displays the build date of firmware running in switch.
Flash:	Displays the install date of firmware stored in nonvolatile memory.
BootProm:	Displays the version of the firmware stored in the boot PROM.

Obtaining and Decompressing Firmware

Firmware upgrades are available for customers with support service contracts and partners on the Brocade Web site at *http://www.brocade.com*.

At the Brocade Web site, click *Brocade Connect* and follow the instructions to register and download firmware. Partners with authorized accounts can use the *Brocade Partner Network*.

You must decompress the firmware (using the UNIX **tar** or **gzip** command for all .gzip files, or a Windows unzip program for all .zip files) before you can use the **firmwareDownload** command to update the firmware on your equipment.

When you unpack the downloaded firmware it expands into a directory that is named according to the version of Fabric OS it contains. For example, if you download and unzip *Fabric OS v5.1.0.zip*, it expands into a directory called *v5.1.0*. When you issue the **firmwareDownload** command, there is an automatic search for the correct package file type associated with your switch. Specify the path to the *v5.1.0* directory and append the keyword *release.plist* to the path even though *release.plist* is not located in the root of the firmware archive. Do not reference any subdirectory containing a *release.plist* file–the root of the archive must be the path.

Performing Firmware Download on SilkWorm Switches

SilkWorm 200E, 3016, 3250, 3850, 3900, 4012, 4100, 4900, and 7500 switches maintain primary and secondary partitions for firmware. The **firmwareDownload** command defaults to an autocommit option that automatically copies the firmware from one partition to the other.

You should not override autocommit under normal circumstances; use the default. Refer to "Testing and Restoring Firmware: SilkWorm Directors" on page 17 for details about overriding the autocommit option.

Summary of the Firmware Download Process

The following summary describes the default behavior after you enter the **firmwareDownload** command (without options) on SilkWorm 200E, 3016, 3250, 3850, 3900, 4012, 4100, 4900 and 7500 models:

- The Fabric OS downloads the firmware to the secondary partition.
- The system performs a high-availability reboot (**haReboot**). After the **haReboot**, the former secondary partition is the primary partition.
- The system replicates the firmware from the primary to the secondary partition.

SilkWorm 200E, 3016, 3250, 3850, 3900, 4012, 4100, 4900 and 7500 Firmware Download Procedure

The upgrade process first downloads and then commits the firmware to the switch. While the upgrade is proceeding, you can start another telnet session on the switch and observe the upgrade progress if you wish.

Note

After you start the process, do not enter any disruptive commands (such as reboot) that will interrupt the process. The entire firmware download and commit process takes approximately 17 minutes. If there is a problem, wait for the time-out (30 minutes for network problems). Disrupting the process can render the switch inoperable and require you to seek help from your switch service provider.

Do not disconnect the switch from power during the process, because the switch could become inoperable upon reboot.

To upgrade firmware for SilkWorm 200E, 3016, 3250, 3850, 3900, 4012, 4100, 4900, and 7500 switches

1. Verify that the FTP service is running on the host server and that you have a user ID on that server.
2. Obtain the firmware file from the Brocade Web site at *http://www.brocade.com* and store the file on the FTP server. Verify that the FTP service is running and unpack the compressed files preserving directory structures.
3. Use the **firmwareShow** command to check the current firmware version on connected switches. Upgrade their firmware if necessary before proceeding with upgrading this switch.

   Refer to "Checking Connected Switches" on page 7 for more details.
4. Connect to the switch and log in as admin.
5. Enter the **firmwareDownload** command.
6. At the "Do you want to continue [y/n]" prompt, enter **y**.

7. Respond to the prompts as follows:

Server Name or IP Address	Enter the name or IP address of the FTP server where the firmware file is stored; for example, 192.1.2.3. You can enter a server name if DNS is enabled.
User name	Enter the user name of your account on the server; for example, “JohnDoe”.
File name	Specify the full path name of the firmware directory, appended by release.plist; for example, */pub/v5.1.0/release.plist*. **Note**: For v4.x and v5.x switches only, do not attempt to locate the *release.plist* file in the top level directory; there is a *release.plist* file for each platform, and the correct one is automatically selected.
Password	Enter your account password for the server. Note that this is a required field even if you are logged in as an anonymous user; in such cases, the value may be ignored by the FTP service.

   After the firmware is downloaded, the switch reboots and starts the firmware commit.

8. After the reboot, connect to the switch and log in again as admin.
9. If you want snapshots of the upgrade progress, enter the **firmwareDownloadStatus** command.
10. After the firmware commit completes, enter the **firmwareShow** command to display the firmware level of both partitions. Note that it takes several minutes to complete the commit operation.

```
switch:admin> firmwaredownload
Server Name or IP Address: 10.22.127.127
FTP User Name: JohnDoe
File Name: /pub/v5.1.0/release.plist
FTP Password:
You can run firmwaredownloadstatus to get the status
of this command.

This command will cause the switch to reset and will
require that existing telnet, secure telnet or SSH
sessions be restarted.

Do you want to continue [Y]:y
```

Log in again to view the upgrade progress:

```
switch:admin> firmwaredownloadstatus
[1]: Fri Feb 15 22:17:03 2008
Firmware is being downloaded to the switch. This step may take up to 30 minutes.

[2]: Fri Feb 15 22:20:54 2008
Firmware has been downloaded to the secondary partition of the switch.

[3]: Fri Feb 15 22:22:19 2008
The firmware commit operation has started. This may take up to 10 minutes.

[4]: Fri Feb 15 22:22:51 2008
Switch is relocating an internal firmware image.

[5]: Fri Feb 15 22:25:15 2008
The commit operation has completed successfully.

[6]: Fri Feb 15 22:25:46 2008
The internal firmware image is relocated successfully.

[7]: Fri Feb 15 22:25:46 2008
Firmwaredownload command has completed successfully. Use firmwareshow to verify the firmware
versions.

switch:admin> firmwareshow
Primary partition: v5.1.0
Secondary Partition: v5.1.0
switch:admin>
```

Performing Firmware Download on SilkWorm Directors

You can download firmware to SilkWorm 24000 and 48000 directors without disrupting the overall fabric if the two CP blades are installed and fully synchronized. Use the **haShow** command to confirm synchronization. If only one CP blade is powered on, the switch must reboot to activate firmware, which is disruptive to the overall fabric.

During the upgrade process, the director fails over to its standby CP blade and the IP addresses for the two logical switches move to that CP blade's Ethernet port. This might cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, because the association between the IP addresses and MAC addresses has changed.

Caution
To successfully download firmware you must have an active Ethernet connection on *each* of the CPs.

Do not attempt to perform a firmware downgrade to 4.2.2 when you have a zone configuration larger than 128K. Issue the **cfgSize** command to view the zone configuration size.

If your fabric is set to the extended edge PID format and you want to downgrade to an older Fabric OS version that does not support extended edge, you *must* change the PID to a supported format. Refer to Appendix A, “Configuring the PID Format” in the *Fabric OS Administrator’s Guide* for more information about PID formats.

Use the **haShow** command to verify that your CPs are synchronized prior to running a firmware download. If the CPs are not in sync run the **haSyncStart** command. If the problem persists, review “Troubleshooting Firmware Downloads” on page 21. If the troubleshooting information fails to help resolve the issue, contact your switch service provider.

Summary of the Firmware Download Process on SilkWorm Directors

The following summary describes the default behavior of the **firmwareDownload** command (without options) on SilkWorm 24000 and 48000 directors.

After you enter the **firmwareDownload** command on the active CP blade:

- The standby CP blade downloads firmware.
- The standby CP blade reboots and comes up with the new Fabric OS.
- The active CP blade synchronizes its state with the standby CP blade.
- The active CP blade forces a failover and reboots to become the standby CP blade.
- The *new* standby CP blade (the active CP blade before the failover) downloads firmware.
- The *new* standby CP blade reboots and comes up with the new Fabric OS.
- The new active CP blade synchronizes its state with the new standby CP blade.
- The **firmwareCommit** command runs automatically on both CP blades.

Note

After you start the process, do not enter any disruptive commands (such as reboot) that will interrupt the process. The entire firmware download and commit process takes approximately 15 minutes. If there is a problem, wait for the time-out (30 minutes for network problems). Disrupting the process can render the switch inoperable and require you to seek help from Customer Support.

Do not disconnect the switch from power during the process, because the switch could become inoperable upon reboot.

SilkWorm 24000 and 48000 Firmware Download Procedure

There is one logical switch address for a SilkWorm 48000, and up to two logical switch addresses for the SilkWorm 24000, but either can be used on the SilkWorm 24000 to effect a firmwaredownload (either logical switch).

Note

By default, the **firmwareDownload** command automatically upgrades both the active CP blade and the standby CP blade; this behavior also applies when a FR4-18i blade is present in the SilkWorm 48000.

To upgrade the firmware on SilkWorm 24000 and 48000 directors (including the FR4-18i blade):

1. Verify that the FTP service is running on the host server and that you have a user ID on that server.
2. Obtain the firmware file from the Brocade Web site at *http://www.brocade.com* and store the file on the FTP server. Verify that the FTP service is running and decompress the compressed files preserving directory structures.
3. Use the **firmwareShow** command to check the current firmware version on connected switches. Upgrade the firmware, if necessary, before proceeding with upgrading this switch.

Caution

SilkWorm 48000 with a FR4-18i blade: If you are running v5.1.0 firmware, then you cannot downgrade to earlier versions.

Refer to "Checking Connected Switches" on page 7.

4. Using a telnet session, connect to the switch and log in as admin.
5. Enter the **haShow** command to confirm that the two CP blades are synchronized. In the following example, the active CP blade is CP1 and the standby CP blade is CP0:

```
switch:admin> hashow
Local CP (Slot 6, CP1): Active
Remote CP (Slot 5, CP0): Standby
HA Enabled, Heartbeat up, HA State is in Sync
switch:admin>
```

   CP blades must be synchronized and running Fabric OS v4.2.0 or later to provide a nondisruptive download. If the two CP blades are not synchronized, enter the **haSyncStart** command to synchronize them. If the CPs still are not synchronized, contact your switch service provider.

6. Enter the **firmwareDownload** command.
7. At the "Do you want to continue [y/n]" prompt, enter **y**
8. Respond to the prompts as follows:

Server Name or IP Address	Enter the name or IP address of the server where the firmware file is stored: for example, 192.1.2.3. You can enter a server name if DNS is enabled.
User name	Enter the user name of your account on the server: for example, *JohnDoe*.
File name	Specify the full path name of the firmware directory, appended by release.plist; for example, */pub/v5.1.0/release.plist.* **Note**: For v4.x and v5.x switches only, do not attempt to locate the *release.plist* file in the top level directory; there is a *release.plist* file for each platform, and the correct one is automatically selected.
Password	Enter your account password for the server. Note that this is a required field even if you are logged in as an anonymous user; in such cases, the value may be ignored by the FTP service

   The firmware is downloaded to one CP blade at a time, beginning with the standby CP blade. During the process, the active CP blade is failed over. After the firmware is downloaded, a firmware commit starts on both CP blades. The entire firmware download and commit process takes approximately 35 minutes.

   If there is an FR4-18i blade present: At the point of the failover an *auto-leveling* process is activated. Auto-leveling is triggered when the active CP detects the FR4-18i blade that contains a different version of the firmware, regardless of which version is older. Auto-leveling downloads firmware to the FR4-18i blade, swaps partitions, reboots the blade, and copies the new firmware from the primary partition to the secondary partition. If you have multiple FR4-18i blades, they are updated simultaneously; however, the downloads can occur at different rates.

   Auto-leveling takes place in parallel with the firmware download being performed on the CPs, but does not affect performance. Fibre Channel traffic is not disrupted during auto-leveling, but GbE traffic is.

9. Optionally, after the failover, connect to the switch and log in again as admin.
10. Using a separate telnet session, enter the **firmwareDownloadStatus** command to monitor the firmware download status.

11. Enter the **firmwareShow** command to display the new firmware versions.

```
switch:admin> firmwaredownload
Server Name or IP Address: 10.22.127.127
FTP User Name: JohnDoe
File Name: /pub/v5.1.0/release.plist
FTP Password:
The following AP blades are installed in the system.

Slot Name      Versions        Traffic    Disrupted
-------------------------------------------------------------------
  2  FR4-18i   v5.1.0           GigE
  7  FR4-18i   v5.1.0           GigE

This command will upgrade both CPs and all AP blade above. If
you want to upgrade a single CP only, please use -s option.

You can run firmwaredownloadstatus to get the status of this
command.

This command will cause the active CP to reset and will require
that existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue [Y]: y
FirmwareDownload has started on Standby CP. It may take up to 30 minutes.
Firmwaredownload has completed successfully on Standby CP.
.
.
.
Standby CP reboots.
Standby CP booted up.
Standby CP booted up with new firmware.
cp1: Firmwarecommit has started on both Active and Standby CPs.
cp1: Firmwarecommit has completed successfully on Active CP.
cp1: Firmwaredownload command has completed successfully.
switch:admin>
```

Start a new session to view the upgrade progress:

```
switch:admin> firmwaredownloadstatus
[1]: Mon Dec 19 18:40:19 2005
Slot 6 (CP1, active): Firmware is being downloaded to standby CP. This step may take
up to 30 minutes.

[2]: Mon Dec 19 18:46:18 2005
Slot 6 (CP1, active): Firmware has been downloaded successfully to Standby CP.

[3]: Mon Dec 19 18:46:25 2005
Slot 6 (CP1, active): Standby CP is going to reboot with new firmware.

[4]: Mon Dec 19 18:47:45 2005
Slot 6 (CP1, active): Standby CP booted successfully with new firmware.

[5]: Mon Dec 19 18:47:56 2005
Slot 8 (FR4-18i): Firmware is being downloaded to the blade. This step may take up to
10 minutes.

[6]: Mon Dec 19 18:48:50 2005
Slot 5 (CP0, active): Forced failover succeeded. New Active CP is running new
firmware

[7]: Mon Dec 19 18:48:57 2005
Slot 5 (CP0, active): Firmware is being download to standby CP. This step may take up
to 30 minutes.

[8]: Mon Dec 19 18:49:28 2005
Slot 8 (FR4-18i): Firmware has been downloaded successfully. Blade is rebooting with
the new firmware.

[9]: Mon Dec 19 18:50:12 2005
Slot 8 (FR4-18i): Firmware commit has started on the blade. This may take up to 10
minutes.

[10]: Mon Dec 19 18:50:51 2005
Slot 8 (FR4-18i): The commit operation has completed successfully.

[11]: Mon Dec 19 18:55:39 2005
Slot 5 (CP0, active): Firmware has been downloaded successfully on Standby CP.

[12]: Mon Dec 19 18:55:46 2005
Slot 5 (CP0, active): Standby CP reboots.

[13]: Mon Dec 19 18:57:06 2005
Slot 5 (CP0, active): Standby CP booted successfully with new firmware.

[14]: Mon Dec 19 18:57:10 2005
Slot 5 (CP0, active): Firmware commit operation has started on both active and
standby CPs.

[15]: Mon Dec 19 19:01:38 2005
Slot 5 (CP0, active): Firmware commit operation has completed successfully on active
CP.

[16]: Mon Dec 19 19:01:39 2005
Slot 5 (CP0, active): Firmwaredownload command has completed successfully. Use
firmwareshow to verify the firmware versions.
```

Then confirm the firmware version:

```
switch:admin>> firmwareshow
Slot Name      Primary/Secondary Versions              Status
-----------------------------------------------------------------
  2  FR4-18i   v5.1.0                                  Enabled
               v5.1.0

  5  CP0       v5.1.0                                  Active *
               v5.1.0

  7  FR4-18i   v5.1.0                                  Enabled
               v5.1.0
```

Testing and Restoring Firmware: SilkWorm Switches

Typically, users downgrade firmware after briefly “test driving” a new (or old) version and then restoring the original version of the firmware. Testing a new version of firmware in this manner ensures that you do not compromise your existing firmware because the test drive version only occupies one partition on your switch.

Caution
When you test drive new firmware make sure you have disabled all features that are not supported by the original firmware before restoring to the original version.

1. Prepare

a. Start a telnet session to the Brocade logical switch IP address.

b. Enter the **firmwareShow** command to view the current firmware.

2. Update firmware on your switch

a. Enter the **firmwareDownload -s** command and respond to the prompts as follows:

```
switch:admin> firmwaredownload -s
Server Name or IP Address: 10.32.220.100
FTP User Name: william
File Name: /pub/v5.1.0/release.plist
FTP Password:
Do Auto-Commit after Reboot [Y]: n
Reboot system after download [N]: y
Firmware is being downloaded to the switch. This step may take up to 30
minutes.
Checking system settings for firmwaredownload...
```

The switch will reboot and come up with the new firmware to be tested. Your telnet session will be automatically disconnected.

b. Start a new telnet session and log in as admin; then, enter the **firmwareShow** command to confirm that the primary partition of the switch contains the new firmware.

Note

Stop! If you wish to *restore* the firmware, stop here and skip ahead to step 4; otherwise, continue to step 3 to commit the firmware on the switch, which completes the firmware download operations.

3. Commit the firmware

a. Enter the **firmwareCommit** command to update the secondary partition with new firmware. Note that it takes several minutes to complete the commit operation.

b. Enter the **firmwareShow** command to confirm both partitions on the switch contain the new firmware.

Note

Stop! If you have completed step 3, then you have committed the firmware on the switch and you have completed the firmware download procedure. Step 4 describes how to restore the original firmware, and should be performed after step 2.

4. Restore the firmware

a. Enter the **firmwareRestore** command. The switch will reboot and come up with the original firmware again.

A **firmwareCommit** will automatically begin to copy the original firmware from the primary partition to the secondary partition. At the end of the firmware commit process, both partitions will have the original firmware. Note that it takes several minutes to complete the commit operation.

b. Wait 5 minutes and log into the switch. Enter the **firmwareShow** command and verify that both partitions on the switch have the original firmware.

Testing and Restoring Firmware: SilkWorm Directors

This procedure enables you to perform a firmware download on each CP and verify that the procedure was successful before committing to the new firmware. The old firmware is saved in the secondary partition of each CP until you enter the **firmwareCommit** command. If you decide to back out of the installation prior to the **firmwareCommit** you can enter the **firmwareRestore** command to restore the old firmware version.

Typically, users upgrade or downgrade firmware to briefly “test drive” a new (or old) version and then optionally restore the original firmware. Testing a new version of firmware in this manner ensures that you do not compromise your existing firmware because the test drive version uses a partition on each CP.

Note

Brocade recommends that under normal operating conditions you maintain the same firmware version on both CPs, and on both partitions of each CP. This procedure enables you to test firmware before you commit; however, you should not run mixed firmware levels on CPs as a standard practice.

1. Prepare

a. Start a telnet session to the Brocade logical switch IP address.

b. Enter the **ipAddrShow** command and note the address of CP0 and CP1.

c. Enter the **haShow** command and note which CP is active and which CP is standby. Verify that both CPs are in sync. CP blades must be synchronized and running Fabric OS v4.4.0 or later to provide a nondisruptive download. If the two CP blades are not synchronized, enter the **haSyncStart** command to synchronize them. If the CPs still are not synchronized, contact your switch service provider.

d. Enter the **firmwareShow** command and confirm that the current firmware on both partitions on both CPs is as expected.

e. Exit the telnet session.

2. Update firmware on standby CP

a. Start a telnet session, log in as admin to the standby CP.

b. Enter the **firmwareDownload -s** command and respond to the prompts as follows:

```
switch:admin> firmwaredownload -s
Server Name or IP Address: 10.32.220.100
FTP User Name: william
File Name: /pub/v5.1.0_main_bld34/release.plist
FTP Password:
Do Auto-Commit after Reboot [Y]: n
Reboot system after download [N]: y
Firmware is being downloaded to the switch. This step may take up to 30
minutes.
Checking system settings for firmwaredownload...
```

At this point the firmware should download to the standby CP only and reboot it. The telnet session will be disconnected.

3. Failover to standby CP

a. Start a telnet session on the active CP.

b. Enter the **haShow** command to verify that HA synchronization is complete. It will take a minute or two for the standby CP to reboot and synchronize with the active CP.

If the CPs do not achieve synchronization, *stop here*; log in to the standby CP, and enter the **firmwareRestore** command to restore your original firmware.

c. Enter the **firmwareShow** command to confirm that the primary partition of the standby CP contains the new firmware.

d. Enter the **haFailover** command. The active CP will reboot and the telnet session will be disconnected.

If there is an FR4-18i blade present: At the point of the failover an *auto-leveling* process is activated. Refer to Step 8 in the "SilkWorm 24000 and 48000 Firmware Download Procedure" for details about auto-leveling.

4. Verify failover

a. Start a telnet session on the active CP (which is the old standby CP).

b. Enter the **haShow** command to verify that the HA synchronization is complete. It will take a minute or two for the standby CP (which is the old active CP) to reboot and synchronize with the active CP.

Note

If the CPs fail to synchronize, you can still proceed because the version being tested is already present on the active CP, and subsequent steps will ensure that the standby CP is updated to the same version as the active CP.

c. The test version of firmware is now running on the active CP (you can confirm this by entering the **firmwareShow** command).

5. Update firmware on standby CP

a. Start a telnet session on the standby CP (which is the old active CP).

b. Enter the **firmwareDownload -s** command and respond to the prompts as follows:

```
switch:admin> firmwaredownload -s
Server Name or IP Address: 10.32.220.100
FTP User Name: william
File Name: /pub/v5.1.0/release.plist
FTP Password:
Do Auto-Commit after Reboot [Y]: n
Reboot system after download [N]: y
Firmware is being downloaded to the switch. This step may take up to 30
minutes.
Checking system settings for firmwaredownload...
```

At this point the firmware should download to the standby CP only and reboot it. The telnet session will be disconnected.

c. Wait one minute for the standby CP to reboot, and then start a telnet session and log in as admin.

d. Enter the **firmwareShow** command to confirm that *both* primary partitions now have the test drive firmware in place.

Note

Stop! If you wish to *restore* the firmware, stop here and skip ahead to step 8; otherwise, continue to step 6 to commit the firmware on both CPs, which completes the firmware download operations.

6. Perform commit on standby CP

a. From the telnet session on the standby CP, enter the **firmwareCommit** command to update the secondary partition with new firmware. Note that it takes several minutes to complete the commit operation.

7. Perform commit on active CP

a. From the telnet session on the active CP, enter the **firmwareShow** command and confirm that only the active CP secondary partition contains the old firmware.

b. Enter the **firmwareCommit** command to update the secondary partition with new firmware. Note that it takes several minutes to complete the commit operation.

c. Enter the **firmwareShow** command to confirm both partitions on both CPs contain the new firmware.

d. Enter the **haShow** command to confirm that the HA state is in sync.

Note

Stop! If you have completed step 7, then you have committed the firmware on both CPs and you have completed the firmware download procedure. Steps 8-10 describe how to restore the original firmware, and should be performed after step 5.

8. Restore the firmware on the standby CP

a. In the telnet session for the standby CP, enter the **firmwareRestore** command. The standby CP will reboot and the telnet session will end. Both partitions will be made equal after several minutes.

9. Perform haFailover on active CP

a. In the telnet session for the active CP, enter the **haShow** command to verify that HA synchronization is complete. It will take a minute or two for the standby CP to reboot and synchronize with the active CP.

b. Enter the **haFailover** command. The active CP will reboot and the telnet session will end. Your switch is now running the original firmware.

10. Restore firmware on the “new” standby CP

a. Wait one minute and start a telnet session on the new standby CP, which is the old active CP.

b. Enter the **firmwareRestore** command. The standby CP will reboot and the telnet session will end. Both partitions will be made equal after several minutes.

c. Wait 5 minutes and log into the switch. Enter the **firmwareShow** command and verify that all partitions have the original firmware.

If an FR4-18i blade is present: FR4-18i blade partitions always contain the same version of the firmware on both partitions (it does not keep two copies). The firmware is stored on the FR4-18i blade’s compact flash card and is always synchronized with the active CP’s firmware. Thus, if you restore the active CP firmware, the FR4-18i firmware is automatically downloaded to become consistent with the new CP firmware (the FR4-18i firmware is basically restored).

Your system is now restored to the original partitions on both CPs. Make sure that servers using the fabric can access their storage devices.

If you wish to upgrade a director with only one CP in it, follow the procedures in “Testing and Restoring Firmware: SilkWorm Switches” on page 16. Note, however, that upgrading a director with only one CP in it will be disruptive to Fibre Channel traffic.

Validating the Firmware Download

Validate the firmware download by running the following commands: **firmwareShow**, **nsShow**, **nsAllShow**, and **fabricShow**.

Note

As you prepared for the firmware download, you should have issued either the **supportShow** (4.2.0 or earlier) or **supportSave** (4.4.0 or later) command. While you can issue the command again and compare the outputs from before and after, be aware that it may take as long as 30 minutes for the command to execute. To save time, it is recommended that you use the commands listed below, which are all are subsets of the **supportSave** output.

All of the connected servers, storage, and switches should be present in the output of these commands. If there is a discrepancy, it is possible that a device or switch cannot connect to the fabric and further troubleshooting is necessary.

firmwareShow Displays the current firmware level on the switch. For SilkWorm directors this command displays the firmware loaded on both partitions (primary and secondary) for both CPs. Brocade recommends that you maintain the same firmware level on both partitions of each CP within the SilkWorm director.

nsShow (Optional) Displays all devices directly connected to the switch that have logged into the Name Server. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

nsAllShow (Optional) Displays all connected devices to a fabric. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

fabricShow (Optional) Displays all switches in a fabric. Make sure the number of switches in the fabric after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

Troubleshooting Firmware Downloads

Good troubleshooting practices for firmware download should begin before you start the procedure, and include the following:

- Keep all telnet sessions and serial console logs.
- Enter the **supportSave** (for Fabric OS v4.4.0 or 5.x; for Fabric OS 4.2 or earlier, enter **supportShow**) command *before and after* entering the **firmwareDownload** command.
- If a problem persists, package together all of the information (the telnet session logs and serial console logs, output from the **supportSave** command) for support. Make sure you identify which information was gathered before and after issuing the **firmwareDownload** command.

If the firmware download fails to complete, refer to the *Fabric OS System Error Message Reference Manual* for details about any error messages.

If a firmware download fails in a director, the **firmwareDownload** command synchronizes the firmware on the two partitions of each CP by starting a firmware commit operation. Wait *at least* 10 minutes for this commit operation to complete before attempting another firmware download.

If the firmware download fails in a director, then the CPs may end up with different versions of firmware and be unable to achieve HA synchronization. In such cases, issue the **firmwareDownload -s** command; the single mode (-s) option upgrades the firmware on the standby CP to match the firmware version running on the active CP. Then re-issue the **firmwareDownload** command to download the desired firmware version to both CPs. For example, if CP0 is running v5.0.1 on the primary and secondary partitions, and CP1 is running v4.4.0e on the primary and secondary partition, then synchronize them by issuing the **firmwareDownload -s** command.

If you encounter an "unable to access the required package list file" message (0x12), verify on the FTP server that the path to the firmware download archive is entered using the correct case (that is, the capitalization of directories used in the path). Only use forward slashes in path names (there is no support for backslash characters in the path name). You must specify the full path name of the .plist file, *excluding* the *SWBDxx* directory. For example, if the full path is */dist/SWBDxx/release.plist*, then you need to enter */dist/release.plist*. Other reasons the .plist file may be inaccessible are:

- The host is unknown to the switch
- The host is not accessible from the switch
- The user does not have permission on \flhost\fR
- The .pfile does not exist on the host
- The FTP server is not running on the host
- The platform does not support the indicated firmware

Refer to the *Fabric OS System Error Message Reference Manual* for detailed information about .plist-related error messages.

FR4-18i Blade Troubleshooting Tips

Typically, issues evolving during firmware downloads to the FR4-18i blade do not require explicit actions on your part. However, if any of the following events occur, perform the suggestion action to correct:

- The FR4-18i blade is faulty (issue **slotShow** to confirm)

  If the FR4-18i blade is faulty, enter the **slotPowerOff** and **slotPowerOn** commands for the blade. If the blade still appears to be faulty, remove it and re-insert it into the chassis.

- The FR4-18i blade is stuck in the loading state (issue **slotShow** to confirm)

  If the blade remains in the loading state for a significant period of time, the firmware download will time-out. Remove the blade and re-insert it. Upon booting up, auto-leveling will be triggered and the firmware download will be attempted.

If you experience frequent failovers between CPs that have different versions of firmware, then you may notice multiple blade firmware downloads and a longer start-up time.

Synchronizing Firmware Versions on Partitions

It is possible for firmware to become out of sync on the partitions. This can occur when a user issues the **firmwareDownload -s** command to test drive the firmware, but does not issue the **firmwareRestore** and **firmwareCommit** commands—in such a case the user ends up with different levels of firmware on the two partitions.

If you end up with different versions of firmware on one of your partitions, for example, CP0 is running v5.0.1 on the primary and secondary partitions, and CP1 is running v5.0.1 on the primary partition and v4.4.0e on the secondary partition, then synchronize the partitions on CP1 as follows:

1. Start a telnet session on the CP with the out-of-sync partitions.
2. Enter the **firmwareCommit** command, which will copy the primary partition to the secondary partition.S

If there is a discrepancy in the number of switches or attached devices in the fabric after a firmware download it may be due to a fabric segmentation or a device that failed to log in. For assistance refer to the following:

- Chapter 12, “Troubleshooting” in the *Fabric OS Administrator’s Guide* for basic troubleshooting steps.
- Contact your switch service provider.

FTP Server Recommendations

The **firmwareDownload** command has a time-out of ten minutes for v4.0 and v4.1 and thirty minutes for v4.2 and later. The following tips may be of help if you are having problems with the firmware download timing out before the process is complete:

- Verify that you can ping the FTP server from another host on the LAN, prior to running the **firmwareDownload** command.
- Disable any VPN, firewall or anti-virus applications on the FTP server.
- Remove any Ethernet hub between the FTP server and the switch.
- Optionally, set the switch's autonegotiating Ethernet port to match the speed and duplex setting of the IP environment (for example, enter the **ifModeSet** command to change the switch settings to match both ends of the Ethernet link. Enter **help ifModeSet** and **help ifModeShow** on the switch to view more details about these commands).
- Enable session logging on the FTP server so that the log can be viewed during the execution of the **firmwareDownload** command.
- Set the FTP server's time-out value to sixty minutes.
- Ensure that the decompress process created multiple *SWBDxx* folders (where *xx* is a number) in the main folder. If the files are unpacked without folder creation, then the **firmwareDownload** command will be unable to locate the *.plist* file.